



Views from the C-suite:

**Why endpoint
management is
more critical than
ever before**





Views from the C-suite:

Why endpoint management is more critical than ever before

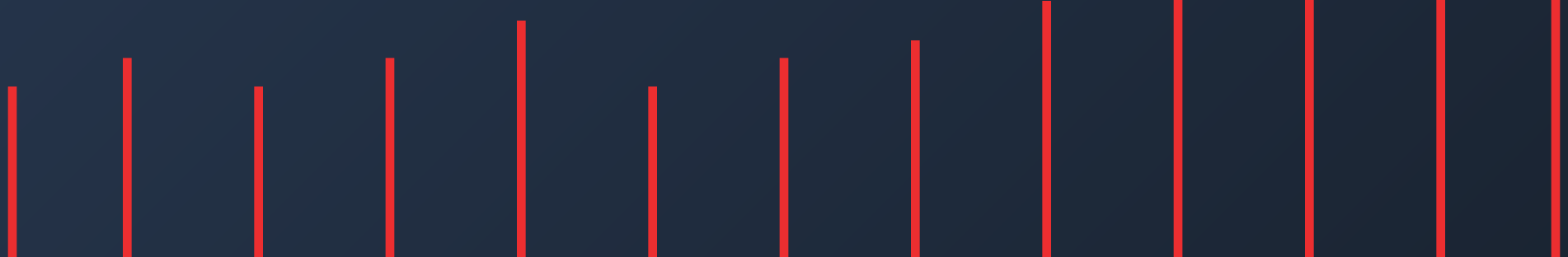
Endpoints are the new network edge. Defending them is critical.

Cloud architectures and remote workforces have effectively dissolved the network perimeter, the traditional line of defense for IT security. Lacking that decisive boundary, the work of security teams has changed. Now to guard against data breaches, ransomware, and other types of cyber threats, protecting network endpoints is more important than ever.

But protecting endpoints is a daunting challenge, in part because the scope of the work is so vast. Endpoints encompass everything from employee laptops, desktops, and tablets to on-premises servers, containers, and applications running in the cloud. Done right, endpoint security requires a more comprehensive and flexible strategy than security teams might have relied on a decade ago when IT assets were nearly all on-premises and protected by a firewall.

In this eBook, we take a quick look at the biggest IT security threats now, consider their impacts on endpoints and endpoint management, and offer some best-practice guidelines from IT security leaders.

In 2021, 26% of attacks led to disruptions that lasted a week or longer.
In 2022, that number jumped to 43%



The evolving threat landscape

Ransomware and other threats continue to evolve, evading previously successful defense strategies.

Ransomware continues to be a major threat to organizations of all sizes. After declining for a couple of years, ransomware attacks are on the rise again. They increased 23% from 2021 to 2022.

Not only are attacks more frequent, they're also more disruptive. In 2021, 26% of attacks led to disruptions that lasted a week or longer. In 2022, that number jumped to 43%.¹

On average, each of these attacks cost its victim \$4.54 million, including

ransom payments made as well as costs for remediation.²

As bad as these numbers are, they're poised to get worse. That's because in the past year, attackers have adopted new models for extorting money from victims.

The original idea behind ransomware was to encrypt victims' data and prevent them from decrypting it unless they paid a ransom with cryptocurrency. But as companies got better at segmenting their networks

and making secure backups, this mode of attack became less effective. Companies could skip the ransom, restore their data more or less to its previous state, and continue operating as usual.

In the face of this resistance, attackers have shifted their strategy.³ Instead of threatening to leave companies' data encrypted indefinitely, now they threaten to release it to the public, leaking personal information, financial records, support logs, source code, patent filings, and whatever other valuable data they have managed to access.

This second level of extortion is even easier for attackers to manage than the first. That's because encrypting vast amounts of data is difficult. Attackers often rely on affiliates with expertise in encryption. But even with that expertise, encryption doesn't always work as planned. Sometimes data isn't encrypted correctly. Sometimes it ends up corrupted instead. Then companies can't decrypt their data even if they pay the ransom.

If other companies learn that a particular ransomware gang's decryption software doesn't work, they're not likely to pay the ransom when their own data is encrypted as part of an attack.

But criminals don't necessarily need to rely on encryption at all if their plan is simply to steal victims' data to a remote location. No company wants to have its internal data leaked to the public. That data could sour relations with customers and partners, making it hard to regain reputational brand damage. It could also reveal trade secrets, forever eroding competitive advantage.

Attackers might also attempt a third level of extortion: contacting customers, partners, and employees of the company directly and letting them know that their data has been surreptitiously copied. The attackers then encourage these stakeholders to urge the company to pay the ransom, so the data won't be leaked. Or they demand that these stakeholders make their own ransom payments to protect their personal data. The Clop criminal gang adopted this strategy in 2021, demanding two ransoms: one for decrypting data, and another for not having that data leaked to the public.⁴

With three levels of extortion now possible, the stakes from ransomware are higher than ever.

To guard against these new forms of extortion, it's not enough to have backups of your data. Now you need to protect your data, wherever it is. That means you need to secure all your endpoints, wherever they are, so that they don't become gateways to an attack.



How ransomware reaches endpoints

How does ransomware reach endpoints? In its recent research reports, analyst firm IDC identified these paths:

- Opening a malicious attachment or clicking a link in a phishing email
- Falling victim to a drive-by compromise in which malicious adversaries gain access to an endpoint in the course of normal internet browsing
- Accessing peripheral devices or removable media infected with malware⁵

Vulnerabilities are now one of the leading sources of data breaches. Patching is more critical than ever before. But patching requires visibility into all endpoints—something that most organizations lack.



“The more difficult we make it for criminals to hack authentication systems, the more they’ll rely on software vulnerabilities for attacks. Vulnerabilities are always going to occur. That’s why you’ve got to find them and patch them so quickly. That’s also why you see such a rise in companies establishing bug bounty programs. Internal teams and software vendors themselves know the stakes have never been higher.”

Tim Morris
Chief Security Advisor, Americas
Tanium



Business email compromise (BEC) attacks

Another prevalent form of attack is a business email compromise (BEC). In this type of attack, criminals send an email impersonating a trusted business contact, such as a company CEO, an HR director, or a purchasing manager. The email, often written to convey a sense of urgency, instructs the recipient to pay an invoice, wire money, send W-2 information, send serial numbers of gift cards, or to take some other action that appears legitimate, even if unusual. If the recipient follows these instructions, the requested money or data is actually sent to the criminals, not the purported recipient. Funds might even be surreptitiously converted to cryptocurrencies along the way, making recovery almost impossible.

Between June 2016 and December 2021, the FBI recorded over 240,000 national and international complaints about BEC attacks, which cumulatively resulted in losses of \$43 billion. Ransomware might make more headlines, but BEC attacks are 64 times as costly.⁶ And they are becoming more frequent, increasing 65% between 2019 and 2021.⁷

BEC attacks are very difficult to detect because criminals have become quite skilled at impersonating CEOs and other company executives. They can glean a lot of personal information about these executives and their personal lives — including their social activities, families, philanthropic work, and travel schedules — from social media accounts, news articles, and other sources. This enables them to send messages that include information recipients might think only the executive being impersonated would know.

Criminals can also intercept legitimate email threads, and then send a message that appears to be a response from a party in the thread. Since the other messages in the thread are legitimate, recipients assume the BEC message is legitimate, too. Then they act on the instructions included in the message.

Now that employees are working remotely, they are even more susceptible to these forms of attack.⁸

In BEC attacks, endpoints themselves are not necessarily compromised. Rather, endpoints become the staging grounds where the attack takes place. As such, they can provide valuable contextual information to security teams trying to understand how the attack took place and what other related threats might be lurking.



Strategies for endpoint management

How should IT security teams respond to these evolving threats? Here are 10 suggestions.

1

Treat endpoints as the new network edge.

With so many people working remotely and 48% of applications running in the cloud, it's time to recognize that the new line of defense is around every endpoint, no matter where it is and what type of network connection — VPN or not — it's operating with.

2

Ensure you have a way of identifying all devices connecting to the network, even personal devices not officially authorized for use.

“You can't secure what you can't manage,” says Tim Morris, Chief Security Advisor for the Americas at Tanium. “And you can't manage what you don't know.” Security Operations Centers need to ensure they can know about all the endpoints they are responsible for. In-depth audits of enterprise networks routinely find that endpoint management systems miss about 20% of endpoints. SOC teams should put tools and processes in place to ensure that they have a complete inventory of endpoints and can monitor the status of those endpoints in real time.



3

Keep in mind that even if you issue employees hardened devices, most of them will continue to also use personal devices as well.

The BYOD era isn't over yet. When IDC asked users if they would continue using personal devices for work even if their employer provided them with devices, most said they would continue to use personal devices at least some of the time. Endpoint security strategies need to take into account the idea that many endpoints connecting to the network and handling sensitive data will be personal devices over which the security team has only partial control.

4

Patch continually.

Patching has always been important to ensure that endpoints have access to the latest features and bug fixes. But now that software vulnerabilities have emerged as a major inroad for attackers, rivaling stolen credentials as a vector for data breaches, it's more important than ever before to ensure that patches are applied promptly. Organizations can't hope to respond to supply chain attacks like Log4j without automated solutions for software bills of materials and patching in place.

5

Gain visibility into software components on endpoints, so you can be ready for the next supply chain attack.

Supply chain attacks take advantage of vulnerabilities in software components that are widely used in enterprises today in both commercial applications and applications developed internally. When the Log4j vulnerability was announced, criminals wasted no time developing new attacks to take advantage of the Log4j's weakness, knowing that the advantage was theirs as long as enterprises struggled to identify vulnerable applications and patch them. To defend against future attacks like these, SOC teams need real-time visibility into all the software components installed on endpoints, so that dangerous loopholes can be quickly closed. It's time for security teams to make having a software bill-of-materials (SBOM) a standard requirement for any SOC toolset.

6

Enforce multifactor authentication to make it harder for attackers to take advantage of compromised endpoints.

Phishing attacks continue to trick employees into divulging their login credentials. Criminals can also access login credentials by hacking into directory servers or data breaches or leaked by malicious insiders. To make it harder for criminals to take advantage of these credentials, it's a good idea to enforce multifactor authentication (MFA) wherever possible — especially for back-office systems and consoles used for network management and other IT functions. Multifactor authentication requires a user to use different, unrelated types of data or actions to authenticate. These factors are usually described as something you know (e.g., a password), something you have (e.g., hardware token), and something you are (e.g., a biometric signifier such as a fingerprint).

7

Get endpoint context.

When attacks occur, it's important to respond as quickly as possible. To respond effectively, security teams need to understand what's happening on the affected endpoints, no matter where in the world they are. Which processes are running? What network traffic is taking place? What files have been recently downloaded? What was the patch status? It was easier to perform this type of investigation when all endpoints were on-premises. Now analysts might need answers in minutes from endpoints thousands of miles away. And they don't have time to install new software or hope that the remote user can help them set up a connection. Security teams need to have a system already in place for analyzing endpoints and collecting this data, so that when any type of attack occurs — even attacks like BEC attacks — they can collect the contextual information needed for understanding exactly what happened and what threats remain active. Make sure your organization has the ability to get contextual information for any endpoint, anytime, anywhere.



“Endpoint monitoring won't stop a BEC attack, but it might tell you a little more about the person who actually opened the email and then what they did with it, and where did they go or what else was going on. Context can give you the clues you need for determining whether this attack isn't part of a broader campaign, reaching other recipients with deceptive messages.”

Tim Morris
Chief Security Advisor, Americas
Tanium



8

Think like a first responder.

Can you act quickly to diagnose problems and act quickly to contain them? Does your team have the tools, training, and processes they need? Be sure your team can spring into action when endpoints anywhere are attacked.

Minutes matter. A rapid response can contain threats before they spread to other endpoints and locations, potentially saving an organization millions of dollars.

“Stay ready so you don’t have to get ready.”

Tim Morris, Chief Security Advisor, Americas

9

Drill.

Once you have a cybersecurity plan, a cybersecurity toolset, and a trained staff, it’s important to practice hunting for threats and responding to attacks of all kinds. It’s helpful to take a Red Team/Blue Team approach, pitting a team of trusted security analysts assigned to break into a network against a team of other trusted security analysts to defend.⁹ No matter the organization, these drills almost always uncover gaps in security coverage, highlighting the need for new tools or processes. Drills also help teams learn to build trust and work together more effectively.

10

Think big.

The number of endpoints is only going to increase. Security teams should put tools and processes in place now, so they can have effective security strategies and controls in place when they have many more endpoints to monitor, manage, and protect.

Conclusion

Cyber threats like ransomware are increasing, and endpoints are more varied, numerous, and distributed than ever before. By following the strategies outlined in this eBook, security teams can reduce the risk of cyberattacks and ensure that when attacks occur, they can be contained quickly and efficiently.

To learn more about Tanium's Converge Endpoint Management (XEM) solution, visit www.tanium.com.

Endnotes

- 1 IDC, Michael Suby, Tanium Converge presentation, 2022.
- 2 *Cost of a Data Breach Report 2022*, IBM. <https://www.ibm.com/reports/data-breach>
- 3 <https://www.darkreading.com/vulnerabilities-threats/fool-me-thrice-how-to-avoid-double-and-triple-ransomware-extortion->
- 4 <https://krebsonsecurity.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/>
- 5 *Future Enterprise Resiliency & Spending Survey*, March 2022, cited by IDC Vice President Michael Suby
- 6 <https://www.lifars.com/bec-attacks-account-for-losses-64-times-worse-than-ransomware/>
- 7 <https://www.techrepublic.com/article/fbi-43-billion-losses-are-business-email-compromise-fraud-between-2016-2021/>
- 8 Business Email Compromise: The \$43 Billion Scam, FBI Public Service Announcement, Alert I-050422-PSA, March 4, 2022, <https://www.ic3.gov/Media/Y2022/PSA220504>
- 9 https://csrc.nist.gov/glossary/term/red_team_blue_team_approach



Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on [LinkedIn](#) and [Twitter](#).

© Tanium 2023