DECEMBER, 2020 | ISSUE 1

VIGYAN GYAN

Information That Matters

Endpoint Security in the Co-Covid Word

The term "new normal" has different connotations for different people. For some, the term is synonymous with a return to the office while others think that co-located teams are a distant reality now. The reality is probably in some middle ground.

Household names like Google and Facebook are planning for a future where most of their employees work remotely most of the time. And other organizations tend to follow these tech giants.

Over 70 percent of CFOs surveyed in a recent Gartner survey say that more employees will be transitioned to working remotely even after the COVID-19 pandemic recedes. Naturally, cybersecurity needs to evolve. This new normal opens up a whole host of questions about how to ensure endpoint security with a highly distributed workforce. How can companies deal with endpoint security threats like evasive malware, fileless attacks, and increasing numbers of zero-day attacks when most of their staff are working from home?

Remote and distributed workforces are here to stay, so IT security teams need to have a complete rethink about their endpoint security policy. To keep companies safe, advanced endpoint security tools must be deployed to remote endpoints–even if those are personal computers that employees use to conduct their work–to ensure that everyone is working securely no matter where they are.

This rethink is needed because cybercriminals have noticed the rise in remote work too.

Once end users move beyond the relative safety of their office buildings, they're essentially out in the wild. They might be using their own devices rather than standard issue machines to connect to the corporate network, and conforming to IT policies is probably not their highest priority right now. Perhaps their kids are playing on their devices, or maybe they are surfing the net in their downtime, taking corporate-maintained endpoints to new, potentially dangerous sites. And these are just some of the new complications IT administrators face on the end user side. It becomes even more complex when you consider the implications of widespread remote connectivity on network performance.

When countering this new wave of threats, your IT security team shouldn't be the first line of defense. Instead, everyone in your organization who works remotely needs to be on the front line of your company's endpoint security.

Organizations need to provide employees with security awareness training. Every employee should know good security habits such as when to use two-factor authentication for their devices and how to keep software up to date.

Cont. to Page 2

Cont. from Page 1

Companies can improve their employees' network security by insisting on the use of a virtual private network (VPN) to access the company networks. VPNs create a secure tunnel from your employees' computers to your corporate network. VPN use grew by 41% during one week in March alone. VPNs only provide security across one dimension, however, and don't necessarily provide security against all possible threats.

Back when most of the teams were co-located, in-house IT teams could quickly fix compromised machines. But without multiple threat-focused monitors, secure high-speed network connections, and the ability to interact with one another in real-time, distributed security teams aren't able to "close the door" and counter a live threat securely.

Inconsistent employee internet connections also seriously hinder remote remediation and if it happens to a security professional remotely remediating an issue with a compromised machine, the results can be devastating. Remote access tools are also far from secure.

While you can't rely on remediation to protect against endpoint attacks, you can stop them before they cause any damage. One way to do this is by using software that allows moving target defense, which prevents advanced endpoint threats from compromising remote machines in the first place.

The reality of the "new normal" is going to mean a larger percentage of your company will be working remotely more often than not. A knock-on effect of this change is an increased number of vulnerable endpoints in your company's network and a rise in the likelihood of a successful endpoint security breach. The key to staying safe in this new threat environment is to stop relying on remediation and start training and equipping all employees on the security front with the right tools and training.

IPM+ NEWS & VIEWS

- Rising Endpoint Security Star SentinelOne raises $267M." **- CRN**
- Coalition and Malwarebytes partner to deliver a joint solution that combines cyber insurance and endpoint security." **- MSSPAlert**
- MobileIron: 'Endpoint Protection Shouldn't Be Limited To Desktop' " **-CRN**
- Sophos Intercept X Named Best Endpoint Security Solution by CRN® for Fourth Consecutive Year" **- GlobeNewswire**
- Endpoint Security Market to Reach $22.40 Billion; Surge in Product Demand during Covid-19 to Influence Market Growth, says Fortune Business Insights." **- GlobeNewswire**
- Cybereason Takes An 'Operation-Centric' Approach To Security." **- Forbes**
- Census 2021 cyber security measures only 'partly appropriate', audit finds" **- itNews**
- FireEye Buys Cybersecurity Automation Firm Respond Software For $186M" **- CRN**
- Young talents should create robust cyber security solutions to protect data and IT based products, says Prime Minister Modi" **- All India Radio**
- Computer Misuse Act: Most UKcybersecurity pros fear breaking the law by simply doing their jobs." **- The Daily Swig**

IPM+ Corner

SBI SAVING WITH IPM+

When it comes to IT power consumption management, many think of server virtualization and consolidation. But a number of IT organizations are still focused on the savings they can achieve with endpoint power management software.

A number of companies whose sole focus used to be on security monitoring, automated configuration and patching have expanded their tools to monitor endpoint and server activity in order to create and enforce power management policy that will power down machines when they are inactive and alert network managers when they are reaching power usage caps.

And this is where IPM+ revolutionary Endpoint Energy Management Technology comes into play.

Our patented AI PowerMind Technology, Low TCO and High Scalability is what sets us apart from others in the industry.

State Bank of India is the leading public sector banking institution in India. It is the 43rd largest bank in the world and ranked 236th in the Fortune Global 500 list of the world's biggest corporations of 2019. With over 24000 branches all over the country, SBI is every Indian's go-to bank.

A huge problem facing SBI was increasing data consumption and an immense carbon footprint. To address this issue, the bank wanted to implement 1 pan-India energy savings project and quantify the impact created. So, SBI installed IPM+ Power Management Utility Software in their office desktops across India.

The impacts of our software were:

- Energy Savings - 33.17 GWh
- GHG emissions avoided - 33190 tCO2e
- Water Savings - 31.5 lakh m3
- Cost Savings - ₹ 33.17 crore

The energy saving initiative of installing the IPM+ Power Management Utility Software across all Circles in India has resulted in a cumulative saving of **33.17 GWh.**