INDIA'S FRONTLINE IT MAGAZINE

VARINDIA

THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

CDS 2021:
BE ACQUAINTED WITH TODAY'S CYBER SECURITY THREATS AND ITS IMPACT
PG 34

VOLUME XXII ISSUE 6 FEBRUARY 2021 PRICE Rs. 50

yubico

iVALUE
Maximizing Value of Technology Investments

PROTECT YOUR DIGITAL WORLD WITH YUBIKEY

BROUGHT TO YOU BY iVALUE

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS

VOLUME XXII ISSUE 6 FEBRUARY 2021 PRICE Rs. 50 SUBSCRIPTION COPY NOT FOR SALE

21 INDIAN ORIGIN STAR EXECUTIVES LEADING GLOBAL COMPANIES

46PG

Cabinet approves PLI scheme for manufacturing laptops, tablets, PCs, servers locally

The Union Cabinet has approved the production-linked Incentive scheme for IT Hardware. The scheme proposes an incentive to boost domestic manufacturing and attract large investments in the value chain of IT Hardware. The target segment under the proposed scheme includes laptops, tablets, all-in-one PCs, and servers said Union Minister Ravi Shankar Prasad.

The total cost of the PLI scheme for IT hardware is approximately Rs 7,350 crore over 4 years. The scheme intends to provide incentives between 4-1 per cent on net incremental sales (over base year i.e. 2019-20) of goods manufactured in India and covered under the target segment, to eligible companies, for a period of four years. As per the Cabinet statement, the scheme is expected to lead production worth Rs 3.26 lakh crore and exports worth Rs 2.45 lakh crore in four years.

Web Werks singned with Iron Mountain for US$150mn equity investment

Web Werks, one of India's leading independent data center providers, today announced that it has entered into a strategic relationship with Iron Mountain (NYSE: IRM), who will invest US$150mn primary equity into Web Werks over the next two years. After the investment period, Iron Mountain will be the majority investor in the venture. Once completed, this transaction will allow Web Werks to accelerate its expansion across different Indian cities and build capacity to cater to one of the fastest-growing data center markets globally. The transaction is expected to close within the next 90 days, subject to customary closing conditions.

ROLE OF CYBER SECURITY IN THE 4TH INDUSTRIAL REVOLUTION

With each passing day, the latest technologies such as cloud-computing, IoT and robotics are disrupting the traditional manufacturing process. With automation, IoT, Cloud & Edge computing, Robotics and data analytics are making production processes smarter, intelligent and more productive, the Industrial Revolution 4.0 has been demonstrably evident.

The world has become digital. Majority of the world's population is now online, contributing to the digital economy, which is fundamental to our economic growth, as well as being the creator of trillion-dollar companies. India has the opportunity, not just to catch up with the leaders but to emerge as a global leader itself.

Technology is transforming businesses in many different ways with most of the industries relying heavily on connected technology and software as part of their daily operations, whether it is customer-facing websites, cloud platforms, email services, network infrastructure, computers used by employees, and more. This leads to increasing cyber-security risks. Hackers are increasingly exploiting flaws in software and hardware, and by doing so, they are able to hack into corporate systems and cause all sorts of damages.

New challenges and vulnerabilities are faced by cybersecurity professionals in India and the rest of the world every day, putting multiple organisations at risk. Digitization has not only paved the way towards new opportunities but has also driven the industry towards multiple unforeseen threats, highlighting the need for cybersecurity, making it a continuous, perpetual, always-on and a proactive process rather than a single point or a one-time activity.

For cyber criminals, vulnerabilities in software and hardware present a backdoor into targeted businesses – and they are constantly trying to find and leverage them. With this in mind, cyber security teams must be proactive in discovering and fixing vulnerabilities so they cannot be exploited.

The year 2020 has been a roller-coaster year with full of cybersecurity attacks. India has seen a 37% increase in cyber-attacks in 2020 as compared to 2019, witnessing the malware to cross 4 Lakh daily and a total of 696,938 cyber-attacks. India is among the largest consumers of the internet, 3rd largest in the planet, after USA and China.

Now, the Industrial IoT (IIoT) devices are a pressing concern for security teams. Companies invest large sums of money to keep cyber-criminals out of industrial systems, but what happens when the hacker is already inside?

Secondly, we have also seen growth in the sextortion attack in January. Most of these attacks targeted English-speaking users including 3,980 in India. All of the sextortion campaigns use the same modus operandi, with scammers sending emails to users claiming they recorded the user during private, intimate moments, and threatening to expose them to the public unless the victim pays money to the attacker.

Now talking about the 5G roll out in the country, it'll be the most transformative communications technology in a generation and enable a universe of new services, including advanced energy management capabilities that will be critical to solving growing energy and sustainability challenges. Telecom giants Jio and Airtel are announcing the plans for 5G in India, awaiting the spectrum auction slated for March 2021 and government approvals, but new research highlights the practical challenges of 5G energy management facing telecommunications operators.

Estimates suggest 5G networks can be up to 90% more efficient per traffic unit than their 4G predecessors, but they still require far more energy due to increased network density, heavy reliance on IT systems and infrastructure, and increased network use and accelerated traffic growth.

Telecom operators making meaningful energy and cost reductions are doing so by evaluating the entire ecosystems around their network operations – people, objectives, infrastructure and partners. Because of the reliance on IT to enable 5G applications, a high degree of collaboration will be required across operators, OEMs and infrastructure providers, and customers to ensure deployments are optimized and every possible efficiency is pursued. Operators are deploying 5G networks to grow new revenues.

However, some experts speaking on 5G say, the shift to 5G will create new security challenges, driving significant traffic increases, consuming more bandwidth, and requires more speed and less latency. For this, a combination of multiple networks, clouds, CDNs, and edge are integrated, exposing new ways for attackers to exploit vulnerabilities.

The year 2021 is very significant for all the industries as it's the dawn of a new digital age. Since everything is happening online & digitally, the need for cybersecurity is now greater than ever.

Finally, in order, to sustain businesses online and create a safe workflow, cybersecurity solutions are of great importance.

S. Mohini Ratna
Editor, VARINDIA
mohini@varindia.com

CADYCE

CA-T3DPD
Thunderbolt™ 3 DisplayPort™ Docking Station (8K@60Hz)

CA-WCHP
USB-C™ Dock with Wireless Charging

CA-CAUC
USB-C™ to Audio Adapter + USB-C™ PD Charging

CA-C4H
USB-C™ to USB 3.0 4 Port Hub

CA-IP100MW
Megapixel Wireless Day/Night Internet Camera with 2-Way Audio

CA-CT568
Network Crimping Tool

CA-PC624/648
Patch Panel 24/48 Port CAT 6

CA-HDX120/50
HDMI Extender Over Ethernet (120/50m)

CA-HDK200
2 Port HDMI USB KVM Switch

CA-2HDS
2 x 1 HDMI Switch with 4K support

CA-KE100
USB KVM Extender

CA-GSFC20
10/100/1000 Base-TX to1000 Base-FX Gigabit Single-Mode Fiber Converter

CA-PC61/62/63M
CAT 6 Patch Cord 1/2/3M

CA-C2C(2m)
USB-C™ Sync & Charge Cable (2m) CADMiUM Space Gray

CA-ULCG (1.2/2/3m)
Cadyce CADMiUM Lightning to USB Cable

CA-T3HDD
Thunderbolt™ 3 HDMI Docking Station

FREE PICK UP & DELIVERY

Warranty rma@cadyce.com
Online Chat www.cadyce.com
Email Support support@cadyce.com
Sales sales@cadyce.com

Toll Free: 1800 266 9910
Tech Support: +91 9172212959

Pune: 08087635350, 08793014270/71 • **Mumbai/Rajasthan:** 09769726552 • **Gujarat:** 09974800847 • **North:** 09999071626 • **Delhi:** 09313122475 • **Haryana:** 09716619191
Bangalore: 09972534115, 09880660912 • **Hyderabad & AP:** 09949976234 • **Maharashtra:** 09226923696 • **Rest of India:** 09595207300 • **Tamil Nadu:** 09500052809

INDIA'S FRONTLINE IT MAGAZINE
VARINDIA
THE ULTIMATE Voice OF INDIAN VALUE ADDED RESELLERS
Website: www.varindia.com

Publisher: Dr. Deepak Kumar Sahu
Editor: S Mohini Ratna
Executive Editor: Dr. Vijay Anand
Sub - Editor: Aparna Mullick
Correspondent: Lopamudra Das
Art Director: Rakesh Kumar
Network Administrator: Ashok Kumar Singh
Visualizer: Ravinder Barthwal
Manager-IT: Subhash Mohanta
Manager-SEO: Bidyadhar Behera

BUSINESS:
Commercial Manager: Amit Kumar Jha
Sr. Marketing Manager: Ashok Ranjan Dash
Circulation Executive: Manish Kumar

CORPORATE OFFICE:
VAR House, A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030
Tel: 011-41656383, 46061809
Email: edit@varindia.com

Bangalore: Bureau office
Marketing Manager: S. Kamala kar
Correspondent: L. G. Swami
D-103 G.F., Ashish JK Apartments
Thubarahalli Extended Road
Bangaluru- 560066
Tel: 080-49530399 I Mobile:09886280836
E-mail: kamlakar@varindia.com

Mumbai: Bureau office
Regional Manager (West): Anil Kumar
Sr. Correspondent: Mamta S.
Anurag Residency, 203 - "B" Wing, Plot No-5, Sector-9, Kamothe, Navi Mumbai-410 209
Tel: 022-65561292, Mobile: 08108017479
E-mail: anil@varindia.com, mamta@varindia.com

Chennai: Bureau office
Branch Manager: K. Parthiban
F1, Meadows Green Apartments, 64, Chetty Street
1st Cross, Mel Ayanambakkam, Chennai - 600 095
Cell No. : 98400 55626
E-mail: parthiban@varindia.com

Hyderabad: Bureau office
Branch Manager: Sunil Kumar Sahu
32-161/3, 202 Neha Paradise, Nr. Maissamma Temple, Venketeswara colony
Ramakrishna Puram, Hyderabad - 500056
Telangana, Tel: 040-32989844/ Cell No. 08100298033
E-mail: sunil@varindia.com

Kolkata: Bureau office
Marketing Officer: Sunil Kumar
Correspondent: B Kiran Dutta
Megatherm Electronics Pvt. Ltd.
Second Floor, Megatherm Building, Unit -E, Plot - L1
Block GP, Sector V, Salt Lake, Kolkata - 700091
Mobile: 08100298033, E-mail: sunil@varindia.com
Mobile: 09903088480, E-mail: kiran@varindia.com

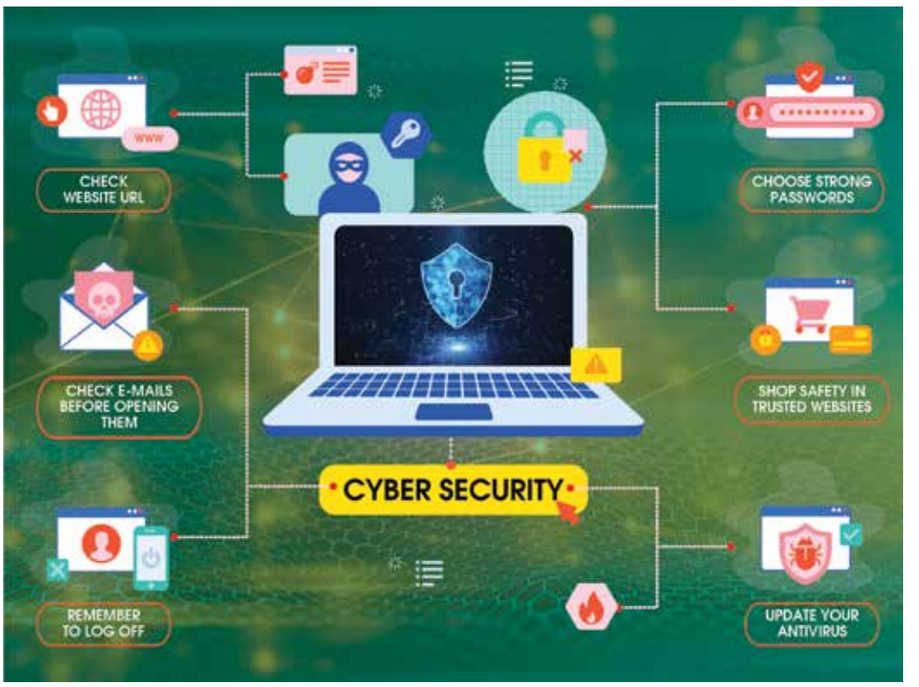
Printed and Published by **Deepak Kumar Sahu** on behalf of M/s. Kalinga Digital Media Pvt. Ltd. and Printed at Pushpak Press Pvt. Ltd. Shed No. 203 - 204, DSIDC Complex, Okhla Industrial Area, Phase-I, New Delhi-110020 and Published at A-84A/3 Rose Apartment, Paryavaran complex, IGNOU Road, New Delhi - 110030, Editor - S Mohini Ratna.

For Subscription queries contact: info@varindia.com
Subscription: Rs. 500(12 issues)Rs. 1000 (24 issues)

All payments favouring:
KALINGA DIGITAL MEDIA PVT LTD

CONTENTS

COVER STORY / 22pg



REGULARS

FACE TO FACE

VAR GLOBAL

COVER STORY

CYBER SECURITY EVENT

BUDGET 2021

TECHNOMANIA

VAR SECURITY

Intel® Evo™ platform powered by
Intel® Core™ i7 processor

STYLE. PERFORMANCE. AWARDS.

Stand out from the ordinary with the Acer **Swift** series.

Designed on the Intel® Evo™ platform for an exceptional experience anywhere.

Swift 3 *Swift* 5 *Swift* 3X

Ultra-sleek metal body

Anti-microbial coating

Dedicated graphics

Edge-to-edge display

OFFERS WORTH ₹9,999 | NO COST EMI

AWARDED BY THE BEST

SWIFT 5 — reddot winner 2020 — CES INNOVATION AWARDS 2020 — SWIFT 3X — digit ZERO 1 AWARDS 2020 — GADGET BRIDGE AWARDS 2020

SHOP NOW AT

ACER EXCLUSIVE STORE STORE.ACER.COM

THE ART OF RE-IMAGINING

Asoke K. Laha
President & MD, Interra IT

One coinage, which I often hear amidst the din of cataclysmic developments that have been taking place in the Covid-19 pandemic is "reimagining". The usage can be contextual; such as reimagining ideas, technologies, behavior and politics. What does it mean? The phrase, I believe, is esoteric; only people with higher understanding of the subject can understand fully the nuances of the word.

I may not have fully absorbed the semantics of that word; yet I would like to narrate what I have understood. To me, it connects with a generational shift in thinking to move in the value chain and at the same time snapping the bonds from the past and the present to become more relevant to the future. The change that can be envisioned can be all encompassing. It will not leave out anything that comes in your way. For instance, you can re-imagine your work places, you can have a similar view on education, technology, healthcare, diplomacy, economic policies involving both micro and macro elements. It is analogous to "Think Different" coined by Steve Jobs.

Let me start with re-imagining work places. I read somewhere recently that CISCO has moved 16,000 employees it had in its sprawling campus in Bengaluru to 109 towns spread across the country just before the lockdown had started. The US IT giant has provided tools to its employees to work from home, to attend meetings in secured ambience, discuss with colleagues and bosses, to attend training sessions and a lot more.

Amidst welcoming reviews by the peers about the advantages of the system, there are nagging doubts cast by the psychologists and social scientists about the flip side of the emerging situation. Foremost is the psychological pressure on the employee by sitting all the while alone without any creative diversion. Should we not therefore, evolve a hybrid model that can provide opportunities for occasional group meetings in person to provide for an escape route to the employees? It is instructive how that model can be developed since some of the companies may not have the financial muscle power to implement such schemes that may prove to be costly.

The next in importance is cyber security: Cloud and cyber security go hand in hand. Cloud makes remote work easier. At the same time, it increases security vulnerabilities. The employers will be comfortable to switch over the distance working only when the data and content are not compromised. How can that be ensured? Do we require any fine tuning in the cyber security laws and if so what are those crucial changes needed? A case in point is if the employee is in India and the employer is in the US or Europe, for any breach in security happens, where will be the jurisdiction to adjudicate-the US or India? A lot more clarity has to be evolved on working hours, accountability, contractual obligations from either side etc. Hopefully, their imagining process will emerge through consultations and deliberations at various levels.

Reimagining healthcare has become a hotly debated issue. Healthcare segment is undergoing a silent revolution both in the predictive and preventive realms. Physicians are now creating matrices based on individuals' physical, genomic, behavioral risk factors, to map the likely diseases the person is vulnerable to. Many companies are working on software that can predict the possibility of a heart attack well in time and to help the patient to take preventive care. The intelligent systems that are in the making are based on the creation of a digital twin, an electronic replica of a person. Using remote sensors, analytics including artificial intelligence, bio digital twins can be used to predict diseases. The good news is that some of the Indian laboratories are gearing up to create digital twins. They claim that digital twins are only a few years from now. Coupled with the developments in big data analytics, scientists will be able to analyze root causes of many diseases including Parkinson's, diabetes and amnesia, among other things. Will there be a time when organs can be harvested outside the human body to replace the existing ones, which get damaged due to one reason or the other? Personalized human organ harvesting using the DNA of a person, scientists say may not be too distant going by the progress in research. Of course, that will be an improvement over transplant, which depends on the magnanimity of a deceased person or his relatives to avail of the organs.

I feel that the revolutionary changes are going to take place in the education sector. That is already happening in a limited way through distance education limited to certain classes and groups. Now that is going to be universal.

We have to re-imagine manufacturing and agriculture with the type of technologies that are in the pipeline. I feel in the course of one year or slightly more than that there would be massive shifts in manufacturing electric vehicles, batteries, particularly for enhancing its storage capacities, agriculture to induce greater precision to increase productivity and quality, spacecraft and the list goes on.

I feel the interplay of artificial intelligence, cloud computing, robotics, machine language and what have you can expand the vistas of innovation, disruption and discovery. I can visualize mines and hazardous works being done by robots supervised by drones. I can also visualize people doing other types of hazardous works such as fire fighters being replaced by robots. That work will be re-imagined and one may need in future people, who are tech savvy and tackle the situation using their brains and skills rather than their physical strength.

In the same way, there will be shakeup in police and defense forces with the increased use of technologies. Cyber crimes have become a major menace. In cyber parlance what constitutes a crime and what not is a difficult task since the line between the two is blurred. One may have to have more intelligent evidence to prove guilt or disprove that. The future crimes are going to be more complex and most often cyber linked. Investigation and proving the crime may not be through questioning and other conventional methods being used by the police. Complex software will have to be used to prove them and nab the culprit. Does it mean that the police personnel should be recruited and trained more on the attributes of their mental agility and technical knowledge? Yes, we need to re-imagine a new protocol and norms for police personnel also.

During the Covid-19 days, empirical evidence proved that lockdowns forced people to buy things digitally, make the payments through the virtual medium, so much so that almost all e-commerce companies world-wide made enormous profits.

These days, I understand, political people are using gadgets more often to make their points clear. When a minister is making the presentation, he or she does through power points or by displaying visuals. Most of the politicians across the world use twitter handles and Facebook, WhatsApp etc. to communicate with the people on a real time basis. Some of the more tech savvy guys use Instagram to reach out to their target group. Such communication strategies are going to be the buzzword hereafter-a sort of reimagining political demagogue.

The last one that I would like to explain is the likely impact on the judiciary. Can a robot be a good judge? Many say it could be possible. A powerful robot endowed with high configurations can browse through thousands of cases, examine the affidavits of witnesses, petitioners, respondents, case laws and arrive at an accurate judgment in record time. Should that happen it would be the ultimate re-imagination.

DELL Technologies

NEW PRECISION MOBILE WORKSTATIONS

AS POWERFUL AS IT IS INTELLIGENT.

Let's make genius real.

Precision 15/17 3000/5000/7000 Series (Models 3551, 5550, 5750, 7750, 3550) Mobile Workstations

Intel® Xeon® Processor

Please Contact

IRIS Global Services

Iris Global Services Pvt Ltd

Mahipalpur Extension, Mahipalpur, New Delhi, Delhi 110037

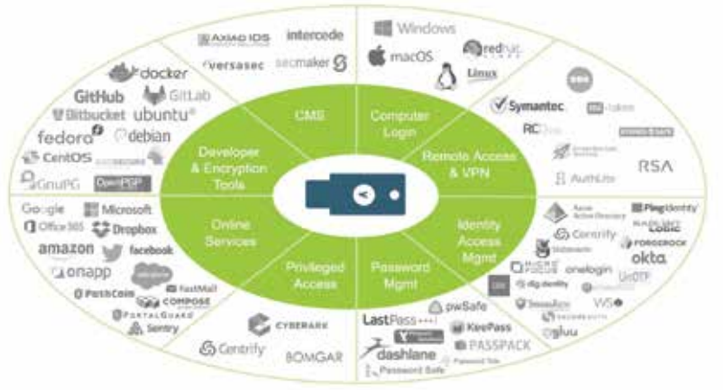
Achin Kumar : +91 9873592171

yubico

iVALUE
Maximizing Value of Technology Investments

iValue presents YubiKey by Yubico – pioneer in modernizing multifactor authentication by putting an end to account takeovers and going passwordless. Get the world's leading security key for superior security, user experience and return on investment.

ONE KEY FOR MANY APPLICATIONS



One touch, two-factor secure

Once you register your Yubikey with services, just tap your Yubikey for easy, strong two-factor authentication, for computers, networks, and online accounts. No need for text messages or one-time passcodes.

One key for your accounts

The YubiKey is a small hardware device used to secure access on mobile devices, computers, and servers. Choose from multiple form factors to suit your needs.

The YubiKey works with hundreds of enterprise, developer and consumer applications, out-of-the-box and with no client software. Combined with leading password managers, social login and enterprise single sign on systems the YubiKey enables secure access to millions of online services.

How the YubiKey works

Register your YubiKey

To use the YubiKey,, go to the Security Settings of a supported service and select two-factor authentication.

Insert YubiKey & tap

On a computer, insert the YubiKey into a USB-port and touch the YubiKey to verify you are human and not a remote hacker.

Tap on phone

For NFC-enabled phones, just tap a YubiKey NFC against the phone to complete authentication.

YouTube

LAPCARE®
Expect More Explore More

NEW YEAR DHAMAKA

Buy Lapcare products & win exciting prizes

LUCKY DRAW

1st Dec-2020 to 28th Feb 2021

1 PRIZE

KIA SELTOS 1.5
Petrol H T E G
(Petrol Base Model)

2 PRIZE

TATA Tiago XE
Petrol Base Model

3 PRIZE

HONDA Activa 5G (4 Nos.)
One in Every Zone

4 PRIZE

Apple iPhone 11- 64GB (4 Nos.)
One in Every Zone

5 PRIZE

Branded i3 Laptop (24 Nos.)
Six in Every Zone

Terms & Conditions

- Vehicles mentioned will be given on Ex Showroom price. Insurance /Reg charges and all other expenses will be borne by the Winner
- All warranties and subjective claims on products and goods will be as per the schemes/offers by the respective companies. RIPL will not be responsible for any of those issues
- RIPL reserves the rights to change, extend or withdraw any terms & conditions of the offer at any time, without prior notice or assigning any reason
- The Company's decision will be final in case of any ambiguity related to any offer and qualification of the free gift
- All Disputes are subject to the Jurisdiction of Faridabad (Haryana) Court

For more information contact your nearest Lapcare distributor or WhatsApp at 8800736969

Rx Infotech P Ltd
Authorised Distributor of Lapcare
sales@rxinfotech.in

24X7 SERVICE

8800736969
www.facebook.com/lapcareworld
Toll Free : 1800 120 0852

Lapcare India P Limited
1201-1208, 12th Floor, Puri Business HUB,
Sector - 81, Faridabad - 121004, Haryana
Enquiries at **customercare@lapcare.com**

JUNIPER NETWORKS ENSURING TECHNICAL INNOVATIONS ALONG WITH ITS PARTNERS

In a chat with VARINDIA, **HARSHAVARDHAN KATHALEY,** *Director- Partner Sales, India & SAARC, Juniper Networks* discusses about cloud networking market, production service solution architecture, cyber security, partner program etc.

As the industry is moving to the cloud, or in some cases hybrid mode, on this backdrop how are you positioned in the cloud networking market?

The next decadeis all about cloud networking. It has already started, but it is not now, next decade is all about cloud networking, which means that when it comes to network assets or network infrastructure -- it either has to be cloud ready or it has to be cloud now. So, all our solutions and products fall in these two categories. In order to support this we have Cloud-ready data center, automated WAN solutions, AI driven enterprise and of course they are all covered with all pervasive connected security. All these are clearly for our customers who are in either of these two buckets, Cloud-ready or Cloud now.

When a customer wants to automate the entire network starting from operating system to DC modernization or to business at the heads, Juniper network plays a role. How the production service solution architecture works?

The most important part is from its inception of all our products, we have deployed open standards because there is no proprietary about it.

So that is why it is very easy for customers to ensure that there is interoperability across the various platforms, and at the same timeCLIs. I know of some of the companies or competitors itself who have different operating systems, and then there is a proprietary CLIs, so even for management of those Partners are the one who typically help customers in ensuring that their networks are installed and they are running right. So, during this process, if the CLIs are different it actually adds in a whole lot of unwarranted thing. So, that is why across our platforms we have one single Junos operating system. And I want to now go to the next level, we have virtual network assistant and it is named as Marvis. Now, Marvis comes to us from our Mist portfolio. Mist is our Wi-Fi portfolio. Marvisis AI enabled kind of assistance. So, what it does is that over the period of time it has gained a lot of knowledge about the various correlations, anomalies or whatever that comes in. So, as AI it keeps on building its own library and continuously pushing out thesolutions to it. So we have something called as -- earlier, we started with Wired Assurance. What it means is that you have a Mist client, a Marvis client, where we are able to provide assured service quality of service to the customer for their wireless network. So, Mist scope has now increased not only to wireless, but to our switching portfolio. And obviously there is a roadmap, we are going to cover various other aspects like automated WAN, DC and all those things. I am happy to tell you that this is a natural language client. You don't need to know the CLIs. You ask the question in English, it will give you answer, solutions.On every Wednesday, on a weekly basis, it continuously keeps coming out with patches and it's completely applying those patches so that old problems do not happen again. And this is the industry's first artificial intelligence virtual.

How you are focused on the cyber security, which is very important nowadays?

Security as it started, earlier it was all about perimeter security like building some barriers like firewalls etc. So, we believe that today security has to be all pervasive that means it has to be available and it has to be part of the overall architecture and every component in the networkshould be able to handle security and its threat. It is possible because of companies like us, we have been having security portfolio for very long now. There is lot of security related intelligence, which is built over a period of time. So, as a part of innovation and design all these components of security, the intelligence around this, they are now part of our entire portfoliobe it switching, routing, security, wireless, it is all part of this.

Can you share about your partnering system and partner policy?

I think Juniper is selling through partners especially in India. 100% of our business happens through our partners. We believe that as a vendor, while we continue to focuson ensuring that the technology innovation happens, but it is our partners and the ecosystem with whom we go to market and we ensure that the deployment -- because many a times many customers want an end-to-end ownership while I do the networking piece, obviously a customer has something else also. So, that job is done by partners for us and we have this partner program called Juniper Partner Advantage.It is been in existence for many years now, and it is continuously improving. I think 2021 Partner Program is already announced globally. It is a very structured based program so that we take out any kind of subjectivity and the rules of engagement so that it becomes very easy for partners and us to work with each other. This year, I think Juniper has made significant investment in the partner program, over $100 million globally is invested into this year's Juniper Partner Advantage Program. It addresses all our partners be it the regular system integration partners, VARs, distributors, our service provider partners, cloud partners so on and so forth. There are specializations of different nature, like no AIDE AI driven enterprise, data center, routing, security, cloud etc. There is a tremendous focus this year on rewarding partners for the business they bring to us. I mean, it has always been a joint kind of membership, but we have something called as a Deal Registration Program, and there is a huge focus this year from Juniper on deal registration, which basically incentivize partner and rewards them for new leads and new business that they bring to us, we close it jointly. Then there are some other kind of programs, for example, there are plus programs or acceleration programs like there is an Enterprise Plus Program, Service Provider Plus Program. So, these are for the partners who want to focus in a specific customer vertical. It needs a little bit of different kinds of yardstick. So, all those things are also incorporated in these kind of plus programs, making it one single umbrella under which partner can engage with us. It starts from the entire partnership life cycles, right from recruitment to enablement to building funnel with each other, closing business, getting rewards, then not only that, even loyalty also. So, it is a complete lifecycle when it comes to partnership. So, I must say the program has evolved extremely very well.We have a good set of partners in India. I can say proudly, who have been working with us over these yearsfor mutual business growth, they have grown and we have also grown.

kemp

Earn and Save with the Kemp Partner Program!

Make your customer's budget go further and join the network of partners who benefit from selling Award-Winning Application Delivery Controllers (ADC).

- #1 rated load balancer on leading review sites
- Unmatched value and cost savings
- Flexible licensing options
- World-Class technical support
- Training and certification provided

Promotional discounts and SPIFF available for limited time.

Kemp India, 516-520, 5th Floor, International Trade Tower, Nehru Place, New Delhi 110019.

Visit us at kemp.ax

For more, please contact:
Parthasarathy Raghupathy
Country Sales Manager
praghupathy@kemp.ax
+91-9958471010

Veeam continues to grow as demand for Modern Data Protection increases from businesses

Veeam Software reported results for its fiscal year 2020. Veeam kicked off 2020 with the completion of its acquisition by Insight Partners, which was announced on Jan. 9 at a valuation of $5 billion, setting the pace for a year of substantial growth and expanded success across all market segments, culminating with Veeam's acquisition of Kasten, the market leader for Kubernetes Backup and Disaster Recovery (DR), in Q4'20.

"2020 was a defining moment for data protection and management. More than ever, we are seeing our customers looking for reliability and ease of use in their Cloud Data Management solutions, and in Q4, APJ demonstrated another quarter of double-digit growth with an annual recurring revenue (ARR) increase of 24 percent year-over-year (YoY). This is a testament to our ongoing commitment to our customers and partners, enabling them to unleash the power of digital and data mobility," said Shiva Pillay, Vice President, Sales and Field Operations, Asia Pacific and Japan.

HONEYWELL AND IDEMIA ANNOUNCE STRATEGIC ALLIANCE

Honeywell and IDEMIA have announced a strategic alliance to create and cultivate an intelligent building ecosystem that provides a more seamless and enhanced experience for operators and occupants alike. The alliance will integrate Honeywell's security and building management systems with IDEMIA's biometric-based access control systems to create frictionless, safer and more efficient buildings.

The Honeywell and IDEMIA alliance is intended to design solutions that will allow occupants to easily and securely have contactless engagement with a building – from vehicle recognition at the car park and automatic elevator calls to biometric-based access and personalized conference room settings. With a focus on security and data privacy, these next-generation solutions will provide occupants with a safer, more efficient and more enjoyable experience that will help building owners attract tenants.

Tenable enters definitive agreement to acquire Alsid

Tenable Holdings, Inc. announced that it has entered into a definitive agreement to acquire Alsid SAS ("Alsid"), an Active Directory security player. Alsid for Active Directory is a Software as a Service (SaaS) solution with an on-premises deployment option that monitors the security of Active Directory in real time. The solution enables users to find and fix existing weaknesses with dynamic threat scoring, complexity ratings and recommended actions. Alsid continuously and non-disruptively discovers new attack pathways and detects ongoing attacks in real time, recommending remediations without the need to deploy agents or leverage privileged accounts.

Exploiting user privileges via Active Directory is a favorite and predictable tactic in many sophisticated compromises and common hacks. This risk has never been more acute than it is today, with so many people working remotely and often using personal devices to connect to corporate systems, with Active Directory playing a critical role in managed single sign on. For this reason, organizations are increasingly focusing on securing accounts -- employees, service contractors, temporary workers, systems accounts and others -- and their access to and permissions across systems as strategic to their cybersecurity posture. Understanding account access to systems and how those cascade across compute environments is a strategic and important complement to vulnerability management and systems hygiene and is increasingly imperative to managing risk holistically, especially in complex cloud and hybrid environments.

Accenture unveils new Business Group with VMware to help organizations adopt 'cloud first' strategy

Accenture and VMware announced an expanded partnership and the launch of a dedicated business group that will help organizations adopt a 'cloud first' strategy – accelerating migration to the cloud, building modern apps more rapidly, and using the cloud as a foundation for innovation and new business models, ultimately realizing greater value.

The Accenture VMware Business Group represents a new multi-year, multi-million-dollar investment from the two companies, which have a relationship spanning more than two decades. The new business group brings together dedicated professionals with deep expertise in hybrid cloud and cloud migrations, cloud native and application modernization and security across key industries. Supported by approximately 2,000 Accenture cloud professionals trained in VMware products and services, the Accenture VMware Business Group will help clients tap into the powerful capabilities and elasticity of the cloud – which has become essential to quickly scaling business services, operating efficiently and enabling innovation at scale.

Brightcove expands its video platform, launches Cloud Playout

Brightcove Inc. launches Brightcove Cloud Playout, a new feature that enhances its end-to-end video platform and makes it one of the few online video providers to offer this capability. Brightcove helps propel businesses forward through video, offering a complete video ecosystem with cutting edge technology, tools, incomparable knowledge, and customer support.

Brightcove Cloud Playout is a brand-new feature of Brightcove Video Cloud that enables content owners and organizations to quickly and seamlessly program a scheduled Playout of both on-demand video assets and live footage or events into a single stream. This provides a broadcast-grade "live TV" experience that leverages pre-recorded content to increase audience engagement and create new revenue opportunities. Customers also benefit from a highly streamlined workflow, as every possible video need is met within Brightcove's singular all-inclusive platform.

Lenovo announces 100 new Lenovo Exclusive Stores in FY 2122

Lenovo has announced that the company will open 100 new Lenovo Exclusive Stores in FY 2122 in India. This comes as an addition to their recent opening of the 400th LES in Bengaluru as part of its effort to continue offline retail expansion during the pandemic. This state-of-the-art store is located in the bustling Phoenix Market City Mall decked in a new and enhanced premium design focused on enriching customer experience in the store.

Lenovo currently has four such stores with the new premium design namely in Mumbai, two in Bengaluru, and another in Lucknow. These premium stores are built on the "Stay and Play" model emphasizing improving customer browsing experience in the store with dedicated customer service on a need basis. The premium stores also see a significant shift in the design with changes in layout, branding, lighting, color schemes, and much more.

As an industry first for the PC Brand, Lenovo completely digitized the customer journey in LES and introduced an Offline to Online (O2O) model enabling customers to complete their purchase on Lenovo.com if the product is not in stock in the stores. Additionally, during the lockdown – Lenovo introduced a 100% contactless purchase model for customers keeping their employees and customers safety in mind.

PERFORMANCE STORAGE, PURPOSE-BUILT FOR GAMING

BECAUSE THE GAME NEVER WAITS.

INTRODUCING THE EXPANDED WD_BLACK™ LINEUP

Stop staring at load screens. Increase your capacity and speed to get in fast and take them out faster. The WD_BLACK™ portfolio is purpose-built for gaming.

NEW WD_BLACK™ SN850 NVMe™ SSD

WD_BLACK™ P50 GAME DRIVE SSD

WD_BLACK™ P10 GAME DRIVE

WD_BLACK™ P10 GAME DRIVE FOR XBOX™

NEW WD_BLACK™ AN1500 NVMe™ SSD AIC

WD_BLACK™

DRIVE YOUR GAME AT **WDBLACK.COM**

McAfee and IngramMicro ink relationship to provide leading security solutions

McAfee has entered into an expanded worldwide alliance with Ingram Micro Inc. The alliance builds on the transformation of the McAfee channel program. The new agreement will provide access to McAfee products and solutions across Ingram Micro's global distribution network, including its regional Cloud Marketplaces and Centers of Excellence.

McAfee's SaaS portfolio on the U.S. Ingram Micro Cloud Marketplace was launched in late 2020, and the former plans to expand its footprint on Ingram Micro's network of e-commerce platforms throughout 2021. Both companies recognize the opportunity and impact of cloud transformation happening within the channel landscape. The two companies are working together to help channel partners embrace these dynamics and enhance their offerings to address customer needs and drive initiatives to accelerate the opportunity by offering McAfee Device to Cloud Suites designed to help organizations accelerate cloud adoption.

HCL Technologies celebrates $10 billion-revenue milestone by offering one-time bonus worth over Rs 700 crore to employees

To celebrate the USD 10 billion (about Rs 72,800 crore) revenue milestone, HCL Technologies has declared a special one-time bonus worth over Rs 700 crore for its employees.

"In celebration and gratitude all employees with one year of service or greater will receive a bonus, the equivalent of ten days' salary," the statement said.

In February 2021, the employees will get the special bonus which amounts to nearly USD 90 million plus payroll taxes in some countries, the impact of which is excluded from FY21 EBIT (earnings before interest and taxes) guidance provided by the company last month, HCL Tech said in a statement.

The company has issued this special bonus to employees across globe worth over Rs 700 crore in recognition of its recent milestone of crossing the USD 10 billion mark in revenue for 2020.

Amazon signs an MoU with Government of Karnataka

Amazon India has signed a Memorandum of Understanding (MoU) with Department of Industries & Commerce, Government of Karnataka to help drive e-commerce exports from the state. As part of the MoU, Amazon will train and onboard MSMEs from the state on Amazon Global Selling, its Exports Program, enabling them to sell their unique Made in India products globally to millions of Amazon customers across 200+ countries and territories. Amazon Global Selling lowers the entry barrier for motivated Indian MSMEs to expand their business and launch their brands globally from anywhere in India. With this program, homegrown businesses get instant access to global markets from Day 1, benefiting from Amazon's distribution capabilities and global footprint to scale rapidly, creating a sustainable exports business.

Amazon will conduct trainings, webinars and on-boarding workshops for exporters from key MSME clusters like Bellary, Mysore, Channapatna and others. The workshops will focus on sharing knowledge and imparting trainings to MSMEs about B2C e-commerce exports and selling worldwide through Amazon's 17 international marketplaces to over 300 million customers worldwide. These workshops aim to enable MSMEs with the knowledge and tools to launch their brands and grow their business in international markets through Amazon Global Selling.

Google Cloud cements partnership with Netmagic

Netmagic announced that it has elevated its strategic alliance with Google Cloud and has been recognized with the Managed Services Provider (MSP) status, an initiative under the Google Cloud Partner Advantage Program. Netmagic, with this partnership, aims to help enterprises optimize their business workloads on the Google Cloud and accelerate their transformation journey.

Enterprises are embracing cloud infrastructure to power business critical applications, aiming to balance – costs, performance, control and security. With over 20 years of deep understanding of the unique business demands of Indian enterprises, strong market reach and robust technological backbone, Netmagic is uniquely positioned to support enterprises with enabling cloud-led transformation for enterprises across industries including – Media, Fintech, digital native organisations and more. The company's solution offerings are focused on delivering a seamless and secure modernization of mission critical IT infrastructure, ensuring scalable performance for advanced applications and voluminous data.

Tata Power Delhi Distribution Limited Collaborates with OpenText to Enable a Remote Workforce During the Pandemic

OpenText has announced that Tata Power Delhi Distribution Limited (Tata Power-DDL), a leading power utility serving a populace of 7 million in North Delhi, India's national capital, has implemented OpenText Documentum as part of their digital transformation journey and response to COVID-19. With help from Documentum, Tata Power-DDL was able to automate complex, information-centric processes, maintain productivity and keep critical business moving forward during the pandemic.

Tata Power-DDL is a joint venture between Tata Power, India's largest integrated power company, and the Government of NCT of Delhi. When the pandemic struck approximately 70% of their employees shifted to remote work. The company needed to ensure employees, customers, regulators and external stakeholders retained access to mission-critical content and business processes.

"OpenText Documentum helped during the COVID-19 situation," said Santadyuti Samanta, Head of IT at Tata Power Delhi Distribution Limited. "We needed to establish communication with authorities, including the Delhi government, healthcare organizations and municipal corporations, so we created workflows on top of Documentum. Access was provided to people inside and the outside of the organization. As a result, we have remained resilient, enabled our employees to work from home, and continued to deliver for our customers throughout the pandemic."

Xerox Expands CareAR's Software Portfolio with Acquisition

Xerox with CareAR, an augmented reality support platform company that provides real-time access to expertise for customers, employees and field workers, has expanded its growing software portfolio with the acquisition.

With CareAR software, remote agents and experts can virtually see the situation and visually guide a solution using a suite of augmented reality tools via desktop, mobile, and smart glass devices. "Our software solutions address some of the biggest needs for customers - content management, digital transformation and personalised communications. And now we've added enterprise augmented reality," said Steve Bandrowczak, President and Chief Operations Officer, Xerox.

WE HAVE SEEN A STRONG GROWTH WITH LENOVO AS WE KEPT SUFFICIENT WORKING CAPITAL FOR THE BUSINESS OPERATION DURING LOCKDOWN

Partner Name: Focus Computers Pvt Ltd.
Spokesperson: P Ravi
Designation: Director

Please tell us about your business experience before & during COVID

With COVID, organizations have been under pressure on cash flows. As businesses bounce back, the dilemma around prioritizing expenses and restricting workflow is difficult to solve in the board room. The social distancing norms during the lockdown demanded zero physical interaction and the organizations required infrastructure to be managed remotely. The impact of COVID 19 is extensive and far reaching on every business. Customer satisfaction matters a lot for our business to thrive especially during and post pandemic. With our strong base of satisfied customers and our goodwill we have seen a trajectory growth of potential customers post pandemic.

How are you able to cope up with the business struggles during the PANDEMIC?

The workplaces are continuously adopting digital transformation, as organizations are either Working from Home (WFH) or having a satellite office. Many organizations, which include IT companies, business process outsourcing firms, small and medium businesses, etc. have adopted WFH and this will be the new normal even after the lockdown. As most of India's workforce is going to work from home and hence, organizations must equip themselves for the same. We had kept adequate working capital and reached customers to find out their needs proactively, which gave confidence to customers on our ability to meet needs and build strong customer base. This transition to 'Modern IT' has been years in the making, but the pandemic has accelerated the timeline. Modern IT essentially means moving away from onsite IT infrastructure to Managed Services, that offload aspects of a company's IT responsibilities to external sources, like Lenovo. This saves companies time, money and frees up their IT teams to focus on driving the business forward.

Please tell us about your core competencies and how well Lenovo Products & Services fits into your portfolio.

Strong technical knowledge and ability to customize to the needs of the customers, along with sufficient working capital and experienced engineers, with over 20+ years working experience has helped us to build robust one stop solutions for customers.

With respect to Lenovo's portfolio, we expect the consumer market to raise to 4 million. It has been flat for the last 5 years. The explosion is sudden because of learning from home and working from home trends, which is growing by 40 per cent. As per the analyst reports, Indian traditional PC market, inclusive of desktops, notebooks, and workstations, delivered a strong 9.2 per cent year-on-year growth in July-September quarter driven by these trends. Lenovo alone witnessed 40 per cent growth in the consumer segment in October-December period. Lenovo's renewed commitment to local manufacturing for its PC will significantly help us and we expect that this localized production strategy will further enhance our GTM. Lenovo has various solutions and services besides the products enabled for WFH. Lenovo's advanced solutions and new models help manage the cost, efficiency, and security, helping consumers embrace the new normal.

How has Lenovo helped you in building a successful business model?

Availability of various configurations, as off shelf models with adequate stocks with various T1, has helped in many ways to meet the demand raised during the pandemic time. Moreover, the business model of Lenovo is very partner friendly. We strongly feel that our partnership with Lenovo is not only a time-saver – indirectly, but it has also helped us channel the energy, and talent towards strategic initiatives that help drive the business forward which allows us to grow along with the brand's growth.

We are also proud to be associated with a socially responsible brand like Lenovo. They have done a lot of good work to grow the education sector in the country. To quote just one of many examples - Lenovo in partnership with Meghshala, empowered over 2,10,000 students across India amidst the pandemic. With an investment of $80,000 from the company, Meghshala had implemented e-learning classrooms in Karnataka, Manipur, Sikkim, and Meghalaya to aid students and teachers amid the COVID-19 pandemic. They even announced SmarterEd during the pandemic allowing educators to volunteer to close the gap and teach students who didn't have access to schooling.

What are the key verticals & drivers for your business growth?

Our end customer & channel base built over the years, which has helped us to meet the demands raised out WFH requirements and our stock levels has given confidence of customers to reach out to us for delivering the IT Solutions. Our core segment of the growth is the ITES sector and it was the key to our growth during the pandemic. However, our connection with the key decision makers in Lenovo has also helped us to reach this level of growth.

Microsoft announces Azure Stack HCI in India

Microsoft India has announced the general availability of Azure Stack HCI, a new hyperconverged infrastructure (HCI) solution, that combines the flexibility, scalability, and price-performance advantages of hyperconverged infrastructure with native Azure hybrid capabilities.

Part of the Azure Stack portfolio, it provides organizations seamless access to Microsoft Azure for hybrid cloud scenarios across datacenters, remote offices, cloud and edge locations Compatible with both Windows and Linux virtual machines, Azure Stack HCI solutions will be available from 20 partners offering Microsoft-validated hardware systems to ensure optimal performance and reliability.

Azure Stack HCI aims to empower businesses by enabling them to build and run cloud-native applications with seamless access to cloud services on-premises with existing tool, processes, and skillsets. It combines infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services in a software stack that spans on-premises datacenters and Microsoft's Azure cloud, providing the latest and up to date security, performance, and feature updates.

Fortinet Delivers SASE and Zero Trust Network Access Capabilities

Fortinet announced version 7.0 of FortiOS, Fortinet's flagship operating system. With over 300 new features, FortiOS 7.0 enhances the Fortinet Security Fabric and Fortinet's ability to deliver consistent security for all networks, endpoints, and clouds.

Rajesh Maurya, Regional Vice President, India & SAARC at Fortinet says, "Most vendors are focused on a single slice of security, but the reality is it's impossible to keep up with the complexity of today's threat landscape with that approach. New innovations in FortiOS 7.0 continue Fortinet's commitment to delivering a cybersecurity platform that expands across the entire digital attack surface to enable security that is broad, integrated, and automated to protect devices, data, and applications."

Microchip launches SparX-5i family of Ethernet switches

Microchip Technology Inc. announced its SparX-5i family of Ethernet switches – a single-chip, IEEE standards-based solution that offers the industry's most complete TSN feature set.

The SparX-5i family supports the key TSN IEEE standards needed for a complete real-time communication solution. These include IEEE 1588v2 and IEEE 802.1AS-REV profile for Time Synchronization, IEEE 802.1Qbv for Traffic Shaping, IEEE 802.1Qbu/802.3br for Delay Reduction, IEEE 802.1Qci for Stream Policing and IEEE 802.1CB for Seamless Redundancy. Offering these standards in a single chip guarantees end-to-end transmission of high-priority traffic with extremely low latency. In addition, the family supports standard L2/L3 Ethernet with up to 200G of bandwidth, incorporating 100M, 1G, 2.5G, 5G, 10G and 25 GbE interfaces for the most flexible connectivity solution available in the market.

"With Microchip's SparX-5i family of Ethernet switches, we're providing our customers with a simplified pathway to a TSN compatible infrastructure, helping them achieve real-time data communication across their entire network," said Charles Forni, vice president of Microchip's USB and networking business unit. "The SparX-5i family is the first Microchip device in a line of TSN switch developments that will address all levels of the industrial automation network, from the field bus to the factory backbone."

Oracle enhances Hybrid Cloud Portfolio with its Roving Edge Infrastructure

Oracle has expanded its hybrid cloud portfolio with Oracle Roving Edge Infrastructure, a new offering that brings core infrastructure services to the edge with Roving Edge Devices (REDs) – ruggedized, portable, scalable server nodes. Using Oracle Roving Edge Infrastructure, organizations can run cloud workloads wherever they need them, even in the most remote locations.

The new service is part of Oracle's comprehensive hybrid cloud portfolio, which provides customers with more flexibility and control over their cloud deployments than other vendors. Global customers across financial services, public sector, healthcare, logistics, and communications industries are using Oracle's hybrid cloud solutions to support their cloud transformations without the trade-offs in scale, data sovereignty, and control that they have had to make in the past.

OpenText Launches BrightCloud Cloud Service Intelligence

OpenText has announced the release of BrightCloud® Cloud Service Intelligence, enabling Cloud Access Security Brokers (CASB) and other security and technology vendors to enforce data-centric security policies and prevent unwanted interactions with cloud services and associated applications.

"The risks in securing cloud applications are fairly straightforward; if IT doesn't know about an unsanctioned application or service, they can't adequately protect it or the data it accesses and stores," stated OpenText Chief Product Officer Muhi Majzoub. "Modern user practices, tools and remote work are demanding a new era of real-time visibility. Which is why real-time threat intelligence is built into this new cloud-specific solution, utilizing over 10 years of innovation at the forefront of AI and ML."

Through a suite of three components – Cloud Application Classification, Cloud Application Function, and Cloud Application Reputation – partners can use BrightCloud® Cloud Service Intelligence to identify, classify, and block/allow access based on the application's classification, functions, and reputation score.

Commvault brings new SaaS and Hybrid Cloud Workloads for Metallic

Commvault announced another expansion of its Metallic Backup-as-a-Service (BaaS) portfolio. On the heels of last quarter's accelerated innovation, Metallic is adding new data protection solutions, features, and enterprise workload support including: enhanced SaaS application protection with the introduction of Metallic Salesforce Backup and Microsoft Teams recovery enhancements; the addition of Oracle and Active Directory to Metallic Database Backup; and the expansion of its hybrid cloud capabilities with the addition of HyperScale X as a fully integrated appliance and edge offering for Metallic.

"As we continue our global rollout of Metallic, we're finding more and more customers around the world are immediately grasping the value and inherent simplicity that cloud-native, as-a-service data protection can bring to their environments," said Manoj Nair, General Manager, Metallic. "With our new offerings like Salesforce and Oracle backup and our unique SaaS Plus capabilities, Metallic solutions offer customers what no other cloud-delivered backup service can match: the most comprehensive portfolio of BaaS solutions and the flexibility to backup each data source to the optimal storage target--whether that be cloud or on-premises storage, or the new HyperScale X for Metallic at the edge for ultimate performance with BaaS simplicity."

IBM introduces Elite Hybrid Cloud Build Team

IBM has unveiled its highly-specialized Hybrid Cloud Build Team to support the migration and modernization of ecosystem partner products, services, and other offerings across open hybrid cloud environments. Following the successful model of the IBM Data Science and AI Elite Team and the recent introduction of the IBM AIOps Elite Team, both focused on artificial intelligence, the Hybrid Cloud Build Team concentrates on helping partners update their workloads for deployment on premises, in the cloud, or any environment of their choosing.

A recent IBM Institute for Business Value (IBV) study that included responses from over 5,000 executives globally across industries found that the adoption of hybrid cloud – the combination of public clouds, private clouds, and on-premises IT – is expected to grow by 47% in the next three years and the average organization will be using six hybrid clouds. The report notes that the value derived from a full hybrid, multicloud platform technology and operating model is 2.5 times the value derived from a single platform, single cloud vendor approach. IBM's Hybrid Cloud Build Team was created to help partners maximize the value of an open hybrid cloud.

The elite engagement team consists of over 100 cloud architects, data scientists, cloud developers, security specialists, and developer advocates who work on the agile co-creation of advanced technology solutions for partners and their clients. The team also advises partners how they can best accelerate the transition of their products, services and other offerings to open hybrid cloud environments, including those in some of the most highly-regulated and sensitive industries like financial services and telecommunications.

Seagate introduces new Storage Expansion Card for Xbox Series X|S

Seagate Technology has announced the launch of Seagate Storage Expansion Card for Xbox Series X|S in India. The Storage Expansion Card will deliver an additional 1 TB of external storage for a streamlined gaming experience, replicating the speed and performance of the consoles' internal SSDs and Xbox Velocity Architecture.

Designed in collaboration with Microsoft, the Seagate Expansion Card for Xbox Series X|S is the only external storage device that enables users to achieve the same performance as the Xbox Velocity Architecture when playing games that have been optimised for next-generation Xbox consoles. The custom storage card seamlessly mirrors the functionality of the Xbox Series X and Xbox Series S internal SSDs and adds 1 TB of capacity letting gamers collect new and legacy games across four generations of Xbox including existing backwards compatible Xbox One, Xbox 360 and original Xbox games.

Zendesk unveils new Suite with powerful messaging solution

Zendesk, Inc. has announced the general availability of its comprehensive messaging solution as part of the new Zendesk Suite. The new package brings together all Zendesk's service capabilities, including messaging, into one complete offering that brings radical simplicity to the enterprise software space.

Zendesk's powerful messaging tools are designed to give businesses the ability to have continuous, convenient and personalized conversations whether customers want to text, chat on their computer, reach out over WhatsApp, and more. Companies can now provide connected conversational experiences across web, mobile, and social channels that work easily out-of-the-box with built in automation and the power to scale to support modern enterprise needs. Zendesk's messaging solution also offers advanced capabilities including proactive notifications, enabling specialized third-party bots, and allowing customers to transact directly within the conversation when browsing products, reserving seats, or making payments.

Salesforce brings Vaccine Cloud to speed up Global Vaccine Management

Salesforce announced Vaccine Cloud, technology to help government agencies, healthcare organizations, businesses, nonprofits and educational institutions more rapidly, safely and efficiently deploy and manage their vaccine programs. Today, international, federal, state and local agencies, healthcare providers and nonprofits worldwide are using Salesforce technology specifically for vaccine administration, including Northwell Health, Illinois' Lake County, University of Massachusetts Amherst, Gavi, the Vaccine Alliance and more.

Now that safe and effective COVID-19 vaccines are available, every country, state and city is rapidly establishing vaccination programs to get shots in the arms of billions of people. However, many government agencies and healthcare organizations don't have the technology infrastructure in place to handle the complexity, speed and scale necessary for vaccine administration, such as inventory and logistics management, getting people registered and scheduled for their vaccines, and recipient outreach and vaccine outcome monitoring.

HP brings new Latex printer portfolio to help print service providers

HP has introduced new Latex large format print solutions to help print service providers diversify their offerings and meet more challenging customers' needs. After a year of business disruption across the large format industry, the HP Latex 700 and 800 series brings a suite of features that enable PSPs to be more agile, tackle ambitious projects and take on the highest value work. The new portfolio also delivers fast workflows that help businesses hit deadlines, while sharpening their sustainability edge.

Vitesh Sharma, Country Manager, Large Format Production Business, HP India says, "The new HP Latex 700 and 800 series portfolios will offer professional color quality, with a purpose to address every customer request, regardless of fast-changing schedule or application demands. They will also be able to bring significant improvements in productivity and efficiency by up to 50% to meet organization goals. With our new HP Latex 700W and 800 printers we will empower PSPs to navigate customer challenges in the next normal and embrace more ambitious projects."

The new HP Latex range in India consists of two devices – the HP Latex 700W and 800, which offer white ink capability for the first time in this category. It is the whitest white ink available on the market that does not yellow over time, enabling print businesses to produce neater outlines and add more contrast to darker supports.

Prama Hikvision launches new ITS camera for improvement of road safety

The new All-Rounder ITS camera is engineered with an all-in-one structure, embedding video, radar, and supplemental light in one module, helping traffic authorities to easily ramp up the detection of violations.

Prama Hikvision, the India's leading video security solution provider, has introduced its latest traffic product offering - the All-Rounder ITS camera - designed to improve road safety and optimize traffic flow. As the name implies, the camera encompasses different skills and abilities, boasting speed detection, traffic violation detection, automated plate recognition, and vehicle attribute analysis in one housing.

Hikvision is always pushing the boundaries of video technologies. Beyond the visual range that is perceived by video cameras, the abilities to understand other kinds of "senses" would allow even more precise monitoring and reporting of events or accidents. This is multi-dimensional perception, a trend that will drive the security industry in the future.

Airtel becomes 5G Ready Network

Bharti Airtel ("Airtel") announces that it has become the country's first telco to successfully demonstrate & orchestrate LIVE 5G service over a commercial network in Hyderabad city.

Airtel did this over its existing liberalised spectrum in the 1800 MHz band through the NSA (Non-Stand Alone) network technology. Using a first of its kind, dynamic spectrum sharing, Airtel seamlessly operated 5G and 4G concurrently within the same spectrum block. This demonstration has emphatically validated the 5G readiness of Airtel's network across all domains - Radio, Core and Transport.

Airtel 5G is capable of delivering 10x speeds, 10x latency and 100x concurrency when compared to existing technologies. Specifically, in Hyderabad, users were able to download a full-length movie in a matter of seconds on a 5G phone. This demonstration has underlined the company's technology capabilities. The full impact of the 5G experience, however, will be available to our customers, when adequate spectrum is available and government approvals are received.

Vi signs a strategic partnership with Voot Select

Vodafone Idea Limited (VIL) has announced a strategic partnership with Viacom18's premium subscription led video on demand streaming service, VOOT Select, to offer premium content on its digital platform- Vi Movies and TV app. Under this partnership, aimed at bolstering the growth of the digital ecosystem in India, customers of Vodafone Idea can now enjoy the curated content offering of VOOT Select, with a seamless viewing experience on their Smartphones.

To strengthen current content offering on Digital platform - Vi Movies & TV app, the partnership will give customers access to hours of exclusive content pieces from Voot Select which includes the very successful original mini-series The Gone Game, high octane espionage series Crackdown and other critically acclaimed series such as Asur, Illegal & The Raikar Case, to name a few. Vi customers will now have full access to watch premium Hindi Shows of Colors & MTV like BIGG BOSS season14, Roadies Season 18, Splitsvilla & Khatron Ke Khiladi.

Vi users can also enjoy a host of International shows like Shark Tank, Top Gear, The Office, Tin Star, Nancy Drew, Pink Collar Crimes to name a few. With continuous content addition, users can look forward to an exciting library of content that will keep them entertained 24/7. Voot Select, through its immersive content slate across genres offers a great value for India's screenagers seeking diverse content experiences.

NETGEAR's Orbi Tri-band RBK853: The Next Generation Wi-Fi 6 Mesh Router

We have all experienced the pain of having a slow and unstable Wi-Fi router; most of us experienced the frustration of a network delay during lockdown especially when we are trying to stream our favourite movie or when we are having an important work discussion with our team. Even though we have stepped out of our homes and are getting back to office, remote working has now become a norm and is here to stay and many organizations are still providing the option to work remotely.

Our home networks need to be able to keep up with the demands of accessing and transferring large files and using video conferencing tools when we are working remotely, hence having a strong Wi-Fi has become a necessity for us.

Speaking on the current scenario, Marthesh Nagendra, Country Manager India, ME & SAARC, NETGEAR commented, "NETGEAR has been a leader in the Wi-Fi industry for well over 20 years and has been constantly providing various innovative products that meet the customer's requirement. Recently, we have introduced the Orbi Mesh Wi-Fi 6 range to tackle the current challenges due to rising demand for home networks."

Keysight's RAN Solution Portfolio Drives Performance Reliability in Multi-Vendor 5G Networks

Keysight Technologies has introduced a suite of end-to-end solutions that enables an ecosystem of Open Radio Access Network (O-RAN) vendors and mobile operators to verify interoperability, performance, conformance and security of multi-vendor 5G networks based on O-RAN standard interfaces.

Many mobile operators are deploying cloud-native and virtualized radio access network (RAN) architectures based on specifications set by the O-RAN Alliance to deliver 5G services. The transition towards multi-vendor networks introduces interoperability and performance complexity. End-to-end testing, from the edge of the RAN to the 5G core (5GC), as well as from early pre-silicon development to system integration, ensures performance levels are met. Comprehensive testing across a heterogeneous network enables vendors to extend the capabilities of their designs and mobile operators to deliver solutions that support innovative service offerings.

Verizon Business teams up with Deloitte to bring 5G to retail

Verizon Business and Deloitte unveiled a 5G and mobile edge computing (MEC) retail industry digital platform that is designed to give retailers the ability to gain significant efficiencies in their retail operations and transform customer experiences. This innovative platform can unlock retail in-store data with near real-time analytics to improve customer engagement, inventory efficiency, and associate productivity. The in-store experience should be significantly enhanced by addressing challenges retailers typically face, such as out-of-stock items, plan-o-gram compliance, and frictionless/cashierless checkout.

Verizon's 5G network and MEC, combined with advanced technologies such as video camera and sensor-based analytics, artificial intelligence (AI), and augmented reality (AR), are the foundational elements of the retail platform. Together with Deloitte's retail industry and solution engineering experience, the two organizations have developed a set of enterprise-wide use cases that can be enabled by the platform, a reference architecture that amplifies back-office application integration value, and a customizable approach to accelerate outcomes and ROI.

HFCL partners with Qualcomm Technologies over development of Wi-Fi 6 Portfolio of Products

HFCL has strengthened its IO product portfolio of Wireless Solutions with the roll-out of Wi-Fi 6 products in addition to their existing Wi-Fi 5 Access Points (APs). This new range of IO products by HFCL is targeted to serve global Carriers, Enterprises and Internet Service Providers to provide seamless data connectivity to their consumers.

The perpetually growing demand for higher speeds, increasing density of connected devices and diverse applications have strained the wireless access networks to their limits. This critical challenge gets addressed by Wi-Fi 6 which is based on the IEEE 802.11ax standards. Wi-Fi 6 is capable of delivering >2 times the capacity & at 75% lower latency as compared to Wi-Fi 5 products.

Furthermore, the Wi-Fi 6 products are compatible and complementary to the upcoming 5G technology, offering a seamless integration with 5G core, enabling a smooth mobile data offload implementation for operators thereby providing lower latency & increased capacity over their predecessors without any hassles of a complex Wi-Fi – 3GPP core integration. Together they bring next-level, seamless functionality to the wireless world.

Vembu partners with Savex to provide comprehensive data protection in India

The backup and disaster recovery company, Vembu has announced a new partnership with Savex Technologies. This partnership will enable Savex to distribute Vembu's flagship product, Vembu BDR Suite, through its wide-ranging network of Value-Added Resellers and Solution Providers to the small, medium and enterprise-level businesses across India.

Raunak Jagasia, Director Enterprise Business and Alliance at Savex Technologies said, "We are incredibly pleased to collaborate with Vembu, a leading player in Backup and Disaster Recovery market for small and medium businesses. This partnership bundles their flagship offering of – Vembu BRD Suite which will support us address the data protection requirements of organizations, hosted in both physical & virtual environments. We believe this association will go a long way in enhancing Vembu's presence and addressing specific needs of our customers across the country."

Vembu BDR Suite is a comprehensive and affordable backup and disaster recovery solution designed to protect the data across diverse IT environments that include virtual (VMware, Hyper-V), physical (Windows, Linux, Mac), cloud workloads (AWS, Azure) and SaaS applications (Office 365, G Suite).

Nagarajan Chandrasekaran, Vice President of Product Marketing & Management, Vembu Technologies said, "We are thrilled to announce a new partnership with Savex Technologies. With our affordable and top-notch backup and disaster recovery software and Savex's knowledge and expertise along with cutting edge technology and rigorous process control, we aim to reach more business in need of a capable solution for complete data protection of their business infrastructures."

Vertiv Brings Together a Powerhouse Panel to Discuss the 2021 Data Centre Trends

Vertiv has hosted a LinkedIn Live event, Trendspotting: The Track Ahead for the Data Centre Industry in 2021 on January 19th, 2021 at 7:30 pm IST.

This event brings together experts from around the globe with a combined 60+ years of experience in the IT, data centre and manufacturing world to share their regional insights into the recently announced 2021 data centre trends and discuss how these predictions resonate in their regions and impact their customers.

"We've seen first-hand with the pandemic how it has accelerated existing trends of technological adoption, and it's clear the world is not going to return to its pre-pandemic state. With this global digital dependency, data centres have gained utility-like status but with great power comes great responsibility and sustainability and governance is becoming of rising importance" says Andrew Donoghue, global director of analyst relations for Vertiv and moderator of the event.

Participating in this discussion are Vertiv experts:

Andrew Donoghue, global director analyst relations

Andrew is the global director, analyst relations for Vertiv. He specialises in data centres and critical infrastructure. He is the author of several influential reports covering topics including renewable energy and the data centre; IT power management; and data centre cooling. He has worked for analyst companies such as 451 Research and has also held senior editorial roles at business publishing companies including CBS Interactive and Incisive Media. He has also been involved in a number of European Commission-funded IT research projects into data centre energy efficiency and sustainability.

Fortune Marketing becomes National Distributors for Panasonic India

Fortune Marketing shared that they have been appointed as value added distributors for Panasonic India for distributing Panasonic's enterprise range consisting of - Commercial Android Signage Display, 4K UHD Commercial high brightness displays, Multi touch Interactive professional displays and Professional Video wall range of products.

"We are glad to partner with Panasonic. Their century plus legacy, cutting-edge quality products and distinguished solutions will be a value add to our portfolio. It will further enhance our B2B solutions range to the Indian market by offering best-in-class products through our strong distribution network," Manoj Gupta, MD, Fortune Marketing said.

Fortune Marketing is one of the leaders in distribution business across India. Present across the Nation, Fortune Marketing works with their 24 operational branches which caters to end-to-end requirements of the customers. Fortune has one of the largest sales and distribution networks in the country and provides value added distribution for partners including last mile connect and support across marketing and promotions for Networking, IT, Security& Surveillance, Storage solutions and electronics products covering more than 7000 towns across 664 districts in India.

Dassault Systemes showcases Digitalization for Aerospace, Defense and Space Ecosystem at Aero India 2021

Dassault Systèmes at the 13th edition of Aero India 2021 showcases technology solutions to Improve Supply Chain Collaboration, to Design for Flexible Manufacturing, to Manage Complex Systems and Accelerate Program Integration and to Deliver High Performance Operations. Experts from Dassault Systèmes will be present at booth numbers A6.6 and A6.8, to discuss how to bridge the gap between the virtual and real world to accelerate concept to operations by 50% through industry solution experiences based on the 3DEXPERIENCE platform.

Today, supplier-created parts and content represents 50%-60% of the value of an aerospace system. Relentless price pressures are compelling aircraft manufacturers and suppliers to reinvent the way they work with the supply chain. The new model requires a closer partnership to improve visibility, on-time delivery and first-time quality. The "Program Excellence" industry solution experience enables companies to optimize their product strategy and reach a high level of efficiency in program execution. Companies can implement their digital transformation around governance, configuration, collaboration and analytics. The "Engineered to Fly" industry solution experience helps suppliers win more business and more efficiently deliver on time, on budget, on target. Best in class engineering, simulation and project tools delivered on a single platform can improve productivity up to 40% while reducing total cost of ownership by at least 15%.

Aerospace companies must integrate new technologies into ever-increasing complex aircraft that can meet passenger demands as well as operator cost and uptime targets. To drive down costs, companies must find efficiencies in how they conceptualize, design, manufacture, test, certify and support new aircraft. It requires a model-based and data-driven approach to drive significant process improvements to transform their ability to deliver on schedule, on cost, and on specification. Dassault Systèmes supports them in accelerating program maturity from concept to manufacturing while driving 40-60% of cost out. The "Winning Concept" industry solution experience increases success rates of new concepts and bid proposals by uniting the proposal authoring, concept alternatives definition and analysis trade process on a single business platform. The "Cleared To Operate" industry solution experience helps Aerospace & Defense programs test and certify on time and improve confidence between aviation authorities and their suppliers.

The entire globe has undergone a 360 degree change with the sudden outbreak of COVID-19 pandemic. It has not only changed the way people lived their lives but also the way they used to work. The pandemic has forced people to work from home or anywhere and it is not at all a protected environment in terms of IT security. This has put the data of any organization not only in a vulnerable state and also exposed to cyberthreats.

As per a report by Check Point Software Technologies, the sudden push to provide remote working facilities to employees during the lockdown has made India vulnerable to ransomware attacks in the third quarter of current year. The study also reveals that after the US, India comes second among the top five countries most affected by ransomware attacks in the third quarter. Apart from ransomware, different kinds of attacks are also coming to the surface.

This happened as the organizations were in a rush to facilitate remote access and many companies allowed connectivity from unmanaged home personal computers that often lacked basic cyber hygiene such as updated software patches, anti-malware, among others. Even personal mobile devices were allowed access to networks.

Now, the enterprises are adopting latest technologies to secure their endpoints. At the same time in 2021, the cyber criminals will continue to target the remote workers as their easy targets. On this backdrop, we have gathered insight from the CIOs/ CISOs, vendors and partners on how they are mitigating threats, measures they have adopted to combat threats, how they are safeguarding their employees and customers. Let's take a look at it.

INDIAN CIO's ARE PREPARED FOR A DATA BREACH

VPN AND PRIVILEGED ACCESS MANAGEMENT : THE KEY TECHNOLOGIES

SANDEEP SENGUPTA
MD, ISOAH Data Securities

EDUCATING CUSTOMERS & EMPLOYEES

Over the last 10 years, our "Indian School of Anti Hacking" has conducted several in-house training at top companies like Deshaw, Mjunction, CESC, National Power Grid, Banks; where our ethical hackers have shown LIVE demos of Hacking. This is the new form of training where you not only read and hear, but see practical demonstrations of the consequences of cyber security mistakes. This gives the best awareness. What you see is what you believe.

MITIGATING THREAT SITUATION

Organisations have always invested in perimeter security as the endpoint was supposed to be in the trusted zone. Now with employees working from anywhere and everywhere, companies will invest a lot on endpoint security, as well as the authentication and authorisation tools and techniques. VPN, privileged access management, etc. will be the key technology. Cloud adoption which was mostly for the servers, now will also be used to put desktops on cloud, so that employees log into virtual offices in the cloud and all data is still in control with the organisation.

SAFEGUARDING CUSTOMERS & EMPLOYEES

People have always been the weakest link whether they are working from home or office or client site. Providing them awareness is the key solution. The awareness should be in a language which they can relate to their day to day operations. Coupled with real life case studies related to their work, and focussing on the consequences proved by some LIVE demo, can open up their eyes. Usually companies make mistakes of making content which appears to be preaching without giving much insight. Organisations must think of people behaviour and award people who not only help to embed security in the company culture, but also bring innovation into the rapidly dynamic cyber security in today's world.

TRAINING – THE ONLY MANTRA OF SUCCESS IN CYBERSECURITY

DR. CHITRANJAN KESARI
CIO & IT Head, Ahuja Hive Ltd. (Fosun Group)

MEASURES ADOPTED FOR COMBATTING THREAT

Technology is playing great roles to safeguard our network. But when work from home is coming, all technology installations in corporate premises are not helpful to safeguard our users. A little contribution of user training for cyber security for basic things helps us in the long run.

EDUCATING CUSTOMERS & EMPLOYEES

Education about cyber security plays an important role in our company and on customer sites also. My continuous training about basic cyber security helps our users.

MITIGATING THREAT SITUATION

In our industry of construction, engineering and real estate, customer data and design are very important. As we are using ransomware protected information security solutions and backup on the great platform with reliable DNS protection solutions help us in protecting our data.

UPCOMING THREAT

Plenty of problems happen and deepfake is one of the same as we as well as the government is also facing the same issues. Lots of people are facing the problem and losing lots of money due to this. I only tell that the fake has always been fake. Take your decision wisely by dealing with any person or call, or online links.

SAFEGUARDING CUSTOMERS & EMPLOYEES

This is very challenging these days as users are using work from home environments to work and this is going to stay for safety and companies are saving lots by using work from home environments. But security is one of the concerns and regular interaction and training of our users help us for protection. Cyber security training for users plays important roles. Training, Training and Training is my mantra for success in cyber security.

"DEEPFAKE THREATS ARE GROWING POTENTIALLY ALONG WITH SIGNIFICANT GROWTH IN AI/ML TECHNOLOGIES"

DR. SAYED PEERZADE
Group Chief Information Officer, Reliance Big Entertainment, Reliance Group

MEASURES ADOPTED FOR COMBATTING THREAT

We are a digitally matured organisation, well ahead in curve on implementing the new age technologies, experimenting and bringing the things stability. Being in the worldwide operations and headquartered in Mumbai, most of remote connectivity essentials like Uniform Threat protection, Firewalls, and VPN's, AV protection, DLP's were in place. Only change in this pandemic is even regular office employees need to be shifted to home and for us it is just extending these services to everyone. We are the fastest of the lot in industry who moved to WFH and did not face single downtime on any of users because of cyber risk issues.

MITIGATING THREAT SITUATION

We have mitigated all attacks effectively. In my point of view Network design and Data centralization are a major enemy of cyber threats like ransomware and that most of regulatory efforts increasingly push against this. From a CIO point of view or DPO's perspective, opting for decentralized, interconnected data sources is not only a more agile and efficient way to access only the data you need but actually mitigates machine learning risk. Due to faulty network design individual attacks can spread to other devices within no time. User awareness also plays a very important role here. We have the following processes inside organisations below enterprise wide for IT teams and endpoints, apart from decentralised network and data design. Decentralised networks will help in isolating the attack quickly before it spreads to all of the network.

UPCOMING THREAT

As technology moves ahead, there is a parallel industry working on exploiting the new techs. Deepfake is one of them. Cybersecurity as a large has to act on every single threat and deepfake is no exception. Deepfake threats are growing potentially along with significant growth in AI/ML technologies. In the engine, deepfakes is not enchantment, it is pure mathematics. The application utilizes deep learning application, which implies it depends on neural networks to play out its functions. Neural networks are programming structures generally planned after the human brain. When you give a neural network numerous examples of a particular kind of data, state photos of an individual, it will figure out how to perform functions, for example, recognizing that individual's face in photographs, or on account of deepfakes, replace another person's face with it. However, as deepfake innovation improves, the tech business will probably play a smart game to try to remain one stride ahead that does not imply that staying aware of deepfakes is outlandish. New AI-based tools that identify frauds will probably help significantly, as will automated tools that can compare digital artefacts that have been filed by various companies and track changes in them after some time.

SAFEGUARDING CUSTOMERS & EMPLOYEES

It is a wide topic to discuss. However, we can always summarise the four important aspects - Thought, Security, Culture & team. What is that 'thought' process needed to bring digital innovations, what is the 'security' role in these transformations, how to bring 'culture' of innovations, how to build an effective innovative 'team', and sustain innovative approach in the organisation for both business growth and security.

With security regaining priority in digital strategies, CISOs are definitely dispersing security responsibility throughout the organization and working to transform the IT culture.

My thought process of digital transformations and security combines, which I always put forward during all of my discussions

Transformations should be aligned to organisational business goals

Bring the transformations throughout organisation

Information Security should be a part of the Digital design, be it product or platform.

AN INFORMED CITIZEN IS THE BEST DEFENCE AGAINST DEEPFAKE

DR. RAJEEV PAPNEJA
Chief Growth Officer, ESDS Software Solution

MEASURES ADOPTED FOR COMBATTING THREAT

Work-from-anywhere is not something new for IT companies such as ours. Our employees have been used to this but for many of our customers this has brought in a paradigm shift in their way of working. The first and most important thing is to be vary of the fact that no matter where we work from, systems are vulnerable as soon as they are connected to the network. Layered defence mechanism works best for any kind of security, be it physical or virtual. It is important to identify the attack points in the landscape.

For example, if someone is using a SaaS application, the attack points besides the endpoint would be the data in motion over the Internet, data at rest, data during processing, the virtual machine itself that can be compromised, and the SaaS application which could be vulnerable. Every attack point has different ways of making them secure.

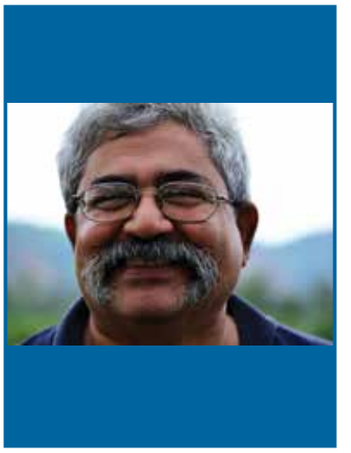
We should make sure that the basics are not neglected as part of the security framework, something as simple as having updated antivirus running on systems. Use of trusted and encrypted WiFi connection, https for secure connection over Internet or use of Web VPN etc. should be part of the defence mechanism. While technology can help us, the most important thing is to educate the customers and employees about the types of threats such as email phishing, link jacking, unsecured WiFi connections etc., and common safety measures for keeping their work safe. It would also make sense to promote mandatory backups and frequent password recycling which are real basics and mostly overlooked.

UPCOMING THREAT

Deepfake is, and will be one of the most damaging threats in coming times. It has the power to bring down nations, forget an organization, by creating communal violence for example, by simply creating few doctored videos. We see a lot of doctored videos today floating on the internet and WhatsApp, and these videos can sometimes cause unrepairable damages.

As AI/ML technology is maturing, supported by the advances in neural networks and deep learning, it would not be surprising if the original video looked fake against the fake one. With the technology available in every common person's fingertips, we are sitting on a potential time bomb. With all the nuclear weapons and military on one side, and few Deepfake images/ videos on another side, it would be difficult to gauge which side can cause more harm to a nation. As mentioned before, technology can be used to mitigate the risks, but till then it goes back to the basics of educating the people of the possibilities and increase awareness. An informed citizen is the best defence against such threats.

"THE 'DEEP FAKE' CAN BE WELL COUNTERED WITH THE 'DEEP TRUST'"



JAIDEEP KHANDUJA
Chief Technology Officer, AccioMango Pvt Ltd

EDUCATING CUSTOMERS & EMPLOYEES

Pandemic has transformed the whole concept of automation, digitalization, and IT security in a very different manner. Gone are the days of virtualization and digitalization of an organization within the boundaries of its physical existence. The same goes true for boardroom to boardroom virtualization and digitalization. The organizational perimeters have expanded to the homes of its employees. Each employee's home has become his or her workplace.

Hence, that each endpoint having different geography was supposed to be strong in terms of security as an endpoint within the organizational boundaries. The immediate role of the organization was to make each individual accessing the servers and databases from 'anywhere' be more cautious and aware about it. IT training had a complete paradigm shift to build a new kind of strong security culture.

MITIGATING THREAT SITUATION

I do not think threats and vulnerabilities have increased or this new situation will open more gates for attacks provided appropriate measures, checks and controls, and real time audits are there as a new layer of security to handle work from home or work from anywhere kind of situation. 'No Trust' is the best way to handle it. Hardware, be it a smartphone or a laptop at home, needs to be scanned thoroughly every time it connects to the business applications.

UPCOMING THREAT

Deepfakes are the next threat on which cybersecurity has to act on. Rather, it has already started. But in my opinion, besides technology, HR and organization has a highly demanding role in this to build each workforce as a fully trusted warrior of the organization. The 'deep fake' can be well countered with the 'deep trust'. So, basically 'No Trust' and 'Deep Trust' will go hand in hand provided the organizations know what it means.

SAFEGUARDING CUSTOMERS & EMPLOYEES

I think banking is the best example of this. Even before pandemic we all were (and are) doing mobile banking or online banking. For banks, every customer and every transaction is crucial. It is now required for every organization's business applications to be well equipped with stronger security layers (software & hardware) as well as appropriate checks and controls.

"ESTABLISHING A CULTURE OF AWARENESS AROUND CYBER-SECURITY IS CRUCIAL TO THE ONGOING INFORMATION SECURITY"

KAPIL MADAAN
CISO, Minda Corporation

MEASURES ADOPTED FOR COMBATTING THREAT

Since the COVID-19 pandemic started approximately one year ago, the world has changed in many ways. The biggest, most damaging and most widespread threat that all businesses are facing is phishing attacks. They have grown approximately 65% over the last year, and they account in billions in business losses.

A Cyber security leader strategy is needed, as the attack surface grows, and we rely more on digital technologies in all areas of business and industry. Cybersecurity challenges are increasing and cyber resilience can help organizations prevent, detect, respond, and recover.

The functions—Identify, Protect, Detect, Respond, and Recover remind us of how important it is to balance proactive safeguards while preparing for worst-case scenarios. This balance is especially important in all the business settings where a worst-case incident could drastically affect the solvency of a business

UPCOMING THREAT

Deepfake is going to be the biggest threat. Deepfake, a combination of the words 'deep learning' and 'fake'. I will suggest preparing strategy against such incidents.

Social engineering attempts & Email based phishing – Make Employee training and awareness mandatory. By offering adequate training and creating awareness employees can be turned into an additional line of defence.

Plan, Act & Response Strategy – Ensure that your organization is ready to adequately respond to such incidents.

Further So many Security service providers are working on an AI-powered deepfake detection software for this purpose. The tool can automatically analyse videos and photos to provide a confidence score that the media has been manipulated.

SAFEGUARDING CUSTOMERS & EMPLOYEES

Remote workers are typically the first to face security threats. They are often the source of network security incidents that can wave quickly through the rest of the organization. Even if we do not have remote employees, mobile devices like smartphones and laptops pose security risks.

Now the Cybersecurity leader role comes in picture to prepare strategy. We have to think from a broader perspective like Application Security, Network Security, Endpoint security, Email Security, IoT Security and so many based on the environment.

From support to strategy and set the culture, while most companies recognise the pressing need for technical security measures, without a culture of security in the workplace, the risk of threat can remain high. Human error can very quickly and easily undo even the most stringent digital protection, so establishing a culture of awareness around cyber-security is crucial to the ongoing information security.

STRENGTHENING REMOTE PROTOCOLS WITH MULTIPLE INTERFACES AND SET UP OF STRONG LOCAL SECURITY POLICIES WITHIN LAPTOPS CAN MITIGATE RISK

DR. HARSHA E THENNARASU
Chief IT & Cyber Security Advisor, HKIT Security Solutions

MEASURES ADOPTED FOR COMBATTING THREAT

Customers must ensure, are there any vulnerabilities that are residing in their laptops, those are major challenges for customers. Their laptops might consist of hidden BOTs and malware, spyware, etc., employee safety depends on the customers, IT and security guys to ensure patches and updates, etc.

EDUCATING CUSTOMERS & EMPLOYEES

Regular webinars and video conferences are being used to bring continuous awareness. Increased the frequency of training from quarterly to monthly and bimonthly. Also we have designed an online survey type assessment which can evaluate the understanding of the employees.

MITIGATING THREAT SITUATION

We have a solution like MDR with a proactive approach and instant response on the incidents reported, not being allowed to reach to employees. Even if there is any new variant of ransomware, employees are well educated to understand malicious files received and links over email. Even we have customized rules to block file less Ransomware.

UPCOMING THREAT

There is an increase of traditional malware/viruses/spyware with new methodologies, where industry is overlooking these vulnerabilities. More raise on file less ransomware is expected, those are targeted through simple text codes which are compiled by local svchost.exe file and compile ransomware internally by passing all security mechanisms built around.

SAFEGUARDING CUSTOMERS & EMPLOYEES

By strengthening remote protocols with multiple interfaces and set up of strong local security policies within their laptops, can mitigate the risk. Which is the only solution to prevent security breaches on remote workers. Definitely cybercriminal will have less mileage.

OEM's are reinventing their security strategies

The 2020 ongoing pandemic is still alive and remote working for many companies too. Ransomware attacks, cyber threats, cyber-crime is still going on, with this now a new cyber fear- Deepfake has cropped its head and is making its way to the cyber fear world.

A few Cyber gurus have shared their information with VARIndia to fight against the ongoing CyberWar.

Here's what each has to say:

AKAMAI- ANOTHER NAME FOR BEST EDGE SECURITY SOLUTIONS

Prasad Mandava
MD India & VP of Engineering at Akamai Technologies

Measures adopted: Remote working has caused new opportunities for cyber criminals to take advantage of the security trade-offs by individuals for ease of use and access to engage in credential stuffing attacks. The most common security threat seen during the pandemic is primarily based on phishing scams. As work from home continues, multiple measures are needed to be followed by the enterprises to protect the data.

Securing Enterprise Assets became of major importance as more enterprise servers, applications, and services become accessible to remote users.

Protect and Secure Remotely Connected Devices: As working from home will become a norm, and more devices will be connecting with the enterprise asset, it will become even more important for an enterprise to enhance the security aspect to cut down moderation.

Reducing the Attack Surface from Threat Actors: The Zero Trust approach, if enabled, will reduce the malicious and threat actors attacking major company devices, putting all data and security under direct risk.

Mitigating threat situation: Akamai's API security is mission-critical for organizations to develop partnerships, create connections for employees, and enable modern application architectures. For security teams who are looking for more comprehensive protection. Akamai offers some of the best edge security which gives one full control over security implementation with the following solutions:

API Gateway - It takes care of the business management and governance of your API traffic.

Kona Site Defender – It provides the same automated rule set plus a positive security model that can be further enhanced with client reputation to provide a reputation score on suspicious IP client behavior.

Bot Manager Premier –This enables security teams to manage exponentially growing good and bad bot traffic.

In the spirit of remote working and rapid innovation, secure API solutions can protect your system from DDoS attacks and protect your infrastructure improving your security controls and services.

"SECURITY IS THE BEDROCK OF WHAT CITRIX HAS DONE FOR MANY YEARS"

Ravindra Kelkar
Area Vice President, Indian Subcontinent, Citrix

Measures adopted: Innumerable organizations across the globe are tackling cyber security threats and data breaches at any given time. With applications being modernized for web-based access and deployed in multi-cloud environments, the traditional VPN model does not adequately meet the needs of the evolving use cases and falls short on end-user experience and security. By implementing Zero Trust approach or a VPN-less access business can eliminate the need to maintain VPN servers and limit access to specific IP addresses.

Bad actors are targeting web and cloud applications via the local internet connections that remote workers use. Secure access service edge technology (SASE) delivers security services like web filtering, data loss prevention, and next-generation firewalls to protect these workers across a network.

Way to tackle this is Fast Identity Online (FIDO2) authentication which enables users to prove their identity using biometrics, mobile devices, or specialized security tokens.

Mitigating threat situation: Security is the bedrock of what Citrix has done for many years — securing apps, access, networks, data, and endpoints. Our solutions let employees work securely, the way they want. As mentioned earlier, SD-WAN networking solution can help the IT teams improve monitoring, and overall security. Our virtualization and container-based solutions help organizations isolate environments.

Password-less multi-factor authentication (MFA) also helps add an additional layer of security to users, devices, and resource authentication, authorization, and access.

All these combined, can help organizations become more robust and resilient to any huge, unprecedented wave of disruption in the future without compromising the security and privacy of the organization.

Upcoming threat: Deepfakes are becoming more and more sophisticated with time. The algorithms associated with it are also evolving rapidly. These factors combined have made it increasingly challenging to combat the threats and their adverse consequences. Additionally, with the increasing amount of work and content being accessed and shared online due to the pandemic, the use of deepfake video and audio technologies is expected to evolve into a major cyber threat to businesses within the next few years.

CYBERARK ADOPTED TOOLS AND PROCESSES ENABLE EMPLOYEES TO SHIFT TO REMOTE WORK SEAMLESSLY

Rohan Vaidya
Managing Director – India, CyberArk

Measures adopted: As remote work strategy is being implemented for the long term, distributed IT environments are only going to continue to expand. Adoption of public cloud services, SaaS applications and remote access have dissolved the traditional network perimeter, so authentication and authorisation of all identities become paramount in order to stop the organisation's critical data and assets being potentially accessible in many more ways than previously possible. Identity becomes the key line of defence for most organisations and the de facto 'new perimeter.'

Mitigating threat situation: Ransomware is a type of malware designed to infect machines, encrypt files and hold the needed decryption key for ransom until the victim submits the required payment. Ransomware attacks on enterprises and government entities – cities, police stations, hospitals and schools – are on the rise, costing organisations millions as some pay off the attackers to untangle themselves and restore vital systems.

Research by CyberArk Labs has evaluated what mitigation strategies are most effective against ransomware. One of the key findings is that when local administrator rights were removed and application control policies were in place with a solution like CyberArk Endpoint Privilege Manager, 100 percent of ransomware samples were prevented from encrypting files. We also use application grey listing to proactively defend against previously unknown ransomware variants. With a greylisting approach, you can restrict read, write and modify permissions for unknown applications to prevent ransomware from encrypting data. You can also use greylisting to block access to network drives to prevent ransomware attacks from propagating across the enterprise.

Upcoming threat: Video and recordings of executives and business leaders are readily available across marketing collaterals, social media channels, and more. Attackers could coordinate deepfakes from these properties as a strategic follow-on to phishing attempts (which will also move away from email to other platforms like chat and collaboration apps) to make manipulated communications feel even more authentic.

For example, phishing emails spoofing IT asking for passwords are common. Attackers could also use manipulated videos of executive leaders on social channels to entice customers, employees, partners and more to click on malicious links – creating broader new attack avenues for malicious actors.

Safeguarding customers & employees: We at CyberArk have adopted various tools and processes which allow employees to shift from working in designated office spaces to remote work seamlessly. We collaborate with our colleagues across the globe in different time zones and different physical locations to ensure that the best talent is available to work with our customers using various workspace collaboration tools, from Slack to Teams to Webex. Our end devices are secured using combinations of security tools, including Endpoint Privilege Manager (EPM) which allows our employee to work effectively from any location around the globe. Our helpdesk team works round the clock to support our global employees.

"F5 ENABLES ORGANIZATIONS TO SECURE AND DELIVER SUPERIOR DIGITAL EXPERIENCES"

Santosh Matam
Security Manager, F5 Networks

Measures adopted: Traditional perimeter security depended on firewalls, VPNs, and web gateways that separate trusted from untrusted users are blurred. Protection is now needed where applications and data, and users and devices, are located. As work from home continues, implementing a Zero Trust approach should be the priority for CISOs, their security teams, and users. We are fortunate that there are devices accessible today to shift to remote work seamlessly. With a robust application security portfolio and ability to secure the new control points in a Zero Trust environment, F5 provides the building blocks necessary to address a "Never trust, always verify" approach to securing today's applications, and also adds a third principle to Zero Trust, "Continuously monitor".

Mitigating threat situation: Ransomware continues to be the prevailing form of malware used by attackers for illicit gain and to cause disruption. According to the F5 Labs recent Phishing and Fraud Report 2020, phishing continues to be a popular enabler of ransomware and nearly 72% of phishing links send victims to HTTPS encrypted websites. A common security hole—and one that is easy to close—is weak authentication on Internet-linked logins. Locking down Internet-linked logins with better authentication is the first step organizations should take to protect against ransomware, ideally using multi-factor authentication. If you can't manage that, then at least make sure default passwords and known leaked credentials are changed.

Another common entry point for ransomware is a drive-by download, where attackers will trap websites with browser exploits that inject their ransomware. This means a user surfing a site and viewing a weaponized banner ad can unwittingly land ransomware on their network. These attacks typically leverage one of the much vulnerability in web browsers, web scripting languages, and web animation tools.

Safeguarding customers & employees: Phishing is a growing problem as an unprecedented number of unaware and unprotected users and devices are connected. The 2020 Phishing and Fraud Report found a 15% annual increase in phishing attacks in 2020 as well as an increase in phishing domains using HTTPS and sophisticated URLs.

An organization may have employees working from around the globe. Because of this, old access security measures are no longer enough and must be replaced with safeguards that allow employees and other verified users safe and secure access from anywhere, on any device, at any time. F5 enables organizations to secure and deliver superior digital experiences. For organizations adopting Zero Trust architecture, F5 BIG-IP APM delivers the industry's most scalable access management solution, APM consolidates remote access, web access management, and Identity Aware Proxy (which helps drive Zero Trust Application Access), enabling organizations to enable the formation of a secure application access that their organization and users require.

MANAGEENGINE BE ABREAST OF LATEST SECURITY ATTACKS AND MITIGATION STRATEGIES

Ananthakrishnan Vaidyanathan
Product Manager, ManageEngine

Measures adopted: For employees, it is imperative they provide full visibility into their work-from-home setup for easier implementation of adequate safety measures to ensure corporate data is always accessed through authorized devices on secure networks.

For customers, the best option is to be alert. If there's even an inkling of doubt about the legitimacy of files or links, it is always safe to refrain from clicking or opening them to prevent falling victim to phishing attacks. Another option is to ensure you update enterprise software only from the product website to avoid installing malicious updates.

Educating customers & employees: As a company dealing with cybersecurity products, we, at ManageEngine, organize regular training webinars and online meetups to ensure all our customers understand the current security environment and how to best utilize the products at hand to ensure optimal security. We also regularly share checklists and questionnaires for customers to periodically check on their setup and be abreast of the latest security attacks and mitigation strategies.

Mitigating threat situation: ManageEngine's dedicated suite of endpoint security and management products lets you manage different servers, workstations, smartphones, and other types of endpoints running different OSes, all from a centralized console. It lets you authorize entities such as endpoints, apps, peripheral devices or even the employees themselves before accessing enterprise data thereby protecting enterprise data at rest, in use, and in transit.

Safeguarding customers & employees: We, at ManageEngine, have been constantly striving to come up with products that cater to the advancing security needs of enterprise, and 2021 will represent yet another step in that direction just like the last year. In 2020, we launched a suite of products that provide UEBA capabilities for threat analytics, enforce the principle of least privileges (POLP) as well as products that grant just-in-time privilege elevation to ensure a secure Zero-Trust setup. One of our core commitments this year is to bring in AI and ML into our entire suite of solutions to build security models that proactively identify attacks and recognize underlying user actions before mitigating them.

"CYBERSECURITY AWARENESS FOR OUR CUSTOMERS AND PARTNERS IS ONE OF THE KEY FOCUS AREAS FOR SOPHOS"

Sunil Sharma
Managing Director Sales, Sophos India & SAARC

Measures adopted: As many companies are adopting WFH as a permanent company policy or even the adoption of hybrid working solutions, this shift has certainly caused some critical challenges for businesses in terms of cybersecurity. Some of the protective measures we recommend are:

Ensure devices and systems are fully protected and security solutions are up to date with the latest patches and versions. All too often malware breaches an organisation's defenses via an unpatched or unprotected device.

Create a secure connection back to the office using a Virtual Private Network (VPN) ensures that all the data transferred between the home user and the office network is encrypted and protected in transit.

Scan and secure email and establish healthy practice

Home working has led to a big increase in email as people can no longer speak to colleagues in person. The crooks are wise to this and are already using phishing emails to entice users to click on malicious links. Ensure email protection is up-to-date and raise awareness of phishing.

Enable web filtering

Applying web filtering rules on devices will ensure that users can only access content appropriate for 'work' while protecting them from malicious websites.

Make sure people have a way to report security issues

With home working people can't walk over to the IT team if they have an issue. Give people a quick and easy way to report security issues.

Educating customers & employees: We have a dedicated tool-Sophos Phish Threat that provides phishing attack simulation and training for end users. It helps our customers to nurture a culture of positive security awareness. Effective security training is also a part of Sophos Phish Threat, available through Sophos Central, which is a cloud-based management platform. Additionally, our customers can take advantage of more than 30 security awareness training modules, covering both security and compliance topics. Sophos Phish Threat integrates testing and training into simple, easy-to-use campaigns that provide automated on-the-spot training to employees as necessary.

Upcoming threat: Sophos Intercept X combines ransomware protection, deep learning malware detection, exploit prevention, End Point Detection and Response (EDR) - all in a single solution. Sophos' synchronized security strategy enables multiple security products to work together seamlessly with simpler management and better security. It allows Sophos endpoint (Intercept X) and firewall (XG firewall) to share threat intelligence, and provide faster comprehensive protection against advanced threats like ransomware.

Safeguarding customers & employees: Sophos has always been prepared for the reality of a remote workforce. Additionally, our Sophos partners can easily provide cybersecurity solutions and services to their customers, by using the many options from our portfolio that secure the current fluctuating protocols around remote working such as in Sophos' RED (Remote Ethernet Devices), VPNs (IPSEC and SSL), virtual firewalls, and synchronized security.

MAINTAINING GOOD PASSWORDS AND PASSPHRASES IS MANTRA OF CYBER SAFETY

Sandeep Bhargava
Managing Director APJ, Rackspace Technology

Measures adopted: Threat actors can be disastrous to an individual or organization, and it is the job of security professionals to ensure that proper security measures are in place to protect against it. For example, it is a good idea to ensure that the business has backups of its critical data so that an attack does not immobilize the organization for an extended period.

Things to be kept in mind to safeguard remote workforce: Use firewall protection solutions: Firewall solutions can leverage a single-pass architecture designed to prevent network vulnerabilities, block the download of known malware, and prevent malicious encrypted content from circulating around your network.

Back up the data. Maintaining recent backups of your data is essential. Companies that follow this fundamental best practice can safely ignore ransom demands and revert to stored files with little data loss.

Keep up with patches and check your security software. Merely keeping up with the latest patches for Windows, Mac, and Linux operating systems and your third-party applications will go a long way to reducing your exposure to ransomware.

Be sure that the security software installed and that it's up-to-date. New malware surfaces every day, so keeping current with your anti-virus software helps keep your data safe.

Educate staff to spot scams. Employee awareness is crucial in avoiding a ransomware attack. Staff should be coached on how to spot scams and urged to take the time to pause and check emails that don't look right.

Take the "Security First" approach. Weave security awareness and practice into the process from beginning to end. DevSecOps is a concept that emphasizes the importance of integrating security into all parts of IT system development and operations, rather than leaving them disconnected. While perfect security is not possible, concepts like this bring it closer.

Educating customers & employees: At the onset of COVID-19 and the shift to Work from Home one of our key priorities was ensuring that an open line of communication was established between Rackspace Technology and our customers. In fact, we looked to over communicate in order to ensure customers knew how and who to reach out to during this time. Over this last year we've looked to educate and support our customers, including setting up roundtables on security with global experts available to answer questions and give advice, we've ensure customers know who to reach out to in our customer success team in order to guide innovation and secure infrastructure from possible attacks.

Safeguarding the customers and employees: One of the most important ways to safeguard customers and employees is to put in place policies to guide staff to better help them understand their responsibilities and what is acceptable when they use or share data, emails, internet sites and additional computers and devices. It's important to make sure the staffs knows about the threats they can face and the role they play in keeping the business safe. All should know how to maintaining good passwords and passphrases, how to identify and avoid cyber threats, what to do when they encounter a cyber threat and, importantly, how to report a cyber threat.

"MCAFEE WORKS TOWARDS PROTECTING EVERY ASPECT OF A CUSTOMERS' DIGITAL EXPERIENCE"

Vamsi Ponnekanti
Head of Technical Sales, India & SAARC, McAfee

Safeguarding customers & employees: McAfee works towards protecting every aspect of a customers' digital experience - from device to the cloud. The company is responsible for protecting over 680 million+ total endpoints and provide security solutions to over 97 million enterprise endpoints, which include 75% of the world's Fortune 500 firms.

For employees, McAfee's robust set of SaaS applications provide a secure environment to work remotely and get work done with ease. Together, we are working on developing stronger defences to ensure that the 'future of work' is a secure one.

Educating customers & employees: Implementing a cloud-based secure web gateway so corporate devices can be protected against web- based threats without routing through VPN.

Allowing employees to connect to sanctioned cloud services from their corporate devices without using their VPN, protecting data with a cloud access security broker (CASB).

Setting policy in your CASB so that cloud services have device checks, data controls, and are protected against attackers who can access SaaS accounts over the internet.

Implementing multi-factor authentication for sanctioned cloud services where applicable to reduce the risk of stolen credentials being used to access accounts.

Letting employees use their personal devices to access corporate SaaS applications to maintain productivity, with conditional access to sensitive data in the cloud.

Upcoming threat: While deepfakes technology is at a relatively nascent stage in India, considering its quick proliferation, it is essential to develop guidelines and regulations to curbits rampant misuse. Effective monitoring and punishable laws for such offences will be crucial in controlling this menace before it causes irreversible damage. Until then, it is up us as consumers to remain resilient, cautious to defend ourselves from the dark world of deepfakes.

"RISK-BASED VULNERABILITY MANAGEMENT (RBVM)- THE PROCESS OF REDUCING VULNERABILITIES ACROSS AN ORGANIZATION'S ATTACK SURFACE"

Kartik Shahani
Country Manager, Tenable India

Educating customers & employees: Employee awareness regarding the importance of multifactor authentication, software updates including patches, and awareness of phishing and other tactics used by bad actors to access networks is foundational and should not be underestimated.

However, the onus of ensuring the security of a business lies with the organization. With employees working from home and using personal and work devices - each device, each asset in the infrastructure needs to be considered as potentially becoming rogue. Therefore security teams need to continue to minimize privileges where necessary and the attack surface to which they have access.

A lot of the issues organizations are facing are simple foundational things that they're not doing well such as patching. By and large, the MO for most cybercriminals — whether they be rogue actors or state-sponsored — is the path of least resistance: they're getting in through known but unpatched vulnerabilities. Security teams within organizations need to get the basics right, address vulnerability patching diligently and implement the right security controls.

Mitigating threat situation: To avoid falling victim to ransomware, organizations need to implement security awareness training and a risk-based vulnerability management program. Security awareness training can help thwart the threats posed by malicious spam and phishing attacks. When it comes to vulnerabilities, it is crucial to observe that with the number of vulnerability disclosures constantly climbing, keeping on top of them can seem insurmountable.

Risk-based vulnerability management (RBVM) is the process of reducing vulnerabilities across an organization's attack surface by prioritizing remediation efforts based on risk. Put simple, RBVM is about understanding vulnerability risk in the context of threat and business impact. By focusing on the vulnerabilities that are both dangerous and likely to be exploited, organizations can make the best use of their resources and increase the return on their risk management investments.

Safeguarding customers & employees: Most remote workers have a variety of connected devices such as smart television sets, doorbells, baby monitors and more in their homes in addition to their laptops and tablets. This means that every time a remote employee logs into their laptop, each of those devices becomes part of the enterprise attack surface. Since security teams won't be able to run network vulnerability scans of personal devices, installing local vulnerability detection agents to provide off-network visibility is beneficial. Risk can also be mitigated by adding IT systems management onto laptops so that the security team can control software updates and patching. This is a simple, but effective strategy.

VARs ARE GEARED UP TO TAKE CYBER SECURITY AS AN OPPORTUNITY

After the unprecedented time of lockdown and the beginning of the new normal, businesses all over the world are facing newer challenges. The year 2020 has seen a surge in crimes and growing in 2021 as well. One of these is the danger of the Deep Fake technology, which can be used to make users believe something is real when it is not. This poses a major threat to businesses across the globe as it can be used to deceive people online. Deepfakes will also likely increase extortion attempts against influential business leaders. It also has significant potential to enhance market manipulation attacks in addition to scams and direct impersonation. On this backdrop, industry leaders have shared their views.

"TO HAVE STRONG FIRST LINE OF DEFENCE, EMPLOYEES AND ASSOCIATES NEEDED TO EDUCATE"

VIBHORE SHRIVASTAVA
MD, VIBS Infosol

To keep customers safe: We realise, apparently, customers have started discussing of security at first. Our enterprise customers were earlier more concerned about perimeter security and basic endpoint management solutions, however, with the sudden rise in cyber threats and different attack patterns, they are now looking for endpoint threat management suite, including anti-malware, anti-Ransomware, EDR, MDR, APT, encryption, anti-phishing, APT, Email Security and many more.

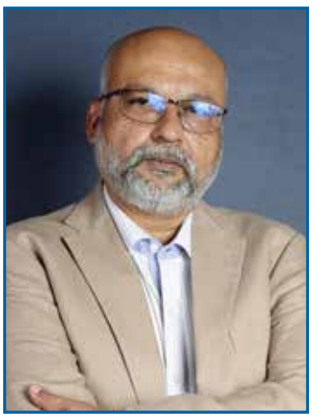
Thanks to all our customers who engaged us at the initial phase and treated VIBS as their trusted advisor in difficult times. Our solid inputs are real value to them to manage major cyber threats and malicious acts during work from home / work from anywhere.

On educating customers: We all have great expectations from 2021 since last year was full of struggle for most of the businesses. However, this year, with hope there are more serious threats associated. There are multiple ways to address and build a strong secured environment. Most importantly, out of all, is to manage and control our internal threats. Report claims, major setback happens due to lack of awareness and negligence by internal team. To have a strong first line of defence, we need to educate our team, employees and associates.

Safeguarding the customers and employees: In 2021, Cyber security trends flow majorly towards Endpoint management suite, Network optimisation, Email protection and secured cloud practices. We were the early technology adapters & Solution partner to bring immediate protection for unknown threats to our large enterprise customers. We had arranged many interactive knowledge sharing sessions with customers & our own employees to enhance their learning curves and to ensure the ability to serve in critical times for unknown threats.

'STRAIGHTFORWARD METHODOLOGY CAN HELP TO PREPARE FOR THE IMPACT OF MALICIOUS ATTACKS'

PRASHANT JAIN
CEO, JNR Management Resources



The upcoming threat: To help define an adequate response to the growing deep fake threat, we in our organization have brought together our security experts and team. By doing this we have designed a straightforward methodology that you can implement to help prepare for the impact of malicious deep fake attacks. This methodology is based on three pillars:

- **Employee training & awareness:** By offering proper training to the employees and increasing awareness employees can be turned into an additional line of defense.
- **Detection:** Detecting the fraudulent media beforehand can minimize the risk to the organization.
- **Response strategy:** We are making our organization ready to adequately respond to the deep fakes.

Safeguarding the Customers and Employees: As most employees work remotely, we educate our employees on key cyber risks and arrange training sessions so that they can learn how to spot threats and be an effective line of defense for their organization.

With advancements in technologies like Cryptography HSM, SSL Certificate, Encryption, & Digital Signature we can be assured that we are keeping our data and our clients/users' data safe & secured.

To keep customers safe: With advancements in technologies like Cryptography HSM, SSL Certificate, Encryption, & Digital Signature we can be assured that we are keeping our clients/users' data safe & secured.

'EVERY ORGANIZATIONAL EMPLOYEE SHOULD BE MADE AWARE OF THE EMERGING THREATS VECTORS'

V.ANAND
CEO, Raksha Technologies

To keep customers safe: The current situation has increased the number of teleworkers to multifold than what organizations have factored for. We have also seen a rise in the number of security breaches. Organizations must relook into their infrastructure, invest in tools of new age that ensure secure connectivity to access public & organization resources and manage every endpoint connecting the organization. Organization should ensure visibility into the security incidents which can be prioritized & remediated. Customers should also conduct periodic training to all employees on security awareness as end user ignorance on cyber hygiene is the major contributor to security breaches.

The upcoming threat: An emerging threat in cybersecurity space, Deepfake that uses the artificial intelligence to recreate fake data. Though it is said to be still emerging, the estimate of the impact looks high. Every organizational employee should be made aware of the emerging threats vectors, enforce a data policy to make sure data is available to the right people only & detection mechanisms are fine tuned to detect and prevent any data exfiltration.

Safeguarding the customers and employees: Being a trusted security partner, we keep our customers aware of the market trends, best practices, threat information, tools that customers could leverage to detect, contain, remediate & reinforce security of their infrastructure & sensitive data. We also extend our wide range of consulting, implementation, managed services that helps customers to bridge the skill gaps. We ensure the best of our services are delivered at all times.

"OUR ENDEAVOUR IS TO SAFEGUARD IT SYSTEMS FROM CYBER-ATTACK AND TAKE IMPERATIVE STEPS"

VIPUL DATTA
CEO, FutureSoft Solutions

To keep customers safe: FSPL has always been customer centric and proactive in educating and keeping our customers informed about various checks adherence whilst moving from work from home to work from anywhere.

We are in regular touch with our customers and man-oeuvre our discussion on investing in solid technical infrastructure that will support their legacy and modern applications, their investments into identity and access management, in the cloud, in modernizing their network architectures and maintaining Security standards and solutions for more secure remote work in the longer term on connections and devices, operations and access and while co-ordinating internally and externally.

Safeguarding the customers and employees: As our customers and employees work remotely, our endeavour is to safeguard their IT systems from cyber attack and take imperative steps to protect them against cyber risks namely;

1. Assess core IT infrastructure regularly
2. Secure applications and devices
3. Embed cybersecurity into business continuity plans
4. Update access and security measures in short intervals

The upcoming threat: Deep fake is a combo of Deep learning and AI based technology, "Fake" which is used to alter images, audio, video etc.

With the world more connected by digital media and the costs for creating deep fakes slumping dramatically, this emerging technology can pose a serious risk. As workplaces have become virtual, due to Covid19, video conferencing and other digital tools pose a threat and an opportunity to be deceived.

At FSPL, we explore the benefits and risks of new technologies by applying a multi-disciplinary lens. We focus on preparing, protecting, detecting, responding and recovering all points of the security lifecycle and define a response in line to the threat. We are also prompt in preparing employee training and awareness, detecting false media at an early stage can mitigate the risk and adequately respond to such issues proactively.

"IT IS ENSURED A SUITABLE ENDPOINT SECURITY IS INSTALLED AND MONITORED FOR TIMELY UPDATES"

VIJAYAKUMAR V
COO, Symmetrix
Computer Systems

To keep customers safe: Depending on the affordability, sensitivity of data and to have good control over the computing devices, it is highly recommended to connect thro VPN. Wherever the affordability is an issue, we ensured a suitable endpoint security is installed and monitored for timely updates are happening. Data backup schedule are implemented to synchronize the data on the cloud. In a nutshell, safeguard each computing device with suitable endpoint security, use VPN for safer connectivity and practice regular backup processes.

On educating customers: We regularly meet our customers, explaining to them the risk of an un-secured IT environment at home, specifically due to the pandemic situation. The organizations are understanding the importance of Data & network Security and most of them have implemented the required data & network security.

Safeguarding the customers and employees: We handle data & network security in two angles: Protecting the data / network with required security practices implemented and reliable data backup solution. Choose & use suitable DLP software, monitor the activities and timely action for any issue is noticed. Human errors continue to exist and cyber criminals will look for the opportunities to take the advantage of the situation. There are plenty of data protection / backup solutions available in the market. Proper data backup process will ensure timely recovery of the system and to put the user back in action with minimum loss of time.

'GOOD GOVERNANCE IS ESSENTIAL FOR MANAGING CYBERSECURITY ISSUES'

MANOJ KANODIA
CEO, Inspira Enterprise

To keep customers safe: The WFH has increased the threat vector for the hackers and made it a bit easier for them to penetrate into an organisation's network as we are aware that the employees are one of the weak links in the chain.

The key mitigation strategy is not technology alone. With whatever technology investment an organisation plans and invests in, it will not be successful until the organisation has a strong foundation of cybersecurity aware employees.

On educating customers: Building resilience and mitigating risk are critical in the current climate. Considering the future of work involves making informed decisions about safety, legal liabilities, and potential threats to both capital and employees.

Some practices that we have been focusing on, not just for our clients, but even internally are:

The upcoming threat: Deep-fake technology can create such realistic-looking content that represents an unprecedented development in the ecosystem of disinformation. The content produced by deep fakes seems so real that the viewers are induced to trust it and share it on social networks thus hastening the spread of disinformation. This can tarnish a company's reputation.

Deepfakes will provide an unprecedented means of impersonating individuals, contributing to fraud that will target individuals in traditionally 'secure' contexts, such as phone calls and video conferences. This could see the creation of highly realistic synthetic voice audio of a CEO requesting the transfer of certain assets, or the synthetic impersonation of a client over Skype, asking for sensitive details on a project.

"TO SET UP TWO-FACTOR AUTHENTICATION IS ONE OF THE BEST PRACTICES SUGGESTED TO CLIENTS"

DHIRENDRA KHANDELWAL
MD, E Square System & Technologies

To keep customers safe: Technology is the great enabler allowing large numbers of people to work from home during the coronavirus pandemic and also in the coming future it is enabling a work-from-anywhere environment. Although working from home permits a business to keep working, it brings huge security risks, setting a more prominent need to keep up compliance with significant data security necessities.

Organizations need to guarantee that their information is protected and resilient outside the security of the work environment. We always suggest our customers maintain the security of company data, as it is the responsibility of both the organization and their employees to maintain appropriate security. The best practices we suggest to our clients is to set up two-factor authentication, preconfigure work-from-home arrangements, regularly back up data, control access to VPNs, if possible, use of company laptop for remote work, and educating the organization on phishing scams.

On educating customers: Remote working today has become a norm for enterprises to manage remote teams and for individuals to work as a full-time remote employee. The foremost task we recommend to our customers is planning with each functional team through collaboration tools and solving any issues they face. With efficient communication, clients can support their team's productivity, creativity, and build better security practices. We act as security advisors for our customers guiding strategy, processes, and technologies to better protect the organization.

Moving ahead we help building guidelines on how to handle private data, clarifying their accountability, and full transparency on how the data is handled. By collaboration with vendors and OEMs, we are ensuring that all devices implemented with the client are secured by design, which doesn't compromise personal privacy and security.

Safeguarding the customers and employees: In the current business environment, the cumulative depth and volume of private and corporate data has made it a rewarding target for cyber crooks and sabotages. The increase in remote work demands improvement in the cybersecurity infrastructure and assesses what people will need to work safely and be able to securely sign-in to corporate systems.

After evaluating the data security scenario in 2021 for data security, we identified initiatives across these security verticals are essential such as security operations, cyber risk & cyber intelligence, data loss & fraud prevention, security architecture, identity & access management, program management, investigations, and Governance policies. We have taken instant steps in curbing these vulnerabilities and to evaluate & rethink how to oversee the business and protect the assets and data both for our organization and clients.

'ONE HAS TO BE ALERT AS CYBER SCAMSTERS ARE ALWAYS A STEP AHEAD'

JITEN MEHTA
Director, Magnamious Systems

On educating customers: We have started educating the customer rather this has been by their business division only and now the security demands are coming from business and not from IT. This is a major shift.

Robust product and solutions: There is no solution which is robust. You need to keep monitoring and fine tune the products and keep adding the new features or develop the same. Most important is the end-users need to be alert and get them trained to keep the system robust.

Safeguarding the customers and employees: A; Educating the users/Business heads/IT Team. Also suggest proactive approach like MTR, a managed threat response so that threats can be managed at beforehand only.

PRODUCT OF THE MONTH

Toggle between Two Computers With 2-port USB HDMI KVM Switch

Setting up a business is the most tedious job. And as a part of your profile, you may need two or sometimes three computers at your workstation. So, what would be your action plan? Set up two monitors, two mice, and two keyboards? Wouldn't that lead to an obnoxious investment that might take years to recover?

The same situation may arise if you are a gaming enthusiast. Too many devices would hog all your space and money. What if you get a simple remedy to this mess and a chance to save enormous capital? For that, you must smartly invest in Cadyce's 2 Port HDMI USB KVM Switch (CA-HDK200). CA-HDK200 controls two independent computers having HDMI port with one set of mouse, keyboard, and monitor. It comes with two fixed cables of USB, HDMI, and Audio/Mic Combo that is 1.2 meters long.

Isn't that the best-suited device for saving capital? But, before we delve into the features of CA-HDK200; let's try and understand what a KVM switch is all about!

WHAT IS A KVM SWITCH?

The term KVM stands for 'keyboard, video (monitor), and mouse.' The most pivotal feature of the KVM switch is that it ably controls multiple computers or servers using a single set of peripheral also called a console. It comprises of keyboard, mouse, monitor, speakers/microphones.

With a KVM switch by your side, you save a fortune on hardware estimates.

A 2-port USB HDMI KVM switch boasts a box-like design. The machines including the audio jack are connected to the switch and the switch further is connected to the keyboard, monitor, speaker/mic, and mouse. Besides, a KVM switch is equipped with a plethora of benefits. So, let's explore more about them!

BENEFITS OF USING A 2-PORT USB HDMI CABLE KVM

- Access is way too easier with a 2-port USB HDMI cable KVM switch. You don't have to run around to different corners managing your computers. If they are attached to a switch then handle them effortlessly using one set of keyboard, mouse, and monitor.
- The switching process is comparatively fast, and one doesn't experience any lag while handling the peripherals.
- Too many wires hanging around the desk is a bit discouraging. However, with a 2-port USB HDMI KVM switch by your side, you can declutter your workspace. With this, bid adieu, to messy wires.
- Set of two peripherals each is going to eat up your space. Instead, imagine having one set of each to manage two CPUs; isn't it eye-pleasing? You will be subjected to enormous space. And that's possible with a KVM switch. With waiving off multiple peripherals, your cost will come down to a minimum. And that's the main highlight of using a 2-port USB HDMI cable KVM switch.

Now we have explored the basics of a KVM switch. Now let's see what our product CA-HDK200 has to offer!

WHY 2-PORT USB HDMI KVM SWITCH – CA-HDK200 IS A MUST-BUY?

- **Enthralling display standards**

Working for hours on two displays can be tiresome for the eyes, especially if you have a poor quality display. So, CA-HDK200 is equipped with a rich resolution of 3840 x 2160 i.e. 4K display. And a 4K display is far richer than full HD. The picture quality is so crystal clear that it will leave you awe-struck. Besides, HDMI 2.0 compatibility makes CA-HDK200 an irresistible buy.

With HDMI 2.0 compatibility, one can experience a bandwidth of 18Gbps. Thus, with higher resolution, the data transfer is also augmented.

- **Accessibility at your fingertips**

Wondering how to toggle your computers? Don't worry, because our 2-port USB HDMI KVM switch – CA-HDK200 has got you covered. It comes with a wired QuickSwitch button that helps in switching between the computers with a flip. Thus, enabling you to work on both the consoles simultaneously and handled with one click.

Besides, if you do not wish to use the switch, then there are user-definable hotkeys and universal hotkeys for computer switching. Also, there is an LED light on the port that shows the selected device.

- **Easy switching between OS and audio**

If you think that 2-port USB HDMI KVM switch – CA-HDK200 switches between computers alone, then that's a misconception. It supports efficient switching between two operating systems as well, like Mac and Windows. CA-HDK200 comes with a CD that includes software utilities. As you switch between OS, those utilities get automatically configured depending upon the OS.

Moreover, the audio channels can be either switched simultaneously or independently using the QuickSwitch button or the keyboard hotkeys.

CDS 2021:

BE ACQUAINTED WITH TODAY'S CYBER SECURITY THREATS AND ITS IMPACT

Technology has become an increasingly integral aspect of the workplace and society. From email correspondence and financial transactions, to professional networking and collaborative work documents, businesses rely on technology to be connected at all times and conduct work effectively. However, when these lines of communication are threatened or even compromised, it can have a disastrous effect on the business. All businesses, no matter its size, need to ensure everyone involved in the company is up to date on the latest cyber security threats and the best methods for protecting data.

The 5th edition of Cyber and Data Security Summit 2021 (CDS) witnesses an overwhelming response from the industry leaders. Most of the corporate who are into security say that, security is foundational to everything we do as the Cybercrime damages will cost the world $6 trillion by 2021. The pandemic was a difficult test for the technology leaders and the success based on how they navigated their organisations through changing consumption patterns. In this CDS 2021, we have understood from the crème de la crème from the Industry, Corporate world and the policy makers what will be the trend in the coming year and how the leaders are prioritising things.

In the summit, there were four tracks of Panel Discussion sessions along with a live show case of the probable threat of using VPN (Virtual Private Networks) and the potential risk associated with the growing payments through RTGS. Followed by the Corporate presentation/ FireSide chat with VARINDIA and Experts speech.

The event kick-started with the welcome address by Dr. Deepak Kumar Sahu, Editor-in-chief- VARINDIA. Welcoming everyone, Deepak said, "The outbreak of Covid-19 posed life threatening challenges but our high speed 4G connectivity infrastructure has proved to be India's digital lifeline. Throughout 2020 the whole world worked online, studied online, worked online, received healthcare online, socialized online, played online simply put thrive online."

ENLIGHTENING ON VARIOUS FACTS RELATED TO THE CYBER SECURITY THE INDUSTRY LEADERS SAID:

TECHNOLOGY RELATED CRIMES WILL INCREASE EVERY DAY

LOKNATHBEHRA
IPS, Director General
Police, Government of Kerala

"Hi-tech crimes will increase as our way of living is very intimately connected to technology, whether it is Information Technology or BioTechnology. There will be an increase in the number of crimes which are committed either by using technology or the technical mind. As a police officer, I feel that technology related crimes or information related crimes will increase every day. We have a knowledge management system for training. We even teach the constables and sub-inspectors, who are directly recruited and those people who are sent for institute training."

AS PEOPLE ARE FORCED TO MOVE TO DIGITAL PLATFORMS THE GAP HAS COMPLETELY GONE

ANYESH ROY
IPS- DCP, Cyber Crime- Delhi Police

"The country is evolving in terms of usage of the internet and as well as devices which rely on the internet for communication. The devices gradually metamorphose into smaller things and becoming portable, more accessible on the move plus the number of applications used in these devices have gone manifold. Whatever gap that is remaining, has gone with the lockdown in March 2020. People who are reluctant, they are forced to move to digital platforms and in a way the gap has completely gone. We have actually made a quantum leap towards integrating our society to the digital platforms."

THE SURVIVAL OF THE BUSINESS DEPENDS ON MAINTAINING TRUST

DR. SANJAY BAHL
Director General- CERT

"Accelerating business transformation means accelerating change management strategy which can be defined as accelerating any shift or re-alignment or fundamental change in business operations. This acceleration is required as the business can survive and thrive in an environment, which is throwing new innovation driven opportunities as its response to shifting market demands while navigating the evolving regulatory complexities. The survival of the business is now dependent on maintaining trust in the services that it provides."

IN EVERY 11 SECONDS ONE COMPANY GLOBALLY BECOME VICTIM OF HIGH-TECH CRIME

DR. PAWAN DUGGAL
Expert in cyberlaw and e-commerce law- Supreme Court of India

"The Indian BFSI sector is neither safe nor good zone to be in, as this is now a fertile potential attack target. This shall be attacked by state and non-state actors.Globally, ransomware has become a big menace and challenge. Infact every 11 seconds, one company, anywhere in the world, becomes a victim of this high-tech crime. Government on the other hand has launched an online diploma for Law Enforcement agencies in terms of helping them in assisting in investigation of high-tech crimes"

UP POLICE'S DEDICATED APP HELPING PEOPLE TO FIGHT CYBER CRIMES

PROF. TRIVENI SINGH
IPS, UP POLICE

"Cyber-crime has increased during the pandemic in the fields of social media account, corporate sector, financial sectors and phishing attacks. We are facing an increase rate of child pornography cases in this period. Many people have committed suicide due to bank account fraud cases. There is also a major problem regarding fake accounts in Social media. We have a dedicated app for UP Police where people can lodge an FIR online."

CYBERCRIME IS THE FUTURE OF GEN-NEXT CRIMES

D SIVANANADAN
IPS- Ex Commissioner, Mumbai Police

"Since pandemic as people are jobless, property crime has gone up. Cyber-crime is the most important property crime, as in this crime, one does not have to visit the crime spot. Future crimes will be cyber related.Police is an integral part of society. They have to upgrade themselves- hardware and software. Not only officers, but even constables too have to be trained in cyber usage, and detection and prevention of crime, by using cyber instruments.

ONLINE TRANSACTIONS COME WITH A BIT OF DANGER

DR. HAROLD D'COSTA
CEO- IQSS

"Practically since last one year, there was no work for people, and even if there was any, it was done from home. And hence, the cyber security breaches have gone up exponentially. In today's circumstances and scenario, every bank account holder should question a bank about its cyber security policy, if they are followed by the bank and if they are examined by RBI. The RBI also in 2017 in cyber security practises has laid down specific rules and regulations, which seem good on a piece of paper but when it comes for implementation, it's a big shock. Corporative banks put the onus that nationalist bank is responsible to pay the money to them. This flashed as a heading on a certain channel. This has been in process from their side. Here, the nationalist bank is not at fault, as it has two security practices in place."

DATA HAS BECOME AN INTEGRAL PART OF EVERYONE'S LIFE

RAJSHEKHAR RAJAHARIA
Internet Security Researcher

"These days we see every single person using the internet. Be it farmer, sitting on the border, he talks about cyber security, and his personal data along with other things. These days one's data is vulnerable to cybercrime, or even fraud, hence cyber security is not just important for companies, but for individuals too.

We have to prevent financial data with much precaution as Whatsapp banking etc., are risky. As everything is now coming under eCommerce, as one shall hardly visit the store, he/she shall use the card instead. In that case one has to limit his card. Banks these days give such offer limits, but at times common man generally neglects it and falls victim to these traps."

CYBERSECURITY IS AS IMPORTANT AS PHYSICAL STRENGTH

TRISHNEET ARORA
Founder- TAC Security

"People are unaware about cyber security. They don't believe that their data can be stolen. Not large enterprises, even SME level or MSME level enterprises' data are at risk, as they become easy victims of cybercrime or cyber threat. They are unaware about digital assets that can be hacked, as they are unaware about any digital asset they are holding. Unless organizations are aware about the digital asset they are holding, only then they will be aware of cyber security".

EVERY ORGANIZATION MUST BE PRE-PREPARED FOR THE THREAT ATTACKS

BISWAJIT MOHAPATRA
Partner & Executive Director- Global Hybrid
Cloud Transformation Services- IBM

"Social media is becoming the best platform for the cyber criminals to conduct their criminal activities- be it identifying the data leakage, or phishing or even malware attacks; it is like a breeding ground for most of the hackers or cyber criminals. The first thing any organization has to do is to create a cyber security response intelligence plant- a living document that needs to be constantly, continuously and consistently monitored. Every organization needs to implement a security operation center- that will monitor any vulnerabilities and if any, is taken care of. Also, let's not forget ODR practice- Observe, Dictate & Remediate at a very faster pace. Hi-Tech crime may increase, but if one implements right platforms, right solutions to prevent those, then one can save their organization from big time crises."

4G CONNECTIVITY INFRASTRUCTURE HAS PROVED TO BE INDIA'S DIGITAL LIFELINE

DR. DEEPAK KUMAR SAHU
Editor-in-chief
VARINDIA

"The outbreak of Covid-19 posed life threatening challenges but our high speed 4G connectivity infrastructure has proved to be India's digital lifeline. Throughout 2020 the whole world worked online, studied online, worked online, received healthcare online, socialized online, played online simply put thrive online. I thank all the CIOs', CTO's, CISOs, the digital transformation leaders and the VARs of India for sharing their valuable inputs related to security journey. And I am here to share the vision of VARIndia on how India's digital future looks like. As we step into 4th industrial revolution, India has an opportunity not just to catch up with the leaders but to emerges as a global leader itself. Gone are the days of simple firewalls, antivirus being your sole security measures. From website intrusion, and malware propagation, malicious code, phishing, distribution denial of service attack, website defacements, unauthorized scanning and activities and ransomware data links- all these major threats have shown us the importance of high-tech cyber security measures in 2020. With the growth of a connected eco system upon which the vast majority of businesses rely will continue to face existing and emerging security threats in years to come. But by designing and enforcing a vulnerability management program companies can identify and mitigate these accordingly. The year 2021 is very much significant for all the industries as it is a drone of the digital age. Since everything is happening online and digitally, the need for cyber security is now greater than ever. Therefore, in order to sustain business online, and create a safe workflow, cyber security solutions are of great importance."

SPAM AND PHISHING ATTACKS WILL CONTINUE TO GROW IN 2021

NITIN DUBEY
Senior PreSales Manager,
South Asia- Kaspersky

"In this pandemic time, we have seen cyber threats increasing multi fold and major reasons for that are human error, unpatched vulnerabilities, accessible RDP and weak passwords. When we talk about human errors, without surprises spam and phishing is the number one attack factor. We have seen an increase and the trend will continue in 2021. The pandemic has pushed us to work from home and we have seen a significant increase in RDP attacks in comparison to earlier times. Ransomware is the fourth major attack factor and becoming a serious threat to all the organizations."

INGRAM MICRO HELPS ORGANIZATIONS DEPLOY ROBUST AND RELIABLE SOLUTIONS

NAVNEET SINGH BINDRA
VP & Country Chief Executive,
Ingram Micro India

"Ingram Micro security provides access to leading cyber security OEMs along with a comprehensive set of services that help organizations deploy robust and reliable solutions that are well suited for their needs. Our portfolio of security vendors covers domains such as identity management, threat management, data protection, risk assessment etc. We offer a diverse set of security vendors ranging from industry leaders to innovative ISPs that provide every kind of security that businesses today may need."

DATA AND PEOPLE WITH THEIR EXPERIENCES SHOULD BE SAFEGUARDED WITH SECURITY

SUDEEP DAS
Technical Sales Leader, IBM Security

"I will focus on the two primary aspects that I want to safeguard, first is data and the second is people and their experiences with security. The identity and how they are accessing the data and the applications. These two things are going to sit on the ecosystem of different technologies and different infrastructure. When I put this data security in identity access management in an open security ecosystem and manage the threats against this then we have sort of starting blocks like threat management, data security, identity access management and an open platform where each of these elements can talk to each other and leverage each other's things."

POST LOCKDOWN ENTERPRISES LOOKED AT BUSINESS RESILIENCE AS THE PRIORITY

R. VENKATESH
President, Enterprise Business Group, Redington India

"As you all know we are in a forced lockdown scenario, enterprises had to prioritize business continuity. Work from anywhere and work from home became the model, there was no other option. That is when one level of security evolved and organizations had to think about it and post that slowly things got better. Post lockdown enterprises looked at business resilience as the priority. That is why they had to adopt hybrid cloud, and started moving applications to cloud."

THERE IS AN EXPONENTIAL INCREASE IN THE NUMBER OF ATTACKS

RADHESH WALWADKAR
Manager - Systems Engineering (India & SAARC)- Fortinet

"As an endpoint security customer, you might be coming across various terminologies like next-generation anti-virus, EDR, XDR. There is an exponential increase in the number of attacks which are becoming successful on the endpoint from 3.2 million to 1 billion in a very short period of time. This raises a question about whatever endpoint security mechanism I am using today whether it is really effective or do I need to change that certain endpoint security mechanism."

THE RISE OF CYBER-ATTACK TARGETING THE DATA AND CRITICAL INFRASTRUCTURE OF NATIONS IS UNDENIABLE

MALAY UPADHYAY
Sophos Sales Engineer-Sophos India

"Much has been talked about cyber security and the threat landscape, as we know that the threats are getting more and more sophisticated in nature and on rise than ever before. There is a strong need to automate the defence mechanism. The rise of cyber-attack targeting the data and critical infrastructure of nations is undeniable. With no signs of slowing down from state-sponsored hackers to activists to criminal enterprises groups are leveraging the power of automation to deploy malware with speed and scale given the automated nature of many of the attacks."

CYBER-CRIME IS MARCHING WITH TIME AND SPEED

SUNIL SHARMA
Managing Director(Sales)- Sophos

"If you look at data, cybercrime has increased but today the crime which has increased is where people are targeted. There are sophisticated attacks which are happening to the larger enterprises' data account. There they know what the criminals want to do and at the same time if you look over all in terms of numbers and data, the cybercrime is also marching with at the same time and same speed. It has actually not increased. As people are working from their homes and become more vulnerable, hence the crime is seen more."

THE VALUE OF VISIBILITY COMES FROM INTELLIGENCE

GURUPRAKASHRAYASA
Country Head of Sales- NSS INDIA- Keysight

"The acquisition of Ixia strengthens Keysight's position in Network visibility, network testing and network security as well as the visibility for cloud services in traditional and software defined.

Network visibility is a fancy way to say make it easy for the security and marketing team to find issues which could be critical cyber security threats and fix it. The value of visibility comes from intelligence, not just data but understanding what is happening in the network."

THE FASTER TO DETECT A BREACH; THE LESS THE DAMAGE WILL BE TAKEN

HO YEOW SIN
Technical Lead in Southeast Asia, Hillstone Networks

"Enterprise security has been focusing on prevention. Security defences like firewall, IPS etc are always the parameter of trying to keep the bad guys out. Parameter defences are still useful, but interestingly there are ways to get around the parameter because of technology changes. Needless to say, there are also internal attackers who do not even need to cross a parameter."

INDIAN MARKET WILL BE THE NEXT GROWTH FOR HILLSTONE

WILL RONG
Regional Sales Director, SEA, Hillstone Networks

"Hillstone Networks is funded by industry veterans to deliver innovative proven & effective narrow security solutions to more than 18, 00 customer worldwide, including 4500 enterprises financial and educational organizations, government and service providers.

In 2021 we are really focused on this region especially in Indian markets. We have put a lot of resources including sales and technical team and also our partner in Indian market. I do believe Indian market will be the next growth for our company. I also believe all of you can benefit from Network security solutions."

THE PANEL DISCUSSION SESSIONS WITH THE LEADERS FROM THE BFSI (BANKING, FINANCIAL SERVICES AND INSURANCE SECTOR) WERE VERY INFORMATIONAL AND IMPACTFUL. THE DISCUSSION IN THE BFSI IS IMPORTANT AS THE MAJOR DRIVING FORCE FOR THE GROWTH OF THE IT SECURITY MARKET IN INDIA. THE PANELLISTS SAID:

60-70% ORGANIZATIONS ARE NOT READY TO FACE THE CHALLENGES

KAPIL MEHROTRA
Group CTO- National Capital Management Services

"Nowadays vectors are getting stronger day by day but most of the organizations are not ready with that change. In terms of percentage 60-70% organizations are not ready. This is one of the big risks. The people are not fully aware of it till now. Looking at these two major challenges we have to take care of the right implementation part and look for the right solution."

INDIA NEVER HAD THE CULTURE TO WORK FROM HOME

PAWAN CHAWLA,
CISO-Future Generali India Life Insurance

"Ever since the COVID-19 started, it has changed many things. One, it has changed the way we look at cyber security, secondly the way it does the business, third the way the threat factor used to perform their task. India never had the culture to work from home, with COVID-19 things have changed drastically. Every organisation today has this culture of Work from Home. They have adopted the WFH culture, although they were not ready in the initial few days."

THE PANDEMIC HAS INCREASED THE ATTACKS

MILIND VAREKARM
CIO- Saraswat Bank

"We need to ensure the safety of end customers. So, when we are taking care of the base at the infrastructure level one more challenge remains is to make each and every employee aware about their bank's security perspective. During the pandemic it has been noticed that the attacks have been increased. We also need to ensure that the customers are aware of taking care of their own banking transactions."

CYBER-ATTACKS HAVE NOT COME OUT ALL OF A SUDDEN

DR. SINDHU BHASKAR
Co-Chairman & Founder-EST Group

"We were in the digital world but neglected it from the beginning. We had the computerized environment but did not take full care of all the malwares and attacks. We were trying to be on the expansion mode rather than safeguarding our technologies. But now the focus has come due to the pandemic. The cyber-attacks were present all of these years; it is not that these have come out all of a sudden."

CISOS FILL THE GAP BETWEEN BUSINESS, TECHNOLOGY AND SECURITY

KAPIL MADAAN
CISO- Spark Minda

"Cyber security has continued to take the centre stage. India is the second most ideal country for ransomware. It increased approximately 40-50 % in 2020 compared to last year. It is important that we start taking cyber security seriously. It completely depends on CISO's strategy and preparedness to handle newer security risks, CISOs fill the gap between business, technology and security. We should come with an approach of a single click awareness solution."

THE SECURITY URBANIZATION IS PARAMOUNT OF IMPORTANCE

UPKAR SINGH
Director IT- FIS GLOBAL

"Security for us is basically two-fold, internal and external. It is very critical for any service organization like us. The security has to be built on multiple levels, not only as the batch processing of the code we build. Security urbanization is of paramount importance from the beginning. From physical security, network security or software security or endpoint security is of much more importance."

FUTURE DIGITAL ENTERPRISE WILL ONLY DEPEND ON COMPANIES WITH GOOD DIGITAL FOOTPRINT

PARNA GHOSH
Vice President & Group CIO-UNO Minda Group

"Cyber security challenges are not only impacting the enterprises within their boundaries; it is also impacting the employees or individuals who are working in the enterprises. It is also impacting the individual's devices like mobile phones or laptops and other devices and applications. It is spreading across and covering both the employees and the enterprise. In our organization we are doing a lot of reforms as we have understood one thing, future digital enterprise will only depend on companies who are really good and strong in processes with good digital footprint."

SECURITY SHOULD BE THE PRIME FOCUS NOW

SUBROTO K PANDA
CIO-ANAND & ANAND

"The pandemic has actually helped in development and adopting the security measures. Prior to pandemic our organization was completely offline but it became online all of a sudden. Security should be the prime focus now with enterprises getting into work from anywhere or work from any device and be always available."

THE PRIVACY OF THE USERS AND THE DATA SECURITY SHOULD BE MAINTAINED

RISHI MEHTA
Technology Evangelist- Silicon Valley (USA)

"The one big challenge is how much data should be used. As part of cyber security, you need to protect, but you need to use the data also and those lines have to be drawn somewhere on how you use the customer's data or the company data or the supplier's data. As you build the regulations to protect the privacy of the users and the data security, the way should be that you are not only protecting the assets around the data and the users but at the same time you are not stifling the innovation."

IF A PERSON THINKS HE IS 100% SECURED THEN HE IS REALLY A FOOL

BHARAT B ANAND
Group IT Head & Security- EC Council

"There is nothing called inside in security whether it is physical or cyber. There is no term called full proof security, if a person thinks he is 100% secured then he is really a fool. We always say it is not about if, it is always about when. The concept we should always remember is to keep working, keep testing hypotheses continuously to figure out the gaps and work on them to shore up our fences so that we are better placed."

DIGITALIZATION HAS A SIGNIFICANT IMPACT ON BUSINESS IN TERMS OF TRANSFORMATION

CHANDRA MOULI
CIO & CTO-Sankara Nethalaya

"Looking at my own experience in the financial services industry, I can say we have seen a lot of digital transformation now the way the business is going. Every risk that you see with all the digital initiatives that are coming around is also adding an element of risk. There is a quantum change particularly with all the digital play coming into the picture. Digitalization has a significant impact on business in terms of transformation but equally adding to the issues around another compliance and security particularly."

CYBER SECURITY IS THE KEY COMPONENT FOR ANY BUSINESS

DR. VINEET BANSAL
CIO-Greenpanel Industries

"Cyber security is very important when we talk about the digital transformation which is happening today in all industries, specifically in the manufacturing sector. Cyber security is the key component as we have seen during the Covid time. Most of our resources were working from home and there was a big challenge of managing cyber security."

THE NEXT SESSION FOCUSES ON HOW THE CORPORATE AND VARS ARE GEARED TO OFFER THE SECURITY AND CYBER SECURITY AS THEIR SOLUTION OFFERINGS.

PHARMA BREACHES CAN BE TERMED AS MOST CRITICAL

B. RAJARAMAN
Manager – Technical, Raksha Technologies

"Work from Home was new to many of the organizations, as they have embraced this. Though it is a common term used in the IT landscape, it comes along with challenges. Many IT organizations are struggling to implement the entire compliance requirements. On the other hand, we can see many breaches happening. Pharma breaches can be termed as the critical ones. It is clearly seen though we have security problems, the infrastructure is growing protected, and there are a lot of gaps that every organization has to fill yet. There are a lot of vulnerabilities seen to the known software which are used by the organization to run their day-to-day operations. And these softwares are used in the industry for many years."

The summit continues with the next panel discussion session. In this session we had various take-aways from the Cyber Security consultants, Cyber law makers and the Influencers in the Industry. The topic of the discussion was " Sophisticated cyber criminals adopting Hi-tech cyberattack techniques to target end-users".

CORPORATES HAVE TO BOTHER FOR CYBER SECURITY IN GENERAL

DR.KARNIKA SETH
Founder-Seth Associates

"Data is huge, and data is the new oil. So we are worried about Cyber security not just from the point of view from how we protect just non personal data of people, which could be of businesses- not only their consumers, contacts, but also about the data of their citizens. Corporates need to worry on all fronts- legal, technical and cyberspace in general."

CYBER SECURITY IS NOT JUST AN IT GAME, BUT MUCH DIFFERENT!

ANUJ AGARWAL
Chairman- CybrotechDigiventure

"In terms of Corporate, the threat is from inside and outside- mostly from outside. The risk is mostly the management people are not involving themselves into cyber security and they are leaving it on their IT people as they are good at delivering IT solutions. Cyber security is totally a different ball game."

INSIDE HACKER IS MOST DANGEROUS THAN THE OUTSIDE HACKER

HAROLD D'COSTA
President-Cyber Security Corporation

"There are two types of hackers- Inside hacker and outside hacker. If an inside hacker does not provide any information to an outside entity, then there will be very less element of any unauthorised hacking taking place.As far as outside hackers are concerned, they can commit any attacks like ransomware attack, modifying the part of your folders... But mainly corporate problems are when the inside person provides information to the outside entity for the crime to be taken."

ORGANIZATIONS HAVE TO BE MUCH AWARE ABOUT CYBER SECURITY

SANDEEP SENGUPTA
CEO- ISOAH

"Lack of awareness is the most important point brought into awareness that starts from the top management. Most of the top management are clueless about the risk and the type of control. Thinking from a country point of view, the PSU, power grid, stock market, banks are the biggest vulnerable points as they are still using a lot of back-dated technology. If there is war breaking out, we will be in serious trouble. Because small time hackers etc cannot do much damage, but if the Power sector becomes a victim, it becomes a national security issue."

CYBER SECURITY HAS BECOME A HOT TOPIC THESE DAYS

HARNATH BABU
CIO-KPMG India

"Cyber security is becoming one of the top concerns in most of the organisations as we are dealing with data.With the advancement of technology, the more opportunities (hacking) that have been created, we are making it more vulnerable from a data security point of view."

CYBER SECURITY IS NOT AS EASY AS FEW PEOPLE THINK

SUBHOSHAN MUKHERJEE
Founder-Prime Info Serve

"Any enterprises across the globe are trying to prevent the attack. Attack cannot be prevented. Many breaches across the globe, starting from Equifax to Sony, the moment attack takes place. At this point of time Cyber security is not as easy as few people think. As we are talking of multifactor attack, signature less attack, hence cyber security has to be treated like a family. To handle ransomware attacks, check on every possible threat."

THE NEXT PANEL DISCUSSION WAS ON "BUSINESS RESILIENCE WITH DIGITAL CAPABILITIES IS A BARE NECESSITY FOR VAR'S TO SURVIVE".

PROACTIVENESS IS THE BEST SOLUTION FOR RANSOMWARE

KRISHNARAJ SHARMA
Director &CEO-IVALUE Info Solutions

"Ransomware is a very reactive problem to happen. Proactiveness is the best solution for ransomware. As long as we protect our data, we can minimise the chances of ransomware. Understand first which data is critical to the organization. Attackers very well know what data is critical for the organization. It is important for the organization to identify the critical data before the hacker does. In a large network it is necessary to identify where the critical data is, especially when you have customer data, customer asset data etc, and also identify the people handling it."

RANSOMWARE ATTACK CAN ONLY BE PREVENTED IF ALL SECURITY UNITS ARE TOGETHER

N K MEHTA
M.D.& CEO-Secure Network Solutions

"Ransomware is still coming to traditional channels- like email, web and the end point. According to Verizon Security Reports, 90% is delivered by email. Earlier, the organization used to have a point approach- the best of parameter security or best of the end point from different vendors from different partners.

Today, we need to look at a solution which integrates all various channels into one. One may have parameter security or email security- but if neither of them works together, we are surely opening the doors for smart ransomware attackers to get into the system. But if all the security work together is like a tightly closed unit, with a centralized view, then there is a chance to protect against ransomware attack".

RANSOMWARE IS CERTAINLY ONE OF THE LARGEST THREATS FACED BY CORPORATES

VISHAL BINDRA
CEO-ACPL Systems

"Ransomware is one of the largest threats faced by corporations. The biggest testimony is that added more than 500 thousand endpoints, more than EDR in the last 4 months itself. It is true that endpoint security is not going to be that strong, but with COVID coming in, it has really changed everything.

After doing such a large implementation, we can realize one thing, we are buying tools which will give us a lot of indicators of compromise, what is happening, and they will give us a lot of indications. We are deliberately looking at data coming to us from all of these devices. We have created tools to do that."

RANSOMWARE ATTACKS ARE THESE DAYS HAPPENING CONTINUOUSLY

AJAY BHAYANI
Director-Ambisure Technologies

"Ransomware has been into the picture since decades. And here the most important thing is it is happening relevantly, but what has really changed is the organizations had really prepared themselves to fight against ransomware in the pre COVID scenario where everything was inside their environment.

And that's what has changed. The scenarios to protect oneself from ransomware have completely changed. If one really wants to protect themselves from such scenarios, backup is the way."

TO TAKE THE CHALLENGES ONE SHOULD BE TECHNICALLY EQUIPPED

MANASI SAHA
Founder-Macaws Infotech

"For last 20 years Macaws has been in the cyber security business. I started the journey with network security, went to infrastructure security and now into cyber security.

As per Macaws is concerned, we believe in three things first, we have to take challenges. Secondly, we have to be equipped enough technically and third, customers have to be with me. I rely into innovation and transformation."

RANSOMWARE COMES WITH STAGES TO BE DEALT WITH

RAMANDEEP SINGH
Director-QOS

"The most important thing about Ransomware is the stage it comes to the surface or known to the organisation which is trying to deal with it- that defines with protection scale it should be defined. Every small or big organization is well aware about ransomware. Ransomware is one such problem, and is known in the common man's space. There is protection, prevention solutions available, to commensurate to the risk an organisation has. But it is all about the managed services, the subsequent services layers that have been built by the virtue of the inside team, or by the outsource team or sub contract team."

SECURITY IS A MUCH-SPECIALISED THING

RANJAN CHOPRA
CEO & MD-Team Computers

"During security operations, when close monitoring is being done, expert services are being provided. A massive opportunity has been seen on the application side. As we were running managed services for 24*7 remote operation for a lot of customers, we have now added on security operations as well. I see this as a high growth area. Security is a much-specialised thing. Hence, we use both approaches- build and buy. We build some expertise internally and we will buy and partner with organizations on the panel, so that our customers get the best. Security threats are all over- email, parameter security, application security; all areas are very vulnerable."

NEXT ON THE AGENDA WAS TO PRESENT THE MOST AWAITED AWARDS CEREMONY BASED ON HOW THE CORPORATES HAVE PERFORMED IN VARIOUS CYBER SECURITY SOLUTIONS IN THE INDIAN MARKET.

Award winners in the 5th Cyber Security Summit 2021

Best Identity & Access Management (IAM) solution	IBM India Pvt. Ltd.
Best Next Generation Firewall	Fortinet Technologies India Pvt. Ltd.
Best DLP solution provider	Broadcom India Pvt. Ltd.
Best DDoS protection company	Radware India Pvt. Ltd.
Best cloud security company	Cisco System India Pvt. Ltd.
Best company into malware protection	Sophos Technologies Pvt. Ltd.
Best EDR solutions	Crowdstrike India Pvt. Ltd.
Best company into email security	Checkpoint Software Technologies
Best Internet security	Kaspersky
Best Cyber security company of the year (On Cloud)	Akamai Technologies
Best Cyber security company of the year (On Hybrid)	IBM India Pvt. Ltd.

NEXT WAS THE MOST INTERESTING SESSION ON HOW THE "VIRTUAL PRIVATE NETWORK" (VPN) CAN ALSO BE HACKED.

AREAS OF ATTACKS ARE REDUCED

PRASAD T
CISO- INSTASAFE

"No company can overnight become highly secured. In today's world every company is using VPNs and firewalls to protect their parameter of infrastructure. It is the time to move on from VPN to Zero trust, because VPN technology has evolved over the time and Zero trust makes sure that these infrastructure and elements of it, like devices and applications are completely hidden. Areas of attacks are reduced when it comes to hacking an organization. It is a journey, not an easy game. Sometimes companies take up upto a year. We have to mature; we have to ensure that all our infrastructures are protected. Zero trust is a way to go, is all I would say."

IT IS TIME TO MOVE FROM VPNS TO ZERO TRUST

Next in the Fireside chat was
SANDIP PANDA
Founder- Instasafe

"Through this session the CIOs, CISOs and risk management professionals got an opportunity to understand what are the key vulnerabilities of the existing VPNs and how they could be exploited with readily available scripts on tools. Known vulnerabilities were always there. It is the time to move from VPNs to zero trust."

AI HAS BEEN PARAMOUNT IN BUILDING AUTOMATED SECURITY SYSTEMS

S MOHINI RATNA
Editor-VARINDIA

"With AI being introduced across the industry and most of the sectors are geared for the challenges and opportunities. The technology comes with a combination of machine learning that has brought tremendous changes in cybersecurity. AI has been paramount in building automated security systems, natural language processing, face detection, and automatic threat detection. AI-enabled threat detection systems can predict new attacks and notify admins for any data breach instantly, making it the next cyber security trend in 2021."

"AT SNOWFLAKE WE TAKE SECURITY EXTREMELY SERIOUSLY"

In a chat with VARINDIA, Vimal Venkatram, Country Manager, Snowflake – India talks about the company's fully encrypted storage, its data localization, security issues regarding hybrid or multi-cloud, etc.

DOES THE EXPONENTIAL INCREASE OF VALUE OF DATA CAN LEAD TO SECURITY BREACHES?

From a security standpoint, this is going to be a key focus not only from a Snowflake perspective, but from an overall security perspective as well right. We are seeing that customers are engaging in a lot more spending on cyber resilience and they are also doing a lot of excess spending in emerging technology risk management. From a Snowflake standpoint, we are absolutely secure by design, by providing end to end encryption, our storage is fully encrypted as well. We have strong multi-factor authentication and the profiles of customers who are Snowflake customers are some of the most heavily regulated and sensitive industries like financial services, telecommunications and healthcare. There are customers globally from an Fs standpoint, we have Capital One, Allianz from healthcare, McKesson which is a Fortune 10 company. So we absolutely take security very seriously from a Snowflake standpoint.

INDIA IS WORKING ON ITS OWN DATA PROTECTION LAWS AND IT IS TALKING ABOUT DATA LOCALIZATION. HOW DOES THAT AFFECT YOUR BUSINESS? IF YOU CAN, TALK ABOUT THAT?

In India, we launched in May 2020, on AWS. So from a data localization standpoint, if customers are utilizing the Snowflake for instance, in AWS in Mumbai, they are covered with data localization, because we are present in India today. So we are hosted on the three major public cloud platforms globally, which is AWS, Microsoft Azure, and Google Cloud GCP. This is why we have also seen, increasingly, a lot of focus around sensitive industries, financial services, telecommunications, retail, for example, we can absolutely work with these organizations who have laws where they need to store data locally in India, so Snowflakes are protected on that front.

WOULD YOU LIKE TO DISPEL THE MYTH THAT DATA ON CLOUD IS NOT SAFE OR DATA ON MULTI-CLOUD IS NOT SAFE? WOULD YOU WANT TO DISPEL THAT THREAT MYTH TODAY?

So yes, I would love to dispel that myth. So, data is absolutely secure. When I say data is absolutely secure, Snowflake takes a lot of effort and our solution was built from the ground up to take advantage of the public clouds. We are only available on the public cloud, we see the highest certification levels for security from a Snowflake standpoint, we have an end to end encryption, where the data is in transit or rest, the data is encrypted. We have role-based access control, very strong authentication systems, which multifactor. For example, we are also FedRAMP ready, we meet NIST 800 145. Specifications, SOC type 2, we are PCI DSS compliant as well. Also, we are HIPA compliant for a lot of healthcare customers. So, McKesson is a significant customer for Snowflake. Customers trust their data, to be on us, because of the security and the governance that we built into our system from the grounds up. As we expand our footprint in India, this is a very key conversation with a lot of CEOs, CIOs, analytics officers, and we take the pains to make them understand how secure the data is. There are times where data on the cloud is sometimes even more secure than on-premise systems.

HOW DO YOU ADDRESS THE SECURITY ISSUES WHEN YOU TALK ABOUT THE HYBRID CLOUD OR A MULTI CLOUD?

At Snowflake we take security extremely seriously. We have built our solution around security, some of the most highly regulated and sensitive industries like healthcare, financial services, government, telecommunications, retail, we have reference customers, and each one of these are key verticals globally. Without security, being at the centre of the conversation, we would have never been able to win some good accounts. In any campaign that we go, we work closely with the people in the organization, whether it means we share our certifications we have pretty much as I said earlier, we are HIPAA compliant, SOC type 2, PCI DSS compliant. Snowflake is encrypted end to end when the data is in transit or in flight. There is on top of that role-based access control.

On top of that, we also allow customers to bring your own encryption key, which means if you ever revoke your credentials of an encryption key, the data is basically meaningless to anyone who wants to access that. We also provide a lot of flexibility for customers to ensure that data is absolutely secure.

WHO ARE YOUR COMPETITORS AND HOW DO YOU DIFFERENTIATE WITH THEM?

There is obviously competition in the market. From an architecture standpoint, it is absolutely a key USP of Snowflake - one is we are across the cloud, which means we are available on multi-cloud technologies like AWS, Microsoft Azure, and GCP. We are a true pay as you go model, which means customers only pay for what they use and consume on Snowflake. The unique architecture of Snowflake makes instant availability, scalability, elasticity or reality. Finally, we are a single source of truth, which means it is one common platform, or we have one single source of truth from a data standpoint where customers can load all kinds of data, whether it is structured, semi-structured data, and soon to be announced unstructured data as well in a single platform, which means you are not maintaining different siloed data sets, one for structured data, one for semi-structured data, and then trying to figure out join these two at some level. It is very complex to do that. Snowflake makes it extremely easy. Finally, I have been speaking about the rise of the Data Cloud or how customers can now share data, customers can now monetize their data or ingest data from third parties as well. Customers can securely share data with partners, suppliers can even host it on our data marketplace and potentially even monetize that data.

IBM is considering sale of Watson Health amid cloud focus

IBM is considering a sale of its IBM Watson Health business, the move that would help newly appointed Chief Executive Officer Arvind Krishna focus on faster-growing cloud computing operations.

IBM is exploring a range of alternatives, from a sale to a private equity firm or a merger with a blank-check company. IBM is going to boost its share of revenue from hybrid-cloud software and services, which lets customers store data in private servers and on multiple public clouds.

IBM has been trying to boost its share of revenue from hybrid-cloud software and services, which lets customers store data in private servers and on multiple public clouds, including the rivals Amazon.com Inc. and Microsoft Corp. IBM bought RedHat for $34 billion in 2018 to boost this effort.

Krishna said in October that he would spin off IBM's managed infrastructure services unit into a separate publicly traded company. The division, currently part of the Global Technology Services division, handles day-to-day infrastructure service operations, like managing client data centers and traditional information-technology support for installing, repairing and operating equipment.

While the unit accounts for about a quarter of IBM's sales and staff, it has seen business shrink as customers embraced the shift to the cloud, and many clients delayed infrastructure upgrades during the pandemic. The spinoff is scheduled to be completed by end of 2021.

In 2020 Chennai records over 8 million malware threats

According to news reports, Chennai has recorded more than 8 million malware threats in 2020 as attackers tricked users into opening infected files and links through fake Covid-19 information and fake Aarogya Setu app.

A report published by cybersecurity firm Quick Heal revealed that threat actors targeted users by offering them free data, subscriptions to OTT platforms, fake COVID-19 vaccines and job offers.

Quick Heal said it detected and blocked over 80,000 malware threats every hour while a total of 1.91 million ransomware were detected.

Quick Heal said, "Although consumers are increasingly adopting digital tools, what they might be lacking is knowledge of safe cyber hygiene practices, along with awareness around the evolving threat landscape, and how they can tackle malware attacks".

Himanshu Dubey, Director, Quick Heal Total Security said, "People should follow basic security measures such as avoiding internet banking while using public Wi-Fi, using strong passwords, enabling multi-factor authentication, & changing passwords frequently".

Amongst the malwares, Trojan was the most detected followed by Infector, Worm and Potentially Unwanted Application (PUA). Besides, ransomware continued its dominance by encrypting user data and selling it on the dark web for financial gains.

Thiruvananthapuram to become another smart city by NEC Corporation

Hon'ble Prime Minister Shri Narendra Modi inaugurated the project alongside Hon'ble Chief Minister of Kerala, Shri Pinarayi Vijayan. NEC Corporation India has won the mandate to drive Thiruvananthapuram's Smart City project. As the master system integrator for the city's Integrated Command and Control Centre (ICCC), NEC Corporation India (NEC India) aims to complete the project in 2022.

Thiruvananthapuram is among the 100 smart cities selected in the third round of the smart cities challenge under the Ministry of Housing and Urban Affairs' Smart City Mission. Thiruvananthapuram has incorporated a special purpose vehicle (SPV) – Smart City Thiruvananthapuram Limited (SCTL) to plan, design, implement, coordinate and monitor the smart city projects in the city.

NEC will help SCTL to create the ICCC to bring various departments together to work as a single unit. It will also help SCTL utilize information technology to modernize key functions of city operations including traffic management, traffic control, traffic law enforcement, security and safety, e-governance, municipal operations, and information dissemination to build well-informed, connected, smart and smooth city-wide operations for citizens of the city.

P Bala Kiran (IAS), CEO, Smart City Thiruvananthapuram Limited said, "We look forward to a fruitful association with the NEC India, which will help in scaling up and uplifting Thiruvananthapuram as a promising business and tourist destination".

Aalok Kumar, President & CEO of NEC Corporation India said, "As an organization that has been at the helm of delivering turnkey projects for the central and state governments, NEC has had the opportunity to work with the state of Kerala in the public safety domain previously. This new project win reflects our commitment to co-creating solutions of the future with the Government who aims to create a seamless and robust city infrastructure. NEC, with our expertise in designing and implementing Smart City projects around the world, will continue to innovate and deliver new solutions that benefit cities and their residents as we navigate the booming digital economy."

NEC will work towards integrating all the smart components at the centralized Command and Control Centre with the integrated operations and dashboard. This Software platform will act as the centralized integration point for various departments under the Smart City ambit. Some of the key highlights of the project besides the ICCC Platform include a One City Mobile App, Sola Scada, E Governance Application Support, Integrated Transit Management, a Smart Parking Management Solution, Environmental Sensor monitoring system and, Smart Water Management.

OPTOMA HOPEFUL ABOUT THE MARKET IN 2021

VIJAY SHARMA
Country Head India, Optoma Corporation

Optoma, a dominant player in the home AV segment world-wide, plans to spread its wings further and is eyeing on interactive flat panel category other than projectors. In DLP (Digital Light Processing) Projection technology, Optoma dominates the market share and is No.1 DLP Projector brand in world.

While talking with VARINDIA, Optoma Head, Vijay Sharma spilled the commercial beans about the company's further plans and much more. Let's take a look at the excerpts from the chat.

Range of products Optoma eyeing for Indian market

Optoma plans to take a high leap further than pro AV sector. It further wishes to emerge as a strong player in Indian market.

"We have a wide range of products for education and pro AV sector thanks to Coretronics, our parent company. For last one year we have been dominating the home AV segment world-wide. Now with this trend we want to continue, and make sure that we emerge strong with our home AV product line up in India. Other than projectors, we see huge opportunity in the interactive flat panel category and that is something we are going to introduce in first half of 2021. Going forward, we will focus on projectors and interactive flat panels this year," says Vijay.

GTM strategy

A 'go to market strategy' aka GTM strategy varies for different market segment. For education segment the approach is much different from home segment.

"The strategy varies from vertical to vertical. For example, our home segment is very specific to customers or the partners who have the experience zones. Whereas the education segment has a different approach where we have the model of our national distributor then the regional distributor and then the educational system integrator across India. And if we talk about the new product line-up which is the interactive flat panel then it is a B2B product line-up which goes from the national distributor to the customers directly, without any regional integration in between," reveals Vijay.

Optoma's USP

USP is a next step towards progress. It makes a brand different from its competition. Optoma believes in brining forth the latest technology in the global market.

"The USP is bringing the latest technology in the world market. We have always been the first movers in the industry by introducing new products. We recently launched a 4K laser TV which is a consumer product integrated with smart features which allows the consumer the flexibility in terms of installation as well as watching content without any external set up. We also have launched industry's first 4k gaming projector, which is a growing segment in India. Optoma has introduced a 240hz refresh rate 4k laser projector in this segment to enhance gaming experience. Optoma is also the leading player in smart features with the Amazon Alexa enabled and Google Assist," explains Vijay.

Channel policies & future of Optoma

The major part of what channel has to do is to make sure that they are able to sell their products, and make money by selling the products. The channel policies are very clear and transparent and they are strict on it and that is one of the reasons that Optoma has taken position as a dominant player in the 4k home segment space.

"We are quite hopeful about the government initiatives in the projectors space, the way they are investing. We are hopeful to see the trend which was there in 2020 in the home segment; it will continue in the 2021 and will grow further. Secondly, the education segment, which was completely shut down in 2020, it will open and grow in 2021 and then the government segment, where the investment is coming through digitization of education, so I am quite hopeful about the market in 2021," concludes Vijay.

21 INDIAN ORIGIN STAR EXECUTIVES LEADING GLOBAL COMPANIES

We are familiar with the names like Google's parent company Alphabet CEO Sundar Pichai or Microsoft CEO Satya Nadella, who are Indian in origin technology leaders leading the two most important technology companies of the world. But apart from these two executives, there are few more India born leaders who with their abilities, capabilities, hard work etc. have reached the pinnacle and made us proud as an Indian with their achievements irrespective of the verticals. Let's take a look at the most important executive leaders who are Indian in origin.

AJAYPAL SINGH BANGA
Executive Chairman, Mastercard

Padma Shri awardee, Ajaypal Singh Banga is an Indian-American business executive. At present he is the Executive Chairman of the Board of Directors of Mastercard. Before this, he served the company as President and CEO. He served as a member of President Obama's Commission on Enhancing National Cybersecurity. He is a past member of the U.S. President's Advisory Committee for Trade Policy and Negotiations. He is a graduate of Delhi University and the Indian Institute of Management, Ahmedabad.

AJIT JAIN
Vice Chairman, Berkshire Hathaway

Ajit Jain, an Indian American executive, is the Vice Chairman of Insurance Operations for Berkshire Hathaway.

He started his career as a salesman in IBM for their data-processing operations in India. He was also associated with McKinsey & Co. In 1986 he joined Berkshire Hathaway. He holds an MBA degree from Harvard University.

AMAN BHUTANI
CEO, GoDaddy

In 2019, Aman Bhutani joined GoDaddy as CEO. Before joining GoDaddy, he served Expedia. He held different senior positions there. Bhutani did his bachelor's degree from Delhi University and MBA from Lancaster University.

ANEEL BHUSRI
co-founder, CEO, Workday

With Dave Duffield, the founder of PeopleSoft, Aneel Bhusri co-founded Workday in 2005. Earlier he held positions at PeopleSoft. He has a bachelor's degree from Brown University and completed his MBA at Stanford University.

ANJALI SUD
CEO, Vimeo

Anjali Sud holds the position of Vimeo's CEO and she has been serving this position since 2017. Vimeo is an open video platform. Prior to this she has worked with Amazon and Time Warner. She holds an MBA from Harvard Business School.

ANIRUDH DEVGAN
President, Cadence Design

In 2018 Anirudh Devgan was appointed as President of Cadence Design. He was also associated with Magma Design Automation and IBM. He has a bachelor's degree from the Indian Institute of Technology, Delhi, and did his master's and PhD from Carnegie Mellon University.

ARVIND KRISHNA
CEO, IBM

Arvind Krishna is associated with IBM for almost 30 years and played several senior-level positions in the company. He became the CEO of the company in 2020. Arvind is an electrical engineer from IIT Kanpur and completed his PhD from the University of Illinois at Urbana-Champaign.

ASHOK VEMURI
Chairman of the Board at OSG Connect

An Indian- American business executive, Ashok Vemuri is Chairman of the Board at OSG Connect. He also holds the position of Board of Director for Financial Policy and Public Responsibilities at Kroger. Prior to this he was associated with IGATE and Conduent as CEO. He has done PGDM from IIM, Ahmedabad.

GEORGE KURIAN
CEO and president, NetApp

George Kurian in the year 2015 takes up the position of CEO and President of NetApp. Before NetApp, he also served companies like Cisco Systems, Akamai Technologies and McKinsey & Company. He holds a bachelor's degree in electrical engineering from Princeton University and went on to receive his MBA from Stanford University.

JAYASHREE ULLAL
president and CEO, Arista Network

Since 2008, Arista Networks has been under the able leadership of Jayshree Ullal. She is the President and CEO of the company. Ullal led the company to IPO on the New York Stock Exchange in 2014. Apart from Arista, she has also served companies like Cisco and AMD. She studied BS in electrical engineering from San Francisco State University and completed her master's in engineering management from Santa Clara University.

LAXMAN NARASIMHAN
CEO, Reckitt Benckiser

Laxman Narasimhan presently assumes the position of CEO at Reckitt Benckiser. Earlier, he was associated with PepsiCo and held various roles. He was previously Global Chief Commercial Officer, with responsibility for R&D, categories, e-commerce, design, go-to-market, global customers and strategy. He holds a degree in Mechanical Engineering from the College of Engineering, Savitribai Phule Pune University and did his MBA in Finance from the Wharton School at the University of Pennsylvania.

NIKESH ARORA
CEO, Palo Alto Networks

In 2018, Nikesh Arora became the CEO of Palo Alto Networks. Before this, he served Google and SoftBank. He has a bachelor's degree from the Institute of Technology at Banaras Hindu University, MBA from Northeastern University, and master's of science from Boston College.

PARAG AGRAWAL
CTO, Twitter

From 2011, Parag Agrawal is positioned as Chief Technology Officer of Twitter. Before joining Twitter, Parag was associated with Microsoft, AT&T and Yahoo's research teams. He holds a bachelor's degree from Indian Institute of Technology, Bombay.

REVATHI ADVAITHI
CEO, Flex

Revathi Advaithi is the CEO of Flex Ltd., an American Singaporean-domiciled multinational electronics contract manufacturer. She became CEO in the year 2019. Earlier, she was associated with Eaton's electrical sector business as the President and COO. She holds a degree from the Birla Institute of Technology and Science, Pilani, and MBA from the Thunderbird School of Global Management.

SAMIR KAPURIA
president, NortonLifeLock

Samir Kapuria holds the position of President at NortonLifeLock. In 2004, he got associated with Symantec and was also head of the company's Cyber Security Services business including its global security operations centers. He has done his bachelor's degree in Finance from the University of Massachusetts.

SATYA NADELLA
CEO, Microsoft

After Steve Ballmer, Satya Nadella became the CEO of Microsoft in February 2014. He started his career with Microsoft in the year 1992 as a developer of Windows NT operating system. He did his engineering at Manipal Institute of Technology and did MS from the University of Wisconsin–Milwaukee, and MBA from the University of Chicago Booth School of Business.

SHANTANU NARAYEN
CEO, Adobe

Shantanu Narayen, the CEO of Adobe joined the company in the year 1998 as the Senior Vice-President of Worldwide Product Research. He took over as COO in the year 2005 and became CEO in 2007. Prior to Adobe, he was associated with Apple and Silicon Graphics. He is a Bachelor of Science from Osmania University, an MBA from the University of California, Berkeley, and an MS from Bowling Green State University.

SIVA SIVARAM
President, Western Digital

Siva Sivaram holds the position of President at Western Digital. Before this, he worked at Intel, Matrix Semiconductors and Sandisk. From 2008 to 2012, he founded and served as CEO of Twin Peaks Technologies. Sivaram received his bachelor's degree from the National Institute of Technology, Triuchi. He did his master's and doctorate degrees from the Rensselaer Polytechnic Institute.

STEVE SANGHI
CEO and chairman, Microchip Technology.

Microchip Technology was founded in 1989 by Steve Sanghi and he assumed the position of CEO in 1991. He was also associated with Intel. Sanghi holds a bachelor's degree from Punjab University and completed his master's in Electrical and Computer Engineering from the University of Massachusetts.

SUNDAR PICHAI
CEO, Alphabet

In 2019, Indian origin techie Sundar Pichai became the CEO of Alphabet Inc., the parent company of Google. He also became the Google head in August 2014. He has served the company for more than 15 years and he spearheaded key businesses like Android, Chrome, Maps, and more. He did his BTech from IIT Kharagpur, MS from Stanford (MS) and MBA from Wharton.

THOMAS KURIAN
CEO, Google Cloud

In 2019, Thomas Kurian assumes the position of Chief Executive Office of Google Cloud. Prior to this, he was associated with Oracle and served the company for 22 years. He led product development as a Member of Oracle's Executive Committee for 13 Years. He also led a 35,000-person software development team in 32 countries; 53 cities; R&D Budget of $4.0 Billion for Oracle. He holds a Bachelor's degree in Electrical Engineering and Computer Science from Princeton University. He also has a master's degree in Business Administration from Stanford University Graduate School of Business.

FOCUS ON VISION OF AATMANIRBHAR BHARAT AND START-UPS

The Union Budget turns out to be an excellent budget but not a transformational budget as was made out to be. It has adopted a brilliant strategy of large scale infrastructure rollout, funded by asset monetization of existing road, power lines, gas pipelines and railway assets.

The budget also covers funding of New Education Policy which is what I have been asking for as it will provide the human resources needed for growth in this decade. Adequate provisions have been made for health, education, agriculture, MSME's and startups. Hope there is removal of GST on digital payments and removal of Angel tax as a followup of the budget.

The Union budget 2021 has brought relief for a lot of industries and is poised to take India to greater heights. For start-ups and entrepreneurs, one key highlight from the budget is the capital gains exemption for one more year to 31 March 2022, and secondly they will be eligible to claim a tax holiday for an additional year. These extensions presented by the Honourable Finance Minister will provide a much-needed post-pandemic boost to the upstarts.

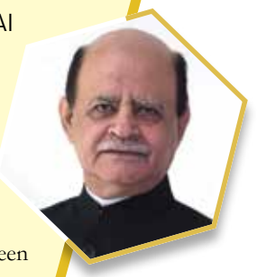
Secondly, increased focus on Innovation and on ease of doing business. This budget appears to have set the right pace for India's journey to a digital first approach. It has brought relief for a lot of industries and is poised to take India to greater heights.

Union Budget lays an increased emphasis on use of data analytics, artificial intelligence and machine learning across industries. Welcoming the Government of India's move in taking definitive steps towards using the power of digital technologies and boosting the fintech and startup ecosystem through initiatives such as fintech hub in Gujarat International Fintech Tec (GIFT). The benefits accrued through the allocation of Rs. 1,500 crores for promoting digital modes of payment as well as the increased tax audit limit for those who carry 95% of their transactions digitally will enable businesses, especially MSMEs to digitise their entire value chain and drive exponential impact on key business levers – innovation, growth and efficiency.

Overall, the budget manages to put up a convincing package to fund the desired goals while providing revenue lines for the same.

BUDGET 2021 TO PUSH ECONOMIC GROWTH POST PANDEMIC AND LEAD TOWARDS ATMANIRBHAR BHARAT

LT. GEN. DR. SP KOCHHAR
DG, COAI



"We welcome the budget as it is pro-investment and pro-growth. It will provide the much-needed impetus to economic growth post the pandemic and will set us on the path to becoming Atmanirbhar Bharat. However, we are a bit disappointed that concerns of the telecom sector, which is the backbone of digital India, remained unaddressed. We were expecting a reduction in the burden of levies, such as LF and SUC on the telecom sector. The Government has also not considered the request of the Industry to exempt the GST from the payment of Government Levies such as LF, SUC and spectrum installments etc. As the telecom operators are going to launch 5G services in the country, it is imperative that 5G enabled telecom equipment are available to them at a reasonable price. Thus, there was the need for a reduction in customs duties on telecom equipment. It would have been a much awaited relief if the government provided the right incentives to the sector."

CP GURNANI
MD & CEO,
Tech Mahindra

"BUDGET 2021 PROMISES TO PROVIDE THE MUCH-NEEDED ECONOMIC VELOCITY TO INDIA'S GROWTH CYCLE"

"This budget is a step in the direction towards Atmanirbharta, clearly providing every opportunity that is required for a sustainable economic momentum and growth. The Finance Minister has provided for ample opportunity to boost and sustain the gig economy, digital payments and research and development taking place within the country. The focus on innovation and R&D (Research & Development) as an important pillar is a critical step in increasing the export income of Indian IT sector. Along with this, the 'Atmanirbhar Bharat' budget also outlines initiatives for gig economy, digital payments, human capital while also setting up fintech hub and National Natural Language Translation Missions. Therefore, with increased allocation towards infrastructure, financial inclusion and healthcare, Budget 2021 promises to provide the much-needed economic velocity to India's growth cycle."

VEHICLE SCRAPPAGE POLICY TO BOOST THE AUTO SECTOR IMPACTED BY THE PANDEMIC

WARREN HARRIS
CEO & MD,
Tata Technologies

"With a significant outlay on Infrastructure spend and the much-needed Vehicle Scrappage policy, the government of India has finally set the tone for recovery of Auto Sector which has been significantly impacted by the pandemic. This will not only help boost the demand for production of Commercial vehicles but also support the entire transportation ecosystem.

Also, while it would have been good to see some more initiatives to promote Electric Vehicles in this budget, we are glad that the government has noted India's critical role in the global automotive supply chain post COVID 19. Specific initiatives through Production linked schemes, creation of infrastructure for R&D and enabling skill development in new-gen technologies such as artificial intelligence (AI) and Machine Learning (ML) will help drive investment in Engineering and Research."

DR. KESHAB PANDA
CEO & MD,
L&T Technology Services

IMPETUS TO MANUFACTURING SECTOR TO PAVE THE WAY FOR ENHANCED ADOPTION OF DIGITAL ENGINEERING CAPABILITIES

"The move to provide greater impetus to India's manufacturing sector with outlay of almost Rs 2 trillion over the next five years is indeed a welcome move. We are hopeful, this will pave the way for enhanced adoption of digital engineering capabilities by domestic players, especially in the Industry 4.0 segment, to give them a global edge. With patents and innovations being at the core of our proposition as a pure-play engineering services provider, it was encouraging to know that Innovation and R&D was classified under the six pillars of focus for this year's union budget. Unlike last year where explicit mention to initiatives such as National Mission on Quantum Computing and Technology were announced, one would have hoped that this year's budget would have made provision for further focus."

GOVERNMENT PROJECTS TO INCREASE THE IMPORTANCE OF SECURITY

RAJESH MAURYA,
Regional Vice President,
India & SAARC, Fortinet

"The budget has announced big-ticket projects to add to the digital capabilities with the next general census in the country being the first digital one and along with marque MCA 21 project this is likely to garner massive 'crown jewel' assets in terms of the sensitivity and quantity of data. As these projects are rolled out it will increase the importance of security as the government builds the tools and workflows supporting these services. These projects will need to prioritize solutions such as Zero Trust Access, automated endpoint security, users awareness training to counter a range of threats, and will also need to ensure that solutions such as software defined networking and multi-cloud services are implemented securely.

The real challenge in securing these digital assets that will continue to be targeted by both criminal and nation state (APT) actors is the availability of skilled resources."

PRAKASH MALLYA

VP and MD – Sales, Marketing and Communications Group, Intel India

"AT INTEL, WE ARE STEADFAST IN OUR COMMITMENT TO PARTNERING WITH THE INDIAN GOVERNMENT ON THIS JOURNEY OF TECHNOLOGY FUELED INNOVATION AND GROWTH"

"At a time of great uncertainty, the first ever paperless Union Budget 2021 stood out for its unremitting focus on economic recovery through higher spending and inclusive growth opportunities. The allocation of Rs. 50,000 crores over the next five years through the National Research Foundation to develop India's potential as a global innovation hub is particularly exciting. This will undoubtedly provide greater impetus to the Indian innovation story and cement our position on the global map of leading economies. At Intel, we are steadfast in our commitment to partnering with the Indian government on this journey of technology fueled innovation and growth. It is evident that the government is banking on India's digital technology foundation to power its revival journey. It is encouraging to see the government's sharpened focus on adoption of cutting edge technologies like Artificial Intelligence and Machine Learning. We are excited to see the future of Indian innovation and economic resurgence unfold over the next few months."

BUDGET 2021 FOCUSES ON 'ATMANIRBHAR' ECOSYSTEM

BALAKRISHNAN ANANTHARAMAN

VP and MD Sales, Nutanix India

"The outlook for innovation from the 2021 budget remains strong, with a lot more focus on making an 'Atmanirbhar' ecosystem. Today tech startup companies have become the backbone for the growth of the country, we are optimistic about the initiatives taken to strengthen India's digital drive and to further amplify the digital economy. The impact of the pandemic has forced sectors that operate traditionally to change their models rapidly to support modern trends. Two-thirds (70%) of the public sector are of the opinion that COVID-19 has caused IT to be viewed more strategically in their organisations, and hence the budgets intention to push for innovation and R&D is one step in the right direction for the tech sector, in establishing a Digital First mindset throughout India."

VIVEK SHARMA

MD - India, Lenovo Data Center Group

BUDGET 2021: A MOVE TOWARDS PRO-GROWTH AND PRO-TECHNOLOGY

"This is a pro-growth, pro-technology budget with a vision to disinvest where required and re-energize infrastructure, healthcare, banking, and agriculture sectors through numerous employment and capital generating reforms.

There is a strong focus on Digital India be it through setting a fintech hub at GIFT city, enhancing digital payments and use of AI, ML etc. in governance, or making tax appellates faceless and tech enabled – all provide a solid foundation for a forward looking data-economy."

"A HISTORIC BUDGET MAKING A MARK OF THE BEGINNING OF A NEW INDIA"

HARI OM RAI

CMD, Lava International

"It is a historic budget making a mark of the beginning of a new India.

Government has given a clarion call to the industry with the announcement of creating global champions from India and backing this strategy with new, "development finance institution".

Now the responsibility shifts to the industry to not only dream but dream big and stand together with the government to make the country progress from poverty to wealth over the next three decades."

DIPESH KAURA

GM, Kaspersky (South Asia)

CYBERSECURITY TOOLS NEEDED FOR THE FUNCTIONING OF ADVANCED TECHNOLOGIES

"The budget for FY 2021- 22 was one with the aim to achieve and enhance our country's top priorities, by investing in the healthcare sector and major infrastructures. Enhanced healthcare systems, extensive research and development, and major infrastructure developments are definitely the need of the hour and have been effectively taken care of by the budget allocation set by our Finance Minister. The goal to empower 15000 schools and adapt to a hybrid education model is also a very promising step taken towards the digital transformation of the country. However, to make this a success, securing the hybrid education system is equally important, especially in the near future.

Similarly, cybersecurity tools will also be needed for the seamless functioning of advanced technologies like deep analytics and artificial intelligence that the government plans to use to identify tax evaders, fake billers and for the digital census."

INVESTMENT IN NATIONAL RESEARCH FOUNDATION TO BOOST OVERALL RESEARCH AND INNOVATION ECOSYSTEM OF THE COUNTRY

SANJAY GUPTA
VP and India Country Manager,
NXP Semiconductors

"The Union Budget 2021 has been the first-ever digital budget marking a major milestone in the digital journey of India. The budget has put the much-needed focus on Atmanirbhar Bharat and the need to grow the innovation and R&D sector in the country on a sustained basis. We are excited about the announcement of Rs 50,000 crores for the National Research Foundation over the period of five years. This will surely boost the overall research and innovation ecosystem of the country. In India, we have to focus parallelly on 'design-in-India' in addition to 'Make-in-India' to continue to be ahead of the curve. Looking forward to having more and more companies leverage this increased R&D budget from government and develop future researchers and Innovators. Overall, we are hopeful that Budget 2021 will propel India in the direction of becoming a global economic superpower."

VIKAS GARG
Chief Financial Officer, Paytm

THE PROPOSED SCHEME TO INCENTIVIZE DIGITAL PAYMENTS TO ACCELERATE GROWTH OF CASHLESS TRANSACTIONS

"The Finance Minister has presented a balanced budget that is aimed at maximum growth of all sectors in the coming year. The Rs.1500 crore proposed scheme to incentivize digital payments is a welcome move that will accelerate the growth of cashless transactions in our country.

During the pandemic, digital payments emerged as one of the key enablers of empowerment at the grassroots and brought millions of people under the fold of the formal economy. Government's continued emphasis on increasing investment in Infrastructure, Insurance and digital payments will ensure financial inclusion of the masses."

PRAMA HIKVISION WELCOMES THE PROGRESSIVE BUDGET AND LOOKS FORWARD TO ECONOMIC GROWTH AND STABILITY

ASHISH P. DHAKAN
MD & CEO,
Prama Hikvision India

"The Union Budget FY 2021-22 is a transformative budget with positive resolve for India to grow further with a vision of the AtmaNirbhar Bharat Abhiyan that compliments the 'Make-in-India' initiative of the Government. AtmaNirbhar Bharat is an expression of 130 cr Indians, who have full confidence in their capabilities and skills. The Union Budget has identified the six pillars of Atmanirbhar Bharat's vision. On behalf of Prama Hikvision, we welcome the progressive and visionary budget and look forward to economic growth and stability. The budget has sincere intent to provide momentum to strengthen local manufacturing capabilities. The Production Linked Incentive scheme (PLI) is a welcome move by the government. The review of the customs duty structure is clearly seen as a move towards promoting the domestic manufacturing. The move to strengthen the overall research ecosystem to boost innovation and R&D in the country, an outlay of Rs 50,000 crore, is being announced, for National Research Foundation."

RAMANUJAM KOMANDURI
Country Manager, Pure Storage India

"WE ARE LOOKING FORWARD TO THE NEXT PHASE OF DIGITAL INDIA WHICH WILL BE A BIG GROWTH DRIVER FOR BUSINESSES AND INDIVIDUALS"

"Budget 2021 looks promising and rightly focuses on public healthcare, given the disruption caused due to the pandemic. We are particularly excited about the Finance Minister's announcement of smooth delivery of digital services as part of the next wave of digital revolution.

AI, ML, and Data Analytics are making greater inroads in India, as was observed in the budget. These are all essential elements of the modern data experience. We are looking forward to the next phase of Digital India which will be a big growth driver for businesses and individuals alike."

BUDGET 2021 EMPHASISES ON REVIVING THE ECONOMY

ANIL CHAUDHRY
CEO,
Schneider Electric India

"With its extensive focus on infrastructure and healthcare, the Budget FY21-22 clearly focuses on reviving the economy. The key pillars such as health and wellbeing, capital and infrastructure, inclusive development, enhancing human capital, innovation and R&D and minimum government and maximum governance rightly identifies the core areas for sustained growth and provides considerable thrust towards an Atmanirbhar Bharat. The proposal to offer more choice to consumers by introducing competition in the power distribution space by kick-starting Rs 3 lakh crore reforms-based result-linked power distribution sector scheme for state power distribution companies is likely to address the long hanging Transmission & Distribution (T&D) issues and give relief to the power producers, thereby ensuring health for the entire value chain. It is also good to see the government government's focus towards ensuring smart metering, which will help cut the commercial losses in power distribution."

"THE INCENTIVE OF RS. 1,500 CRORE FOR DIGITAL PAYMENTS IS A MOVE IN THE RIGHT DIRECTION"

DILIP MODI
Founder,
Spice Money

"It was encouraging to see the 'Sankalp of Aatmanirbhar Bharat' as well as inclusive and sustainable development come into focus right at the beginning of Financial Minister Nirmala Sitharaman's budget speech. We had hoped for a boost to digital as it has the ability to bridge the gap between haves and have-nots when it comes to access to financial services. This was evident when the lockdown hit last year, when the digital financial infrastructure came to the rescue of millions of citizens. So, the incentive of Rs. 1,500 crore for digital payments is a move in the right direction. We are eagerly waiting to see what the scheme entails and how the industry can benefit from it. We are also excited to see the innovations that emerge out of GIFT International Financial Services Centre to support rural financial infrastructure to be on par with urban India. This is in alignment with Spice Money's vision to bring innovation in rural fintech and uplift the underserved parts of India."

SUNIL SHARMA
MD – sales, Sophos India & SAARC

"THE GOVERNMENT'S UNION BUDGET 2021 IS BUILT ON THE FOUNDATION OF NEW TECHNOLOGIES"

"The Government's Union Budget 2021 is built on the foundation of new technologies such as Data Analytics, Artificial Intelligence (AI), and Machine Learning (ML) which will empower businesses with econsultation, escrutiny, and compliance management. This is surely going to enhance enterprise cybersecurity as AI has immense potential to bring in scalable and effective defenses against sophisticated attacks like ransomware. As per our recent survey, with 100% Indian businesses being concerned about their current level of cloud security, there is a need for initiatives that promote the development of cybersecurity skillsets. Additionally, this reskilling process should also take care of security of cloud environments which are the backbone of the accelerated digital transformation that India is witnessing due to the pandemic. While we welcome the Government's proposed steps in strengthening MSMEs that provide employment to millions of people, we need more impetus on building skilled cybersecurity professionals in the country. The Government's allocation of Rs. 3,000 crore towards skill development that will help reskill India's youth and boost the overall economy, is a step in the right direction."

BUDGET 2021 EMPHASIZES ON JOB CREATION AND RURAL DEVELOPMENT

SUPRIA DHANDA
Vice President and Country Manager,
Western Digital India

"We congratulate the Government's initiative in amplifying Atmanirbhar Bharat. Wonderfully captured by our Finance Minister, Atmanirbhar Bharat is an expression of 130 crores Indians who have full confidence in their capabilities and skills. Digitisation, Skill Development and Job Creation are necessary to lead India towards high growth and be self-reliant. With rapid digitisation across industries over the last year, it is an opportune time to enhance our spending in training imparting digital skills to the youth. The budget clearly prioritises job creation and rural development with generous allocations for various developmental schemes. The focus around National Apprenticeship Training Scheme (NATS) with an allocation of INR 3,000 crores will empower a new wave of talent transformation and adequate employability opportunities for the Indian youth."

KARTIK SHAHANI
Country Manager, Tenable India

"THE EVENTS OF 2020 MADE IT CLEAR HOW RELIANT WE ARE ON THE DIGITAL INFRASTRUCTURE AND SUPPLY CHAINS"

"The events of 2020 made it clear how reliant we are on the digital infrastructure and supply chains that underpin modern society. As India seeks continued growth and competitiveness in the global economy through budget allocations in healthcare, infrastructure, innovation and R&D amongst other areas, securing the digital infrastructure that underpins our society needs to sit at the core of every single project. Budget allocations towards healthcare is a necessary step in our race to combat COVID-19. Along with the new opportunities that come from making the internet more accessible to citizens and organizations in various parts of India, there are significant cybersecurity challenges that organizations and governments need to manage. And if there are any lessons to be learnt from last year, it's that cybercriminals are relentless and will seek to test the resilience of all defences whether digital or physical. Therefore, our digital progress must be thoughtfully guided by the considerations for the safety and security of our country."

PLI TO HELP ACHIEVE SCALE AND JOB CREATION FOR THE YOUTH OF INDIA

NITIN KUNKOLIENKER
President
MAIT

"MAIT welcomes the continued focus of the Government on PLI and it is very encouraging. PLI will help achieve scale, and job creation for the youth of India. We look forward to the upcoming PLI including the electronics industry sub-sectors PCs, Datacom, Servers, Wearables, Telecom products, Smart meters and components.

We are happy to see the continued emphasis on the adoption of technology into economic activities. The National Language Translation Mission, earlier proposed by MEITY, will enable Bharat on the digital highway allowing the masses to take ride on the digitization of the economy."

AN OVERALL A BALANCED BUDGET

RAJESH GOENKA
Director, Sales & Marketing,
RP tech India

"Overall it is a very pleasant budget without any surprises which is good because in the current scenario consistency and continuity is more important rather than having mere aspirations. This is overall a balanced budget and only enhances the momentum set by our Prime Minister and Finance Minister in the last two years.

In terms of IT hardware industry, there is no major change, however, with the government investment, the overall market demand is likely to grow up. IMF has also forecasted the industry growth 11 to 11.5%, which is good for the industry. So overall we are optimistic about the budget."

SONIT JAIN
CEO,
GajShield Infotech

"THE BUDGET HAS A VISION OF AATMANIRBHAR BHARAT"

"Budget 2021 lays a strong foundation in Infrastructure, Health and Education. It provides a big boost in making India a leader in the World Economy and manufacturing hub of the world. Not only does it give an impetus to easing in doing business in India, it also gives a big push to rural development, which was impacted, the most, during the pandemic.

The budget has a vision of Aatmanirbhar Bharat and will motivate Indian entrepreneurs to make products in India for the World. Overall it is a pro-growth budget and will further fuel the growth of Indian IT companies with its strong focus on Digital India."

"BUDGET 2021 WAS POSITIVE GIVEN THE CHALLENGE AROUND HIGHER FISCAL DEFICIT DUE TO LOWER INCOME"

S SRIRAM
Chief Strategy Officer,
iValue InfoSolutions

"Budget 2021 was positive given the challenge around higher fiscal deficit due to lower income. It is great to see emphasis on growth front keeping fiscal deficit priority low for the next two to three years. The key highlights of the budget include additional allocation to health and wellbeing in a Covid ravaged year with Rs 35,000 Cr allocation to Covid vaccination with four Indian vaccines shortly. It is also great to see 35% enhancement of Government capital expenditure at Rs 5.54 Lac Cr to revive economy around Road, Rail and Metro infrastructure. It is encouraging to see focus around disinvestment with two PSU banks and one insurance company being planned for the year with Rs 1.75 Lac Cr target. FDI in insurance enhancement from 49% to 74% augers well for a country with very low penetration."

RAMESH MAMGAIN
Country Manager,
India and SAARC, Commvault

"IT IS AN INCLUSIVE AND PRO-GROWTH BUDGET"

"The Union Budget 2021 is sui generis considering that it is India's first-ever 'Digital Budget'. The gesture of doing away with the paper versions of Budget underlines government's commitment towards PM's 'Digital India' vision.

A renewed focus on infrastructure would mean accelerated technology adoption, which cannot be accomplished without data privacy measures, propelled by data protection. This approach would help in strengthening India's data protection framework to protect individual information, with investments in key technologies like artificial intelligence (AI) and machine learning (ML) to secure cloud-based infrastructures. While the capital expenditure on the physical connectivity - road, railway and port - has been highlighted throughout, I am sure that digital connectivity will ultimately become a cornerstone of everything we do in the current times. Overall, it is an inclusive and pro-growth budget, presenting a balanced stance on the pathway to recovery."

"FOCUS ON SETTING UP OF FINTECH HUB, ENHANCING DIGITAL PAYMENTS AND USE OF AI IN GOVERNANCE – ALL PROVIDE A STRONG PLATFORM FOR DIGITAL INDIA"

KARTHIKEYAN NATARAJAN
President and
Chief Operating Officer, Cyient

"Coming out of the pandemic year, the Finance Minister has laid down a well-rounded Budget.

Focus on setting up of Fintech Hub at Gift City, enhancing digital payments and use of AI in governance – all provide a strong platform for Digital India. Allocation of Rs 50,000 cr towards National Research Foundation will work towards boosting India's Innovation Quotient on the global map and is a welcome move.

Allocation of funds as incentives for promoting digital payments is also a step in the right direction and a significant step in ease of doing business. Lastly, increase in allocation for highways and railways will lead to employment generation and boost the economic growth of the nation."

RAJIV BHALLA
MD, Barco India

"THE BUDGET IS A MAJOR STEP IN THE RIGHT DIRECTION"

"The budget is a major step in the right direction. It outlays a strong focus on infrastructure, healthcare, capital spending, disinvestment, monetization, job creation and digitization. These measures are not only progressive and recovery-led, if implemented correctly would ease the burden on the economy and lead India towards the projected v-shaped growth and development. The budget talks about structural reforms in banking, enhancing debt financing and credit limits for businesses and asset monetization.

This will lead to an increase in government spending, which, in turn will spur demand, therefore net positive for the industry. The several initiatives around job-creation, startups, reskilling, rural development and better quality of services to people are positive as a Nation cannot progress without care for the environment and inclusive all-round transformation."

THE INITIATIVE TO SETUP FINTECH HUB WILL ENCOURAGE INVESTMENT AND INNOVATION DESIGNED TO HELP FINANCIAL INSTITUTIONS

SONALI KULKARNI
Lead – Financial Services, Accenture India

"The investment outlay towards digital payments is a welcome inclusion in the Union Budget.

We are seeing some notable innovation coming out of India's fintech ecosystem – be it for digital payments, credit and risk management, underwriting or security. The initiative to set up a fintech hub in Gujarat International Finance Tech-City (GIFT) will spur investment and innovation designed to help financial institutions not just meet compliance requirements but also build more-personalized customer products and services. The move to set up a new asset reconstruction company and an asset management company to take care of stressed assets of banks will facilitate more options for banks to manage their NPAs as the true impact of the pandemic on NPAs is still unclear, and is expected to be fully known only by Q1 FY2022. The disinvestment and privatization related announcements related to the banking and insurance sectors will enable much needed capital infusion, and thereby, unlock new growth opportunities in FY 22."

SHIBU PAUL
Vice President - International Sales, Array Networks

GOVERNMENT'S PROPOSAL TO USE ADVANCED TECHNOLOGIES FOR MINISTRY OF CORPORATE AFFAIRS' DATABASE TO BOOST DIGITALIZATION

"The government's proposal to use data analytics, artificial intelligence, machine learning-driven for the Ministry of Corporate Affairs' database is a boost to the digitalization where the Version 3.0 of MCA-21 includes additional modules for e-scrutiny, e-adjudication, e-consultation and compliance management. Connecting more than 1,000 mandis into E-NAM is an excellent move. Setting up a separate administration structure for ease of doing business would help many organizations from various sectors. The faceless dispute resolution panel would help the citizens by keeping them safe from tax harassment. The importance given to healthcare sector to fight Covid and any future healthcare issues, the stress made in green energy projects like keeping aside Rs 1,000 Cr for solar energy and Rs 1,500 Cr for renewable energy along with voluntary scrapping policy and the weightage given to education has made this budget wholesome." Investment to boost urban infrastructure to be stepping stones towards invigorating Smart Cities planning and urban development

INVESTMENT TO BOOST URBAN INFRASTRUCTURE TO BE STEPPING STONES TOWARDS INVIGORATING SMART CITIES PLANNING AND URBAN DEVELOPMENT

SUDHINDRA HOLLA
Director, Axis Communications, India & SAARC

"We are upbeat on the six pillars of the government agenda including focus on infrastructure, innovation and R&D that is all set to strengthen India's power as a global digital hub. We are optimistic by the renewed focus on road safety with advanced traffic management system with speed radars, variable message signboards, GPS enabled recovery vans along with the outlay of Rs 2.28 lakh crores for developing the highways, roads, and railways. Good to see pertinent steps taken to revitalize the economy with key focus on allocating budget for healthcare, metro railways, ports, airports, and logistics to boost urban infrastructure. These in turn will be stepping stones towards invigorating Smart Cities planning and urban development and help in generating more jobs."

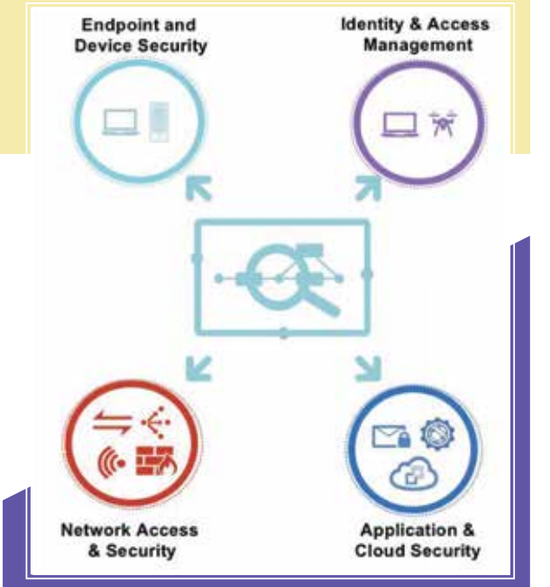
RAJENDRA CHITALE
CFO, Crayon Software Experts India

CRAYON SOFT WELCOMES GOVERNMENT'S MOVE OF IMPLEMENTING DATA ANALYTICS, AI, ML FOR MCA DATABASE

"It is a welcoming move that the government is emphasizing on the implementation of data analytics, artificial intelligence (AI), machine learning (ML) for the Ministry of Corporate Affairs (MCA)' database. We also welcome the digitization process and the introduction of e-scrutiny, e-adjudication, e-consultation and compliance management in MCA 3.0.

After the adversities of 2020, tax holiday for another year to startups is a commendable move for the government. Again, the tax audit bar raised to Rs 10 cr for those transacting 95% digitally shows the government's commitment towards bringing in greater transparency. Apart from that the government's promise on removing GST anomalies and the amount of Rs 1,500 cr earmarked for a scheme to boost digital payments are other welcoming moves for a stronger digitized India."

FortiXDR—FULLY AUTOMATED THREAT DETECTION, INVESTIGATION, AND RESPONSE



Engineered for AI-driven Security Operations

Digital innovation has transformed businesses and the networks they use to run critical applications, perform online transactions, connect remote workers, and collect and process critical data. And as in the past, these advances raised new security challenges, giving rise to new security solutions designed to address those challenges. However, the speed of transformation left organizations with little time to consider the broader security infrastructure when implementing those solutions. And as a result, now more than ever, today's security teams are left trying to manage a vast collection of security tools from a variety of vendors and establish some sort of visibility and consistent policy orchestration and enforcement across their organization. Among other challenges, security teams struggle to detect and respond to more—and more damaging—cyberattacks across a complex and largely isolated security toolset.

Most customers understand the logistical and technological challenges of this complexity and are interested in moving from dozens of different security vendors and products to a handful or less of security platforms, complemented by point products where necessary.

While there are pragmatic considerations like satisfaction with the vendor, breadth of controls available in their platform, effectiveness and features of each control, and more, an organizing principle has emerged to simplify and integrate that process—XDR, or eXtended Detection and Response. Defined by Gartner as "a security incident detection and response platform that automatically collects and correlates data from multiple security products," XDR enables an essential integration principle that leverages existing technologies to create unified vision and control over complex, distributed environments. XDR enables different security solutions to see, share, and analyze data so they can more effectively detect threats and deliver a coordinated response that covers the entire attack surface.

FortiXDR – THE ONLY XDR SOLUTION TO AUTONOMOUSLY MANAGE CYBER INCIDENTS FROM START TO FINISH

At Fortinet, we have been building integrated, multiple product solutions designed to operate as a single cohesive system; first with our Advanced Threat Protection and more recently the Fortinet Security Fabric. The Security Fabric is a broad, integrated and automated cybersecurity platform powered by FortiGuard Labs security services that protects the digital enterprise from endpoint and IoT through network and cloud. FortiXDR is designed to extend the Fortinet Security Fabric, reducing complexity, accelerating detection, automating alert investigations, and coordinating responses to cyberattacks. As part of the Fortinet Security Fabric, FortiXDR is able to leverage the common data structure, correlated telemetry, unified visibility, native integration, and seamless interoperation of Fortinet's portfolio of Fabric-enabled solutions. It then layers on automated analytics, incident investigation, and pre-defined responses out of the box. FortiXDR brings these advanced capabilities to all three steps of finding and mitigating a security incident:

1. Extended Detection: FortiXDR begins by leveraging the diverse security information shared across the Fortinet Security Fabric for correlation and analysis. And because it can collect information across the industry's broadest portfolio, the more threat telemetry that can be used to find an active threat—especially those designed to avoid detection.

2. Extended Investigation: FortiXDR is the first XDR solution to apply artificial intelligence (AI) to the investigation of detected threats—a process every other XDR solution hands off to an overburdened human security analyst, slowing down the process and leaving systems vulnerable to human error. And given the volume of alerts most networks generate, many security teams are simply not resourced to chase down every potential threat.

FortiXDR's first-of-its-kind, AI-based XDR solution fully automates incident investigation rather than relying on scarce human resources. It is powered by a patent-pending Dynamic Control Flow Engine and is continually trained using the threat data and research feeds provided by FortiGuard Labs as well as the frontline expertise of its incident responders. It establishes the context of an alert, performs a thorough investigation to determine if the threat is real, and then identifies the nature and scope of the attack so the response system knows how to proceed. And unlike a security analyst, FortiXDR performs this function in a matter of seconds, effectively closing the exposure gap created by other XDR solutions.

3. Extended Response: Because FortiXDR is fully integrated into the Security Fabric, it is natively able to marshal every available resource needed to mount an effective, automated, and coordinated response. And because its response functions are more uniform than most security information formats, customers are also able to leverage connectors to even tie in many third party solutions in their response.

KEY BENEFITS OF FortiXDR

In addition to speeding detection, investigation, and response, FortiXDR also gives organizations a compelling case to consolidate independent security products.

Early adopters show that it dramatically reduces the number of alerts to be investigated by 77% or more on average, helping ensure that cyberattacks don't get "lost in the noise." And as mentioned, FortiXDR is the only XDR solution augmented with AI across all elements of the detection, investigation, and response process. This eases the operational burden on security teams, handling complex tasks in seconds that would take experts with specialized tools 30 minutes or more to accomplish. And without human error.

And with its broad portfolio of independently top-rated controls, that can be deployed to address the cyber kill chain from end-to-end, there are plenty of opportunities to consolidate more and more vendors over time.

All of this enables organizations to reduce mean time to detection (MTTD) and mean time to response (MTTR), thereby reducing the impact of cyber incidents while improving security operations efficiency and overall security posture. It frees up seasoned security professionals for higher value contributions to the security of the organization, and helps the organization itself continue to compete effectively while addressing the crush of security and vendor sprawl through strategic solution consolidation and automated threat detection and response across the entire distributed network.

VAR SECURITY

SOPHOS AIMS TO CONTINUE WORKING CLOSELY WITH PARTNERS TO MAKE THEM BELIEVE IN THEIR VISION

Headquartered in Oxford, U.K, Sophos protects more than 400,000 organizations in more than 150 countries from cyber threats. Sophos has been driving the transition to next-generation cybersecurity by leveraging advanced capabilities in cloud, machine learning, APIs, automation, managed threat response, and more, to deliver enterprise-grade protection to any size organization. In a chat with VARINDIA, Sunil Sharma, Managing Director Sales, Sophos India & SAARC has shared his views on safeguarding customers, its latest products and technologies, future roadmap etc.

EMPOWERING CUSTOMERS

As a growing number of organizations are adopting work from home (WFH) as a permanent company policy or even the adoption of hybrid working solutions, this shift has certainly caused some critical challenges for businesses in terms of cybersecurity. Irrespective of the size of the organization, ensuring cybersecurity is a crucial consideration for all businesses. Some of the protective measures Sophos recommend are:

- **Ensure devices and systems are fully protected: Go back to basics** – ensure all devices, operating systems, software applications and security solutions are up to date with the latest patches and versions. All too often malware breaches an organization's defenses via an unpatched or unprotected device.
- **Create a secure connection back to the office:** Using a Virtual Private Network (VPN) ensures that all the data transferred between the home user and the office network is encrypted and protected in transit.
- **Scan and secure email and establish healthy practice:** Home- working has led to a big increase in email as people can no longer speak to colleagues in person. The crooks are wise to this and already using phishing emails to entice users to click on malicious links. Ensure email protection is up-to-date and raise awareness of phishing.
- **Enable web filtering:** Applying web filtering rules on devices will ensure that users can only access content appropriate for 'work' while protecting them from malicious websites.
- **Make sure people have a way to report security issues:** With home working people can't walk over to the IT team if they have an issue. Give people a quick and easy way to report security issues.

DEFENSE FOR CUSTOMERS AND EMPLOYEES

According to Sunil, "Cybersecurity awareness for our customers and partners is one of the key focus areas for Sophos. We have a dedicated tool-Sophos Phish Threat that provides phishing attack simulation and training for end-users. It helps our customers to nurture a culture of positive security awareness. Effective security training is also a part of Sophos Phish Threat, available through Sophos Central, which is a cloud-based management platform."

PRODUCTS AND SOLUTIONS TO MITIGATE THE SITUATION

Powered by deep learning neural network Sophos Intercept X uses behavioral analysis to stop previously unseen ransomware and boot record attacks. Intercept X secures endpoints and servers using CryptoGuard technology, which stops both local and remote unauthorized file encryption by malicious software. Then it restores data to its original state, taking ransomware's power over its victims away.

Sophos Intercept X combines ransomware protection, deep learning malware detection, exploit prevention, End Point Detection and Response (EDR) - all in a single solution.

"Sophos' synchronized security strategy enables multiple security products to work together seamlessly with simpler management and better security. It allows Sophos endpoint (Intercept X) and firewall (XG firewall) to share threat intelligence, and provide faster comprehensive protection against advanced threats like ransomware." confirms Sunil.

THE LATEST SECURITY TECHNOLOGIES

The pandemic has accelerated the digital transformation and cloud adoption among businesses across industry sectors. Businesses have understood the importance of cloud in enabling working and doing business from anywhere. While cloud enables digital transformation, cybersecurity makes digital transformation more secure. Organizations should understand that security of cloud infrastructure is a shared responsibility where the cloud provider takes care of the security on the cloud.

On this topic Sunil comments, "However, the safety of what organizations put on the cloud is the responsibility of them and not the cloud provider. We're here to help Indian organizations understand these changing attacker behaviors, so that they can implement the best anti-ransomware technology, like Sophos Intercept X with EDR, and threat hunting services such as our MTR and Rapid Response, to defend against ransomware, both now and in the future."

TO CONCLUDE

In 2021, Sophos aims to continue working closely with their partners to make them believe in their vision. This involves protecting people and enterprises from cybercrime, by developing powerful and intuitive products and services and grow them by protecting their joint customers across every vertical and size.

"Our strategy for the future is very clear – to advance our next-generation solutions that leverage synchronized security. We have a clear vision of how we are going to enable digital transformation. We also know from our threat intelligence that ransomware will continue to be an attack strategy for adversaries across all rungs of the cybercriminal hierarchy. We will continue to focus on our Sophos Global Partner Program, which helps our partners have a clear growth path with Sophos. This helps support partners as they upsell and cross-sell across Sophos' next-generation product portfolio. We also plan to continue the momentum we have seen for Sophos MSP Connect in the region. Partners who are committed to Sophos will see a clear growth path with us," concludes Sunil.

AI COMPUTING PLATFORM "AIWORKS SOLUTION" – A PROMISING PROSPECT FROM ACER FOR SERVERS AND WORKSTATIONS IN INDIA

ACER, one of the leading global technology brands, has announced the launch of "aiWorks solution" - an Artificial Intelligence Computing Platform in India. Acer's all-new "aiWorks Solution" is essentially an Artificial Intelligence Computing Platform that offers a streamlined and cost-effective integrated solution for servers, workstations, networks, and storage. At its core, Acer aiWorks is an amalgamation of Altos BrainSphere™ series of computing system products (including servers, PC workstations, etc.), and Acer Altos Accelerator Resource Manager (AARM) smart accelerator computing resource management system. aiWorks offers artificial intelligence computing system choices, rapid deployment of a development environment, & optimization of artificial intelligence accelerator resource allocation.

The aiWorks Solution is expected to offer a robust, resilient, and reliable IT infrastructure making it one of the keystones of a successful business. It isn't a hidden fact that the increased dynamism and ever-growing consumer demands have resulted in a greater workload than ever before.

Acer Altos server and workstation solutions are therefore being brought to India, complete with a reliable AI platform that will not only help meet the consumer demand but will also help businesses be future-ready.

The Acer aiWorks supports NVIDIA A100 Multi-Instance GPU (MIG) technology, wherein MIG allows each A100 GPU to be divided into up to seven instances. Whether it is high-bandwidth memory, cache, and computing core, they are all independent; GPUs have multiple cutting forms, which can not only withstand workloads of any scale, but also ensure the quality of work services (QoS), which can also accelerate the scalability of computing resources, and maximize utilization rate. Besides, for Volta and Turing series GPUs, the Acer aiWorks solution also supports

NVIDIA CUDA Multi-Process Service (MPS) technology to improve GPU utilization.

Acer Altos Accelerator Resource Manager AARM adopts the container technology that manages AI accelerators and system resources. AARM also brings about Altos's own patented algorithm technology to optimize GPU resources and automate the deployment of functions, which greatly reduces the complexity and barrier for users to deploy workload and application for deep learning and machine learning development.

Besides, AARM allows individual developers to quickly deploy independent workspaces and development environments on the system, allowing multiple users to share hardware resources while still maintaining independent development environments without mutual influence, which helps developers focus more on the research and development of artificial intelligence applications.

Anil Bhasin joins UiPath as MD & and VP- India & South Asia

Anil Bhasin joins UiPath as Managing Director and Vice-President, India, and South Asia, and will take over from Manish Bharti. Anil, formerly the Regional Vice President, India & SAARC, Palo Alto Networks, will be responsible for scaling the business and technology units within the company's India and South Asia operations. He will work closely with Rick Harshman - Senior Vice President and Managing Director of Asia Pacific and Japan. Manish Bharti will take on a new strategic role within UiPath, details of which will be available in near future.

An established technology leader with over 33 years of industry experience in various leadership and senior management roles, Anil Bhasin will help accelerate adoption of automation as the preferred platform for catalyzing digital transformation across various industry verticals and sectors.

VMware chairs Guru Venkatachalam as CTO, Asia Pacific and Japan

VMware, Inc. has appointed Guru Venkatachalam as Vice President and Chief Technology Officer for Asia Pacific and Japan. Prior to this role, he was CTO of Cloud Architecture at VMware.

Guru leads VMware's efforts in Asia Pacific and Japan to build trusted partnerships with customers and partners and deliver solutions aligned to their strategic priorities. He will also play an integral role in the further developing the company's cloud, app modernization, networking, security, and digital workspace platforms.

Greg Lavender, CTO, VMware said, "Guru is a seasoned industry leader who has driven large scale innovation and expanded our CXO engagement in Asia Pacific and Japan. I am delighted to have him in the role of CTO for APJ as we drive customer and partner engagement in the region and help enterprises transform with modern applications, cloud, digital workspace and security."

Blackhawk Network ropes in Nikhil Sathe as Chief Technology Officer

Blackhawk Network announced veteran tech executive, Nikhil (Nik) Sathe, has been named Chief Technology Officer. Sathe will lead Blackhawk's continued innovation in global payments technology, including product development, infrastructure and security.

Sathe brings more than 30 years of experience in numerous leadership positions in the technology and financial space, including CTO roles at American Express and PayPal, and prior payments leadership roles at Google and JPMorgan Chase. Most recently, he served as vice president of engineering for Google Nest, where he was responsible for the strategy, design and development of Google's Nest, Chromecast and Home branded products and Smart Home ecosystem.

Milind Kulkarni appointed as Tech Mahindra CFO

Tech Mahindra has signed Milind Kulkarni as the Chief Financial Officer (CFO) effective 2nd April 2021. Milind Kulkarni will step into the shoes of the current CFO, Manoj Bhat, who will be moving as 'Group Chief Financial Officer', M&M Group as part of the leadership rotation strategy.

CP Gurnani, MD & CEO, Tech Mahindra, said, "It's been a pleasure working with Manoj over the years, and I wish him all the best in his new role as the M&M Group's Chief Financial Officer. He has been instrumental in spearheading the growth of the organization and I would like to thank him for his immense contributions to the finance function. I welcome Milind Kulkarni, who has worked with the company for over 19 years in multiple leadership roles including as CFO till May 2018, in his new role."

Anuj Vaid appointed as the Executive Director in CMS IT

Anuj Vaid has been named CMS IT Services' new Executive Director. In his new role as ED of one of India's leading IT firms, Anuj will be prioritizing bringing into fruition the CMS IT 4.0 Strategy that he has championed and formulated with his expert understanding of the organisation's capabilities and customer profile. His other major focus will be on synergizing the entire business- sales and delivery operations, to ensure the enterprise in future-ready and continues to stay relevant in the new business paradigm.

Prior to this, Anuj was the company's Executive Vice President and CSMO. Since joining CMS IT Services in 2015, he has been responsible for executing the company's strategic agenda. Anuj has been at the helm of prominent achievements like the Defensible Cybersecurity Framework designed specifically for tackling cyberthreats in the COVID-19 scenario, as well as India's First AI-Driven Automation Shared Delivery Model – the 'Remote Automation Centre for Enterprises' (R.A.C.E) with Automation Anywhere.

Bikram Singh Bedi has now joined Google Cloud

Google Cloud has appointed Bikram Singh Bedi as its new India Managing Director. Bedi was the man who set up Amazon Web Services in India and led the vertical for six years long. At Google, Bedi will be responsible for leading Google Cloud's sales and operations teams in this dynamic market.

Bedi's appointment comes as Google Cloud had recently elevated its India head Karan Bajwa as the Vice President of Google Cloud in Asia Pacific. Right before joining Google Cloud, Bedi was the President Strategy and New Initiatives of Indian grocery startup Grofers.

Bedi said, "I'm excited about this new challenge and I look forward to extending Google Cloud's momentum in India. The true test of 2021 will be how enterprises will leverage cloud computing to modernize and scale for growth and Google Cloud is committed to help them accelerate their digital transformation to build a strong foundation for the future."

aruba

a Hewlett Packard Enterprise company

DISCOVER THE FUTURE OF NETWORKING WITH THE LEADER IN EXPERIENCE EDGE

Secure, Simple, Smart Networks

Wireless | Wired | Security | Network Management | Analytics & Assurance | SD-Branch | Location Service

UNITED COMPUTERS

For more details contact:

United Computers- Mr. Karthik Varun B

karthik@unitedcomputers.in | +91 9611111125

RNI - NO 72399/1999 Reg. No: DL-SW-01/4030/18-20 Date of Posting 20 & 21