CrowdStrike White Paper

CROWDSTRIKE

WHAT LEGACY ENDPOINT SECURITY REALLY COSTS

How modern endpoint security improves visibility and reduces risk

CONTENTS

LEGACY SOLUTIONS LEAVE SECURITY TEAMS SHORT

To be competitive, businesses are moving forward with digital transformation projects enabled by cloud services. The number of endpoints operating in these dynamically expanding environments is exploding. According to one estimate, there will be 29.3 billion networked devices globally by 2023, up from 18.4 billion in 2018, 26% of which will exist in the business sector.[1] The perimeter that security teams are expected to protect now extends far beyond the traditional network. The edge of the network is now defined by endpoints, wherever they are located.

Do legacy endpoint security solutions serve security teams well in successfully defending against breaches in dynamic, distributed environments? Are they smart, scalable and flexible enough to protect organizations from the fast, stealthy and complex attacks that can compromise access to valuable assets and critical business operations?

This white paper helps security and IT professionals better understand the costs and risks of trying to make legacy endpoint security solutions effective in today's threat environment — and why only a cloud-native approach to endpoint protection can provide the visibility, intelligence, scalability and speed that security teams need to be successful.

According to one estimate, there will be 29.3 billion networked devices globally by 2023, up from 18.4 billion in 2018, 26% of which will exist in the business sector.

Source: *"Cisco Annual Internet Report (2018–2023) White Paper,"* Cisco, March 9, 2020.

ANTIVIRUS SOLUTIONS DESIGNED FOR YESTERDAY'S ATTACKS

Legacy security systems were originally developed to help security teams identify file-based malware. But attackers quickly developed more sophisticated methods to get to valuable business assets by using the following techniques currently at play today:

- Fileless attack exploitation of platform and app vulnerabilities, especially weaknesses in identity security, leading to credential threat
- Live attacks by insiders and externally managed advanced persistent threats that leave backdoors and ransomware
- Compromised software development pipelines (e.g., the SolarWinds supply chain attack discovered in December 2020)
  - Independent research conducted by a technology market research firm found that 84% of the 2,200 senior IT decision makers and IT security professionals surveyed believe that software supply chain attacks could become one of the biggest cyber threats to organizations like theirs within the next three years.[2]

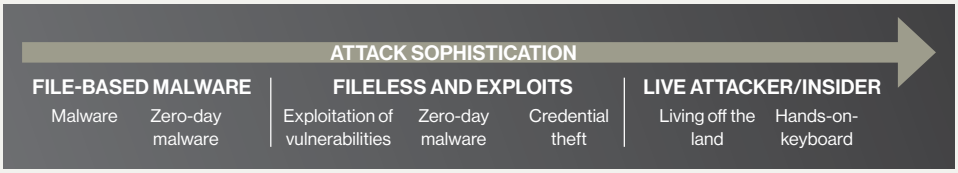


Figure 1. Types of attacks according to sophistication

1 *"Cisco Annual Internet Report (2018–2023) White Paper,"* Cisco, March 9, 2020.
2 *"2021 CrowdStrike Global Security Attitude Survey,"* CrowdStrike, 2021.

In these attacks, an organization's lack of visibility across on-premises and cloud endpoints is the attacker's best friend. Widely distributed endpoints are hard to see and track, as they access valuable assets and mission-critical operations that may be located on premises, in the cloud or in hybrid environments. Dark Reading's "State of Endpoint Security Survey" found that 84% of security pros believe any attack will start with the endpoint.[3]

Lack of visibility extends the time it takes to detect and resolve attacks, maximizing the damage attackers can inflict and increasing the cost of recovery. A 2021 study of organizations across the U.S., EMEA and APAC regions showed that, on average, it took organizations 146 hours in 2021 to detect a cybersecurity incident, compared to 117 hours in 2020 and 120 hours in 2019.[4]

The challenge facing security teams is growing as the volume of attacks is rising. The same study showed that, in the last 12 months, 69% of respondents' organizations had suffered a cybersecurity incident as a direct result of teams working remotely; 66% suffered at least one ransomware attack; and 45% experienced at least one software supply chain attack, compared to 32% in 2018.[5]

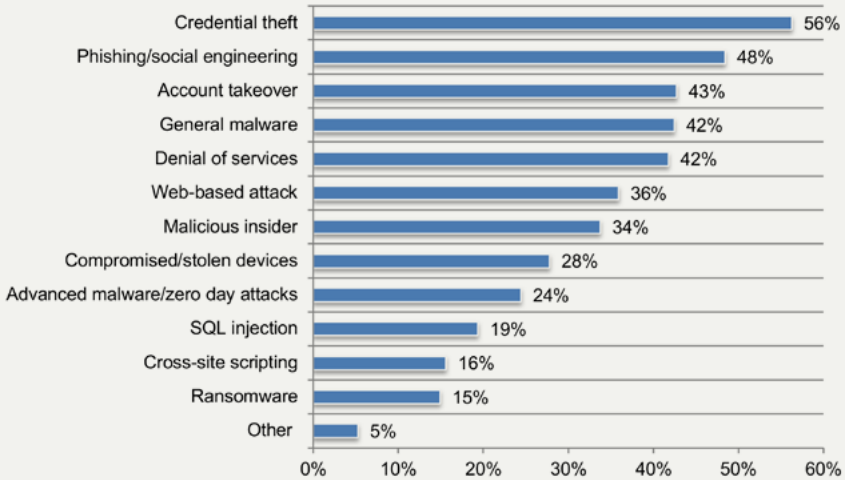
Organizations are bearing a higher cost of attacks as well. In 2020, the average total cost of a data breach rose from $3.86 million USD to $4.24 million USD, the highest in the 17-year history of the Ponemon Institute's annual "Cost of a Data Breach Report."[6] In a similar report published in 2019, the Ponemon Institute found that the average cost of a successful endpoint attack increased from $7.1 million USD (in 2018) to $8.94 million USD (in 2019).[7]

To understand why making choices about how best to provide endpoint protection in today's threat landscape, it's worth taking a look at why endpoints are so vulnerable and what is required to deal with those vulnerabilities with the strongest security posture possible.

Beyond File-based Malware

The Ponemon Institute surveyed over 2,200 IT and IT security personnel and found they had experienced these types of attacks:

Figure 10. What best describes the type of attacks experienced by your organization?
More than one response permitted



Source: *"Cybersecurity in the Remote Work Era: A Global Risk Report,"* Ponemon Institute, October 2020.

A 2021 study of organizations across the U.S., EMEA and APAC regions showed that, on average, it took organizations 146 hours in 2021 to detect a cybersecurity incident, compared to 117 hours in 2020 and 120 hours in 2019.

Source: *"2021 CrowdStrike Global Security Attitude Survey,"* CrowdStrike, 2021.

Dark Reading's "State of Endpoint Security Survey" found that 84% of security pros believe any attack will start with the endpoint.

Source: *"Endpoint Still a Prime Target for Attack,"* Dark Reading, Sept. 24, 2021.

3 *"Endpoint Still a Prime Target for Attack,"* Dark Reading, September 24, 2021.
4 *"2021 CrowdStrike Global Security Attitude Survey,"* CrowdStrike, 2021.
5 *"2021 CrowdStrike Global Security Attitude Survey,"* CrowdStrike, 2021.
6 *"Cost of a Data Breach Report 2021,"* Ponemon, 2021.
7 *"The Third Annual Study on the State of Endpoint Security Risk,"* Ponemon Institute, January 2020.

A BAD ACTOR'S FAVORITE TARGET: ENDPOINTS WITHOUT STRONG PROTECTION

An endpoint is any device that can be connected to a network to access an organization's assets and applications. This includes not only workstations and laptops but also servers and a wide range of mobile and internet-connected devices.

As discussed previously, endpoints are located wherever work is being done, whether on premises, remote or both. And every one of them is a potential entry point for an attack, as well as accidental errors that are not maliciously motivated.

Endpoints are vulnerable for several important reasons.

- The sheer number of endpoints, driven by growing demand to work from anywhere and the continuous introduction of new types of endpoint devices, increase the odds of a successful attack. They are hard to see, let alone track.
- Each endpoint can be running many different applications at different version levels, requiring regular patching and maintenance to protect against vulnerabilities known by attackers that can exploit them. The same is true for endpoint operating systems.
- Corporate-owned endpoints may go home with workers, where extra care must be taken to keep other family members from using them unsafely, while personal devices that may not be sufficiently secure continue to be used for work.

Insufficient endpoint security also increases the risk of damage from errors and accidental misuse. End users and administrators (including web admins) are focused on meeting the demands of their jobs. Security policies are not always top of mind, and if they are too intrusive, they may be counterproductive, driving frustrated users to work around them.

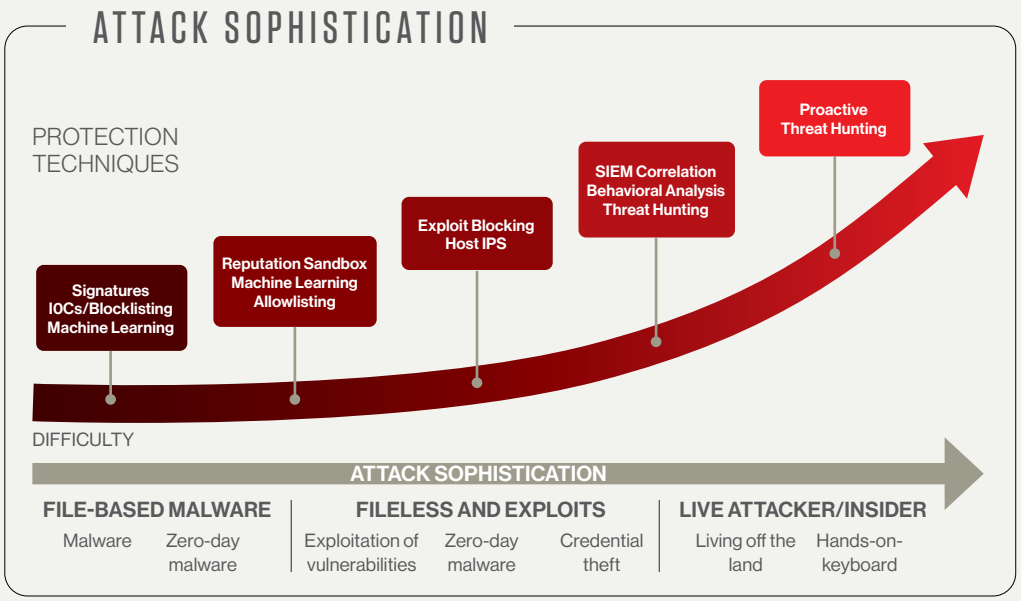


Figure 2. Types of protection techniques used to block attacks — protection difficulty increases with attack sophistication

As shown in Figure 2, the evolution of more sophisticated threats has driven the development and introduction of more powerful endpoint protection techniques and technologies that can help security teams:

- More easily see what's happening on all endpoints, wherever they are, and provide the ability to scale when needed
- Understand and prioritize the volume of incident and alert data — most of which is irrelevant — associated with what's happening on endpoints
- Investigate and remediate what's going on as soon as possible

Unfortunately, legacy antivirus solutions continue to address only the low end of the attack sophistication scale for which they were designed: file-based malware.

It's important to understand the design features that limit the usefulness of legacy antivirus solutions to security teams faced with sophisticated attacks — not only at the point of prevention but beyond.

WHERE DO LEGACY ENDPOINT SECURITY SOLUTIONS MISS THE MARK?

Legacy antivirus solutions were never designed to handle today's environment and endpoint protection challenges. Antivirus solutions focus on the prevention phase of endpoint security, which aims to stop cyber threats from compromising the endpoint. Centralized on-premises antivirus solutions rely on a data center to act as the hub managing connected endpoints through an agent installed on individual devices inside and outside the firewall. Requiring frequent updates, they run in the background, periodically scanning a device's content for patterns that match a database of virus signatures.

This approach to endpoint protection does not deliver the support that security teams need. Legacy solutions lead to:

- **Operational inflexibility.** Legacy system updates are not in real time, leaving windows of opportunity for attackers as IT teams catch up with patches and roll out upgrades. They don't reduce time and complexity for security teams barraged by streams of unprioritized alerts or connect teams to other security solutions for triage and investigation.
- **Gaps in protection.** With remote workers, virtualization and the cloud, devices are not always connected to the corporate network in which the legacy solution hub is running. Devices that are off-network or offline can be vulnerable. When updates and upgrades are implemented, there may be scaling challenges and endpoint performance issues.
- **Little to no help against sophisticated attacks.** Legacy solutions do not provide security teams with access to the threat intelligence essential for recognizing everything from fileless malware up through the latest advanced persistent threats. These solutions also cannot enable security teams to proactively hunt and learn from threats that exploit vulnerabilities or steal or abuse credentials, which can lead to compromised access to vital data and applications.

ENDPOINTS: MORE THAN JUST WORKSTATIONS AND LAPTOPS

Endpoints also include:

- Mobile phones
- Tablets
- Internet-connected devices
- Servers
- Point-of-sale (POS) systems
- Switches
- Digital printers
- Cameras
- Appliances
- Smart watches
- Health trackers
- Navigation systems

Source: **CrowdStrike Cybersecurity 101**

- **Limited visibility.** Legacy solutions provide no real visibility across multiple devices and the entire network, especially when network devices are offline, providing opportunities for adversaries to fly under the radar in real time. They cannot sufficiently monitor endpoint activity or capture details important for remediation or threat hunting.
- **Opportunities for bad actors to break them.** Through hands-on experience, attackers have learned the most important vulnerabilities in legacy security solutions — and now they also have tools to figure out how to break the fixes that solution providers release. Relying on legacy antivirus solutions to do more than their design allows is high risk for security teams. And it also has a high cost.

The expense of renewing legacy security licenses doesn't represent the true costs of maintaining a legacy antivirus solution in terms of people, processes and underlying technology.

At the corporate level, consider the cost of reduced user productivity when bloated agents slow down the responsiveness of thousands of endpoints — or the losses when an incident the legacy system failed to catch results in a breach.

There are direct costs incurred by security teams maintaining legacy antivirus systems, including downloading, implementing, configuring and tuning often-fragile upgrades, running required scans and performing on-premises server maintenance. One economic impact study showed that a fully managed cloud-native approach to endpoint security could reduce the support burden by eliminating 3.4 full-time employees (FTEs), for an estimated savings of $1.5 million USD over three years.[8]

Instead of focusing their talents on protecting the organization from the most dangerous threats, the security team spends time wrangling endpoint protection from a legacy system that can't help them monitor, triage and analyze alerts from thousands of endpoints, delaying their speed in responding to and remediating incidents that become breaches.

So what would deliver not only the benefits of an legacy endpoint protection but would also reduce the threats and risks in today's environment?

WHAT IS ENDPOINT DETECTION AND RESPONSE (EDR)?

Endpoint detection and response (EDR) is a cybersecurity solution that detects and mitigates cyber threats by continuously monitoring endpoint devices and analyzing endpoint data.

True EDR helps security teams with:

- Incident data search and investigation
- Alert triage and suspicious activity validation
- Suspicious activity detection
- Threat hunting and data exploration
- Stopping malicious activity

Source: **CrowdStrike Cybersecurity 101**

TAKE A CLOUD-NATIVE APPROACH TO BETTER ENDPOINT PROTECTION

A cloud-native endpoint protection platform dramatically reduces the overhead of managing a legacy system, which prevents security teams from addressing their organizations' most pressing cybersecurity threats. In turn, security teams gain:

Operational resilience. Cloud-native platforms are updated in real time and their algorithms adjusted constantly. The version in use is always the latest version. Attackers have no lag time opportunities while the security team waits for a legacy system upgrade.

---

8 *"Total Economic Impact™ of CrowdStrike,"* 2021.

Protection that's always available and scalable. Cloud-native platforms that work through a single lightweight agent can be deployed immediately on endpoints and scaled quickly with little effect on endpoint performance. When the endpoints associated with remote workers, virtualization and the cloud lose connection with the corporate network, they remain protected.

An edge on sophisticated attackers. Taking a cloud-native approach to endpoint protection enables the use of new machine learning and artificial intelligence technologies that further empower the security team by recording and learning from new attacks, and apply intelligence about attack techniques on a massive scale.

Full-spectrum, real-time visibility and clarity. A cloud-native endpoint protection platform is positioned to monitor endpoint activity and continuously capture full endpoint details in every location. Combined with threat intelligence, this provides context for real-time and historical analysis and effective threat hunting — both proactive and managed.

An omnipresent ally against adversaries. Even if a bad actor manages to gain access to a system, their attempts to move laterally or gain further access will be observed by the cloud-native platform's solution provider. Instead of attackers evading detection, defenders can observe their techniques to improve and accelerate detection.

A cloud-native endpoint protection can provide the visibility, intelligence and speed security teams need to do their highest-value work, while organizations achieve operational resilience and efficiency by eliminating infrastructure complexity.

TAKE THE NEXT STEP

Are you ready to improve your endpoint protection? Get our eBook **"Five Critical Capabilities for Modern Endpoint Security: Why full visibility leads to stronger endpoint protection"** to learn more about what to look for as you evolve your endpoint security solution.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

© 2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.