CROWDSTRIKE

White Paper

Ransomware Evolution and the Impact of an Outdated Defense

The true cost of legacy endpoint security and why it's time for a change

Table of Contents

The Evolution of Modern Ransomware

Adversaries are faster and more sophisticated than ever — and legacy defenses just can't keep up

According to a March 2022 ESG survey, 79% of organizations experienced a ransomware attack in the prior 12 months, and one in three organizations reported being the victim of a successful attack more than once. As organizations navigate hybrid and remote work and progressively move data and applications into the cloud, adversaries are evolving their tradecraft, finding new ways to gain access to internal systems by moving faster than ever, exploiting new vulnerabilities and adapting attack methods to evade detection. Securing organizations against modern ransomware weighs heavily on security teams and leaders — for the vast majority of organizations (82%), ransomware preparedness was cited as a top five business priority.

Ransomware attacks can generate significant damage to organizations of all sizes, from the immediate cost of paying ransoms to the operational impact of data loss and business disruption. Beyond these tangible costs are the longer-term ripple effects of being the target of successful ransom attacks, including erosion of customer trust and leaked internal or employee data.

With the estimated average cost of a breach rising to $4.45 million USD in 2023, a single payment can be devastating to a business. And paying ransoms is no guarantee of restoration — even if organizations pay a ransom, only 1 in 7 reported getting all of their data back.[1]

Ransomware readiness remains essential to preventing, detecting and responding to emerging attacks. And with attacks constantly increasing in speed, organizations need to deploy modern defenses that can move as fast — if not faster — than today's adversaries. With the average breakout time — the time it takes an adversary to gain initial access and move laterally — dropping to 79 minutes[2] (with 7 minutes the fastest observed time), organizations need to be able to detect and remediate attacks as quickly as possible, including extending automated preventions and real-time response capabilities across their defenses.

In addition to speed, adversary tradecraft is getting more sophisticated — attackers are leveraging stolen credentials (in 80% of attacks[3]) or orchestrating malware-free attacks (71% of attacks[4]). Organizations need to leverage security platforms that enable organizations to monitor and defend multiple domains — some of the most critical threat vectors to protect are network, cloud workloads, email, identities and, of course, endpoints.

Securing endpoints remains an intuitive starting point for organizations. For the modern enterprise, endpoints are the bedrock of productivity, the entry points for employees to connect to internal systems. From providing access to emails and developer environments, to enabling internal messaging and data storage, endpoints are central to enterprise operations. And unsurprisingly, your endpoints are among the most coveted attack vectors in your environment — with multiple sources reporting that as many as 90% of all successful cyberattacks begin on an endpoint.

Ransomware attacks target organizations of all sizes across all major verticals. According to the **CrowdStrike 2023 Threat Hunting Report**, financial services was one of the most targeted verticals, with a year-over-year increase of over 80%. The report states, "Though some adversaries focus on stealing cryptocurrency or non-fungible tokens (NFT), opportunistic big game hunting (BGH) ransomware and data theft campaigns remain the primary eCrime threat to financial institutions. Due to the victim organization's need to maintain system uptime and the sensitive nature of the sector, eCrime threat actors likely conclude that financial institutions are willing and able to pay ransom demands." For similar reasons, the technology sector is also a high-value target for adversaries, with the report citing the sector's access to highly sensitive data that make it a notably attractive target for BGH ransomware attacks.

1. "The Long Road Ahead to Ransomware Preparedness," ESG, March 2022. https://www.crowdstrike.com/resources/white-papers/the-long-road-ahead-to-ransomware-preparedness-ebook/
2. CrowdStrike 2023 Threat Hunting Report. https://www.crowdstrike.com/resources/reports/threat-hunting-report/
3. CrowdStrike 2023 Global Threat Report. https://www.crowdstrike.com/global-threat-report/
4. CrowdStrike 2023 Global Threat Report. https://www.crowdstrike.com/global-threat-report/

Over the last decade, modern technologies like the CrowdStrike Falcon® platform have shaped the landscape of endpoint detection and response (EDR) and more recently extended detection and response (XDR). Built on a cloud-native architecture, next-generation security offerings enable organizations to rapidly deploy and scale defenses to thousands of endpoints in a matter of minutes while alleviating the traditional burden of needing to manage infrastructure or deploy frequent updates. The cloud-scale computing power of modern platforms also enables them to apply the latest innovations in artificial intelligence and machine learning to analyze adversary tradecraft and detect atypical behavior in user environments with increasing levels of fidelity, especially in cases of unknown zero-day threats.

With extensive investments in research and development, next-generation antivirus (NGAV) and modern endpoint security platforms have rapidly become compelling alternatives for combating ever-evolving ransomware compared to more traditional antivirus and endpoint security solutions. Do legacy endpoint security solutions perform as well to successfully defend against breaches in today's dynamic, distributed environment? Are they smart, scalable and flexible enough to protect organizations from fast, stealthy and complex attacks that can compromise access to valuable assets and critical business operations?

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

Yesterday's Tools Can't Stop Today's Tradecraft

File-Base Malware

- Malware
- Zero-day malware

Fileless and Exploits

- Exploitation of vulnerabilities
- Zero-day malware
- Credential theft

Live Attacker/Insider

- Living off the land
- Hands-on-keyboard

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

- Fileless attacks that exploit platform and app vulnerabilities, especially weaknesses in identity security, leading to credential theft
- Live attacks, either by insiders or by externally managed advanced persistent threats (APTs) that leave backdoors and ransomware
- Use of legitimate remote monitoring and management (RMM) tools to monitor enterprise activity in order to blend into typical activity and avoid detection
- Attacks against cloud environments, most notably by exploiting misconfigurations or abusing built-in cloud management tooling
- Leveraging adversarial machine learning to undermine the robustness of ML algorithms in security defenses, and using generative AI, such as new variants of sophisticated phishing attacks and polymorphic code to enable attackers to evade dedication
- Compromised software development pipelines and supply chains

In these attacks, a lack of visibility across on-premises and cloud endpoints is the attacker's best friend. With attack domains and endpoint categories expanding — to include PCs, Internet of Things (IoT) devices, operational technology (OT), mobile devices, servers and more — blind spots can occur across defenses, and widely distributed endpoints are hard to see and track, introducing risk as they're used to access valuable assets and mission-critical operations that may be located on-premises, in the cloud or in hybrid environments.

Lack of visibility extends the time it takes to detect and resolve attacks, increasing the potential damage attackers can inflict and raising the cost of recovery, especially as adversaries find ways to accelerate their attacks.

To understand how to best protect endpoints in today's threat landscape, it's worth looking at why endpoints are so vulnerable and what is required to address vulnerabilities and ensure the strongest possible security posture.

Endpoints Are a Bad Actor's Favorite Target and Need 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 IoT devices.

As discussed, 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 or for accidental errors that are not maliciously motivated.

Endpoints are vulnerable for several reasons:

- The sheer number of them, driven by growing demand to work from anywhere and the continuous introduction of new types of endpoint devices, increases 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 that attackers can exploit. 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.
- The adoption of bring-your-own-devices policies, enabled by mobile device management (MDM) tools, lets employees access internal data or email on personal mobile devices, but they may not be sufficiently secure.

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 top of mind, and if they are too intrusive, they may be counterproductive and drive frustrated users to work around them.

Endpoints: More than Just Workstations and Laptops

Examples of endpoints also include: mobile phones, tablets, IoT devices, servers, point-of-sale (POS) systems, switches and digital printers

Source: What Is an Endpoint?

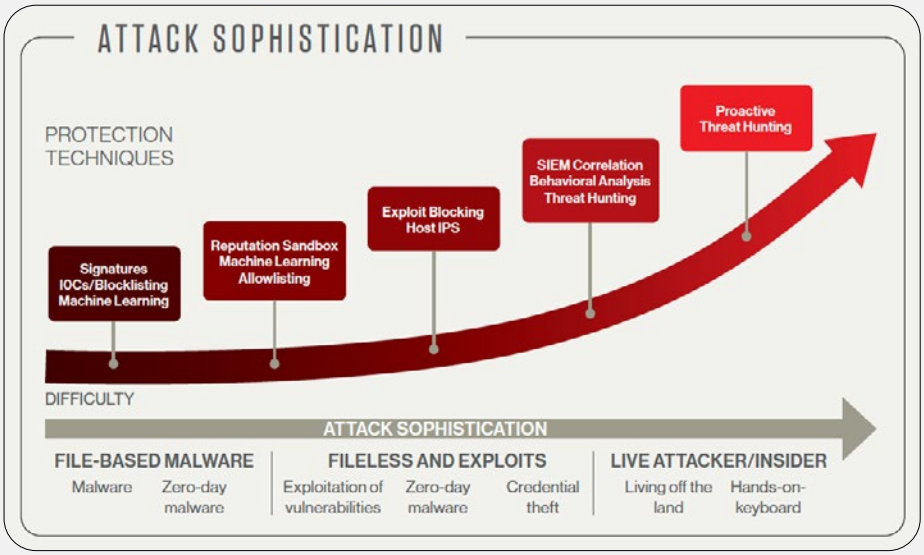

Figure 1. How protection techniques must evolve to keep up with increasingly sophisticated attacks

Fortunately, as shown in Figure 1, 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 (much of which is irrelevant) associated with what's happening on endpoints
- Investigate and remediate what's going on ASAP

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 when security teams are faced with sophisticated attacks — not only at the point of prevention but beyond.

Where Legacy Endpoint Security Solutions Miss the Mark

Legacy antivirus solutions were never designed to handle today's threat 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 modern security teams need.

- **Operational inflexibility.** Legacy system updates are not done in real time, leaving windows of opportunity for attackers as IT teams catch up with patches and roll out upgrades. Legacy antivirus doesn't reduce time or complexity for security teams barraged by streams of unprioritized alerts, and it doesn't connect teams to other security solutions to triage and investigate. Moreover, many legacy platforms are unable to deploy new defenses without leveraging incremental agents, which consume additional endpoint resources and can impact productivity.
- **Gaps in protection.** With today's combination of 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 threat intelligence essential to recognizing everything from fileless malware to the latest advanced persistent threats. These solutions also can't enable security teams to proactively hunt, and learn from, threats that exploit vulnerabilities or steal or abuse credentials, compromising access to vital data and applications.
- **Limited visibility.** Legacy solutions provide no real visibility across multiple devices and the entire network, especially when network devices are offline, giving adversaries opportunities to fly under the radar in real time. They cannot sufficiently monitor endpoint activity or capture details important for remediation or threat hunting.
- **Bad actors can evade them.** Attackers have, through experience, learned about the vulnerabilities in legacy security solutions. Now threat actors also have the tools to figure out how to break the fixes released by solution providers. Relying on legacy antivirus solutions to do more than they were designed for is high risk for security teams — and it also has a high cost.

While renewing licenses may not seem significant by itself, the expense doesn't fully 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 thousands of endpoints — or the associated costs when a legacy system fails to catch an incident that results in a breach.

There are also direct costs incurred by security teams maintaining legacy antivirus systems: downloading, implementing, configuring and tuning often-fragile upgrades, running required scans and performing on-premises server maintenance. Historically, onboarding to legacy solutions has been a sluggish process that can take months, often requiring additional hardware. With a cloud-native approach, organizations can deploy agents to thousands of endpoints in a matter of minutes, configure automatic updates and rapidly deploy the latest protections to new endpoints without interrupting day-to-day operations. This reduces both the cost and complexity of managing legacy security infrastructure. Such was the case, for instance, for the State of Oklahoma, who was able to deploy over 100K agents in a single day, and estimates they'll realize $5.7M in cost savings over the next five years.[5]

Instead of focusing their skills 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, which can turn into breaches.

So what would deliver not only the benefits of an legacy endpoint protection but also address the critical challenges 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: What Is Endpoint Detection and Response (EDR) Security?

5. https://www.crowdstrike.com/resources/case-studies/state-of-oklahoma/

Take a Cloud-Native Approach to Better Endpoint Protection

A cloud-native endpoint protection platform dramatically reduces the legacy system management overhead that 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 are adjusted constantly. The version in use is always the latest version. Attackers have no lag time while the security team waits for a legacy system upgrade.
- **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 ML/AI technologies that further empower the security team by recording and learning from new attacks, which also makes it possible to crowdsource 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 gains access to an endpoint, their attempts to exploit vulnerabilities and move laterally will be observed by the cloud-native security solution. Instead of attackers learning how to subvert endpoint protection, defenders have a view into how attackers think.

A cloud-native endpoint protection solution 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.

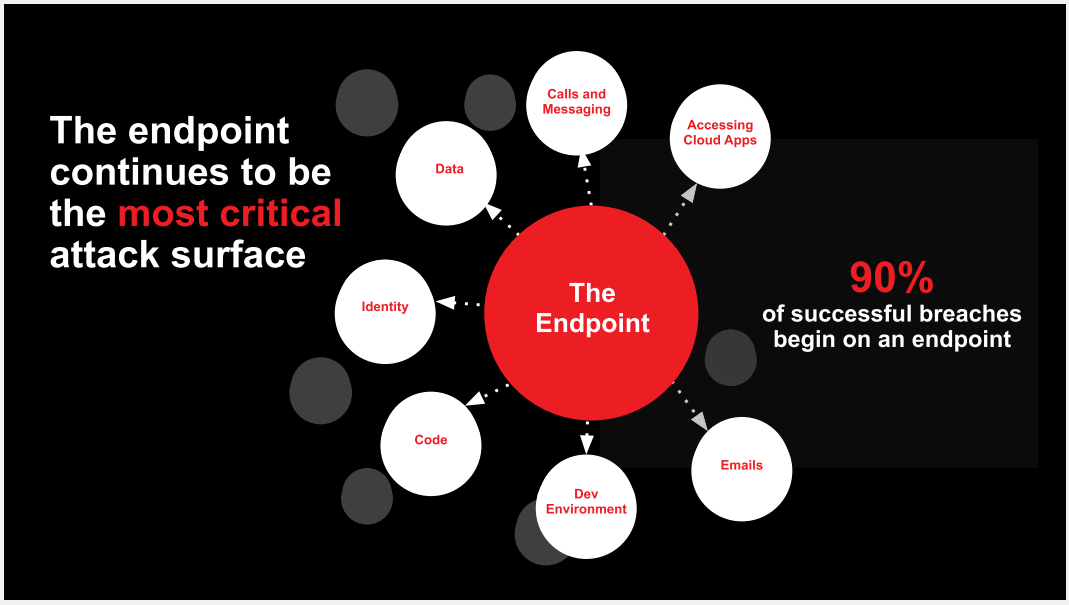

Figure 2. The endpoint enables access to multiple systems — for both users and attackers

Take the Next Step

- **Read the eBook:** 5 Key Capabilities to Secure Against Endpoint Risk
- **Register for the on-demand CrowdCast:** Adversaries that Evade Legacy Endpoint Solutions and What to Do About Them
- **Experience the Falcon platform:** Sign up for a complimentary 15-day trial

About CrowdStrike

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

Powered by the CrowdStrike Security Cloud and world-class AI, 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 delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.