Microsoft Security

Issue 2

CISO Insider

Welcome to the second issue!

Explore

- Ransomware: Help prevent breaches, limit lateral movement, and minimize downtime
- Coordinate signals across the entire ecosystem for effective detection and response
- Use automation to elevate your team's impact

Letter from Rob

Welcome to the second issue of *CISO Insider*. I'm Rob Lefferts, I lead the Microsoft 365 Defender and Sentinel engineering team. At Microsoft Security, we are continually listening to and learning from our customers as they navigate an increasingly complicated security landscape. We designed *CISO Insider* to be a vehicle that shares recommendations we have gleaned from your peers and from our own industry research. In this second issue, we follow up on the vulnerabilities we surfaced in Issue 1, taking a closer look at cyber extortion and the practices security leaders are using to contain such lateral attacks with minimal disruption to the business and the security team.

Executive summary

In Issue 1, we discussed three top of mind concerns for CISOs: adapting to emergent threat trends in a hybrid, multicloud environment; managing supply-chain threats; and addressing the security talent shortage. In this issue, we will take a closer look at this perfect storm of cyber risk factors and determine how organizations are evolving their tactics to defuse escalating threats. First, we examine the changing risk profile of ransomware and the best practices that can help prevent these and other breaches that spread laterally throughout the network. Next, we look at two key resources that are critical in not only helping to prevent a breach but responding quickly in those first critical moments—extended detection and response (XDR) and automation. Both help address vulnerabilities we covered in Issue 1: the extended security and identity boundaries of todays' networks dispersed across hybrid work and supplier ecosystems, and the scarcity of human resources for monitoring and responding to those threats.

Topics

01 /

Ransomware

Help prevent breaches, limit lateral movement, and minimize downtime through planning, segmentation, encryption, and redundancy

02 /

Extended detection and response (XDR)

Coordinate signals across the entire ecosystem—not just endpoints—for effective detection and response

03 /

Automation

Use automation to elevate your team's impact

Ransomware

Defending against ransomware requires more than just strong endpoint security

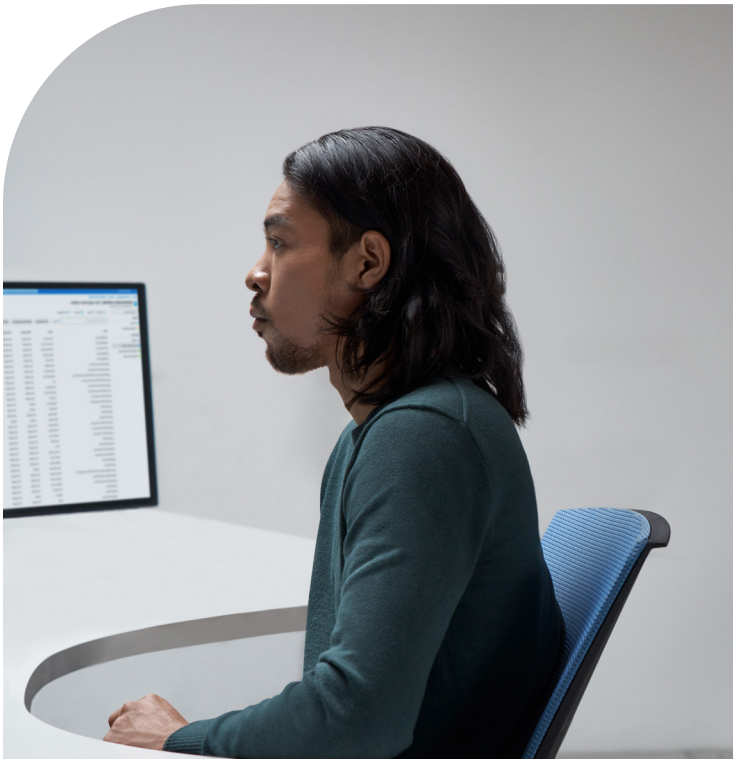
The cybercrime economy is giving average cybercriminals access to better tools and automation to enable scale and drive down costs. When combined with the economics of successful attacks, ransomware is on a rapid trajectory (Microsoft Digital Defense Report, 2021). Attackers have raised the stakes by adopting the double-extortion model, in which a victim is first extorted for ransom and then for the possible publishing of their stolen data. We've also seen a rise in attacks that target operational technology assets to disrupt critical infrastructure. CISOs differ on which is the more catastrophic cost to the business, the business disruption or the data exposure, depending on their industry and their level of preparation. Either way, preparation is the key to managing the risk on both fronts. In addition to mitigation tactics, successful preventative efforts such as stronger endpoint security, identity protection, and encryption are essential given the frequency and severity of these attacks.

CISOs are thinking more strategically on how to address their ransomware risks.

Ransomware attackers are targeting your most valuable assets where they feel they can extract the most money from you, be it the most disruptive or valuable if held hostage, or most sensitive if released.

Industry is an important determinant of an organization's risk profile—while manufacturing leaders cite business disruption as the top concern, retail and financial services CISOs prioritize the protection of sensitive personally identifiable information; healthcare organizations, meanwhile, are equally vulnerable on both fronts. In response, security leaders are aggressively shifting their risk profile away from data loss and exposure through the hardening of their perimeters, backups of critical data, redundant systems, and better encryption.

Business disruption is now the focus for many leaders. The business incurs costs even if the interruption is brief. One healthcare CISO recently told me that, operationally, ransomware was no different than a major power outage. While an adequate backup system can help restore the power quickly, you still have downtime that interrupts the business. Another CISO mentioned that they're thinking about how disruption can extend beyond their main corporate network to operational concerns such as pipeline issues or the secondary effect of key suppliers shut down by ransomware.



Ransomware

Tactics for managing disruption include both redundant systems and segmentation to help minimize downtime, allowing the organization to shift traffic to a different part of the network while containing and restoring an affected segment. However, even the most robust backup or disaster recovery processes can't fully solve the threat of business disruption or data exposure. The flip side of mitigation is prevention.

To help protect your organization from ransomware, we recommend that you:

1. Prepare to defend and recover.

Adopt an internal culture of Zero Trust with assumed breach, while deploying a system of data recovery, backup, and secure access. Many security leaders have already taken the crucial step of mitigating the impact of an attack through backups and encryption, which can help defend against data loss and exposure. It's important to shield these backups against deliberate erasure or encryption by an attacker by designating protected folders. With a rehearsed business continuity/disaster recovery (BC/DR) plan in place, the team can take affected systems offline quickly and disrupt the progress of the attack, restoring operations with minimal downtime. Zero Trust and secure access help an organization defend and recover by isolating the attack and making it much harder for attackers to move laterally across the network.

2. Protect identity from compromise.

Minimize the potential for credential theft and lateral movement with the implementation of a privileged access strategy. An important step in defending against ransomware is a comprehensive audit of your organization's network credentials. Privileged credentials are foundational to all other security assurances—an attacker in control of your privileged accounts can undermine all other security assurances. Microsoft's recommended strategy is to incrementally build a 'closed loop' system for privileged access that ensures only trustworthy 'clean' devices, accounts, and intermediary systems can be used for privileged access to business sensitive systems.

3. Prevent, detect, and respond to threats.

Help defend against threats across all workloads by leveraging comprehensive, integrated threat detection and response capabilities. Siloed point solutions often result in preventative gaps and slow down the detection and response to pre-ransom activities. Microsoft offers an integrated SIEM and XDR to provide a comprehensive threat protection solution that delivers best-in-class prevention, detection, and response across your entire multicloud, multi-platform digital estate.

Ransomware

These three best practices interlock to form a comprehensive security strategy, with integrated data, identity, and network management founded on a Zero Trust approach. For many organizations, implementing Zero Trust calls for a broader security transformation. While most security leaders are moving toward Zero Trust, some have expressed concern that a segmented environment might disrupt worker or security team productivity too much to be worth moving quickly into heavy segmentation.

While every organization has its own requirements that it needs to work around, I'd like to state that it is possible to get the best of both worlds—access *and* security. Segmentation does not need to be disruptive. We see this benefit especially when organizations combine identity management with security transformation efforts like implementing passwordless authentication, so users don't have to manage a bunch of disruptive logins. Stolen credentials are the entry point for most attacks—for example, over 80 percent of web application breaches were due to stolen credentials, according to the 2022 Verizon Data Breach Investigation Report (DBIR)—passwordless also helps close this critical security gap.

"Securing devices is important, but it's not enough. We should also be focused on securing individuals. We can enhance your experience and security by letting you become the password."

– Bret Arsenault, Microsoft's CISO

Ransomware

A comprehensive approach to ransomware requires great tools

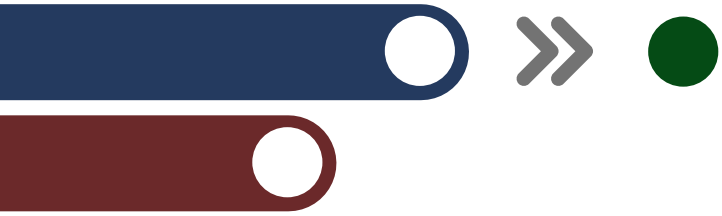
Many of the CISOs I talk with are taking a palette approach to attack prevention and detection; utilizing layers of vendor solutions that cover vulnerability testing, perimeter testing, automated monitoring, endpoint security, and identity protection, etc. For some, this is intentional redundancy, hoping that a layered approach will cover any gaps—like stacks of swiss cheese, in the hope that the holes won't line up.

Our experience has shown that this diversity can complicate remediation efforts, potentially creating more risk exposure. The downside of assembling multiple solutions is a lack of visibility due to fragmentation.

With attackers weaving a complex web that extends across multiple disparate solutions, it can be hard to get a complete picture of the kill chain, identify the extent of the compromise, and fully root out any malware payloads. Stopping an attack in progress requires the ability to look across multiple vectors to detect, deter, and contain/remediate attacks in real time.

"I do have a best-in-breed approach, which in itself presents certain challenges because then there is a lack of insight into aggregate risks because you have these independent consoles that you're managing threats, and not having this aggregate view of what is going on in your place."

– Healthcare, 1,100 employees



The bottom line?

A comprehensive, integrated solution helps you manage vulnerabilities so you can reduce your attack surface and distinguish the critical signals from the noise. This simplicity is crucial for organizations struggling to distinguish a real threat from the steady stream of alerts and false positives.

Extended detection and response (XDR)

Help defend against ransomware and other sophisticated attacks with XDR

Many security leaders are turning to extended detection and response (XDR) for this cross-platform vantage point. XDR helps **coordinate** signals across the entire ecosystem—not just endpoints—to facilitate faster detection and response of sophisticated threats.

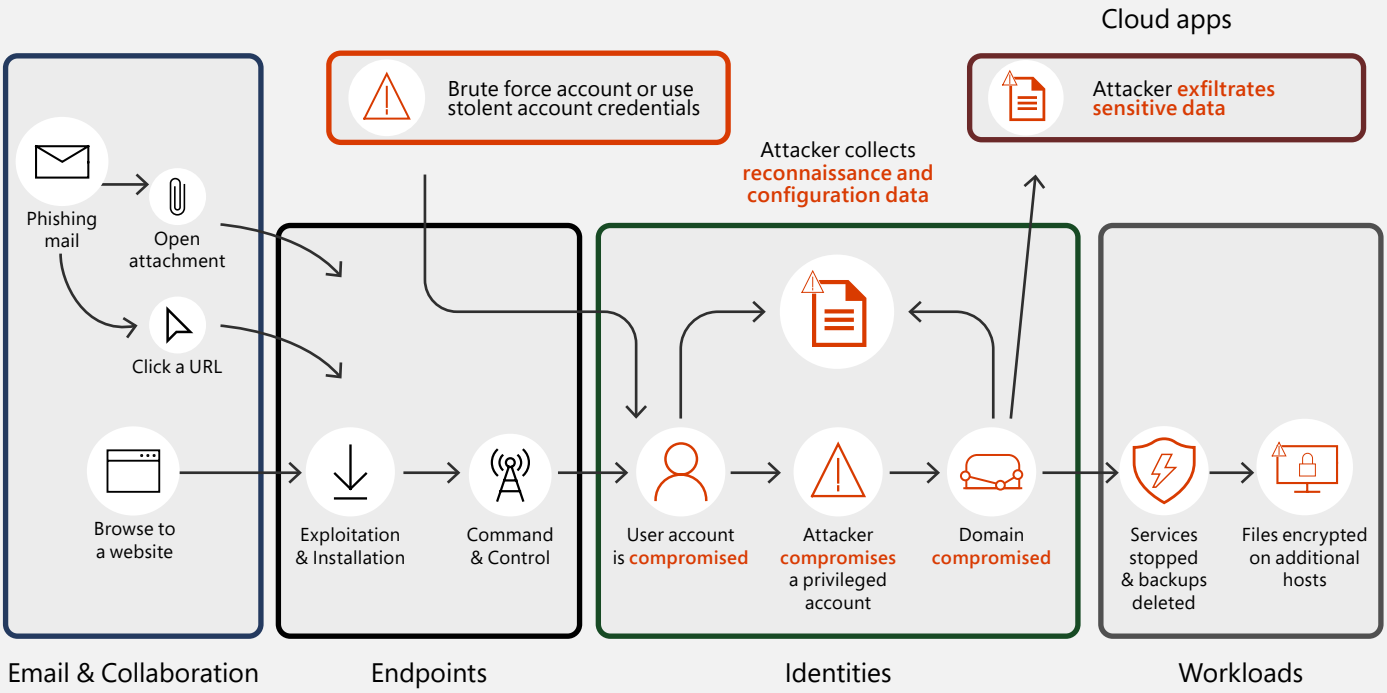
XDR works like endpoint detection and response (EDR) but covers more ground, extending security threat detection and incident response across the entire digital environment—including identities, infrastructure, apps, data, networks, clouds, etc.

This expansive scope is critical given the sophistication of modern attacks that take advantage of today's complex, distributed environment to move laterally across domains. Attacks are increasingly proceeding in a non-linear fashion, moving laterally across different clouds, email, SaaS applications, etc.

XDR can help you bring the data from all your disparate systems together so you can see the entire incident from end to end. Point solutions can make this comprehensive visibility difficult because they only show part of the attack and rely on an often-overwhelmed security team to manually correlate multiple threat signals from different portals. Ultimately, this can make it time-consuming to fully remediate a threat—and in some cases, even impossible.

Example of a typical ransomware attack

Siloed tools make uncovering the entire kill chain extremely difficult



Extended detection and response (XDR)

Making the leap from EDR to XDR

The promise of XDR remains unrealized by most. Many CISOs we talk to have implemented a powerful starting point in EDR. EDR is a proven asset: we have seen that current endpoint detection and response users have a track record of detecting and stopping ransomware faster.

However, because XDR is an evolution of EDR, some CISOs remain skeptical about XDR's utility. *Is XDR just EDR with some point solutions tacked on? Do I really need to use an entirely separate solution, or will my EDR eventually offer the same capabilities?* The current market for XDR solutions adds further confusion as vendors race to add XDR offerings to product portfolios. Some vendors are expanding their EDR tool to incorporate additional threat data while others are more focused on building dedicated XDR platforms.

The latter are built from the ground up to deliver out-of-box integration and capabilities centered around the needs of the security analyst, leaving the fewest gaps for your team to have to fill in manually.

The bottom line?

XDR is so compelling in today's security environment because of its coverage and speed in detecting and containing threats. As ransomware and other malicious attacks become more and more common (one interviewee stated that his org is attacked on average ***daily***), security leaders see automation as a critical tool, offering 24/7 monitoring and near real-time response.

Automation

Use automation to elevate the security team

Faced with a security talent shortage and the need to respond quickly to contain threats, we have encouraged leaders to employ automation to help free up their people to focus on defending against the worst threats instead of handling mundane tasks like resetting passwords. Interestingly, many of the security leaders that I've talked to mentioned that they're not taking full advantage of automated capabilities yet. In some cases, security leaders aren't fully aware of the opportunity, while others hesitate to embrace automation for fear of losing control, inviting inaccuracy, or sacrificing visibility into threats. The latter is a very legitimate concern. However, we're seeing the effective automation adopters achieve just the opposite—more control, fewer false positives, less noise, and more actionable insight—by **deploying automation alongside the security team to guide and focus the team's efforts.**

Automation

Automation covers a range of capabilities from basic automated administrative tasks to smart machine learning-enabled risk assessment. Most CISOs report adopting the former, event-triggered or rule-based automation, but fewer have taken advantage of built-in artificial intelligence and machine learning capabilities that enable real-time risk-based access decisions. Certainly, automating routine tasks helps free up the security team to focus on the more strategic thinking that humans do best. But it's in this strategic realm—in triaging incident response, to name one example—that automation has the most potential to empower the security team as a data-crunching, pattern matching, intelligent partner. For example, AI and automation are adept at correlating security signals to support comprehensive detection and response to a breach. About half of security practitioners that we recently surveyed said they must manually correlate signals.[1] This is incredibly time consuming and makes it almost impossible to respond quickly to contain an attack. With the right application of automation—like the correlation of security signals—attacks can often be detected in near-real-time.

"We need AI because we have thin profit margins and can't hire too many people."

– Restaurant/hospitality, 6,000 employees

Automation

We've found many security teams are under-utilizing the automation built into existing solutions they already use. In many cases, applying automation is as easy (and high-impact!) as configuring available features like replacing fixed-rule access policies with risk-based conditional access policies, creating response playbooks, etc.

CISOs who choose to forgo the opportunities of automation often do so out of distrust, citing concerns about the system making irrecoverable errors while operating without human oversight. Some of the potential scenarios include a system inappropriately deleting user data, inconveniencing an executive who needs access to the system, or worse, lead to a loss of control or visibility about a vulnerability that has been exploited.

But security tends to be a balance between daily small inconvenience weighed against the constant threat of a catastrophic attack. Automation has the potential to serve as an early warning system for such an attack and its inconveniences can be mitigated or eliminated. And besides, automation at its best does not run on its own but alongside human operators, where its artificial intelligence can both inform and be checked by human intelligence.

To help ensure a smooth deployment, we've been adding report-only modes to our solutions in order to offer a trial run before rollout. This allows the security team to implement automation at their own pace, finetuning automation rules and monitoring the automated tools' performance.

"Whenever we try to put things in place that are automatic, it sometimes scares me because what am I overwriting? What am I recovering from? Well, what, what made this action come into play"

– Financial services, 1,125 employees

Automation

The security leaders who are using automation most effectively deploy it alongside their team to fill gaps and serve as a first line of defense. As one CISO recently told me, it's nearly impossible and prohibitively expensive to have a security team focused everywhere at all times—and even if it were, security teams are prone to frequent turnover. Automation provides a layer of always-on continuity and consistency to support the security team in areas that require this consistency, such as traffic monitoring and early warning systems. Deployed in this supportive capacity, automation helps free the team from manually reviewing logs and systems and allows them to be more proactive. Automation doesn't replace humans—these are tools that empower your people to prioritize alerts and focus their efforts where it counts most.

The bottom line?

The most powerful defense strategy combines AI and automated tools with the more nuanced vigilance and tactical response of a security team. Beyond the immediate benefits of completing tasks and taking immediate action to contain an attack, automation helps empower the team to manage their time and coordinate resources more effectively so they can focus on higher-order investigative and remediating activities.

Look to our next issue for more security analysis and insights.
Thanks for reading the CISO Insider!

Learn more

Explore the latest cybersecurity insights and updates at Microsoft Security Insider.
www.microsoft.com/security-insider

[1]2021 Microsoft research study of CISOs and security practitioners

All cited Microsoft research uses independent research firms to contact security professionals for both quantitative and qualitative studies, ensuring privacy protections and analytical rigor. Quotes and findings included in this document, unless specified otherwise, are a result of Microsoft research studies.