FORTINET

WHITE PAPER

# Hidden Costs of Endpoint Security

## Ransomware, Fileless Malware, and Other Advanced Cyber Threats Still Challenge Current Endpoint Protection Systems

## Executive Summary

**When it comes to endpoint security, CISOs are in a bind. Most assume that endpoints will be compromised at some point, and they are right. In a recent survey of CISOs, 81% reported at least one intrusion in the past year, and 22% had more than five.[1] There is little doubt in their minds that traditional antivirus solutions are insufficient to secure endpoints—they need more advanced protection.**

**First-generation endpoint detection and response (EDR) solutions improve endpoint security by offering detection and response capabilities but also incur hidden costs. Inadequate response times expose the organization to risk from ransomware and other fast-acting threats. Security staff struggle to triage a flood of alerts, which increases workplace stress and misclassification of threats. Manual remediation efforts such as wipe and reimage consume IT staff time and lead to production downtime. There is little doubt that current EDR solutions lack the speed and automation that CISOs need to ensure cost-effective, reliable endpoint security.**

**In 2019, the mean time to identify a threat was 206 days, and the mean time to contain the threat after detection was 73 days.[2]**

## 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 more than six months to identify a breach after the threat has penetrated the network.[3] 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, 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 grew, 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. A recent study shows that 47% of organizations surveyed have EDR capabilities, up 11 percentage points from the previous year.

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

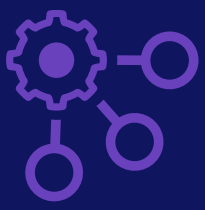
Until recently, mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) response times have been measured in days, weeks, or even months. According to one source, in 2019, MTTD was 206 days, and the mean time to contain (MTTC) after detection was 73 days.[4] Significant improvement is possible: Another study found that 62% of breaches can be detected within 24 hours after arriving at the endpoint.[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. For example, the WannaCry ransomware took only a few seconds to encrypt files and spread globally, infecting 150 countries and over 200,000 computers in a matter of 24 hours.[6]

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.[7] Anything short of real-time blocking increases the organization's risk of a successful attack.

**"NotPetya was saturating victims' systems with terrifying speed: It took 45 seconds to bring down the network of a large Ukrainian bank."[8]**



**Less than 10% of organizations have a fully automated process for endpoint remediation.[9]**

### 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.

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. Further, 97% of security professionals say they trust the wipe-and-reimage process.[10] However, the reimaging process is manual and time-consuming—less than 10% of organizations have a fully automated process for endpoint remediation—and requires the device to be offline during remediation.[11]

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. Moreover, many organizations just replace the infected machine with a clean one to avoid significant downtime. 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.

Faced with a flood of false positives, many organizations rightly regard their legacy security tools as blunt instruments unsuited to the

critical tasks of troubleshooting and remediating threats. Instead, they favor more draconian measures such as reimaging personal computers and quarantining devices. IT managers often perceive these actions to be safer, but they can interfere with business operations as described earlier.

### 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. In the U.S. alone, the cybersecurity workforce gap—the number of open positions—is nearly 500,000.[12] To simply meet current needs of businesses, the cybersecurity workforce must grow by 62%.[13]

**The number of unfilled cybersecurity positions in the United States is nearly 500,000.[15]**

These cybersecurity skills challenges are a major source of concern for CISOs. Indeed, in a recent survey, more than half of CISOs cite the shortage of cybersecurity skills as their top security challenge.[14]

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.

## 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 the advanced threat landscape. The advanced threat landscape is becoming increasingly difficult to address. The sophistication and speed of cyberattacks break traditional endpoint security approaches that simply cannot keep pace.

Filling exposed security gaps is just as difficult, as security leaders struggle to identify, recruit, hire, and retain security professionals with the skills needed. Existing security teams are overwhelmed due to the proliferation of threat alerts and associated false positives. They become paralyzed, and as a result, unable to shift through the enormity of the threat intelligence their security systems generation.

1 "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.
2 "2019 Cost of a Data Breach Report," Ponemon Institute, accessed February 4, 2020.
3 Ibid.
4 Ibid
5 Justin Henderson and John Hubbard, "2019 SANS Survey on Next-Generation Endpoint Risks and Protections," SANS Institute, December 2, 2019.
6 Elizabeth Dwoskin and Karla Adam "More than 150 countries affected by massive cyberattack, Europol says," The Washington Post, May 14, 2017.
7 Mohit Kumar, "TSMC Chip Maker Blames WannaCry Malware for Production Halt," The Hacker News, August 7, 2018.
8 Andy Greenberg "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, August 22, 2018.
9 Justin Henderson and John Hubbard, "2019 SANS Survey on Next-Generation Endpoint Risks and Protections," SANS Institute, December 2, 2019.
10 Ibid.
11 Ibid.
12 "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.
13 Ibid.
14 Jon Oltsik, "Is the Cybersecurity Skills Shortage Getting Worse?" ESG, May 10, 2019.
15 "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.





February 13, 2020 11:18 PM

580266-0-0-EN

D:\Fortinet\Work\2020\February\021320\wp-hidden-costs-endpoint-security