REDUCE STRATEGIC RISK BY RETHINKING YOUR ENDPOINT SECURITY

Unrelenting breaches of sensitive data are driving aggressive scrutiny and increasing penalties from regulators. Enterprises can confront this strategic risk by focusing on the primary point of contact between attackers and critical data: endpoints.

EXECUTIVE SUMMARY

Organizations face strategic risks related to data stored or processed on laptops, workstations, and servers, also known as endpoints. These risks are driven by four key trends:

- The increase in **regulatory penalties** for inadequate information security.
- The ability of **well-resourced state actors** to develop exploits against widely-used trusted software, giving attackers rapid, widespread access to vulnerable networks.
- The **expansion of ransomware** attacks to include extortion demands to retrieve stolen data or prevent its disclosure.
- The **increasing incentives for insiders** to participate in externally-driven cyber attacks.

Collectively these trends point to the potential for most large organizations to incur enormous unexpected costs due to regulatory penalties, actual breaches, or insider attacks. These risks are located primarily on endpoints. Securing them, which has been important for some time, is only getting more critical.

Organizations can reduce the regulatory, breach, and insider-related risks they face by focusing on specific improvements to endpoint security. Recent advances in technology have made it possible to arm security teams with powerful tools to quickly detect malicious events, and to conduct proactive investigations to discover malicious activity and prevent it from becoming catastrophic.

INDICATORS OF GROWING RISK

In its 2021 Global Business Risk Barometer, Allianz found cyber incidents to be the third highest risk faced by businesses, after only business interruption and the pandemic.

Organizations with customer data or valuable intellectual property must contend with growing efforts by outsiders to capitalize on the information they host. A 2019 report by the US Department of Homeland Security found that "the cyber threat landscape is distinguished by an expanding set of actors" and attributed this to the "low barrier of entry for new actors" and the diffusion of expertise from former government and intelligence operatives and commercial practitioners to threat actors.

COMMON THREAT SCENARIOS

External cyber attacker:

- Steals data to sell it for profit.
- Steals data to extort a ransom payment.
- Encrypts data to extort a ransom payment.
- Encrypts data to disable the organization.

Internal authorized user:

- Steals intellectual property (IP) or personally identifiable information (PII) to sell it or commercialize it.
- Executes fraudulent transactions for personal gain.
- Steals IP at the behest of a third party such as a prospective employer.
- Publicizes information to embarrass the organization.

We find seven recent events illustrate the risk environment today.

REGULATORY RISK

- In July 2019 Equifax agreed to pay at least $575M as part of a global settlement for failing to take "reasonable steps" to secure its network. Regulators found Equifax culpable for failing to prevent a data breach that affected 147M people.
- In October 2020, the UK Information Commissioner's Office (ICO) fined British Airways £20M, ICO's largest fine to date. ICO concluded BA had failed to protect customer data that was compromised in a 2018 cyber attack.

INSIDER THREAT RISK

- In August 2020, a Tesla engineer was recruited by a representative of a Russia-based ransomware group. The Tesla engineer was offered $1M to execute ransomware on his work computer. Though he declined to participate, the story revealed the incentives in play as external actors seek **insiders to cooperate** with them.
- In August 2021, the black market price of a Domain Administrator credential to an attractive ransomware target organization was 12 BTC, or about $590,000 according a report by KE-LA. This implies a tremendous incentive for System Administrators to sell usernames and passwords.

CYBER THREAT RISK

- In December 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an Emergency Directive stating SolarWinds Orion products were currently being exploited by malicious actors. At least 18,000 SolarWinds customers worldwide were affected; over 200 were actively targeted in attacks initiated via an apparently legitimate update to the Orion product.
- In March 2021 Microsoft announced a series of vulnerabilities discovered in Microsoft Exchange. Attacks on these vulnerabilities, dubbed Hafnium, allowed remote control of compromised Exchange servers, and affected 21,000 organizations worldwide.
- In May 2021, the ransomware attack on Colonial Pipeline resulted in a shutdown of the company's entire gasoline pipeline system.

Taken together, these events place the modern enterprise in an uncomfortable squeeze between regulators and internal and external threat actors.

IMPLICATIONS FOR TODAY'S ORGANIZATIONS

Among the implications of these events, we would like to focus on four in particular.

1. **In the wake of a breach, regulators are closely scrutinizing the victim organization's information security programs and imposing more fines.** One study found GDPR fines rose by nearly 40% between January 2020 and January 2021. The FTC's complaint against Equifax alleged twelve specific shortcomings in its security program including that it failed "to monitor or log privileged account activity across numerous systems."[1] The ICO's Penalty Notice to BA alleged its failure to use application whitelisting and blacklisting contributed to the breach[2]. In the past these shortcomings might have been overlooked. Now they provide the basis for significant fines. *Prevention via automation and rapid detection and response, and demonstration of vigilance in security programs, reduces the risk of regulator-induced pain.*
2. **Compromising legitimate software updates gives attackers instant, global-scale access.** The group behind the SolarWinds attack managed to compromise the Texas software company's update infrastructure. This enabled them to cause malware to be deployed to some 18,000 systems worldwide. Some affected organizations had dozens of SolarWinds servers that had to be examined for evidence of compromise, even as incident response firms worldwide were overwhelmed by demand. In the case of Hafnium, a similar requirement was leveraged for on-premise Microsoft Exchange servers.

   In both cases, industry and government agencies provided valuable threat intelligence in the form of IP addresses, file hashes, command lines, and other indicators. Those enterprises that were able to efficiently search for and detect these indicators found and evicted the attackers. *These are dramatic illustrations of the need for organizations to be able to conduct large-scale cyber investigations at speed.*
3. **Ransomware attacks, now a proven way to make money, are expanding in scope, leading to longer attacker dwell time**. Recent attacks have featured extortion not just to decrypt data, but also to prevent the attacker from disclosing sensitive information. Obtaining that information requires the attacker to be present on the network for some time, *giving network defenders an opportunity to detect and evict them before they can execute the ransomware.*
4. **The incentives for employees and authorized users to cooperate with external attackers are growing**. While the effort to coopt the Tesla engineer was thankfully thwarted, it illustrates cyber attackers' willingness and ability to target insiders. At the same time, the advent of specialists who focus on acquiring and marketing initial access to ransomware operators reveals the black market value of information that it is trivial for most System Administrators to acquire. These evolving incentives represent one more reason to *appropriately monitor employees who have access to sensitive data, particularly privileged users.*

RISK REDUCTION STARTS WITH ENDPOINTS

A substantial driver of risk for many organizations is the lack of capability to secure the endpoints used to store and process critical information: laptops, desktops, servers, virtual machines, and increasingly, mobile devices.

Capability weaknesses on endpoints make it more difficult both to prevent direct risks and to demonstrate regulatory compliance required to avoid punitive fines. Historically, organizations have relied heavily on two endpoint technologies to manage risk: antivirus software and data loss prevention products.

Antivirus software is an important layer of defense against malware, but many modern attacks don't use traditional malware. External attackers, and particularly those associated with strategic threats, are more likely to make use of utilities that already exist in the target environment – e.g. to live off the land. Antivirus products have a hard time detecting malicious use of these tools. Antivirus tools also aren't effective against deliberate malicious behavior by authorized users.

Some organizations rely on DLP tools to secure endpoints from insider threats. DLP can help detect sensitive data exfiltration. However, they cover only one portion of the insider threat "kill chain" – the final movement of data off the endpoint – and generally do not support broader analysis of user behavior. Common blind spots include document manipulation and internal staging of information in preparation for theft, and the use of file sharing and secure chat applications to move data outside the corporate network.

Risks from authorized users also go beyond data theft. Behaviors such as discrimination, harassment, and substance abuse are usually at odds with enterprise values. Detecting these behaviors helps protect employees from a hostile work climate and assure their well-being, while also protecting the organization from potentially costly complaints and lawsuits by affected employees.

Increased reliance on remote work has also created new visibility gaps for security teams, which have traditionally relied on a variety of network-level tools to detect and investigate threats. Unlike endpoint monitoring, many network monitoring tools are not available when employees are primarily working from home.

CRITICAL QUESTIONS

Organizations seeking to drive down strategic risk by improving their endpoint security posture can ask four key questions of their current capabilities.

1. **How good is our visibility?** Most security teams' understanding of what is happening at any given moment on their endpoints is limited. Increasingly, security teams need the ability to know what is happening on a given system even when there is no alert. This visibility requirement spans system, network, and user activity. Critically, having good visibility isn't just about tooling. It also requires the expertise to interpret the data the tools provide.
2. **Can we investigate our systems both broadly and deeply?** It is very likely that future supply chain compromises and exploits of zero day vulnerabilities similar to the SolarWinds and Hafnium scenario will require security teams to quickly examine dozens or even hundreds of systems for newly revealed indicators of compromise. The ability to perform this task with speed and efficiency will be increasingly essential. No less important is the need to seamlessly move into a deeper forensic examination when the situation calls for it.
3. **Can we detect the subtle indicators of threat without being overwhelmed by noise?** Many organizations grappling with insider threat detection have recognized the difficulty in differentiating innocuous activity from authorized use that presages a problem. The differences are subtle and require the ability to detect complex combinations of behaviors. Similarly, advanced attacks can be detected with behavior indicators like those in the MITRE ATT&CK framework. But successfully implementing these detections on a wide scale requires the ability to quickly and easily tune out false positives, otherwise defenders can be easily inundated with spurious alerts.
4. **How flexible is our detection?** Rapid changes in threat activity, IT infrastructure, and the nature of work itself mean that security teams are constantly faced with new threat scenarios. Often, Security has been forced to wait on vendors to detect the threats that most concern them. In some cases those detections come too late or simply never rise high enough in the vendor's priority set to be developed. Security needs to be armed with flexible tools to adapt their posture detect the behaviors that concern them most.

BALANCING RISK MANAGEMENT AND EMPLOYEE PRIVACY

Employee behavior monitoring at the endpoint is sometimes seen as intrusive and at odds with privacy concerns. Organizations can respect and support employee privacy by:

- Maximizing the use of routinely-collected endpoint telemetry to triage alerts
- Focusing on protecting the enterprise, and the jobs of employees
- Targeting specific areas of user misconduct rather than general user activities
- Engaging with key stakeholders across the enterprise in building a user monitoring program, including legal and HR
- Conducting clear employee education and awareness efforts about the program – hiding 'in the shadows' only increases employee mistrust.

CONCLUSION

Because endpoints are so important and widespread, they present a broad and rich target for attackers seeking to profit from or damage the modern enterprise. Enhancing endpoint security offers organizations the ability to detect and prevent breaches, thereby avoiding the regulatory scrutiny that has brought severe penalties. It also holds the potential to detect and intervene with malicious insiders before they evolve into serious threats. In order to accomplish this, a shift in posture and mindset needs to occur, in which preventive technology is augmented with comprehensive awareness of what is happening on the network and the ability to rapidly evolve detection posture. Organizations that master these capabilities will decrease a critical area of risk, and gain competitive advantage over those that do not.

REFERENCES

[1] https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf

[2] https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf

nuix

Nuix (www.nuix.com, ASX:NXL) is a leading provider of investigative analytics and intelligence software, that empowers our customers to be a force for good by finding truth in the digital world. We help customers collect, process and review massive amounts of structured and unstructured data, making it searchable and usable at scale and speed, and with forensic accuracy.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849