THE SHIFTING SANDS OF TECHNOLOGY

While change has been constant in Technology, this year saw a radical disruption, accelerated by the pandemic. Consequently, several trends gained faster traction from remote work enabling technologies to cloud services and cloud security. GITEX 2020 possibly gives an exclusive opportunity to gauge the changes that the industry is going through

This year's GITEX Technology week, the 40th edition of the iconic Technology expo, is an exhibition of mankind's resilience in the face of immense challenges. The pandemic had brought the entire world to its knees in the earlier part of the year, but the world has fought back with remarkable fortitude.

While the pandemic threat lingers, people have got back to their lives and work, albeit following safety guidelines. Remote working gained ground as a defining trend that is likely to stay on into the future. Technologies have supported remote working and several digital forms of transacting business and finance.

The year has accelerated consumption of cloud services as most applications are now being delivered as a cloud service. While there are many advantages when it comes to the cloud, there are also security concerns that have come to the fore, especially with more people working out of anywhere and accessing corporate networks. Concerns around data management are also very significant in the multi cloud era. At GITEX, there would be solutions showcased that address several of these concerns while also empowering remote working in a more secure manner. It is indeed the era of distributed edge networks and empowering and securing them would be a key focus of solutions at the showcase. The event and the conversations around it enable us a view of the shifts in the industry in terms of what technologies are gaining ground and what are the concerns in the foreground.

On remote working as a defining trend of the year, Rajesh Ganesan, Vice President, ManageEngine says, "Remote working is not entirely new and has been prevalent at least over the last decade. It allowed people the ability to get their normal work done regardless of their location, but for mission critical jobs, they were still required at the office premises. However, with the pandemic forcing everyone out of the office premises for extended periods, businesses have to deploy technologies even to allow sensitive and mission critical jobs remotely. The normal work involved communication, collaboration, access to one's own corporate assets and less critical business applications. Whereas, for mission critical jobs, employees need privileged access to the network, systems, applications and data to be able to perform administrative and sensitive tasks. This need is not just for people in technology, but for everyone across all the business functions."

He adds, "Adding to the challenge of this necessity is the reality that employees will work from random locations, with different devices, connecting from networks with no guarantee of security levels. Businesses do have the option of continuing to use legacy technologies like the VPN, but it neither scales effectively nor allows other forms of remote access to be managed together. This has given rise to a new breed of technology solution that enables unified and secure remote access for every employee in the organization."

ManageEngine is exhibiting at GITEX 2020 to showcase its unified endpoint management tool, Desktop Central; new-gen SIEM solution, Log360, which has UEBA capabilities for proactive threat analytics using AI and ML; and PAM360, which enables enterprises to establish strict privileged access governance and monitor privileged operations. The company will also highlight Device Control Plus and Application Control Plus, which enforce the principle of least privileges for employees using various devices and applications.

As a key trend, accelerated adoption of cloud services has played a key role in the near overnight transitions to remote working when lockdowns were announced across the world.

Fadi Kanafani, Managing Director – Middle East, NetApp says, "Undeniably, cloud has played a crucial role in helping businesses with enabling a large remote workforce and maintain business continuity. Data at the edge took on a heightened relevance during the COVID-19 pandemic as businesses were forced to rapidly transition to remote work and shift large amounts of transferable data to the cloud. Many companies increased or changed their virtual desktop infrastructure (VDI) footprint to meet the demands of their remote users, and end-user computing (EUC) solutions were created to meet these demands across many workloads, on premises, in the cloud, or remote. From collaboration tools, to overall workloads, the cloud has been an indispensable asset for business. It's helped business support remote-access workers, help ensure the availability of data

and applications, and helped prepare for—and avoid—the next wave of potential disruptions."

With business continuity being a key, NetApp helped customers implement Virtual Desktop Infrastructures (VDI), cloud and hybrid cloud models as they deployed a remote working strategy.

"We also gave customers access to our consumption model to gain a cost advantage and to lessen the complexities associated with IT infrastructure and lifecycle management. NetApp is enabling business with end-user computing (EUC), virtual desktop infrastructure (VDI), and cloud solutions make it easy for IT to enable this kind of adaptability. We've also deployed the NetApp ONTAP AI platform in healthcare institutions as researchers worked aggressively on genomics, analytics, " he adds.

NetApp through its virtual presence at GITEX this year will focus on the theme 'Unlock the Best of Cloud' and will be focusing on the new capabilities of its portfolio, showcasing its solutions in Cloud, Business Continuity, Data Services, Hybrid Cloud, Artificial Intelligence and Security.

"We will also emphasize our data fabric vision as businesses rapidly adopt cloud. With AI and cloud & edge computing undeniably being the technologies that are revolutionizing how businesses store, access, analyze and use their data to gain competitive advantage, NetApp is strategically placed to help businesses address the challenges that they have been facing over the past few months – businesses continuity being at the center, " adds Fadi.

IMPACT OF DISTRIBUTED NETWORKS ON SECURITY

A significant shift today is that the technology infrastructure of modern organizations are typically and perhaps completely distributed, across private and public clouds, spanning multiple countries. The optimal upkeep of the infrastructure demands that administrators be given privileged access to every component, for both maintenance and troubleshooting.

"As administrators start to work from remote, using their own devices over insecure networks, the situation calls for a remote access solution that inherently packs layers of security to account for every weak link introduced by extended remote work. Access to systems in public and private cloud, VMs in IaaS platforms, admin consoles of SaaS applications, databases and network devices spread across the infrastructure should all be seamless and unified for the administrators. From within one console, they should be able to launch a secure remote session to any of those components, with the whole session monitored and recorded for both security and compliance reasons," says Rajesh.

ManageEngine exclusively launched a couple of products in the first quarter of 2020, to enable secure remote access for all employees. Remote Access Plus brought the ability for employees to initiate remote connections to Windows, Linux or Mac computers regardless of the user's or device's location. It also allowed technicians the ability to remote access into users' computers at home for troubleshooting assistance. Whereas, Access Manager Plus, allowed administrators to launch RDP, VNC and SSH connections to critical infrastructure components without the need for VPN or any special software in employee devices.

While remote working brings on several security challenges including secure access to devices, the challenges around identity management can be considerable as well when cloud is the predominant form of IT.

Morey Haber, CTO & CISO, BeyondTrust explains, "The single biggest threat to identity management in the era of the cloud is based on the loss of security controls that traditionally were available with on premise technology. For example, identity management in a traditional office environment delegated entitlements and security controls based on network zoning and segmentation to help define how and where an identity can have access from, and to. The identity itself could not have accounts authenticated or be authorized for tasks outside of a defined perimeter. In the era of the cloud, these security controls are no longer available to identity management."

He adds, "Threat actors understand this principle and can leverage identity management in the cloud, unless other additional mitigating controls have been implemented. The most common ones include software defined perimeters, zero trust

Rajesh Ganesan
Vice President, ManageEngine

architectures, just in time access, and endpoint based least privilege security models. These concepts add security controls that improve the confidence."

The impact of edge security and distributed networks on privileged identity management has been significantly impacted by the COVID-19 pandemic. And since this model will continue to grow even after a vaccine is available and the pandemic has subsided, the threat vectors would be substantial.

"Organizations have seen a rapid increase in edge security models based on employees working from home and an intrinsic need to manage and validate identities outside of the traditional corporate perimeter. There is a fundamental truth in the expression "the perimeter is dead" since employees, access, resources, and applications need to be available from almost everywhere and nearly at any time due to the current health crisis, "Morey adds.

He believes that with the remote working trend likely to continue, privileged identity management takes center stage to provide confidence that the user is who they