ENDPOINT PROTECTION BUYERS GUIDE

How to select the best endpoint protection solution
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 hundreds of options on the market and features that sound identical, choosing an endpoint protection solution is anything but straightforward.

CrowdStrike® recommends that a comprehensive and efficient endpoint protection solution should include five key elements. The objectives below 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
- **IT hygiene and vulnerability assessment** to prepare and strengthen the environment against threats and attacks

CrowdStrike recommends that these five elements need to be enabled and delivered via cloud-native architecture in order to meet the speed, flexibility and capacity required to fend off modern attackers. Finally, those elements need to be combined within a single lightweight agent that does not bloat the endpoints or impact their performance.

The CrowdStrike Falcon® next-generation endpoint protection platform integrates all those elements in one lightweight agent, supported by the cloud. Falcon unifies the technologies required to successfully stop breaches, including next-generation antivirus (NGAV), endpoint detection and response (EDR), IT hygiene, vulnerability assessment, 24/7 managed threat hunting and threat intelligence. They combine to provide continuous breach prevention in a single agent that can be deployed within hours with no impact on endpoints or users. The Falcon platform’s ability to continuously stop breaches makes it a true and proven next-generation endpoint protection solution.
INTRODUCTION

Protecting endpoints has long been a critical component of all security strategies, as they are among the largest targets for attackers. Today, almost all organizations are running some form of endpoint protection. But attackers, fully expecting to encounter security measures on endpoints, have become more sophisticated, developing multiple ways to bypass them. This has resulted in thousands of successful breaches, clearly exposing the limitations of traditional endpoint security. In fact, the need for better endpoint protection has become so apparent that 76 percent of organizations are planning to change their AV vendor within the next 12-14 months*, citing a lack of effectiveness in stopping modern threats as the No. 1 reason to switch**.

The need for better endpoint protection has also generated a plethora of new endpoint security products, all claiming to be next-generation game-changers. The confusion caused by this abundance of choices can make finding the right solution overwhelming.

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 product to qualify as a capable endpoint protection solution. To be truly effective, an endpoint solution must be designed to continuously stop breaches across the entire attack continuum, rather than simply accumulating isolated protection features added each time a new attacker technique is discovered.

The ideal endpoint solution should offer a complete package that not only provides more advanced protection technologies, but also makes innovative use of all the means available to meet sophisticated attacks head-on. For defenders to outpace attackers, an effective package should include threat intelligence integration, human-augmented detection and response and cloud-based architecture that can enable defenders to stay ahead of attackers. Only then will the endpoint solution be able to deliver the kind of anticipation, prevention, detection, visibility and response capabilities that can beat a determined attacker time and time again.

To find those capabilities, decision-makers should look for five critical elements in an endpoint security solution: NGAV, EDR, MDR (managed detection and response), threat intelligence, and IT hygiene and vulnerability assessment. Combining these elements will ensure a comprehensive, robust and efficacious endpoint security solution.

*Enterprise Strategy Group: Endpoint Security Survey
** No 1 concern raised by customers inquiring with analyst firms Gartner and Forrester about endpoint security
THE 5 CRITICAL ELEMENTS OF ENDPOINT PROTECTION

<table>
<thead>
<tr>
<th>PREVENTION</th>
<th>DETECTION</th>
<th>MANAGED THREAT HUNTING</th>
<th>ANTICIPATION</th>
<th>READINESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGAV (Next-generation Antivirus)</td>
<td>EDR (Endpoint Detection and Response)</td>
<td>MDR (Managed Detection and Response)</td>
<td>THREAT INTELLIGENCE</td>
<td>IT HYGIENE AND VULNERABILITY ASSESSMENT</td>
</tr>
</tbody>
</table>

CRITICAL ELEMENT ONE: PREVENTION

PROTECTING AGAINST MALWARE AND BEYOND WITH NGAV

Why you need next-gen AV

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.

First, the 99 percent effectiveness rate achieved by malware-focused solutions still leaves a small gap. However, that tiny gap provides a huge window of opportunity for adversaries that can now quickly and easily procure or create zero-day malware. Second, malware-centric protection does not address the increasingly sophisticated fileless and malware-free tactics used by modern adversaries. In fact, studies show that 50 to 60 percent of today’s breaches are not caused by malware at all, but rather carried out through techniques such as social engineering or credential theft from other sources.

A sound endpoint protection solution needs to solve those challenges 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 to be efficient. It should also 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 the necessary technologies for ultimate protection.

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

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.
### NGAV: Use Cases and Essential Capabilities

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Required Features</th>
<th>Evaluation Criteria</th>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent both known and zero-day malware</td>
<td><strong>Required features</strong>&lt;br&gt;■ ML on the endpoint to prevent both known and unknown malware&lt;br&gt; ■ Automated malware analysis (e.g. sandboxing)&lt;br&gt; ■ Integrated threat intelligence&lt;br&gt; ■ Custom whitelisting and blacklisting capabilities&lt;br&gt; ■ Automatic third-party indicator-of-compromise (IOC) ingestion</td>
<td><strong>Evaluation Criteria</strong>&lt;br&gt;● Independent third-party testing results&lt;br&gt; ● False positive rates</td>
<td><strong>Questions to ask</strong>&lt;br&gt;● Is the product signature-based or does it use ML?&lt;br&gt;● If the product uses ML, does the endpoint have to be connected to the cloud to use it?&lt;br&gt;● Which of the prevention features requires a cloud connection?&lt;br&gt;● In case malware is not blocked, what other prevention mechanisms does the product provide?</td>
</tr>
<tr>
<td>Protect against ransomware</td>
<td><strong>Required Features</strong>&lt;br&gt;■ ML on the agent&lt;br&gt; ■ Behavioral analysis/indicators of attack (IOAs) specific to ransomware&lt;br&gt; ■ Integrated threat intelligence</td>
<td><strong>Evaluation Criteria</strong>&lt;br&gt;● Past performance against real-life ransomware such as WannaCry and NotPetya&lt;br&gt;● Third-party test results</td>
<td><strong>Questions to ask</strong>&lt;br&gt;● What methods does it use to prevent ransomware?&lt;br&gt;● What methods does it use to prevent zero-day ransomware?&lt;br&gt;● How did the product handle ransomware outbreaks such as Wannacry and NotPetya?</td>
</tr>
<tr>
<td>Prevent fileless and malware-free attacks: Protects your endpoints against all types of threats, not just malware and exploits</td>
<td><strong>Required Features</strong>&lt;br&gt;■ Protection against known exploits&lt;br&gt; ■ Protection against zero-day exploits&lt;br&gt; ■ Memory protection&lt;br&gt; ■ IOA behavioral blocking</td>
<td><strong>Evaluation Criteria</strong>&lt;br&gt;● Success in MITRE adversary emulation test&lt;br&gt;● Performance against red team exercises</td>
<td><strong>Questions to ask</strong>&lt;br&gt;● What type of non-malware malicious activities can it block?&lt;br&gt;● Can it block an attacker that is logged-on using stolen credentials and legitimate tools to perform their actions?&lt;br&gt;● What areas of the MITRE ATT&amp;CK framework can it protect against?&lt;br&gt;● Can the solution prevent the malicious utilization of legitimate applications such as PowerShell? How?&lt;br&gt;● How does the solution block exploits?&lt;br&gt;● Is the product able to block zero-day exploits?&lt;br&gt;● In case an attack is not blocked, what other prevention mechanisms does the product employ?&lt;br&gt;● What type of memory protection mechanisms does the product offer?</td>
</tr>
</tbody>
</table>
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
- Protects offline when there is no cloud connection
- Enables ML on the endpoint that also works offline without requiring a connection to the cloud

**Evaluation Criteria**
- Frequency and performance impact of updates (product, malware signatures or DAT files, etc.) provided by the vendor — the frequency demonstrates how often the product needs updating to stay efficient
- 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?

Provide rapid response and remediation

**Required Features**
- The ability to quarantine a malicious file
- Keeps detection information for at least 90 days for investigation
- 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
- 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?

---

**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 legacy 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 prevent breaches across the entire attack continuum.

Falcon employs ML on the endpoint for pre-execution prevention of both known and unknown malware. Falcon’s ML feature is so powerful that it protected Falcon customers from the ransomware WannaCry and NotPetya, 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 malware-free 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, whitelisting or sandboxing.
CRITICAL ELEMENT TWO: DETECTION

PROVIDING THE VISIBILITY TO FIND AND KEEP ATTACKERS OUT WITH EDR

Why you need EDR

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 record all activities of interest on an endpoint for deeper inspection, both in real time and after the fact. An efficient EDR solution should also be intelligent and able to automatically detect malicious 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.

Consider the use cases below to guide you in your choice and evaluation of the EDR capabilities of the endpoint solutions you are considering.

EDR: USE CASES AND ESSENTIAL CAPABILITIES

<table>
<thead>
<tr>
<th>Automatically uncover stealthy attackers: Know if you have been breached</th>
<th>Required Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Automatic incident detection — intelligent EDR with built-in, real-time detections</td>
<td></td>
</tr>
<tr>
<td>■ Automatic detection based on behavioral analysis such as IOAs</td>
<td></td>
</tr>
<tr>
<td>■ Integration with threat intelligence</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No fine-tuning, rule writing or complex configuration required</td>
</tr>
<tr>
<td>• Effective performance against pen tests</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What kind of detection or correlation rules need to be written before the product can detect incidents?</td>
</tr>
<tr>
<td>• What expertise level is required to use the solution?</td>
</tr>
</tbody>
</table>
### 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
- Raw event data is available for long periods of time (months to years)
- Operates in kernel mode for full visibility and to eliminate blind spots
- Fully customizable real-time and historical search capabilities
- Simultaneous enterprisewide searches with zero impact on endpoints
- Delivers query answers in five seconds or less

#### Evaluation Criteria
- The types of events the product is capable of observing and collecting, e.g. filesystem, process/thread/DLL/service execution, registry, kernel object, network and user login activities, memory injection, USB drives, command shell commands, etc.
- Retention period available for all raw events

#### 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?
- Where is the raw event data stored and for how long?

### Accelerate investigations and forensics

#### Required Features
- 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
- Provides forensic data even if endpoint is unavailable, inaccessible or destroyed
- Full context detections and alerts including threat intelligence data
- Flexible data retention period for all raw events that can be extended to a full year
- Industry-standard query language to search event data

#### 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?

### 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

#### Evaluation Criteria
- List of response capabilities available in the product

#### 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?
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, eliminating the risk of silent failure.

Falcon also provides both automatic and manual analysis capabilities that can be performed as events are taking place or after the fact. The automatic analysis can immediately detect the attackers’ activity in case they manage to gain access. 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-based architecture provides the speed and scalability to collect and retain all the necessary endpoint events for months if needed, even if the endpoints are unavailable, destroyed or have been deleted (as can be the case for virtual workloads).

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 THREE: MANAGED THREAT HUNTING

ELEVATING DETECTION BEYOND AUTOMATION (MDR)

Why you need managed threat hunting

Passively waiting for security products to automatically detect attacks does not work all the time. 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 less alerts being handled in a timely manner, ultimately resulting in longer dwell times and increased risk that the 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 response systems, but also analyzes them thoroughly and provides customers with response guidelines.

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

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.
## Managed Threat Hunting: Use Cases and Essential Capabilities

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Required Features</th>
<th>Evaluation Criteria</th>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eliminate false negatives and reduce attacker dwell time: Fill the gaps</td>
<td>In-house experienced and dedicated threat hunters</td>
<td>Number of unique breaches detected and prevented per year</td>
<td>Can you provide managed threat hunting services or do you need to rely on a third-party to provide this service?</td>
</tr>
<tr>
<td>in threat detection and incident response</td>
<td>24/7 threat hunting services provided</td>
<td>Number of incident leads investigated per year</td>
<td>What type of platform do you use for threat hunting?</td>
</tr>
<tr>
<td></td>
<td>Ability to find incidents that no other systems have detected</td>
<td>Type of platform used for threat hunting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Immediate access to threat intelligence experts for faster analysis</td>
<td>Red team testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic and native integration with threat intelligence for ultimate efficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prioritize the most urgent alerts and ensure critical alerts are</td>
<td>Ability to pinpoint the most urgent threats in the environment</td>
<td>Service level agreements (SLAs)</td>
<td>What is your process for informing the organization that an incident has been detected?</td>
</tr>
<tr>
<td>not missed</td>
<td>Provide enhanced closed-loop communications to ensure important alerts are noticed</td>
<td>Documented closed-loop feedback process</td>
<td>Do you have an alert escalation process? If so, what type of alerts do you escalate and when?</td>
</tr>
<tr>
<td>Guide you through the response process</td>
<td>Provides actionable alerts</td>
<td>Review sample alerts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provides assistance during incidents</td>
<td>See recommendation samples</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provides guidance on what to do next and potential mitigation suggestions on detections</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Augment current security team: Reach a higher level of security maturity instantaneously and at a low cost.

**Required Features**
- Ability to watch adversary activity live and observe what they are doing as they are doing it
- Monitors after an incident to watch for attackers coming back
- Resolves false positives

**Evaluation Criteria**
- Amount of time elapsed between initial detection and detailed incident report that includes remediation guidance
- Number of incidents detected in addition to what the existing internal team catches
- Number of incident leads investigated in addition to what the customer’s security team processes
- Red team testing
- 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?

---

**THE CROWDSTRIKE APPROACH**

CrowdStrike Falcon OverWatch™ provides an unparalleled team of dedicated threat hunters that when paired with the robustness of the data collected by the Falcon platform, are able to thwart attacks that would never be detected by any other 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 24x7x365 basis. They eliminate false negatives by augmenting existing security capabilities and covering 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 the 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 and also guiding remediation. OverWatch brings an essential human hunting element that ensures nothing gets missed. This is key to stopping breaches.

---

**CRITICAL ELEMENT FOUR: ANTICIPATION**

**GETTING AND STAYING AHEAD OF ATTACKERS WITH THREAT INTELLIGENCE**

**Why you need 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 be 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 solution and that its consumption can be automated.

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

### Threat Intelligence Integration: Use Case and Essential Capabilities

<table>
<thead>
<tr>
<th><strong>Maximize defenses: Prioritize activities and resources; proactively defend against future attacks</strong></th>
<th><strong>Required Features</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Automatically generated custom IOCs and intelligence on threats relevant and unique to an environment are delivered within minutes</td>
</tr>
<tr>
<td></td>
<td>■ Automatically ingested third-party IOCs</td>
</tr>
<tr>
<td></td>
<td>■ Adversary profile reports for activity and resource prioritization (what to patch first, etc.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>Evaluation Criteria</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Vendor supplies its own threat intelligence (not dependent on third-party feeds)</td>
</tr>
<tr>
<td></td>
<td>■ Vendor is able to provide multiple levels of threat intelligence and information: strategic, operational, tactical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>Questions to ask</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ How is threat intelligence data integrated with the endpoint protection solution?</td>
</tr>
<tr>
<td></td>
<td>■ How can customers use the threat intelligence data? How is it presented and formatted?</td>
</tr>
<tr>
<td></td>
<td>■ How often is threat intelligence updated?</td>
</tr>
<tr>
<td></td>
<td>■ How many sources and what type of sources does the vendor use to generate its threat intelligence service?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Accelerate detections</strong></th>
<th><strong>Required Features</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Automatic alerts on adversary activities (nation state and eCrime) detected in the environment</td>
</tr>
<tr>
<td></td>
<td>■ Automatic detections based on vendor’s own tactical threat intelligence (e.g., known bad IPs, domain, file, etc.)</td>
</tr>
<tr>
<td></td>
<td>■ Ability to generate and consume IOCs automatically</td>
</tr>
<tr>
<td></td>
<td>■ Ability to perform custom IOC sweeps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>Evaluation Criteria</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Level of threat intelligence integration with the product — how much is automated and how much requires manual processing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>Questions to ask</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>■ Can the product tell me who is attacking my organization?</td>
</tr>
<tr>
<td></td>
<td>■ What is the attacker’s motive?</td>
</tr>
<tr>
<td></td>
<td>■ What tactics and techniques is the attacker using?</td>
</tr>
<tr>
<td></td>
<td>■ What tools might they be employing?</td>
</tr>
</tbody>
</table>
CrowdStrike Products
ENDPOINT PROTECTION BUYERS GUIDE

<table>
<thead>
<tr>
<th>Expedite investigations and remediation</th>
<th>Required Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Provides additional context into alerts and detections for faster investigation</td>
</tr>
<tr>
<td></td>
<td>Provides attack attribution to know who is attacking you, why, and how to help prioritize response and action</td>
</tr>
<tr>
<td></td>
<td>Ability to analyze malware automatically with instant IOC creation and detailed analysis reports</td>
</tr>
<tr>
<td></td>
<td>Provides actor and adversary profiles</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actionable information: How can the threat intelligence information be used?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of threat intelligence information do your alerts and detections include?</td>
</tr>
</tbody>
</table>

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 Falcon 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 Falcon Intelligence team to provide additional context to alerts and incidents.

This eliminates 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.

The instant analysis of threats that reach endpoints, combined with the expertise of the global CrowdStrike Falcon Intelligence team enables any security team, regardless of size or sophistication, to make predictive security a reality.
PREPARING FOR BATTLE WITH VULNERABILITY ASSESSMENT AND IT HYGIENE

Why you need vulnerability assessment and IT hygiene

Security starts with closing gaps to reduce the attack surface and be better prepared to face threats. This requires understanding what systems and applications are vulnerable and who and what are active in your environment. That is why vulnerability assessment 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.

With vulnerability assessment and IT hygiene, a little goes a long way. For example, out-of-date and unpatched applications continue to be a key attack vector into organizations’ IT environments. Thus, the ability to discover, patch and update vulnerable applications running in your environment provides a tremendous advantage against attackers.

In addition, understanding what systems are running on your network proactively addresses gaps in your security architecture. IT hygiene gives you the ability to pinpoint unmanaged systems or those that could be a risk on the network, such as unprotected BYOD or third-party systems.

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 assessment 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.

The table below will help in your evaluation of the vulnerability assessment and IT hygiene features of an endpoint protection solution.

<table>
<thead>
<tr>
<th>Reveals vulnerabilities</th>
<th>Required Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Ability to generate a list of vulnerable hosts and other vulnerabilities present in the environment</td>
<td></td>
</tr>
<tr>
<td>■ Ability to check applications for vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>■ Differentiates between installed patches and successfully applied patches</td>
<td></td>
</tr>
<tr>
<td>■ Causes no impact on endpoints (no scanning)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Impact on endpoints</td>
</tr>
<tr>
<td>■ Accuracy of the information (relevant, up-to-date, complete, etc.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Does this ability require an additional agent?</td>
</tr>
<tr>
<td>■ Can the product differentiate installed patches versus deployed patches?</td>
</tr>
<tr>
<td>■ Is the information up-to-date or is a scan required to get access to the latest status?</td>
</tr>
</tbody>
</table>
## Monitors 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 product?

## Identifies unprotected systems and finds 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?

## Monitors what programs are being run in your environment

**Required Features**
- Lists all applications being used on an endpoint and across all 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 product?

---

### CROWDSTRIKE APPROACH

CrowdStrike Falcon Discover™ and Falcon Spotlight™ enable organizations to close security gaps and be better prepared to face threats by providing awareness and visibility in key areas of an infrastructure. It provides unprecedented visibility over the existing vulnerabilities, assets, applications and accounts being used in an environment. The Falcon agent is unique in its ability to report vulnerabilities in real-time without scanning endpoints, and identifying whether a patch has successfully been applied versus just deployed. It provides real-time visibility into who and what is in the network and identifies rogue, unprotected and unmanaged systems, such as BYOD or third-party systems.

The real-time application inventory 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 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, Falcon provides the vulnerability assessment and IT hygiene necessary for security teams to improve their overall security posture and be better prepared to repel attacks and stop a breach.

As organizations grow and add more distributed endpoints, on-premises endpoint 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.

The cloud, on the other hand, offers a new 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-based 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 (for example: 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
CrowdStrike Falcon’s cloud-based architecture was designed and implemented from the ground up to leverage the power and scale of the cloud.

CrowdStrike Falcon’s cloud-based 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 and running and fully operational in hours, as opposed to the weeks or months usually required for on-premises architectures.

This 100 percent cloud-native approach also enables customers to reduce costs while adding speed, efficacy and automatic scalability.

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.

The CrowdStrike Falcon platform is the perfect solution for customers who are looking to protect endpoints hosted on a cloud platform. It is ideal for those needing to protect endpoints in a hybrid environment, whether they are on- or off-network, or hosted in the cloud.

This architecture is central to CrowdStrike’s ability to collect, analyze and store over one trillion events per week, which would be nearly impossible to achieve with on-premises architecture. The CrowdStrike Cloud model, powered by the Threat Graph database, is designed for storing a large, ever-growing volume of data. That data can be available for long periods of time and the architecture automatically scales to accommodate new data. The architecture also allows thorough and lightning-fast analysis of this large volume of data, returning answers to search queries across petabytes of data within seconds.

Finally, the cloud also enables aggregation of data across environments to fully leverage the knowledge and intelligence of the crowd. This allows all CrowdStrike customers to be protected from new threats found in a single customer environment before it becomes more widespread.

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?

This 100 percent cloud-native approach also enables customers to reduce costs while adding speed, efficacy and automatic scalability.

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.

The CrowdStrike Falcon platform is the perfect solution for customers who are looking to protect endpoints hosted on a cloud platform. It is ideal for those needing to protect endpoints in a hybrid environment, whether they are on- or off-network, or hosted in the cloud.

This architecture is central to CrowdStrike’s ability to collect, analyze and store over one trillion events per week, which would be nearly impossible to achieve with on-premises architecture. The CrowdStrike Cloud model, powered by the Threat Graph database, is designed for storing a large, ever-growing volume of data. That data can be available for long periods of time and the architecture automatically scales to accommodate new data. The architecture also allows thorough and lightning-fast analysis of this large volume of data, returning answers to search queries across petabytes of data within seconds.

Finally, the cloud also enables aggregation of data across environments to fully leverage the knowledge and intelligence of the crowd. This allows all CrowdStrike customers to be protected from new threats found in a single customer environment before it becomes more widespread.
CONCLUSION

Selecting an endpoint protection solution can be challenging, as the endpoint market provides hundreds of options. Each product comes with its own set of features and technologies and the differences are not easily discernible. To simplify and clarify things, CrowdStrike breaks down the requirements of a comprehensive and efficient endpoint protection solution into these five key elements that have been detailed in this guide:

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. IT hygiene and vulnerability assessment to prepare and strengthen the environment against threats and attacks

In addition, these five elements need to be enabled and delivered via cloud-native architecture to meet the speed, flexibility and capacity required to fend off modern attackers.

The CrowdStrike Falcon endpoint protection platform was built from the ground up to address the challenges posed by modern attacks and to stop breaches. It delivers a single lightweight agent for prevention, detection, threat hunting, response, remediation, vulnerability assessment and IT hygiene. There is also an option to be fully managed 24/7 by CrowdStrike security experts, Falcon Complete™, which comes with a warranty of up to $1 million.

The Falcon endpoint protection platform was designed and built in the cloud, leveraging a cutting-edge graph database technology that powers the Falcon endpoint agent, CrowdStrike artificial intelligence, and all other components of the Falcon platform. As new security needs arise, the platform seamlessly expands to provide CrowdStrike customers with the ultimate endpoint protection, via a single lightweight agent.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyberattack types, using sophisticated signatureless AI and Indicator-of-Attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph, Falcon instantly correlates over 1 trillion security events per week from across the globe to immediately prevent and detect threats.