WHITE PAPER

The Hidden Costs of Endpoint Security

Ransomware, Fileless Malware, and Management Issues

Executive Summary

When it comes to endpoint security, CISOs are deeply concerned. Most assume that their endpoints will be compromised at some point, and they are probably right. According to a recent Forrester study, 74% of organizations indicated that they have suffered a business-impacting cyberattack attributed to remote work vulnerabilities.[1] They know that traditional antivirus (AV) solutions are insufficient to secure endpoints and that they need more advanced protection. In fact, since people started working from home, breaches have intensified, now costing on average $1.07M more than before the pandemic, which is nearly a 10% increase.[2]

In 2021, the mean time to identify a threat was 212 days.[3]

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 expose organizations to risk from ransomware and other fast-acting threats.

Also, security staff struggle to triage a flood of alerts, which increases workplace stress and misclassification of threats. And manual remediation tasks such as wipe-and-reimage overwhelm IT staff and lead to production downtime. There is little doubt that current EDR solutions lack the speed and automation that CISOs need.

Beyond Protection

As endpoint threats have advanced in sophistication and virulence over the past few years, CISOs realize that traditional endpoint protection platforms (EPPs) that focused on prevention are no longer enough to protect their endpoints. Prevention can never be 100% effective—advanced threats will always evade prevention-based security. When they do, threats are far harder to detect. One study found that organizations take an average of 212 days to identify a breach after the threat has penetrated the network.[4] In many cases, threats are only detected after the loss of significant amounts of data.

In addition, attackers continue to develop more sophisticated ways to defeat endpoint security. Cyber criminals have stealthier ways to deliver malware such as ransomware via a fileless attack, which can bring the organization's operations to a halt in less than a minute. For example, "living off the land" attacks use legitimate applications to fool AV solutions and infect computers.

Once advanced threats evade endpoint security, they cause significant damage such as costly and embarrassing data theft, industrial espionage, outages affecting production lines and knowledge workers, and exorbitant ransom demands.

Endpoint Security Convergence

Realizing that some percentage of threats will always get through, and to reduce the time to detect threats that have infiltrated their organizations, CISOs began to supplement endpoint security by deploying EDR systems on business-critical devices. EDRs monitor endpoint events and activities to identify suspicious behaviors that may indicate the presence of a threat, for example, attempts to alter process injection, modify registry keys, or disable security solutions. These first-generation EDRs can provide information to help security analysts respond to and investigate security incidents, but largely rely on manual processes.

CISOs realized that these detection tools improved their endpoint visibility and threat detection. As the adoption of EDR tools grows, traditional EPP and first-generation EDR are converging. Currently, enterprise CISOs expect that EPP solutions need to have the capabilities to prevent file-based malware attacks, detect malicious activities, and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts.

Hidden Costs of First-generation EDR Solutions

EDR solutions are 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 the time to identify and contain a breach would be remarkably shorter. In 2021, the average time to identify one was 212 days with an additional 75 days to contain in for a total of 287 days. This is up 2.5% over the year before (280 days), which was flat compared to the year before that (279 days). In fact, compared to the data over the last six years, it is the worst it has ever been.[5]

In the case of cyberattacks with the primary purpose of 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 threats to prevent data theft, many CISOs consider a detection and response time on the order 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. These fast-acting threats execute in minutes and even seconds, shrinking the time frame significantly. Ransomware strains today are designed to find targets in an organization and then to spread laterally to other parts of the organization—including servers and other networks—all within seconds.

Another 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 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 make sure 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, having the ability to remote troubleshoot is an advantage. Although some legacy EDR solutions offer remote shell capabilities, their ability to connect to endpoints in a secure and time-limited fashion opens the door to exploit if the administrator is compromised as we have seen in many high-profile attacks.

In the same vein, 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 organization still prefer to wipe the memory completely and reimage the infected device, due to lack of trust of their traditional antivirus tools that have trouble cleaning up persistency, risking reinfection. Although most security professionals say they trust the wipe-and-reimage process. However, the reimaging process is manual and 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 work-from-home 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 (OT) side of the house. Taking down a critical control system or production machine can shut down the entire production line, incurring substantial costs in terms of order fulfillment delays, lost revenue, and technician time for restarting the line.

False positives

By design, EDR systems generate a large volume of alerts or indicators, which 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, for example, attack simulation testing and instituting incident-response procedures. Also, as the volume of attacks continues to increase, manual triage is difficult to scale, especially considering the talent shortages discussed below. 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. But this is difficult due to a security skills shortage. According to a recent survey, the cybersecurity workforce sits around 2.7 million people needed to fill the gap. That means that the global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets against a very active threat landscape.[6]

As a result of the security 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 workplace 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 huge numbers of false positives.

The number of unfilled cybersecurity positions in the world is around 2.7 million.[7]

Conclusion

Legacy endpoint security solutions lean heavily on prevention or offer detection without real-time response. This is no longer enough to meet the challenges of advanced threats. The advanced threat landscape is becoming increasingly difficult to address. The sophistication and speed of cyberattacks break traditional endpoint security solutions that 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 generation.

[1] "Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work," Forrester, September 2021.

[2] "Cost of a Data Breach Report 2021," IBM, 2021.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] "A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021," (ISC)², 2021.

[7] Ibid.

March 11, 2022 1:57 AM

696181-B-0-EN