CROWDSTRIKE

White Paper

Presented by:

academia
the technology group

Endpoint Protection Buyer's Guide

Critical Capabilities for Modern Endpoint Protection

Protecting endpoints stands out as one of the most critical security challenges in the modern workplace. Despite this, organizations have historically treated endpoint solutions primarily as basic device management tools, overlooking the fact that endpoints are prime targets for attackers. The surge in remote and hybrid work arrangements has further heightened the risk, with adversaries intensifying efforts to exploit any disparities in control and security. The proliferation of new, often unsecured access points to networks and data, coupled with the rapid deployment of new infrastructure, has provided threat actors with an expanded attack surface, allowing them to escalate both the volume and reach of their activities.

According to IBM, "various studies estimate 90% of successful cyberattacks originate at the endpoint," as adversaries seek to establish a foothold for launching identity-based attacks, pivoting to cloud infrastructure, exploiting vulnerabilities and more.[1]

The escalating pace and sophistication of threats have compelled security and IT teams to evaluate their current endpoint security capabilities. Yesterday's signature-dependent security with heavy agents, high maintenance overhead and a disjointed user experience are ineffective and inefficient, bogging down security teams and leaving companies vulnerable to compromise.

In response to these challenges, CrowdStrike has created this guide to assist you in effectively safeguarding your organization against modern threats. The guide aims to delineate the essential components and elements that should constitute a modern endpoint protection strategy.

Necessities in an Endpoint Protection Platform

Yesterday's techniques for detecting and blocking threats at the endpoint prove ineffective against many tactics employed by today's attackers. Breaches can no longer be reliably prevented solely through the monitoring and scanning of files while searching for known malicious entities — especially when done within a vacuum.

Sophisticated threat actors actively seek out gaps in security silos, demanding more than just a collection of disparate security products to qualify as a capable endpoint protection solution. To be genuinely effective, an endpoint protection solution must be meticulously designed to enhance analyst workflows while prioritizing resilience against threats throughout the entire attack continuum.

Modern Endpoint Protection with Artificial Intelligence

To stay ahead of modern-day adversaries, modern endpoint protection is required. The observed average breakout time for interactive eCrime intrusion activity decreased from 84 minutes in 2022 to 62 minutes in 2023, according to the CrowdStrike 2024 Global Threat Report. Artificial intelligence (AI) stands as a foundational element that distinguishes modern-day endpoint protection from legacy alternatives. With AI, your endpoint protection can leverage models trained on trillions of data points daily to predict and thwart threats effectively. This capability is especially crucial when defending against fileless attacks. The same CrowdStrike report revealed that 75% of observed attacks were malware-free in 2023, a notable increase from 51% in 2020.

Embracing a Cloud-Native Approach

Harnessing the data necessary to empower AI-enabled endpoint protection demands a scalable, cloud-native platform.

A cloud-native approach facilitates the effortless aggregation, sharing, and operationalization of this information, providing the kind of anticipation, prevention, detection, visibility, and response capabilities that can consistently outperform a determined attacker time and time again.

[1] IBM, "What is endpoint security?": https://www.ibm.com/topics/endpoint-security

Consolidation with a Single Security Platform

As organizations strive to keep pace with the escalating speed of adversaries, many opt to expand their array of security tools to monitor and manage their entire attack surface. Unfortunately, the addition of more tools often introduces more problems, as organizations attempting to close security gaps may experience poor security outcomes, incur additional costs and allocate resources to manage various tools. On average, organizations have nearly 50 security tools in their environments, with some having more than 140,[2] and according to the CrowdStrike 2024 State of Application Security Report, 70% of critical issues require more than 12 hours to resolve. Moreover, adversaries thrive in the gaps between tools, exploiting vulnerabilities and finding ways to remain undetected in fragmented environments.

When seeking a modern endpoint security solution, it's crucial to choose one that enables your organization to consolidate all security needs into a unified platform solution. A single platform provides complete attack visibility and integrated threat context delivered through a single, lightweight agent that can locally enforce defense without impeding endpoint activity. The agent should also be unified, enabling organizations to expand their security over time without the need to add additional agents in the future. This allows security teams to activate new protections in seconds, all while utilizing the same agent deployed on Day One. As organizations intensify efforts to combat increasingly sophisticated attacks, the ability to surface information effectively becomes paramount. A single platform allows you to query vast data across your entire security posture, extracting the information needed to make better, faster decisions.

These necessities should be a focus when selecting your endpoint security solution. With these considerations in mind, we will now explore the five elements that constitute modern endpoint protection, including the key capabilities they should possess and the features required for those capabilities to be effective:

- Prevention
- Detection and Response
- Identity Threat Detection and Response
- Threat Intelligence
- Managed Threat Hunting

[2] IDC, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans? Document number: #US51973524, Mar 2024, https://www.idc.com/getdoc.jsp?containerId=US51973524

The Five Elements of Modern Endpoint Protection

Element 1: Prevention

Protect against malware and fileless attacks with next-generation antivirus (NGAV)

There are sound reasons why traditional, malware-centric endpoint protection products simply do not provide an adequate level of protection against today's threats and adversaries.

Malware-centric protection fails to address the increasingly sophisticated tactics employed by modern adversaries, particularly in the realm of fileless and malware-free techniques. According to the CrowdStrike 2024 Global Threat Report, 75% of attacks were malware-free, reflecting a continuing upward trend.

An effective endpoint protection solution needs to solve this challenge by expanding beyond merely identifying and addressing known malware. It should:

- Protect against known and unknown malware using technologies such as machine learning (ML) that do not require daily updates and can generalize defenses against never-before-seen attacks.
- Look beyond malware and fully leverage behavioral analytics to automatically look for signs of attack and block them as they occur.
- Protect endpoints against all types of threats — from known and unknown malware to fileless and malware-free attacks — by combining all necessary technologies for ultimate protection.

Key Capabilities	Required Features
Detection of advanced and unknown threats, including fileless attacks	• Protection powered by artificial intelligence and machine learning to prevent known and unknown malware, adware and potentially unwanted programs (PUPs) • Advanced behavioral analysis with indicators of attack (IOAs) • High-performance memory scanning • Exploit mitigation • Automated malware analysis (e.g., sandboxing)
Speed to outpace adversaries	• Signatureless technology to eliminate the need for time-intensive updates • A single, lightweight, unified agent for a fast deployment and instant protection
Integrated threat intelligence	• Understanding of scope and impact of threats found in your environment • Visibility into threats at the adversary level • Threat severity assessments for prioritization • Threat analysis with recovery steps to resolve incidents

Element 2: Detection and Response

Uncover advanced threats faster with endpoint detection and response (EDR)

While NGAV is an important first line of defense for an organization, it is not foolproof. No NGAV solution, no matter how advanced, can outright prevent every threat, particularly in the face of never-before-seen attacks or those that take advantage of stolen credentials or trusted tools.

The next level of protection is EDR with built-in native extended detection and response (XDR). Previous incarnations of threat detection solutions focus on basic functionality for endpoint monitoring. These legacy monitoring tools frequently create extra work for analysts, inundating them with raw, unenriched telemetry and alerts with very little actionable information. The more complicated the security tools, the greater the likelihood that a security gap will be created and go unnoticed until there's a breach.

Modern EDR, delivered on a unified security platform, addresses these issues. Modern EDR unlocks enterprise-wide visibility by unifying and streamlining security analysis, investigation and remediation into one easy-to-use console. Additionally, built-in native XDR extends security data correlation, analysis and workflows beyond the endpoint to encompass other native capabilities of the unified platform such as identity threat prevention. This enhances visibility around advanced and evasive security threats and allows for a more seamless and accurate response. EDR with built-in native XDR dramatically improves threat visibility, accelerates security operations, reduces total cost of ownership (TCO) and eases the ever-present security staffing burden.

To outpace today's adversaries, organizations must use EDR to optimize threat detection, investigation, hunting and response enterprise-wide, and use native XDR to extend visibility and control across key attack surfaces. When evaluating options, look for an EDR solution that includes XDR capabilities so it has the best coverage over your full endpoint estate and beyond.

Key Capabilities	Required Features
Full attack visibility	• Enterprise-wide search with zero impact on endpoints • Cross-domain data correlation beyond the endpoint • Intuitive and comprehensive alert visualization — displays full attack history in a process tree with drill-down and pivot capabilities • Attack steps mapped to a standard industry attack framework such as MITRE ATT&CK
Detection of attacks that circumnavigate prevention	• Captures raw events, even when not associated with alerts and detections • Operates in kernel mode for full visibility and to eliminate blind spots • Centralized data repository to enable advanced detection • Automatic detection based on behavioral analysis such as IOAs
Incident triage and investigation analysis	• Automated triage with intelligent prioritization of malicious and attacker activity • Correlation of individual events into incidents • Intelligent, AI-powered investigation recommendations • Flexible data retention period for events • Fully customizable real-time and historical search capabilities • Cross-domain context • Remote access to and interact with endpoints in real time • Ability for analysts to collaborate and work together on incidents in real time from any location • Correlation of context to identify suspicious behavior and potential at-risk endpoints
Accelerated remediation and response	• Ability to network-contain endpoints • Ability to quarantine files • Ability to run commands on suspicious endpoints remotely and in real time • Ability to take response actions for other native capabilities across domains • API to integrate with the customer's existing orchestration/case management systems • Customizable alert notifications

Element 3: Identity Threat Detection and Response (ITDR)

Stop modern identity-based attacks in real-time

If your endpoint protection doesn't include identity security, you're leaving the door open to opportunistic adversaries. With the continued rise of malware-free attacks, adversaries are hunting for gaps between how endpoints are secured and identities are managed. In many cases, adversaries aren't breaking in, they're logging in. Once they know how to steal identities — and the privileged access credentials that go with them — they can quickly gain access undetected.

Organizations use identity solutions to gain visibility into the security hygiene of their identity infrastructure like Microsoft Active Directory and Entra ID. This helps to proactively prevent identity-based threats before they start. It is critical to identify compromised passwords, over-privileged accounts and other security gaps that can leave your organization exposed. By unifying endpoint protection and identity security, you can also get insights into possible attack paths that adversaries can exploit across the network.

ITDR solutions help organizations detect and respond to identity-based threats in real time. This can include attacks like ransomware, lateral movement, service account misuse, Pass-the-Hash (PtH), Golden Ticket and more. When evaluating ITDR solutions, it is critical to ensure the ability to stop lateral movement, including hybrid lateral movement from on-premises to cloud environments, and from managed to unmanaged devices. You can create policies that correlate with the attack paths you've identified and leverage known adversary tactics, techniques and procedures (TTPs).

While it is critical to stop adversaries with real-time identity protection, organizations must continue to enable business productivity in the process. That's why applying risk-based, conditional access — through multifactor authentication (MFA) — needs to be included in the ITDR solution. Baselines of normal user behavior can be established to quickly identify anomalies as sophisticated adversaries move across endpoints and identities. Then, you can enforce MFA to increase security without disrupting legitimate users.

Key Capabilities	Required Features
Reduce identity store attack surface	• Ensure visibility across cloud (Microsoft Entra ID or Okta), on-premises Microsoft Active Directory and hybrid identity stores • Automatically classify all identities (i.e., human and service accounts) • Gain insights into identity store hygiene including potentially compromised accounts • Identify possible identity-based attack paths that can be exploited
Detect and prevent identity-based threats	• Detect and respond to identity threats across your estate • Create policies that correlate with the attack paths and known adversary TTPs • Address vulnerabilities inherent in cloud and Active Directory identity stores • Ensure that ITDR is included in managed threat hunting
Enable conditional access	• Enable risk-based MFA • Extend MFA protection to legacy apps/tools • Digest risk scores to to baseline risk posture

Element 4: Threat Intelligence

Stay ahead of adversaries by knowing how and why they attack

Without threat intelligence integrated into your endpoint protection, it becomes challenging for both protection technologies and security professionals to keep up with the latest threats and proactively defend against them.

Threat intelligence elevates NGAV and EDR/XDR detections to the next level, not only revealing what happened on the endpoint but also exposing the "who, why and how" behind the attack. Understanding the threat at this level is crucial for staying ahead of future attacks and increasing the cost to the adversary. Moreover, threat intelligence furnishes the information necessary for security teams to comprehend, respond to and resolve incidents more swiftly, thereby accelerating investigations and incident remediation.

When assessing endpoint protection, it's essential to look beyond security infrastructure. Actionable threat intelligence must be an integral part of the total solution. Customers should ensure that the intelligence seamlessly integrates into the endpoint protection solution and that its consumption can be automated.

Key Capabilities	Required Features
Extended endpoint integration	• Threat intelligence built into the EDR/XDR solution to ensure no additional administration or deployment is required • Automatic forwarding of all quarantine files from the endpoint to threat intelligence for immediate investigation
Automation and simplification of incident investigations	• Malware sandbox analysis and malware search • Prioritization for patching critical systems • Ability to pivot from across security platform to view attack context
Sharing of custom IOCs for security orchestration	• Automatically generated custom indicators of compromise (IOCs) and intelligence on threats relevant and unique to an environment, delivered within minutes • Automatically ingested third-party IOCs
Adversary identification	• Identification of adversaries focused on attacking your business, region or industry • Adversary intent and capability data for future attack prediction

Element 5: Managed Threat Hunting

Outpace the adversary with 24/7 expert hunting

Proactive threat hunting, led by human security experts powered by AI, is a must for any organization seeking to achieve or enhance real-time threat detection and incident response.

Threat hunting plays a crucial role in the early detection of attacks and adversaries. Instead of relying on reactive, preset defenses, human-led investigations actively search for suspicious activities, avoiding passive reliance on autonomous solutions to detect and alert automatically. This approach enables organizations to identify malicious activity early and thwart attacks before irreparable damage occurs.

Although critical, threat hunting is only as good as the threat intelligence on which it's based. Threat hunting must be informed by the intelligence gathered from an organization's environment to identify novel attacks, misuse of remote access tools, credential compromises, insider threats and more. When evaluating a threat hunting solution, ensure that it's intelligence-led and can be applied across both endpoint and identity protection.

Unfortunately, a lack of resources and a shortage of security expertise make proactive threat hunting unattainable for most organizations. According to the ISC2 Cybersecurity Workforce Study 2023, nearly 4 million additional cybersecurity workers are needed to effectively secure assets.[3]

Understaffed internal teams struggle to maintain 24/7 monitoring for adversary activity, and often, they lack the capability to efficiently respond to highly sophisticated attacks. This can lead to prolonged investigation times with fewer alerts handled promptly, ultimately resulting in extended dwell times and an increased risk that attackers will successfully achieve their goals.

Managed threat hunting addresses this challenge by providing an elite hunting team. This team not only identifies malicious activities that may have been overlooked by automated security systems but also conducts thorough analyses and provides customers with response guidelines. When considering a modern endpoint security solution, it's crucial to choose one that seamlessly enables managed threat hunting.

Key Capabilities	Required Features
24/7 human expertise	• Experienced and dedicated in-house threat hunters providing 24/7 threat hunting services • Assistance during incidents and guidance on what to do next, including potential mitigation suggestions on detections • Ability to find novel threats that no other systems have detected • Immediate access to threat intelligence experts for faster analysis • Automatic and native integration with threat intelligence for ultimate efficiency • Integration with the endpoint security platform
Visibility into missed alerts	• Ability to pinpoint the most urgent threats in the environment across both endpoint and identity • Enhanced closed-loop communications to ensure important alerts are noticed.

[3] ISC2 Cybersecurity Workforce Study 2023, "How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce," https://media.isc2.org/-/media/Project/ISC2Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

The CrowdStrike Difference

Armed with an understanding of what capabilities you need from a modern endpoint security solution, let's look at CrowdStrike's approach to modern endpoint security.

Advanced Technologies

Since the company's founding in 2011, CrowdStrike has pioneered the use of AI and ML in cybersecurity to solve customers' most pressing challenges. CrowdStrike's endpoint protection solution incorporates innovative technologies — including AI/ML, behavior protection and exploit mitigation — to thwart the rapidly evolving TTPs used by adversaries to breach organizations. This encompasses commodity malware, zero-day malware and even advanced malware-free attacks.

Through the use of AI/ML, CrowdStrike avoids dependence on signature-based methods or IOCs, which can result in "silent failure" and allow data breaches to occur. Instead, CrowdStrike adopts behavioral approaches that actively search for IOAs, ensuring that the business is alerted to suspicious activities before a compromise takes place. AI-powered indicators of attack (IOAs) are the latest evolution of CrowdStrike's industry-first IOAs, expanding protection with the combined power of cloud-native machine learning and human expertise. AI-powered IOAs use the speed, scale and accuracy of the cloud to rapidly detect emerging classes of threats and predict adversarial patterns, regardless of tools or malware used.

Single-Agent, Cloud-Native Approach

The single CrowdStrike Falcon agent is built on a scalable, cloud-native platform that is easy to deploy and manage. All Falcon platform modules are designed to utilize the same lightweight agent, which is unobtrusive, has a minimal impact on the endpoint and allows organizations to seamlessly deploy new defenses without the need for additional agents.

In conjunction with the single, lightweight agent, CrowdStrike's endpoint protection delivers faster deployment times, improved endpoint performance and greater operational ease for the IT team due to its cloud-native approach. The only way to ensure zero impact on endpoints while enabling real-time search, analysis and investigation is by leveraging cloud technology. Deployed in minutes with no reboot required, the Falcon platform operates from Day One without the need for custom tuning, is automatically kept up-to-date, and functions without interrupting your existing AV during migration.

Unified Platform Consolidation

One of the most important factors to consider when selecting an endpoint protection solution is how well it will integrate within the broader cybersecurity architecture without adding complexity or requiring any on-premises management infrastructure.

The CrowdStrike Falcon platform is designed as a highly modular and extensible offering that assists customers in addressing new security challenges with a single agent and without the need to re-architect or re-engineer the architecture, eliminating friction associated with security deployments.

More and more organizations are rethinking their cybersecurity strategies and are looking for a more integrated approach. An example of this is unifying endpoint protection and ITDR in order to remove coverage gaps and the complexity that comes when these solutions are deployed separately. With a consolidated platform that includes endpoint and identity, you can reduce risk, improve productivity, and save money. By having endpoint and identity security on the same platform, organizations can respond to threats up to 85% faster, offsetting up to 5,000 investigation hours annually.[4] Additionally, organizations can save up to $2 million USD over three years by consolidating endpoint and identity protection.[4]

[4] These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

Beyond unifying endpoint protection with ITDR, research shows that consolidating multiple security products into one unified platform has significant benefits. In a recent study conducted by IDC that analyzed the value of consolidating with the Falcon platform, security teams found that the Falcon platform improved their security operations by helping them identify 96% more potential threats in half the time. Additionally, the Falcon platform enhances security teams' ability to keep up with adversaries, making them 2x more effective and enabling them to investigate/respond 66% faster. Lastly, the IDC report identified an average $6 return for every $1 invested, with a rapid five-month payback period.

Managed Security Services

This paper discusses the critical capabilities necessary for a modern endpoint security solution. However, depending on the unique needs of different organizations, these critical capabilities may be best delivered through a managed solution. Many organizations face challenges in hiring, training and retaining cybersecurity staff, hindering them from implementing a mature security program or focusing on key business initiatives. The right expertise, processes and strategies are crucial to ensuring endpoint and identity protection is successfully operational 24/7 without causing business disruption.

CrowdStrike Falcon® Complete managed detection and response (MDR) assists organizations in achieving continuous 24/7 security. Falcon Complete MDR provides customers with implementation, platform management, response and remediation services for advanced threats, alleviating the burden, overhead and costs of independently deploying and managing a 24/7 threat detection and response function. With Falcon Complete MDR, you gain expert endpoint protection and management, incorporating key Falcon product modules including Falcon Insight XDR, CrowdStrike Falcon® Prevent NGAV, CrowdStrike Falcon® Discover for IT hygiene and CrowdStrike Falcon® Device Control. Furthermore, CrowdStrike offers CrowdStrike Falcon® Complete Identity Threat Protection, the first and only fully managed service actively monitoring and responding to identity-based attacks in real time, leveraging the dynamic, cloud-native capabilities of the Falcon Identity Protection module. Lastly, included in Falcon Complete MDR is CrowdStrike Falcon® Adversary OverWatch™, the world's #1 intelligence-led threat hunting service powered by advanced AI and unrivaled expertise for 24/7 protection.

With all of these security options included in Falcon Complete MDR, organizations are able to maximize their return on investment (ROI) and enhance security efficacy. A study commissioned by CrowdStrike and conducted by Forrester examined the ROI realized by organizations deploying Falcon Complete. Through customer interviews, independent analysis and financial modeling, Forrester estimated that a composite customer could generate cumulative savings with a net present value of $5.81 million USD over three years, representing an estimated 403% ROI with payback in less than three months. The results further indicated that Falcon Complete added capacity equivalent to 11 full-time SOC analysts, significantly reduced the risk of data breaches and eliminated redundant cybersecurity tools.

Conclusion

The landscape of endpoint protection has undergone significant evolution, propelled by the increasing sophistication of cyber threats and the dynamic nature of modern work environments. Paired with the critical capabilities outlined in this Buyer's Guide, CrowdStrike Falcon's advanced technologies, single-agent cloud-native approach, unified and consolidated security platform, and managed security services clearly position CrowdStrike as a leader in the realm of modern endpoint security. As organizations navigate the evolving threat landscape, adopting a comprehensive solution that aligns with the outlined necessities becomes imperative for achieving robust protection and resilience against contemporary cyber threats.

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: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram

Academia
info@academia.co.uk
www.academia.co.uk
01992 703 9000