MOOR INSIGHTS & STRATEGY

HOW IT AND SECURITY TEAMS CAN BE READY FOR 2021 AND BEYOND

SUMMARY

Due to the impact of COVID-19, 2020 will be widely regarded as the year that work moved home. In reality, it was the year work moved to the cloud and everywhere in between. As a result, endpoint management and endpoint security are now the cornerstones of effective protection and the foundation for the next generation of security.

As the world moves beyond the pandemic, some people will return to the office and begin traveling again. Research conducted by Moor Insights & Strategy reveals that over 80% of companies will offer more flexible workplaces post-pandemic, and over 70% of employees will take advantage of that flexibility.

Thus, it appears 2021 will be the year of the hybrid workforce, and effective cybersecurity will require a combination of technology, processes, and people.

Security is at a significant inflection point, and organizations must adapt to protect people, places, and things. Enterprises should evaluate not just the financial cost of a security incident but the impact on human resources and the loss of control over one's IT environment.

Our research indicates compromised employees have a 45% reduction in productivity. Compounding this trend, we are seeing a 250% increase in cybercrime targeting work-from-home employees, especially with nation-state attacks emanating from Russia, Iran, North Korea, and China. While the main prize is large public and private sector organizations, these attacks affect home-based employees, business email, endpoints, and internal systems.

THE PERIMETER IS DEAD – SECURE THE DATA AND THE DEVICE

Phishing scams and botnets pose the largest threats to organizations. One of the main reasons is the number of devices outside of the perimeter that are vulnerable to increasingly advanced threats.

From an endpoint perspective, combating attacks requires the ability to rapidly identify changes in behavior at the endpoint and to the state of the environment, such as where a fast-moving security incident expands laterally.

Foster Cyber Hygiene

In recent attacks, especially SolarWinds and FireEye, bad actors were hiding in the network traffic. In the network, they were closing doors they had opened and moving to the next target. The reality is that threat groups and bad actors (e.g., APT29, YTTRIUM, Cozy Bear) exist worldwide and continuously capitalize on human error.

Collectively, all public and private sector entities must reflect on where cybersecurity strategies and programs stand today and proactively educate and foster better cyber hygiene behaviors for their remote workers, as well as those continuing to operate within traditional brick-and-mortar facilities.

There is a need for a concerted effort toward adopting platforms, tools, and services where everyone within an organization actively participates. Having an alibi does not absolve one of responsibility. Security is everyone’s job.

Organizations must understand what they can track and how to mitigate each threat. First, they must know the physical footprint – where threats are coming from, including location and potential groups/organizations targeting them. Second, they must recognize the digital tells (evidence) that outline the activity, aliases, patterns, and psychometric behaviors of bad actors.

To do this, Security Operations (SecOps) must consider and deploy rapid asset discovery and inventory.

- In an attempt to modernize digital infrastructure for high-performance work from home without any compromise on security, many organizations are turning to security platforms that support and enable true endpoint management and endpoint security across all deployed assets and remote workforces.
- By consolidating onto a single cybersecurity platform, or single source of truth, enterprises can holistically detect, triage, and mitigate security incidents more rapidly and more efficiently.
- As the number of network-connected devices grows exponentially, IT organizations must discover unmanaged assets within the network – from public

and hybrid cloud environments to servers, workstations, laptops, VMs, and containers.
- By automating asset discovery and endpoint inventorying, organizations can improve their cybersecurity posture, integrity, and dataflow. Without this, there is a complete inability to protect against even the most basic attack methods, such as exploiting unpatched systems and subsequent lateral movement.

REAL-TIME ENDPOINT PERFORMANCE MONITORING AND CONFIGURATION MANAGEMENT

Most security teams underestimate the importance of performance monitoring, while IT operations tend to focus on performance monitoring and availability as the bellwether. Furthermore, traditional endpoint management, endpoint risk, and security tools scan devices for compliance or security vulnerabilities periodically on an as-needed basis (typically monthly but at times weekly).

Although performance monitoring is a viable way to determine when a system fails or needs maintenance, it can also identify anomalies such as attackers dumping database tables or targeting the boot level – a significant signature of ransomware attacks.

Another core building block for effective and proactive cybersecurity is configuration management. Configuration management databases provide IT and security organizations with a single source of truth to track and manage all aspects of the network, including hardware, endpoints, appliances, network devices, and software, as well as their relationships to and dependencies on each other.

By understanding the relationships and configuration of each endpoint, IT and security operations teams have greater visibility and unity across the organization. By adopting a security platform approach, security operations personnel can identify, find, and fix an anomaly before it becomes a problem. Also, organizations can investigate why the anomaly appeared in the first place, which potentially uncovers and tracks a previously unknown bad actor.

PATCHING AND UPDATES

Like endpoint monitoring, software optimization provides insight into the applications/services deployed on each machine. From an IT operations perspective, software lifecycle management allows for visibility into the warranty, service status, and BIOS and firmware patch/upgrade compatibility. In a recent conversation with a chief security officer (CSO), we found the IT organization had lagged behind nearly 30,000 patches within his organization – especially with remote workers.

Software optimization is often a budgetary tool to ensure companies do not pay for software licenses owned, deployed, or no longer in use. Like a misconfigured firewall, endpoints that are not compliant with the most up-to-date software and patches pose a significant cybersecurity risk to the overall organization.

By having network visibility and a single interface for security, compatibility, and compliance, organizations can decrease their system and business disruption risks while ensuring they cover all corners within the arena.

Computer software and hardware updates are frequent. Most users delay or push off updates, but these updates address security risks for the most part. Before COVID-19, patching was one of the easiest steps security teams could take to reduce risk. However, as the workforce became more distributed, foreign, and uncontrolled, patching and updates became more difficult.

For a department to remain compliant, it is important to have a security platform that ***identifies, controls, and manages all endpoint assets regardless of location.***

DATA RISK AND PRIVACY MANAGEMENT

At the heart of every IT operations and cybersecurity program is the need to protect data and privacy. The next generation of cyber warfare is here, and the main prize is information.

Most successful cyberattacks exploit:

- Failures to patch known vulnerabilities
- Misconfigured firewalls or network infrastructure
- Unsecured databases; or
- Social engineering malware

Taking a holistic, platform-based approach to security, organizations can close the gaps and seal the cracks from a compliance, patching, and deployment perspective and identify or reveal the things that shouldn't make it through the cracks.

In a recent in-field study, we found over 75% of firewalls are misconfigured, largely due to bring-your-own-device (BYOD) policies and requests from executives wanting specific access to devices or opened ports. Some 80% of endpoint devices, including laptops and IoT equipment, have little or no protection, with 35% of these devices using default or weak password protection. Finally, over 60% of remote employees are using corporate credentials to register for online and personal e-commerce services, which creates another level of data risk and privacy management challenges for their employers.

CALL TO ACTION

2021 will not be any easier for CSOs and CISOs than last year. However, forward-thinking organizations are putting the pieces in place to ensure they are ready for whatever comes next. We recommend you:

- **Ensure you have a patching and update program.** This is critical, especially in today's security environment. Nearly 60% of the CSO/CISOs we work with do not know which systems have been patched, which need to be patched, and most importantly, which should be on their networks in the first place.
- **Understand the threat landscape.** It is important to understand which devices and endpoints reside within your network. It is also important to understand the threat landscape, where your devices reside, and who are the probable threats and potential detractors that can harm your business. Intelligence is key.
- **Deploy a plan to protect your customers' data and privacy.** Organizations that ensure their customers' data and privacy will thrive going forward. Having a single platform for managing security, privacy, and data integrity is an excellent step for covering all corners. We have found that 40% of the CSO/CISOs we work with who implement a single platform, flight guides, and a comprehensive incident response program have a 70% improvement in how their organizations respond to cyberattacks, especially when it comes to ransomware.
- **React quickly once your organization is compromised.** While it is difficult to deter sophisticated nation-state attacks, the key is how an organization reacts. The ability to quickly respond to whatever is next is vital to safeguard infrastructure, data, and endpoints. Therefore, turn decentralization and scale into an advantage in the work-from-anywhere era.

To be better prepared for future uncertainties, organizations need to change their approach to managing their IT operations and endpoint security. Now is the time to leverage a powerful integrated platform that delivers full visibility and control of your entire estate. Bringing greater agility and efficiency to your organization with insight, manageability, and security will keep business at the forefront of technology and where digital business begins – **at the endpoint**.

Important Information About This Paper

CONTRIBUTOR

Christopher Wilder, Senior Analyst at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Principal Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

DISCLOSURES

This paper was commissioned by Tanium. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.