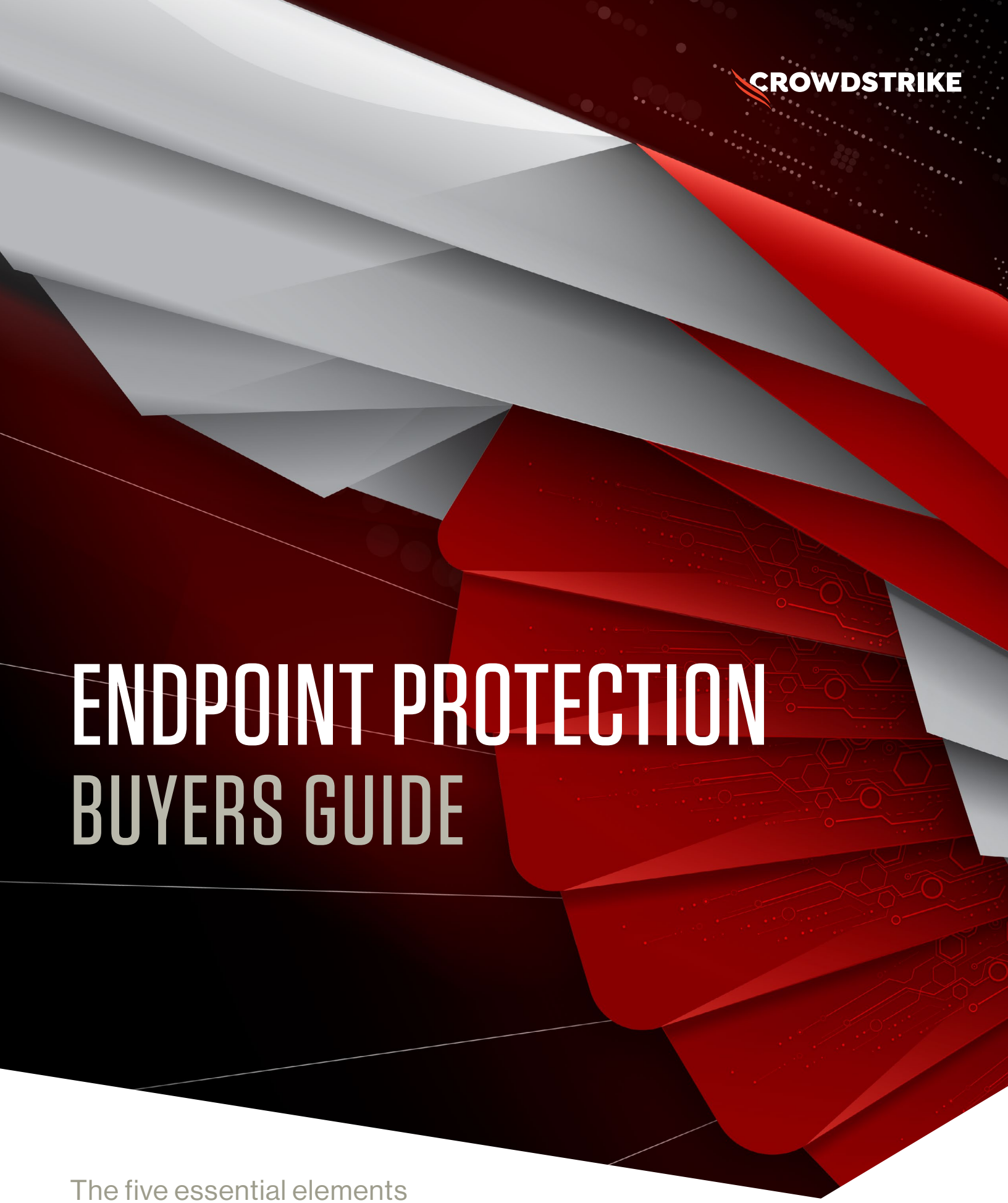

ENDPOINT PROTECTION BUYERS GUIDE

The five essential elements
of cloud-based endpoint protection

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Endpoint security is one of the most critical components of a cybersecurity strategy. Unfortunately, for those responsible for protecting their organizations' endpoints, it has never been more challenging to select the best solution for the job. With so many options on the market and features that sound identical, choosing an endpoint protection solution is anything but straightforward.

CrowdStrike believes that truly effective endpoint protection must provide the highest level of security *and* simplicity — because complexity strains teams and processes, ultimately introducing security gaps and increasing risk. To achieve both security and simplicity, endpoint protection must include five key elements and be delivered through a cloud-native architecture. These objectives can be used as guidelines when evaluating and choosing an endpoint protection platform:

- **Prevention** to keep out as many malicious elements as possible
- **Detection** to find and remove attackers
- **Managed threat hunting** to elevate detection beyond automation
- **Threat intelligence integration** to understand and stay ahead of attackers
- **Vulnerability management and IT hygiene** to prepare and strengthen the environment against threats and attacks

These five elements need to be enabled, integrated and delivered via cloud-native architecture in order to simplify operations and meet the speed, flexibility and capacity required to fend off modern attackers.

So how do you evaluate these elements and find the right solution for your organization? Start by asking the right questions.

We've developed this guide to help you ask those questions and get the information you need to measure and compare different solutions.

As you dive in and gain insight, you'll find CrowdStrike sets a high bar. CrowdStrike delivers everything needed to stop breaches — simply and smartly. The CrowdStrike Falcon® cloud-native endpoint protection platform unifies technology, intelligence and expertise into one solution that's tested and proven to stop breaches. It combines all essential elements in a single agent that can be deployed within minutes, with virtually no impact on endpoints or users. The cloud-native Falcon platform delivers truly effective endpoint protection with the highest-level security *and* simplicity.

With an abundance of options on the market and features that sound identical, choosing an endpoint protection solution is anything but straightforward.

INTRODUCTION

Protecting endpoints has long been a critical component of all security strategies, as they are among the prime targets for attackers. Adversaries often try to exploit crisis and change, and the pandemic has been no exception. With new, often unsecured access points to networks and data along with accelerated setup of new infrastructure, threat actors have been taking advantage of this expanded attack surface and increased both the volume and the reach of their activities.

Increasing threat velocity, along with the need for rapid change as more applications, infrastructure and data move into the cloud, shifted the focus for many security and IT teams. They realize they must be nimble, be efficient and keep security top-of-mind. This transition has placed an even greater emphasis on protection of the endpoint — the new perimeter for many.

This guide was created to help security professionals by defining the critical elements of endpoint protection required to effectively protect an organization against modern threats.

CRITICAL ELEMENTS TO CONSIDER: WHAT YOU REALLY NEED IN AN ENDPOINT PROTECTION PLATFORM

It takes more than a collection of capabilities gathered under one umbrella to qualify as a capable endpoint protection solution. To be truly effective, an endpoint protection solution must be designed to continuously stop breaches across the entire attack continuum.

Yesterday's techniques for detecting and blocking threats at the endpoint are ineffective against today's modern threats. Breaches can no longer be reliably prevented by monitoring and scanning files and looking for known bads.

Security effectiveness is directly related to the quantity and quality of data you're able to collect, and your ability to analyze it regardless of where it comes from. Preventing breaches requires taking this data and applying the best tools, including artificial intelligence (AI), behavioral analytics, threat intelligence and human threat hunters. Effective solutions must leverage this massive data to continuously anticipate where the next serious threat will appear, in time to act.

Harnessing the data and tools to effectively stop breaches requires a scalable, cloud-native platform — a security cloud.

A cloud-native approach enables the seamless aggregation, sharing and operationalization of this information to deliver the kind of anticipation, prevention, detection, visibility and response capabilities that can beat a determined attacker time and time again.

To get those capabilities, decision-makers should look for five critical elements in a cloud-native endpoint protection solution.

THE FIVE CRITICAL ELEMENTS OF ENDPOINT PROTECTION

CRITICAL ELEMENT 1: PREVENTION

PROTECTING AGAINST MALWARE AND BEYOND WITH 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 does not address the increasingly sophisticated fileless and malware-free tactics used by modern adversaries. In fact, the **CrowdStrike 2020 Global Threat Report** noted that the trend toward malware-free attacks is accelerating, with these types of attacks surpassing the volume of malware attacks in 2020.

An effective endpoint protection solution needs to solve this challenge by expanding beyond simply identifying and addressing known malware. First, it should protect against both known and unknown malware by using technologies such as machine learning (ML) that do not require daily updates. It should look beyond malware and fully leverage behavioral analytics to automatically look for signs of attack and block them as they are occurring. In addition, the ideal endpoint protection solution should protect endpoints against all types of threats — from known and unknown malware to fileless and malware-free attacks — by combining all of the necessary technologies for ultimate protection.

Table 1 outlines the key use cases and critical capabilities that the NGAV component of an efficient endpoint protection solution should provide.

NGAV: USE CASES AND ESSENTIAL CAPABILITIES

Prevent both known and zero-day malware	**Required Features** ■ ML on the endpoint to prevent both known and unknown malware, adware and potentially unwanted programs (PUPs) ■ Automated malware analysis (e.g., sandboxing) ■ Integrated threat intelligence ■ Custom allowlist and blocklist capabilities ■ Automatic third-party indicator of compromise (IOC) ingestion
	Evaluation Criteria ● Independent third-party testing results ● False positive rates
	Questions to Ask ● Is the product signature-based or does it use ML? ● If the product uses ML, does the endpoint have to be connected to the cloud to use it? ● Which of the prevention features requires a cloud connection? ● In case malware is not blocked, what other prevention mechanisms does the product provide?
Protect against ransomware	**Required Features** ■ ML on the agent ■ Behavioral analysis/indicators of attack (IOAs) specific to ransomware ■ Integrated threat intelligence
	Evaluation Criteria ● Past performance against real-life ransomware such as WannaCry, NotPetya and Ryuk ● Third-party test results
	Questions to Ask ● What methods does it use to prevent ransomware? ● What methods does it use to prevent zero-day ransomware? ● How did the product handle ransomware outbreaks such as Wannacry, NotPetya and Ryuk?
Prevent fileless and malware-free attacks: Protect your endpoints against all types of threats, not just malware and exploits	**Required Features** ■ Protection against known exploits ■ Protection against zero-day exploits ■ Memory protection ■ Indicator of attack (IOA) behavioral blocking ■ Custom IOA behavioral blocking
	Evaluation Criteria ● Success in MITRE adversary emulation test ● Performance against red team exercises
	Questions to Ask ● What type of non-malware malicious activities can it block? ● Can it block an attacker that is logged-on using stolen credentials and legitimate tools to perform their actions? ● What areas of the MITRE ATT&CK® framework can it protect against? ● Can the solution prevent the malicious utilization of legitimate applications such as PowerShell? How? ● How does the solution block exploits? ● Is the product able to block zero-day exploits? ● In case an attack is not blocked, what other prevention mechanisms does the product employ? ● What type of memory protection mechanisms does the product offer?

Deliver maximum protection at all times: Always protects at the maximum level of its capabilities	**Required Features** ■ Does not require daily updates to keep protection at its highest level ■ Automatically kept up-to-date ■ No reboot on installation or update ■ Protects offline when there is no cloud connection ■ Offers sensor tampering protection ■ Protection across operating systems and OS versions
	Evaluation Criteria ● Frequency and performance impact of updates (product/agent version updates, malware signatures or DAT files, etc.) ● Demo of known, unknown malware and malicious actions on an offline endpoint
	Questions to Ask ● How often does the product need to be updated to ensure the highest level of protection? ● What can the product prevent when offline, if the user opens a file or executable, or performs malicious actions when not connected to the internet? ● How quickly are new OS versions supported? ● Do updates to the sensor require reboots? If so, what impact does this have on critical hosts and servers?
Provide rapid response and remediation	**Required Features** ■ The ability to quarantine a malicious file ■ Keeps detection information for at least 90 days for investigation ■ Provides visibility and context into attacks ■ Submits quarantine files to sandbox for automatic analysis ■ Provides API to integrate with customer's existing orchestration/case management systems
	Evaluation Criteria ● List of actions the solution can take ● Screenshot or demo of alert detail ● Sandbox analysis output ● List of existing security orchestration and ticketing systems the product integrates with
	Questions to Ask ● What response capabilities does the product provide? ● How does the product integrate with existing security tools? ● Do the product alerts provide context to improve overall defenses? ● Can the product generate IOCs from an alert to improve overall defenses?

Table 1. NGAV: Use Cases and Essential Capabilities

THE CROWDSTRIKE APPROACH

The CrowdStrike Falcon endpoint protection platform provides a new generation of prevention features, capable of defeating the sophisticated tools and techniques used by today's attackers and filling the gap left by signature-based antivirus solutions. The Falcon platform combines an array of powerful methods to provide prevention against the tactics, techniques and procedures (TTPs) that make modern attacks successful. That combination of methods allows Falcon to not only protect against commodity malware but also prevent zero-day malware, exploits and importantly, fileless and malware-free attacks. Falcon uses the right prevention feature at the right time to block threats across the entire attack continuum.

Falcon employs ML on the endpoint for pre-execution prevention of both known and unknown malware. Its ML feature is so powerful that it has protected Falcon customers from the ransomware WannaCry, NotPetya and Ryuk, right out of the box — without requiring any action or update from the user.

Falcon also uses exploit mitigation to defend against attackers that leverage exploits as part of either malware-based or malwarefree attacks. Exploit mitigation consists of stopping vulnerability exploit attempts, from both known and zero-day exploits, to prevent hosts from being compromised.

Against sophisticated attackers that will not limit their tactics to the use of malware and exploits, Falcon uses IOAs. These are behavior-based algorithms focused on detecting the intent of the attackers, or what they are trying to accomplish, regardless of the tools used in the attack. IOA-based prevention capabilities allow customers to prevent threats that bypass traditional technologies such as signatures or allowlisting.

Always-on protection means endpoints are secure, whether online or offline. The lightweight Falcon agent has little impact in endpoints, from initial install to day-to-day use, and no reboot is required after installation.

CRITICAL ELEMENT 2: DETECTION

PROVIDING THE RIGHT DATA AT THE RIGHT TIME FOR FAST, CONFIDENT ACTION

Because attackers expect to encounter prevention measures on a target, they have refined their craft to include techniques designed to bypass prevention. These techniques include credential theft, fileless attacks or software supply chain attacks. When an attacker is able to gain a foothold without any alarm being raised, it is called "silent failure," which allows attackers to dwell in an environment for days, weeks or even months without detection. The remedy for silent failure is EDR, which provides the visibility security teams need to uncover attackers as rapidly as possible.

A fully functioning EDR system should tightly integrate with the prevention capability. It should record all activities of interest on an endpoint for deeper inspection, both in real time and after the fact. It should enrich this data with threat intelligence to provide needed context — critical for hunting and investigation. An efficient EDR solution should also be intelligent and able to automatically detect malicious activity and present real attacks (not benign activity) without requiring security teams to write and fine-tune detection rules.

Equally important, the EDR system needs to offer an easy way to mitigate a breach that is uncovered. This could mean containing the exposed endpoints to stop the breach in its tracks, allowing remediation to take place before damage occurs.

Refer to the use cases in Table 2 to guide you in your evaluation of the EDR capabilities for the endpoint protection solutions you are considering.

EDR: USE CASES AND ESSENTIAL CAPABILITIES

Automatically uncover stealthy attackers	**Required Features** ■ Automatic incident detection — intelligent EDR with built-in, real-time detections ■ Automatic detection based on behavioral analysis such as IOAs ■ Integration with threat intelligence ■ Automate triage by intelligently prioritizing malicious and attacker activity ■ Provides real-time organizational threat level
	Evaluation Criteria ● No fine-tuning, rule writing or complex configuration required ● Demo of incident prioritization ● Effective performance against pen tests
	Questions to Ask ● What kind of detection or correlation rules need to be written before the product can detect incidents? ● What expertise level is required to use the solution?
Detect the unknown and hunt for threats: Detect attacks that have circumvented prevention and dramatically reduce attackers' dwell time	**Required Features** ■ Capture raw events, even when not associated with alerts and detections ■ Long-term detection data retention (12 months) ■ Operates in kernel mode for full visibility and to eliminate blind spots ■ Fully customizable real-time and historical search capabilities ■ Simultaneous enterprise-wide searches with zero impact on endpoints ■ Delivers query answers in five seconds or less ■ Centralized data repository to enable advanced detection
	Evaluation Criteria ● The types of events the product is capable of observing and collecting ● Retention period available for both raw events and detections ● Attack detection and specific behavior detection
	Questions to Ask ● What level of visibility does the solution provide (e.g., kernel level)? ● What type of endpoint telemetry data is collected by the agent? ● How does the product facilitate proactive threat hunting? ● How are searches and query results obtained? (e.g., interrogating endpoints, querying a cloud database)? ● Do searches provide real-time results? ● Are there limits on query results? ● Where is the event data stored and for how long? Raw event data? Detection data? ● How does the product provide attack detection and visibility?

Accelerate investigations and forensics	**Required Features** ■ Intuitive and comprehensive alert visualization — displays full attack history in a process tree with drilldown and pivot capabilities ■ Attack steps mapped to a standard industry attack framework such as MITRE ATT&CK ■ Provides forensic data even if an endpoint is unavailable, inaccessible or destroyed ■ Full context detections and alerts including threat intelligence data ■ Flexible data retention period for events ■ Industry-standard query language to search event data ■ Intuitive workflows from a single console ■ Centralized data repository to enable threat hunting and investigation ■ Correlate individual events into incidents
	Evaluation Criteria ● Screenshot or demo of alert visualization ● Proof of concept (POC) or proof of value (POV) ● Adoption of industry framework for attack representation
	Questions to Ask ● Can the product tell me how an attacker is accessing my environment? ● How does the solution allow security analysts to visualize alerts, make the connection between events and pivot to other events and endpoints? ● What type of features allow the product to detect malicious behavior as or after it occurs? ● How does the product detect and visualize lateral movement? ● Does the product correlate individual detection alerts into incidents or attacks?
Accelerated remediation and response	**Required Features** ■ Ability to network-contain endpoints ■ Ability to quarantine files ■ Ability to run commands on suspicious endpoints remotely and in real time ■ API to integrate with customer's existing orchestration/case management systems ■ Customizable alert notifications
	Evaluation Criteria ● List of response capabilities available in the product ● API support and integration with existing security systems and workflows
	Questions to Ask ● What are response capabilities offered by the solution? ● How does the solution integrate with existing security and enterprise tools, such as SOAR solutions and others?

Table 2. EDR: Use Cases and Essential Capabilities

THE CROWDSTRIKE APPROACH

CrowdStrike Falcon Insight™ EDR monitors and records activities taking place on the endpoint, providing the real-time and historical visibility necessary to detect attackers activity while enabling security teams to investigate and resolve incidents quickly. This approach stops attackers before they do damage, essentially eliminating the risk of silent failure.

Falcon also provides both automatic and human-driven analysis capabilities that can be performed as events are taking place or after the fact. The automatic analysis can immediately detect and intelligently prioritize malicious and attacker activity. The manual analysis capability grants security teams the deep visibility and context they need for proactive threat hunting, fast incident investigation and remediation. In addition, CrowdStrike's cloud-native architecture provides the speed and scalability to collect and retain all of the necessary endpoint events, even if the endpoints are unavailable, destroyed or have been deleted (as can be the case for virtual workloads).

CrowdStrike Threat Graph® database, the brain behind the Falcon platform, ingests and analyzes more than 5 trillion events in real time every week, making the Falcon security cloud platform one of the industry's most advanced sources of truth for security insight and adversary intelligence. The CrowdScore™ capability, an innovative detection feature of Falcon Insight, is constantly processing data in Threat Graph, looking for malicious activity by examining all behaviors, whether or not they have been alerted to the user. It is not simply grouping atomic alerts; rather, it is searching for and weighing the evidence of activity that comprises attacker behavior, whether or not it was previously alerted to the user. When an attack is detected, an incident is created. CrowdScore addresses alert fatigue by detecting attacks rather than detecting specific behaviors, resulting in a 98% average reduction in items requiring analysis (comparing alert counts to incident counts).

From a single console, Falcon Insight provides real-time visibility, historical events and the means to analyze data to ensure that organizations can quickly identify any potential silent failures and appropriately respond with the necessary tools.

CRITICAL ELEMENT 3: MANAGED THREAT HUNTING

ELEVATING DETECTION BEYOND AUTOMATION WITH MANAGED THREAT HUNTING

Passively waiting for security products to automatically detect attacks will not uncover and stop sophisticated hidden threats. This is illustrated by the ongoing breaches that happen even in environments where new and advanced security technology has been deployed. This is because passive automated alerts rely on preset parameters that can be tested and bypassed by determined attackers. This is why proactive threat hunting, led by human security experts, is a must-have for any organization looking to achieve or improve real-time threat detection and incident response.

Threat hunting plays a critical role in the early detection of attacks and adversaries. It constitutes a proactive approach that is human-led and actively searches for suspicious activities rather than passively relying on technology to automatically detect and alert on a potential attacker's activity. Early detection and investigation of such activity allow organizations to stop attacks before they can do damage.

Unfortunately, a lack of resources and a shortage in security expertise makes proactive threat hunting unattainable for a majority of organizations. Understaffed internal teams are unable to monitor 24/7 for adversary activity, and in many cases, they are not equipped to efficiently respond to extremely sophisticated attacks. This can result in longer investigation times with fewer alerts being handled in a timely manner, ultimately resulting in longer dwell times and increased risk that attackers will successfully accomplish their goals.

Managed threat hunting solves this challenge by providing an elite hunting team that not only finds malicious activities that may have been missed by automated security systems, but also analyzes them thoroughly and provides customers with response guidelines.

Table 3 will help you identify the essential capabilities a managed threat hunting solution must provide and how to evaluate and assess different options.

MANAGED THREAT HUNTING: USE CASES AND ESSENTIAL CAPABILITIES

See and stop hidden advanced attacks	**Required Features** ■ In-house experienced and dedicated threat hunters ■ 24/7 threat hunting services provided ■ Ability to find 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 endpoint security platform
	Evaluation Criteria • Number of unique breaches detected and prevented per year • Number of incident leads investigated per year • Type of platform used for threat hunting
	Questions to Ask • Can you provide managed threat hunting services, or do you need to rely on a third party to provide this service? • What type of platform do you use for threat hunting?
Prioritize the most urgent threats and ensure critical alerts are not missed	**Required Features** ■ Ability to pinpoint the most urgent threats in the environment ■ Provide enhanced closed-loop communications to ensure important alerts are noticed
	Evaluation Criteria • Service level agreements (SLAs) • Documented closed-loop feedback process
	Questions to Ask • What is your process for informing the organization that an incident has been detected? • Do you have an alert escalation process? If so, what types of alerts do you escalate and when?
Guide you through the response process	**Required Features** ■ Provides actionable alerts ■ Provides assistance during incidents ■ Provides guidance on what to do next and potential mitigation suggestions on detections
	Evaluation Criteria • Review sample alerts • See recommendation samples
	Questions to Ask • How does the threat hunting team communicate with the customer? • What type of information does the team provide about the malicious activity it detected?
Augment current security team: Reach a higher level of security maturity instantaneously, minimizing overhead, complexity and cost	**Required Features** ■ Ability to watch adversary activity live and observe what they are doing as they are doing it ■ Monitor after an incident to watch for attackers coming back
	Evaluation Criteria • Amount of time elapsed between initial detection and detailed incident report that includes remediation guidance • Customer references and testimonials
	Questions to Ask • How experienced is the threat hunting team and what are team members' backgrounds? • Are they dedicated to hunting for threats ? If not, what responsibilities other than threat hunting do they have? • What results are other customers experiencing?

Table 3. Managed Threat Hunting: Use Cases and Essential Capabilities

THE CROWDSTRIKE APPROACH

The unparalleled CrowdStrike Falcon OverWatch™ team of dedicated threat hunters, when paired with the robustness of the data collected by the Falcon platform, is able to thwart attacks that would never be detected by another system or technology.

The OverWatch team is staffed with highly skilled and experienced analysts who take traditional security operations to the next level by offering proactive hunting for threats on a 24/7/365 basis. They augment existing security capabilities and cover the gaps in advanced threat detection and incident response. This results in drastic reduction and even elimination of attackers' dwell times.

OverWatch brings the industry's best threat hunters into customers' security operations. Taking full advantage of the CrowdStrike cloud-native architecture, powered by CrowdStrike Threat Graph, the team proactively hunts for anomalous or otherwise new attacker activity that is invisible to security technologies. Once a threat is identified, OverWatch works side-by-side with the customer, offering expert advice on how to handle the incident. OverWatch brings an essential human hunting element that ensures nothing gets missed. This is key to stopping breaches.

CRITICAL ELEMENT 4: ANTICIPATION

GETTING AND STAYING AHEAD OF ATTACKERS WITH THREAT INTELLIGENCE

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. Threat intelligence enables security products and security teams to understand and effectively predict the cyber threats that might impact them. It empowers organizations to anticipate the "who" and "how" of the next attack, and allows security teams to focus on prioritizing and configuring resources so they can respond effectively to future attacks.

In addition, threat intelligence provides the information that allows security teams to understand, respond to and resolve incidents faster, accelerating investigations and incident remediation. This is why security professionals looking at endpoint protection must ensure that they do not focus solely on the security infrastructure.

It is important that actionable threat intelligence is included as part of the total solution. Putting the appropriate information at security teams' fingertips allows faster and better decisions and responses. When looking at such integration, customers need to ensure that the intelligence provided is seamlessly integrated into the endpoint protection solution and that its consumption can be automated.

Use Table 4 to guide your evaluation of the threat intelligence integration provided in the endpoint protection solutions you are considering.

THREAT INTELLIGENCE INTEGRATION: USE CASES AND ESSENTIAL CAPABILITIES

Maximize defenses: Prioritize activities and resources, proactively defend against future attacks	**Required Features** ■ Automatically generated custom IOCs and intelligence on threats relevant and unique to an environment delivered within minutes ■ Automatically ingested third-party IOCs ■ Adversary profile reports for activity and resource prioritization (what to patch first, etc.)
	Evaluation Criteria ● Vendor supplies its own threat intelligence (not dependent on third-party feeds) ● Vendor is able to provide multiple levels of threat intelligence and information: strategic, operational, tactical
	Questions to Ask ● How is threat intelligence data integrated with the endpoint protection solution? ● How can customers use the threat intelligence data? How is it presented and formatted? ● How often is threat intelligence updated? ● How many sources and what type of sources does the vendor use to generate its threat intelligence service?
Accelerate detections	**Required Features** ■ Automatic alerts on adversary activities (nation-state and eCrime) detected in the environment ■ Automatic detections based on vendor's own tactical threat intelligence (e.g., known bad IPs, domain, file, etc.) ■ Ability to generate and consume IOCs automatically ■ Ability to perform custom IOC sweeps
	Evaluation Criteria ● Level of threat intelligence integration with the product — how much is automated and how much requires manual processing
	Questions to Ask ● Can the product tell me who is attacking my organization? ● What is the attacker's motive? ● What tactics and techniques is the attacker using? ● What tools might they be employing?
Expedite investigations and remediation	**Required Features** ■ Provides additional context into alerts and detections for faster investigation ■ Provides attack attribution to know who is attacking you, why and how to help prioritize response and action ■ Ability to visualize relationships between IOCs, adversaries and endpoints ■ Ability to analyze malware automatically with instant IOC creation and detailed analysis reports ■ Provides actor and adversary profiles
	Evaluation Criteria ● Actionable information: How can the threat intelligence information be used?
	Questions to Ask ● What type of threat intelligence information do your alerts and detections include?

Table 4. Threat Intelligence Integration: Use Cases and Essential Capabilities

THE CROWDSTRIKE APPROACH

CrowdStrike Falcon is the first platform to seamlessly integrate threat intelligence into endpoint protection, automating incident investigations and speeding breach response. The instant analysis of threats that reach endpoints, combined with the expertise of the global CrowdStrike Intelligence team, enables any security team — regardless of size or sophistication — to make predictive security a reality.

Falcon delivers the critical intelligence security teams need to stay ahead of attackers and to prioritize and respond to incidents as fast as possible and in the most appropriate way. Falcon takes full advantage of the information and insights provided by the CrowdStrike Intelligence team to provide additional context to alerts and incidents.

This dramatically reduces the resource-draining complexity of incident investigations and takes endpoint detection and response alerts to the next level. It not only shows what happened on the endpoint, but also provides attribution and reveals "the who, why and how" behind the attack. For example, Falcon automatically provides attribution of tools, domains, IPs, tactics and techniques to known adversaries. It provides detailed adversary profiles that help proactively protect against those threat actors, if found in an environment.

Finally, Falcon can automate malware analysis to deliver actionable intelligence and custom IOCs that specifically match the threats encountered on an organization's endpoints. With this level of automation, security teams can very quickly prioritize which threats they need to analyze first and allocate their resources to the analysis rather than the prioritization.

Falcon combines the tools used by world-class cyber threat investigators into a seamless solution and performs the investigations automatically. This tight and automatic integration between Falcon and threat intelligence enables all teams, regardless of size or sophistication, to understand better, respond faster and proactively get ahead of the attackers.

CRITICAL ELEMENT 5: READINESS

PREPARING FOR BATTLE WITH VULNERABILITY MANAGEMENT AND IT HYGIENE

Security starts with closing gaps to reduce the attack surface and be better prepared to face threats. This requires understanding which systems and applications are vulnerable and who and what are active in your environment. That is why vulnerability management and IT hygiene are the foundational blocks of an efficient security practice and should be part of any robust endpoint protection solution. They provide the visibility and actionable information that security and IT teams need to implement preemptive measures and make sure that they are prepared to face today's sophisticated threats.

When it comes to vulnerability assessment and management, regular, continuous monitoring is critical to identify and prioritize the weaknesses within your organization's systems. For example, if you have out-of-date applications, but do not continuously monitor for vulnerabilities, your environment could become a key attack vector for adversaries. Thus, the ability to discover, patch and update vulnerable applications running in your environment provides a tremendous advantage against attackers.

The same goes for IT hygiene. Knowing who and what is on your network can enable IT to work proactively in addressing unknowns or gaps within your security architecture. IT hygiene solutions offer the ability to pinpoint unmanaged systems or those that could be a risk on the network, such as unprotected BYOD or third-party systems. This solution should also be continuously monitoring for changes within your assets, applications and users.

Credential theft continues to be another popular and efficient vector for attackers. Monitoring and gaining visibility into logon trends (activities/duration) across your environment, wherever credentials are being 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 in the best position to face adversaries.

Table 5 will help in your evaluation of vulnerability management and IT hygiene features offered by an endpoint protection solution.

VULNERABILITY MANAGEMENT AND IT HYGIENE: USE CASES AND ESSENTIAL CAPABILITIES

Reveal vulnerabilities	**Required Features** ■ Ability to generate a list of vulnerable hosts and other vulnerabilities present in the environment ■ Prioritizes vulnerabilities that are critical to your systems ■ Ability to check applications for vulnerabilities ■ Differentiates between installed patches and successfully applied patches ■ Causes no impact on endpoints (no scanning)
	Evaluation Criteria ● Impact on endpoints ● Accuracy of the information (relevant, up-to-date, complete, etc.) ● Prioritization capabilities
	Questions to Ask ● Does this solution require an additional agent? ● Can the product differentiate installed patches versus deployed patches? ● Does the product provide the ability to customize dashboards or filters to streamline vulnerability analysis? ● Is the information up-to-date, or is a scan required to get access to the latest status?
Monitor accounts and privileged account usage	**Required Features** ■ Identifies account usage trends: which hosts the user logged on to, average session length, session lengths on each host, hours that the user typically logged on and type of registration (batch, remote) ■ Provides in-depth local and domain admin account usage information ■ Shows hosts when a user account has been used
	Evaluation Criteria ● Assess the dashboard and the reports of account usage information provided
	Questions to Ask ● Does this capability require an additional agent? ● How is this information collected? ● How does this integrate with the other capabilities of the endpoint protection product?
Identify unprotected systems and find unmanaged "rogue" systems	**Required Features** ■ Provides a real-time view of assets in the environment ■ Differentiates between managed, unmanaged and unsupported assets, including printers, cameras, etc. ■ Does not require a network scan ■ Does not require additional agents
	Evaluation Criteria ● Examine the dashboard and reports of information provided
	Questions to Ask ● Does this capability require an additional agent? ● How is this information collected? ● How does this integrate with the other capabilities of the endpoint security product?

Monitor what programs are being run in your environment	**Required Features** ■ Lists all applications being used on an endpoint and across all of the endpoints in the environment ■ Can identify and search applications used on a particular host or by specific users
	Evaluation Criteria ● Assess the dashboard and the reports of application information provided
	Questions to Ask ● Does this capability require an additional agent? ● How is this information collected? ● How does this integrate with the other capabilities of the endpoint security product?

Table 5. Vulnerability Management and IT Hygiene: Use Cases and Essential Capabilities

THE CROWDSTRIKE APPROACH

CrowdStrike Falcon Discover™ IT hygiene and CrowdStrike Falcon Spotlight™ vulnerability management enable organizations to close security gaps and be better prepared to face threats by providing awareness and visibility in key areas of an infrastructure. These solutions provide robust visibility over the existing vulnerabilities, assets, applications and accounts being used in an environment. By using the Falcon agent, Falcon Spotlight is unique in its ability to report vulnerabilities in real time without scanning endpoints, identifying which patches have successfully been applied versus just deployed. With Falcon Discover, IT staff gain real-time visibility into who and what is in the network and can identify rogue, unprotected and unmanaged systems, such as "bring your own device" (BYOD) or third-party systems.

The real-time application inventory within Falcon Discover provides a view of all applications running in the environment via a simple dashboard with drill-down options. Security teams can instantly see what applications are currently running on which hosts without impacting endpoints. They can also determine when the application was originally launched and pivot to other endpoints running the same app to gain more context by finding usage per application or by host. Falcon Discover also monitors and provides visibility into logon trends (activities/duration) across your environment, wherever existing credentials are being used or new administrator credentials created. This enables security teams to detect and mitigate credential abuse and attacks that employ stolen credentials.

Overall, with Falcon Spotlight and Falcon Discover, you receive comprehensive vulnerability management with continuous monitoring, along with the IT hygiene component needed to improve overall security posture. With these solutions, your organization will be better prepared to repel attacks and stop a breach.

CLOUD-NATIVE ARCHITECTURE TO ENABLE THE CRITICAL ELEMENTS OF ENDPOINT SECURITY

As organizations grow and add more distributed endpoints, on-premises endpoint security solutions can quickly become very complex and take months to implement and be fully operational. Soon, it seems the entire infrastructure needs to be updated to ensure that it operates at the highest level of protection, or a different component needs to be added to protect against a new type of threat. This often requires the entire implementation procedure to start all over again — meanwhile leaving gaps in your protection.

Hybrid deployments with components distributed between on-premises and in the cloud may seem like a logical choice, but they introduce challenges. Infrastructure overhead continues if any on-premises management component is required. Versioning quickly layers in complexity and introduces security gaps as capabilities, protection and update routines vary across the estate. Decentralized data repositories limit detection and response capabilities.

Cloud-native, on the other hand, offers a means of providing pervasive protection throughout the enterprise faster, at a lower cost and with reduced management overhead while offering significantly increased performance, agility and scalability. Without hardware and additional software to procure, deploy, manage and update, rolling out endpoint security from the cloud becomes quick and simple. While on-premises systems can take up to a year to fully roll out, cloud-based solutions can be successfully deployed in environments with tens of thousands of hosts in a matter of hours.

Additionally, updates to the infrastructure are done in the cloud, immediately, under vendor supervision and do not require months of planning that can leave gaps in the protection efficacy and deplete IT teams' resources.

Other benefits of a cloud-native model include the ability to collect rich data sets in real time and to scale on demand, making it possible to store petabytes of data for months and analyze that data in seconds without impacting endpoints. Those are all extremely arduous tasks that are not suited for on-premises models. Finally, cloud deployments are crucial for protecting remote systems when they are off the network or outside the VPN.

A well-designed cloud architecture should provide the following capabilities:

1. Be immediately operational with no infrastructure setup prior to deployment
2. Scale seamlessly as endpoints and events are added, without requiring the customer's intervention
3. Reduce impact on endpoints to a minimum (e.g., no database required on the endpoint to keep event data, no endpoint resource consumption when search or analysis is done)
4. Analyze data at a speed and volume that provide fast and accurate results

The following questions will help you uncover the true abilities provided by an endpoint protection solution's cloud architecture:

- How long does it take for the product to be fully operational?
- What additional hardware and software — servers (physical or virtual), appliances, database licenses, etc. — are required to implement the product?
- Is it a true cloud-designed architecture or a virtualized appliance hosted in the cloud?
- Does the customer need to do anything if the number of endpoints grows or if they add additional locations to the environment?
- How does the solution impact endpoints, disk space, CPU usage and RAM usage?
- How are the endpoints impacted when searches are performed and when events are collected?
- How many events per second can the cloud infrastructure handle?
- How many endpoints can the architecture support?

The CrowdStrike Falcon platform's cloud-native architecture was designed and implemented from the ground up to leverage the power and scale of the cloud. It allows CrowdStrike to provide immediate time-to-value, which means that customers can be up, running and fully operational in hours, as opposed to the weeks or months usually required for on-premises architectures.

In addition to enabling fast and easy implementation, with extremely low maintenance and expansion costs, CrowdStrike's purpose-built cloud architecture delivers a series of unique and powerful advantages that both strengthen protection and reduce complexity.

This architecture is central to CrowdStrike's ability to collect, analyze and store trillions of events per week, which would be nearly impossible to achieve with on-premises architecture. The CrowdStrike security cloud model, one of the biggest cloud architectures in the world, is designed for storing and analyzing a large, ever-growing volume of data. It provides complete real-time visibility and insight into everything happening on your endpoints, workloads and containers throughout your environment. Using powerful graph analytics to scour billions of events in real time, CrowdStrike Threat Graph draws links between security events across the global Falcon agent community to immediately detect and prevent adversary activity, at scale and with unprecedented speed. When a new threat is discovered locally in one environment, all customers benefit from CrowdStrike community-driven intelligence immediately due to Threat Graph's ability to analyze data at cloud scale and take the most effective action to protect all customers. In this way, Threat Graph empowers CrowdStrike customers with an extraordinary level of protection against breaches.

The Falcon platform is designed as a highly modular and extensible solution using a single lightweight agent. This ensures that customers can solve new security challenges with a single click — without the need to re-architect or re-engineer the solution, removing friction associated with security deployments.

CONCLUSION

It might seem hard to see the difference between vendors, but when you look beyond the hype, you can see that only CrowdStrike delivers the essential endpoint protection capabilities:

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 automation
4. **Threat intelligence integration** to understand and stay ahead of attackers
5. **Vulnerability management and IT hygiene** to prepare and strengthen the environment against threats and attacks

CrowdStrike uniquely enables and delivers these elements via a cloud-native architecture to meet the speed, flexibility and capacity required to fend off modern attackers and stop breaches. It delivers a single lightweight agent for prevention, detection, threat hunting, response, remediation, vulnerability management and IT hygiene. The option is also available to be fully managed 24/7 by CrowdStrike security experts through CrowdStrike Falcon Complete™ managed endpoint security, which comes with a warranty of up to $1 million USD.

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 | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**