stryke. CROWDSTRIKE

eBook


# 5 CRITICAL CAPABILITIES FOR MODERN ENDPOINT SECURITY

Why full visibility leads to stronger protection

# What You Can't See on Endpoints *Will* Hurt You

Every day, organizations move more applications, infrastructure and data into the cloud. The number of endpoints accessing them is exploding. An endpoint is any device that can be connected to a network, including computers, laptops, mobile phones, tablets and servers, as well as any other device that can be connected to the internet (i.e., the Internet of Things, or IoT). This is why the endpoint has emerged as one of the great sources of risk for any organization.

Lack of visibility and scalability in this expansive environment poses a serious challenge to the security and IT teams charged with protecting endpoints — and legacy security systems can't really help. These solutions, originally developed to identify known malware files, were never designed to scale and deliver the level of visibility needed to protect today's expansive environment, targeted by attackers using **fileless malware**, exploiting platform and app vulnerabilities, stealing and abusing identities, and injecting **advanced persistent threats**.

Complexity is the attacker's friend. Visibility and control over what is happening on endpoints are made difficult, if not impossible, for many reasons, especially the ever-growing number of endpoints that frequently change locations. Bad actors count on security gaps resulting from insufficient visibility and lack of control to tip the scales in their favor.

What does it take for security and IT teams to stay nimble, efficient and effective in protecting endpoints?

# Modern Endpoint Protection Needs Full Visibility

Truly effective endpoint protection must provide the highest possible level of security, yet be simple to use. Complexity strains teams and processes, introducing security gaps that increase the risk of reduced productivity and harm to an organization's reputation.

To achieve both security and simplicity, endpoint protection must include five key elements:

1. **Prevention** to keep out as many malicious elements as possible
2. **Detection** to find and remove attackers
3. **Managed threat hunting** to elevate detection beyond automated defenses
4. **Threat intelligence** to understand and stay ahead of attacks
5. **Vulnerability management and IT hygiene** to prepare and strengthen the environment against threats and attacks

These five capabilities can only be fully enabled, integrated and delivered through a cloud-native platform that simplifies security operations and meets the speed, flexibility and scalability required to defend against today's most sophisticated threats.

# Prevention: Deny Entry to Bad Actors

Traditional, malware-centric endpoint protection — like antivirus solutions— is typically effective only against known malware, which, given the rise in increasingly sophisticated fileless and malware-free tactics, is insufficient in today's threat landscape.

Security and IT teams need the intelligence of a **next-generation antivirus (NGAV)** solution capable of recognizing and preventing both known and zero-day malware, ransomware, and fileless and malware-free attacks. Advanced NGAV solutions can leverage behavioral analytics to automatically look for signs of attack and block them as they are occurring.

Unlike legacy security solutions requiring daily updates that leave endpoints temporarily unprotected, NGAV solutions can leverage machine learning (ML) to keep security current without burdening security and IT teams. The best NGAV solutions combine these and other advanced techniques that provide the visibility and context needed to prevent modern attack tactics, techniques and procedures (TTPs) from succeeding.

But, as all experienced security teams know, even the best prevention strategy is not enough against today's sophisticated, well-funded attackers. The safest course for an organization is to integrate prevention with a strong detection strategy to identify and block any stealthy attack that gets through.

## BEYOND MALWARE

A recent study showed that 68% of detections from April to June 2021 were not malware-based. Attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint, using legitimate credentials and built-in tools ("living off the land") — deliberate efforts to evade detection by traditional antivirus products. SOURCE: CROWDSTRIKE 2021 THREAT HUNTING REPORT

# Detection: Find and Remove Attackers Who Slip Through

When attackers can gain an initial foothold without raising alarms, they can dwell silently in an environment and do damage for days, weeks or even months without detection.

Endpoint detection and response (EDR) solutions with tightly integrated prevention capabilities provide the visibility security teams need to uncover such attackers as rapidly as possible. To do so, an EDR solution should record all activities of interest on an endpoint for deeper inspection, both in real time and after the fact, and enrich this data with threat intelligence to provide needed context for successful threat hunting and investigation.

Security teams should not have to spend time writing and fine-tuning detection rules. An efficient EDR solution will have the intelligence to automatically detect malicious activity, presenting teams with real attacks and not distracting them with false positives and benign activity. Powerful response actions allow teams to contain and investigate compromised systems, including on-the-fly remote access to take immediate action and stop the breach in its tracks.

While advanced EDR solutions can detect stealthy attacks and uncover threats that have circumvented prevention, organizations can take an even more proactive step in protecting endpoints: incorporating human threat hunters.

## TOO SMART FOR LEGACY ANTIVIRUS SOLUTIONS

In late 2021, a supply chain attack involving a popular software package — with over 7 million weekly downloads from the npm library — was compromised and used to distribute cryptocurrency miners and password stealers. The best defense against this type of attack is behavior-based detection of indicators of attack (IOAs) to identify and block malware delivered through the tainted library. This detection draws on intelligence derived by continuously monitoring TTPs used by actors and unnamed groups. SOURCE: "COMPROMISED NPM PACKAGE USED IN SUPPLY CHAIN ATTACK," CROWDSTRIKE BLOG, OCT. 26, 2021

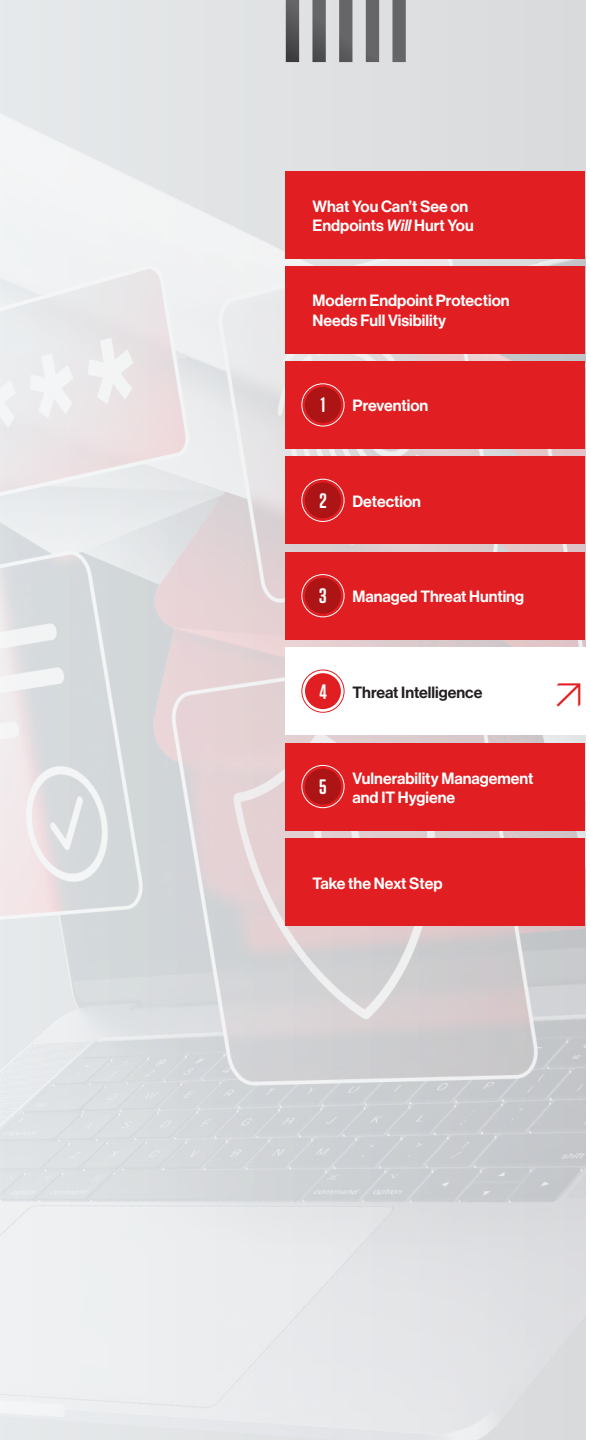
# Managed Threat Hunting: Elevate Detection Beyond Automated Defenses

**Threat hunting** lets organizations take a proactive, human-led approach to actively search for suspicious activities rather than relying on technology alone to automatically detect and alert on a potential attacker's activity.

Managed threat hunting helps organizations that lack the resources and security expertise to find malicious actors and stop advanced threats from silently lurking in their environment. A highly experienced threat hunting team can monitor your environment 24/7 to find stealthy, malicious activities.

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 not just in the moment but over time.

**Threat hunters take a proactive approach** to endpoint protection, drawing on their years of experience. With visibility across the endpoint estate and access to the right threat intelligence, they can not only understand what they are seeing but begin to anticipate cyberthreats against the organization.



# Threat Intelligence: Understand and Anticipate Attacks

Attackers move so quickly and stealthily that it is challenging for both protection technologies and security professionals to keep up with the latest threats and proactively protect against them. To respond just as quickly, endpoint security solutions should always incorporate threat intelligence and/or have the ability to integrate third-party 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 that it's at the fingertips of security and IT teams. Teams should not have to manually switch between different security solutions but instead see context within an alert and simply click to go to another screen with more detail.

The ability to understand and predict attacks informed by threat intelligence is a key part of any organization's readiness for advanced attacks — and vulnerability management and IT hygiene strengthen defenses even further.

# Vulnerability Management and IT Hygiene: Fortify Your Environment Against Attacks

**Vulnerability management** and IT hygiene provide the visibility and actionable information that security and IT teams need to understand which systems and applications are at risk as well as who and what are active in the environment.

Effective vulnerability management requires regular, continuous monitoring of all endpoints to identify security weaknesses wherever they reside, whether on or off premises. To ensure production systems are secure with current patches, organizations must know which vulnerabilities represent the highest level of risk to their organization and target those remediations.

Despite their best efforts, organizations will inevitably miss certain patches and mitigations for the ever-growing volume of critically ranked vulnerabilities. It's a daunting if not impossible task to give each vulnerability the time needed to mitigate and respond to protect the environment. IT hygiene solutions continuously monitor for changes in assets, applications and users and help pinpoint unmanaged systems or those that could be at risk on the network, such as unprotected BYOD or third-party systems.

Gaining visibility into logon trends (e.g., activities and duration) across your environment, wherever credentials are used and administrator credentials created, enables security teams to detect and mitigate credential abuse and attacks that employ stolen credentials.

Vulnerability management and IT hygiene provide security teams with the information they need to take an efficient, proactive stance to improve their overall security posture and be well-positioned to anticipate and defeat adversaries.

# Take the Next Step

This eBook has outlined what security and IT teams should expect in a comprehensive approach to endpoint protection: prevention, detection, managed threat hunting, threat intelligence, and vulnerability management and IT hygiene.

Together, they provide comprehensive, enterprise-wide protection while reducing management overhead and significantly improving performance, agility and scalability.

These five critical capabilities for modern endpoint security can only be fully enabled, integrated and delivered through a cloud-native platform that simplifies security operations and meets the speed, flexibility and capacity required to defend against modern attackers.

Are you ready to find a solution that delivers robust endpoint protection with all five critical capabilities?

- **View this infographic** to quickly understand the differences between legacy and modern endpoint protection
- **Learn how** CrowdStrike cloud-native endpoint protection delivers the visibility that enables all five critical capabilities that organizations need for a strong security posture.

# 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.**

Learn more: https://strykenow.com/



stryke.