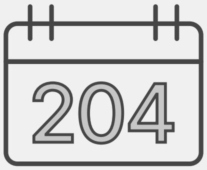
WHITE PAPER

The Hidden Costs of Aging Endpoint Solutions

Ransomware, Fileless Malware, and Management Issues

Executive Summary

CISOs are deeply concerned about endpoint security. Most assume their endpoints will be compromised at some point, and they are probably right. For instance, fewer organizations are successfully detecting ransomware now than they did in 2023 (13% versus 22%), showing us that ransomware is also becoming more sophisticated and targeted.[1] A recent survey identified that of the 78% of leaders who claimed their enterprises were prepared for an attack, half still fell victim to them.[2] Organizations know that traditional antivirus solutions are insufficient to secure endpoints and need more advanced protection, especially when the average data breach in 2023 cost companies a record $4.45 million.[3]



The average time to identify a breach is now averaging 204 days, with an additional 73 to contain the incident.[4]

While first-generation endpoint detection and response (EDR) solutions improved endpoint security by offering detection and response capabilities, they also incurred hidden costs. Their inadequate response times and the lack of cross-platform integration expose organizations to risks from ransomware and other fast-acting threats.

Also, security staff struggle to triage a flood of alerts from multiple security controls, increasing workplace stress and the chances that threats will be classified incorrectly.

And manual remediation tasks such as wipe-and-reimage overwhelm IT staff and lead to production downtime. There is little doubt that current endpoint security solutions lack the speed, integration, event correlation, and automation that CISOs need.

Endpoint Security Convergence

Years ago, realizing that some percentage of threats will always get through and the time to detect threats that have infiltrated their organizations had to be reduced, CISOs began to supplement endpoint security by deploying EDR systems on business-critical devices. These first-generation EDRs monitored endpoint events and activities to identify suspicious behaviors that may indicate the presence of a threat, such as attempts to alter process injection, modify registry keys, or disable security solutions. While these first-generation EDRs provided information to help security analysts respond to and investigate security incidents, they largely relied on manual processes and were not integrated into the rest of the organization's security and IT ecosystem.

Hidden Costs of First-Generation EDR Solutions

Before the expansion into extended detection and response (XDR), EDR solutions were designed to record and store endpoint events and leverage behavior-based detection to identify or alert potential security incidents, respond to threats, and aid forensic investigations. While first-generation EDR solutions have undoubtedly boosted endpoint visibility and threat detection, the improvements have come with costs, many of which are not apparent at first glance.

Inadequate response times

Despite changes and investments into new technologies, one would believe that identifying and containing a breach would be remarkably shorter.

In the case of cyberattacks, with the primary purpose being data theft, the time challenge is somewhat manageable with first-generation EDR solutions. Such attacks move stealthily to gather information, map the network, and identify the location of valuable assets—a process that can take weeks. When fighting this kind of threat and to prevent data theft, many CISOs consider a detection and response time of 24 hours, or even a few days, to be adequate.

In contrast, the goal of other attacks, such as ransomware, is not data theft but sabotage. Attackers execute these threats in minutes and even seconds, shrinking the time frame significantly. Today, ransomware strains are designed to find targets in an organization and then spread laterally to other parts of the organization—including servers and other networks—all within seconds.

One example is NotPetya, a cyber weapon disguised as ransomware but designed to cause destruction. The attack happened much faster than any security team could manually respond to and contain using first-generation EDR solutions. Anything short of real-time blocking increases the organization's risk of falling victim to a successful attack.

Production downtime

When security teams identify a compromised endpoint, the first step is to contain the threat. First-generation EDR tools often quarantine the endpoint to prevent the attack from spreading and avoid data loss. This technique is effective as a containment measure but renders the endpoint useless to the user and may even shut down production processes. Security teams often spend considerable time manually triaging alerts to ensure the threat is real before quarantining endpoints. Furthermore, with many devices located away from IT staff, either through a distributed enterprise model or remote work, conducting remote troubleshooting is an advantage. Although some legacy EDR solutions offer remote-shell capabilities, their ability to connect to endpoints securely and in a timely manner opens the door to exploitation if the administrator is compromised, as we have observed in many high-profile attacks.

Similarly, security analysts are skeptical of endpoint protection tools that promise automated responses, such as terminate-process-and-quarantine-endpoint. If the alert turns out to be a false positive, automated solutions may still impose a quarantine that shuts down the production line—a costly and embarrassing mistake.

During the remediation phase, most IT organizations still prefer to wipe the memory completely and reimage the infected device due to a lack of trust in their traditional antivirus tools that have trouble cleaning up persistency, risking reinfection. However, reimaging is manual, time-consuming, and requires the device to be offline during remediation.

On the IT side of the enterprise, knowledge workers depend on their personal computers to do their jobs. Taking away laptops and desktops for remediation hampers their productivity, especially with a widespread remote workforce. Moreover, many organizations just replace the infected machine with a clean one to avoid significant downtime, which is even more noticeable when shipping new devices to employee homes. The situation is completely different on the operational technology side. Taking down a critical control system or production machine can shut down the entire production line, incurring substantial costs in order fulfillment delays, lost revenue, and technician time for restarting the line.

False positives

EDR systems generate many alerts or indicators that must be manually triaged to separate malicious from benign. This activity represents a substantial productivity drain for security teams and takes time away from activities that advance the organization's security maturity. Also, as the volume of attacks increases, manual triage is difficult to scale, especially considering the ongoing cybersecurity talent shortage. High levels of false positives can lead to alert fatigue, which may cause analysts to overlook a true positive amid all the noise.

Talent shortages

Designing and executing an effective incident detection and response strategy requires talented security professionals. However, this is difficult due to the ongoing security skills shortage. According to a recent survey, the cybersecurity gap has grown by 13%, which means that in 2023, roughly 4 million cybersecurity professionals were needed worldwide.[5]

As a result of this skills shortage, CISOs face a no-win situation. If they fail to fill key positions quickly, the resulting coverage gaps weaken endpoint security and increase stress for existing staff. On the other hand, hiring inexperienced candidates can lead to costly mistakes, such as spotty deployment of critical security updates and misconfigurations that generate false positives.

Conclusion

Legacy endpoint security solutions lean heavily on prevention or offer detection capabilities without real-time response. This is no longer sufficient to meet the challenges of advanced threats. The threat landscape is becoming increasingly difficult to contain. The sophistication and speed of cyberattacks break traditional endpoint security solutions, as they simply cannot keep pace.

Filling exposed security gaps is just as difficult as security leaders struggle to identify, recruit, hire, and retain highly skilled security professionals. Existing security teams are overwhelmed due to the proliferation of threat alerts and associated false positives. They can become paralyzed and, as a result, be unable to shift through the enormity of the threat intelligence their security systems generate. Solutions like EDR and especially XDR deliver security incident detection and automated response capabilities for your security infrastructure.

[1] Global Threat Landscape Report, Fortinet, August 7, 2023.

[2] Fortinet 2023 Ransomware Global Research Report, Fortinet, April 24, 2023.

[3] Cost of a Data Breach Report 2023, IBM, July 24, 2023.

[4] Ibid.

[5] How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, ISC², October 31, 2023.

www.fortinet.com

April 9, 2024 9:32 PM

2618523-0-0-EN