5 Key Capabilities to Secure Against Endpoint Risk

Supercharge detection and response across your enterprise

CrowdStrike eBook

Table of Contents

Defenders Deserve Better

Pre-2020, IT and security teams had a hard enough time managing and securing endpoints. Many organizations were "getting by" with endpoint solutions that acted as basic device management tools. Now, even in the face of managing remote and hybrid teams, operationalizing digital transformation efforts, and navigating a volatile threat landscape, there's hope for improvement with modern endpoint protection.

Endpoint protection is one of the most important security issues facing the modern workplace.

The number of endpoints accessing cloud applications, infrastructure and data is growing.

Disparate point products and legacy security solutions can't provide complete visibility.

Relentless adversaries are taking advantage of complexity with faster and more sophisticated attacks.

Today's endpoint protection is going up against well-resourced adversaries.

Access to credentials has become easier — access brokers increased their ad volume by

112% in 2022

compared to 2021.

Breakout time has decreased to

84 minutes

The average organization is using

45 different security tools

Source: CrowdStrike 2023 Global Threat Report

The Brave New World of Modern Endpoint Protection

The complexity of the threat landscape paired with legacy endpoint solutions creates impassable hurdles for IT and security teams. Day to day, defenders are bogged down by operational inflexibility, manual activities like parsing through logs, and chasing down attacks after the fact.

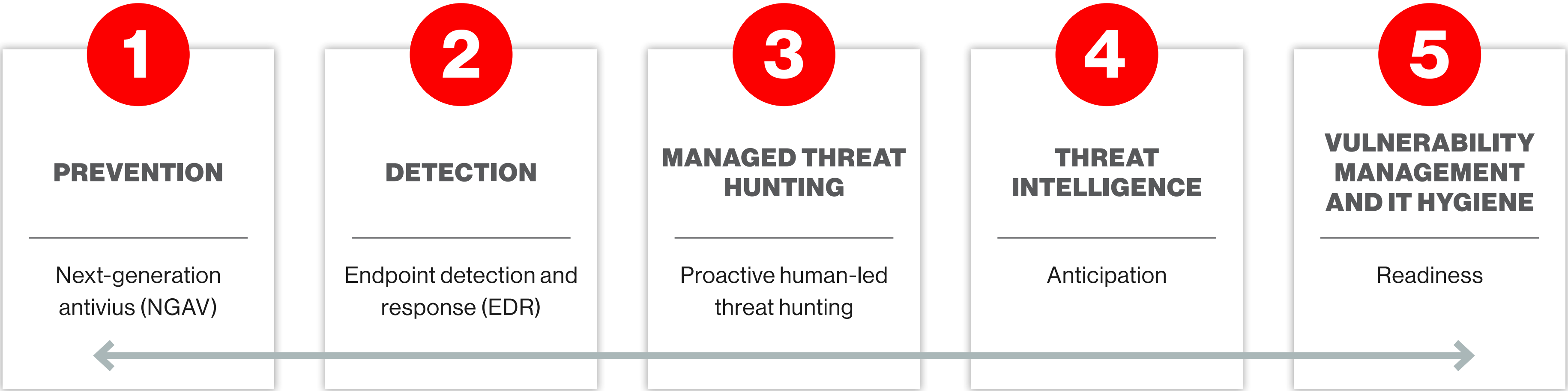
Endpoint protection platforms are designed to fix these problems and improve analyst workflow while prioritizing resilience against threats.

It's time for defenders to feel empowered to take on the most pressing cybersecurity threats.

Modern endpoint protection helps your business:

- ✓ Achieve better outcomes
- ✓ Maximize security, operational and economic value

5 KEY CAPABILITIES



1 **PREVENTION** — Next-generation antivius (NGAV)

2 **DETECTION** — Endpoint detection and response (EDR)

3 **MANAGED THREAT HUNTING** — Proactive human-led threat hunting

4 **THREAT INTELLIGENCE** — Anticipation

5 **VULNERABILITY MANAGEMENT AND IT HYGIENE** — Readiness

In this eBook, we reveal how you can add value to your security team without draining resources. Read on to learn more about each of these key endpoint elements.

Prevention: Deny Entry to Bad Actors

Traditional, malware-centric endpoint protection — like antivirus — is typically only effective against known malware. Since adversaries now favor sophisticated fileless and malware-free tactics, it's time for many organizations to advance their protections.

Security and IT teams need the intelligence of a next-generation antivirus (NGAV) solution capable of recognizing and preventing:

- Known and zero-day malware
- Ransomware
- Fileless and malware-free attacks

Using a combination of artificial intelligence, behavioral detection, machine learning (ML) algorithms and exploit mitigation, advanced NGAV solutions immediately anticipate and prevent known and unknown threats.

Where legacy solutions require daily updates, NGAV solutions use ML to keep security current — freeing up time used for tedious tasks.

Advanced NGAV solutions combine techniques that provide the visibility and context needed to prevent modern attack tactics, techniques and procedures (TTPs) from succeeding.

Malware-free activity is on the rise

71%	**2022**
62%	2021
51%	2020
40%	2019
39%	2018

Source: CrowdStrike 2023 Global Threat Report

What's behind the shift away from malware?

- Prolific abuse of valid credentials to facilitate access and persistence in victim environments
- The rate at which new vulnerabilities are disclosed and the speed with which adversaries are able to operationalize exploits

Detection: Find and Remove Attackers That Slip Through

Even the best prevention strategy is not enough against today's sophisticated, well-funded attackers. The safest course is to integrate prevention with a strong detection strategy to be able to quickly identify and respond to the most sophisticated stealthy attacks.

Survival of the Fastest

CrowdStrike tracks a metric known as breakout time — the time an adversary takes to move laterally, from an initially compromised host to another host within the victim environment. The average breakout time for interactive eCrime intrusion activity declined from 98 minutes in 2021 to just 84 minutes in 2022. Detecting and responding within the breakout time window gives defenders the best chance to minimize the costs and other damages caused by attackers.

For defenders, disconnected tools, siloed platforms and separate consoles allow adversaries to easily gain an initial foothold without raising alarms. As security stacks grow in complexity, attackers are able to hide amid the gaps and extend their stay.

Modern endpoint security should provide full-spectrum visibility, detection and response across the entire endpoint fleet, wherever those endpoints might be in the world. The unified CrowdStrike Falcon® platform empowers security teams with easy-to-use, enterprise-grade extended detection and response (XDR) built on a foundation of industry-leading endpoint detection and response (EDR).

With this detection strategy, even if a bad actor manages to gain access to a system, EDR paints a clear picture of their attempts to move laterally or gain further access and:

- Records all activities of interest for deeper inspection in real time and post-activity
- Visualizes the suspicious behavior from start to finish
- Enriches the data with adversary-driven threat intelligence to provide needed context for successful threat hunting and triage
- Enables quick, complete and remote response across multiple endpoints

84 minutes is all it takes for an attacker to start moving laterally. This is known as **breakout time** — the time an adversary takes to move laterally, from an initially compromised host to another host within the victim environment.

Source: CrowdStrike 2023 Global Threat Report

Managed Threat Hunting: Elevate Detection Beyond Automated Defenses

A proactive, human-led approach to actively search for suspicious activities strikes the right balance of technology and expertise. Rather than relying on technology alone to automatically detect and alert on a potential attacker's activity, threat hunters can anticipate cyber threats against an organization.

Staffing an expert team to monitor your environment 24/7 to find malicious activities is often unrealistic. Managed threat hunting helps solve staffing and expertise issues.

Threat hunters take a proactive approach to endpoint protection. Drawing on their years of experience, organizations receive full-cycle remediation without the overhead. With visibility across the endpoint estate and access to the right threat intelligence, they can understand what they are seeing and begin to anticipate cyber threats against the organization to mitigate risk.

Global cybersecurity workforce gap

3.4 million people

Source: (ISC)² 2022 Cybersecurity Workforce Study

> Managed threat hunting teams analyze threats and work closely with in-house teams, guiding them from detection through response. This interaction with experts raises the maturity level of in-house security and IT teams over time, not just in the moment.

Threat Intelligence: Understand and Anticipate Attacks

The ability to understand and predict attacks informed by threat intelligence is a vital part of every organization's readiness for advanced attacks. To supercharge your SOC, your endpoint security solutions should incorporate threat intelligence beyond publicly sourced, low-fidelity, after-the-fact intelligence.

Threat intelligence should:

- **Deliver actionable information** that allows security teams and the security solutions they use to understand, respond to and resolve incidents faster, accelerating investigations and incident remediation.
- **Generate and prioritize alerts** that help security teams better understand the tactics and campaigns associated with specific bad actors.
- **Be seamlessly integrated into any endpoint protection solution** so intelligence is at the fingertips of security and IT teams. And when delivered through a single console, analysts can see context within an alert and uncover details with a simple click.

Threat intelligence must be integrated into the SOC workflow, correlated to the latest vulnerability information and, most importantly, trusted by the entire security team to continuously provide timely, unique and relevant threat insights.

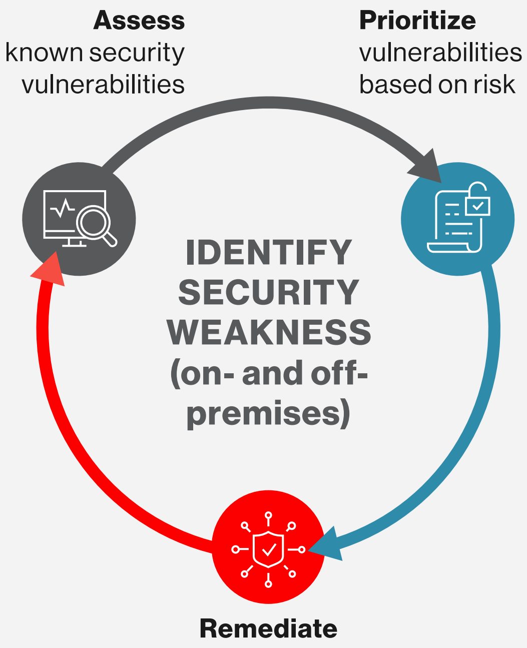
Vulnerability Management and IT Hygiene: Fortify Your Environment Against Attacks

Security and IT teams need to be able to understand which systems and applications are at risk, and who and what are active in the environment. Vulnerability management and IT hygiene provide the visibility and actionable information to make that happen.

Despite their best efforts, organizations will inevitably miss certain patches and mitigations for the ever-growing volume of critically ranked vulnerabilities. It's daunting, if not impossible, to give each vulnerability the time needed to mitigate and respond to protect the environment.

Human-activated threats are a leading cause of today's breaches. IT hygiene solutions offer visibility into log-on trends (e.g., activities and duration) across your environment, wherever credentials are used and administrator credentials are created. With the ability to see every detail, security teams can detect and mitigate credential abuse and attacks that employ stolen credentials with confidence.

REQUIREMENTS FOR EFFECTIVE VULNERABILITY MANAGEMENT


Assess
known security vulnerabilities
Prioritize
vulnerabilities based on risk
IDENTIFY SECURITY WEAKNESS (on- and off-premises)
Remediate

88%

of all data breaches are caused by an employee mistake

Source: Stanford, Psychology of Human Error

IT hygiene solutions continuously monitor for changes in assets, applications and users. Using this insight helps pinpoint unmanaged systems and those that could be at risk on the network, such as unprotected "bring-your-own" devices and third-party systems.

Take the Next Step

With attacker breakout time now faster than ever, and ML and AI becoming easier to use by the day, it is clear that attackers will continue to move faster and faster. Your organization needs an endpoint security solution that puts time on its side.

Start here with better technology and expertise. End with better protection.
The five key capabilities outlined in this eBook will set you up for the in-depth visibility and control needed to outpace the adversary. But point products for the capabilities won't offer you the maximum speed, flexibility and capacity required to defend against modern attackers.

Organizations will benefit most from adopting a fully enabled, integrated solution delivered through a cloud-native platform like CrowdStrike Falcon. With hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities, CrowdStrike's industry-leading solution can protect all companies, from small businesses to global enterprises.

Eradicate threats with multi-domain, multi-vendor protection without disruption to your business, maximizing your ROI.

Share

Share this eBook on your social channels to help spread the word about securing against endpoint risk.

Tweet | Share | Share

Engage

Get fast and easy protection against all threats with our free trial. One cloud-native platform, fully deployed in minutes.

Try

Connect

Book a meeting with CrowdStrike to learn more with our easy-to-use scheduler tool. Simply select a time that works best for you.

Schedule

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.

Learn More

Follow us:

- **Blog ›**
- **Twitter ›**
- **LinkedIn ›**
- **Facebook ›**
- **Instagram ›**

Start a free trial today

CROWDSTRIKE