SPECIAL SUPPLEMENT BY
Enterprise CHANNELS MEA

CYBER SENTINELS

TRENDS FOR CYBER AND INDUSTRIAL SECURITY EXECUTIVES

APRIL 2019

ABDULLAH HAMOOD KHALID AL BARWANI,
GENERAL MANAGER CORPORATE SECURITY

OMANTEL

ROLLING OUT A CYBER RESILIENCE PROGRAMME

There are many areas that need to be protected and controlled, existing gaps closed, backup plans tested, and the organisation made cyber resilient.

Paul Potgieter, Dimension Data

USING AUTOMATION AND ORCHESTRATION TO TRANSFORM SECURITY

Joe Baguley, VMware

FIVE BASIC SECURITY TIPS TO REMAIN AHEAD OF THREAT ACTORS

Snehaa E, ManageEngine

DEVELOPING A 360-SECURITY PROTECTION SOLUTION

Gamal Emara, Aruba HPE

MONITOR NETWORK ALERTS LIKE YOUR JOB DEPENDS ON IT

Shyam Sundar, Valto

USING A PROTECTED SHELL BROWSER TO ISOLATE RANSOMWARE

Firas Jadalla, Genetec

REDUCING LIABILITIES BY INVESTING IN CYBER INSURANCE

DEVELOPING A 360-SECURITY PROTECTION SOLUTION

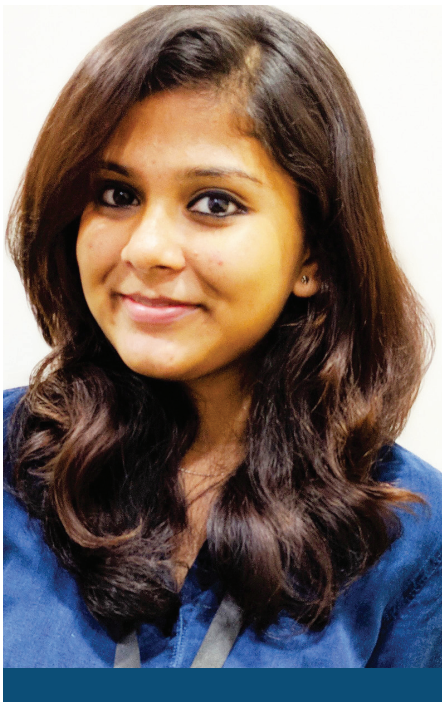
Here are six definitive steps implementing versatile security covering networks, applications, end points according to Snehaa E, at ManageEngine.

Every IT administrator has succumbed to at least one sleepless night from worrying about data security and fearing the outcome of a security breach. Overthinking is second nature to humans, but there would be one less problem to worry about if we found a permanent fix for cyberattacks.

But is there a cyberdefense strategy out there that is completely foolproof? One that keeps all cyberattacks at bay? No, a perfect strategy does not currently exist, but that does not have to stop us from striving for a well-rounded one. Understanding the nature of attacks and employing different security solutions to cover all bases will help us approach the ideal security strategy.

So, where do we start? You should opt for a combination of network security solutions and endpoint management solutions. This combination will provide robust protection against most known cyberattack variants.

Let us break down these solutions' components to get a better understanding of how they keep cyberattacks at bay:



SNEHAA E,

MARKETING ANALYST, MANAGEENGINE.

#1 FIREWALL

Setting up a firewall for your organisation forms the first line of defense against malicious network connections. A firewall controls incoming and outgoing traffic, and protects your network based on a defined set of security rules.

You can adjust your security rules to allow outgoing traffic from particular applications while preventing incoming traffic for certain applications. Combine a firewall with an intrusion prevention system that selectively prevents threats or controls applications based on the type of firewall.

#2 PROXY

Configuring a proxy server forms the next line of defense in cybersecurity. Whereas a firewall detects and blocks certain network traffic, a proxy server acts as a gateway between your network and the Internet. Configuring your proxy to block known malicious websites helps protect your network from malware, phishing, and other cyberattacks.

#3 INVENTORY

Taking inventory of all the devices that are present in your organisation helps you identify devices that should not be present. You should also identify the applications and software that these devices use.

# APPLICATION CONTROL

Blacklisting unwanted or possibly malicious applications reduces the opportunities for data to be lost or stolen.

#5 PATCHES

Consistently patching the software used in your infrastructure is crucial for eliminating potential attacks that occur through vulnerabilities present in outdated versions of software.

#6 ANTIVIRUS

Using antivirus software stops known malware from being installed on your endpoints. Antivirus software also typically scans downloads for malware and blocks malicious executable files from being downloaded.

With the complexity of cyberattacks steadily increasing, the most common attack vector into an organisation is shifting towards browsers and since browsers are an integral part of today's mobility-first, cloud-based world, this trend will only continue to increase.

So, here is the final step to realising your ideal security strategy: implement a dedicated solution that scans for and secures all the loopholes present in your browsers, monitors and controls the add-ons used by your browsers, and controls the traffic accessed through your browsers.

With a browser security solution, you will round out your security strategy, ensuring that you have fortified your enterprise's defenses against cyberattacks.

KEY TAKEAWAYS

- TRADITIONAL ENDPOINT MANAGEMENT SOLUTIONS DO NOT EXTEND THEIR PROTECTION TO BROWSERS.
- SETTING UP A FIREWALL FORMS THE FIRST LINE OF DEFENSE AGAINST MALICIOUS NETWORK CONNECTIONS.
- CONFIGURING A PROXY SERVER FORMS THE NEXT LINE OF DEFENSE IN CYBERSECURITY.