CROWDSTRIKE **FALCON**: SETTING THE **NEW** STANDARD **IN** ENDPOINT **PROTECTION**

THE FIVE ESSENTIAL ELEMENTS OF NEXT-GENERATION ENDPOINT PROTECTION

NAVIGATING MARKET CONFUSION

WHAT DOES NEXT-GENERATION ENDPOINT PROTECTION REALLY LOOK LIKE?

Vendors old and new have laid claim to the next-generation moniker. The field has become crowded with dozens of endpoint security products marketed as game-changers. Some may include behavioral detection elements. Others might offer some degree of machine learning. Still others might claim to offer cloud-based protection.

But scratch below the surface of these new solutions and it becomes apparent that most are simply iterations on the old platforms that powered the first generation of endpoint protection. While they might incorporate one or two new methods, the majority still rely heavily on dated techniques such as signature-based threat detection and increasingly obsolete architectures designed for on-premises delivery. As a result, even when they're sold as cloud solutions, they're highly segmented and lack the scale and efficacy of a purpose-built cloud solution.

And most detrimentally, the majority of endpoint solutions are still fixated on stopping malicious executables rather than seeking out indicators of attack (IOAs) that can point to breach activity, even when malware isn't present.

CrowdStrike® believes it takes more than a few new detection features to qualify as a true next-generation endpoint security platform. Real "next-gen" solutions should offer a complete package of more advanced technology and human-powered intelligence to meet sophisticated attacks head-on. For an endpoint security product to be taken seriously as a next-generation solution, it needs to deliver the kind of anticipation, prevention, detection, visibility, and intelligence that can beat a determined attacker time and time again.

In order to find those capabilities, decision-makers should look for five crucial elements in a next-generation endpoint security solution.

Element 1:
IT HYGIENE

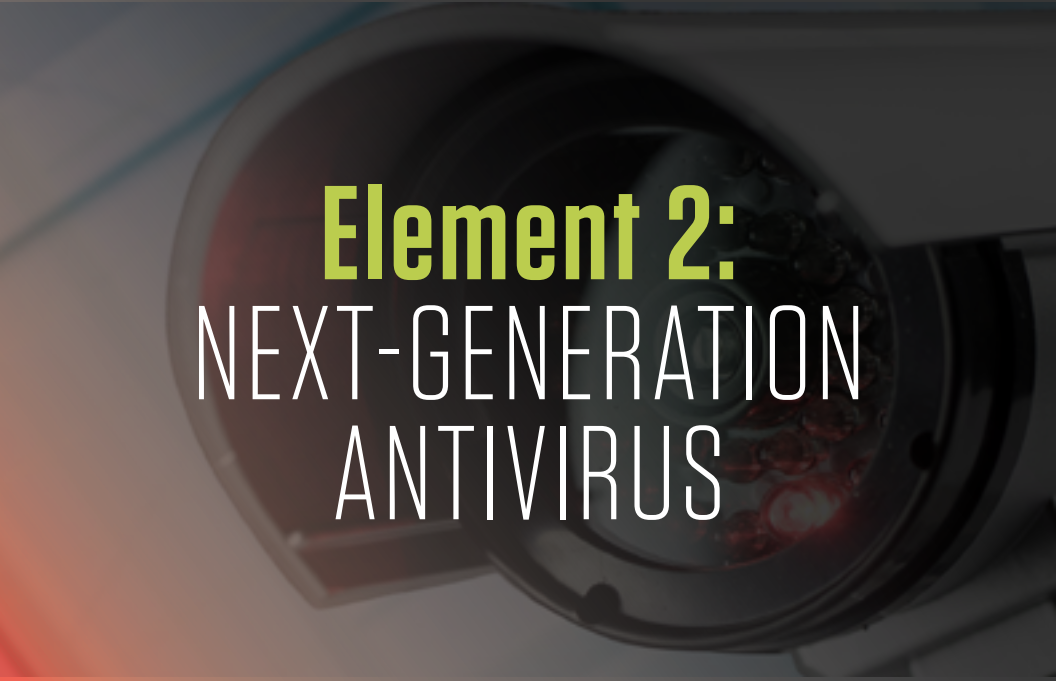
Security starts with discovering where you're not protected, so you can close security gaps and be better prepared to face threats. It is imperative that you understand who and what is running in your environment. IT hygiene is the foundational block of an efficient security practice. It provides the visibility and information that security and IT teams need to implement preemptive measures and make sure that they are as ready as possible to face today's sophisticated threats.

With 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. A recent survey notes that 75 percent of organizations cite unpatched and outdated software as their greatest security risk. 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 give 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 high-velocity 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.

TIP: IT hygiene provides a solid foundation for improving an organization's security posture. Monitoring and inventorying systems, application usage and user account activity in real time allows security teams to identify and address issues ahead of attacks, ensuring the best possible defense readiness.



Element 2: NEXT-GENERATION ANTIVIRUS

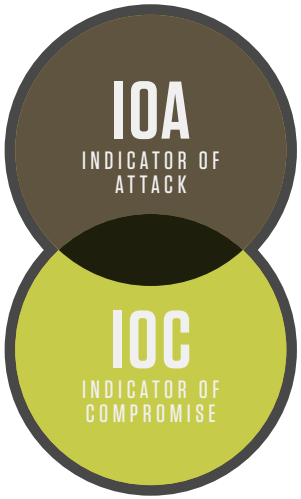
Traditional antivirus (AV) has coasted a long way in the market by touting 97 to 99 percent effectiveness rates. But as most security professionals have learned the hard way, this seemingly small gap of one to three percent provides a huge window of opportunity for adversaries using either known or unknown malware. In addition, the dated AV approach does nothing to address increasingly sophisticated fileless methods. In fact, studies indicate that many 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.

Despite the shortcomings of traditional AV, it is far from being a worthless tool. In the past, some analysts have posited that the death of AV was imminent, but AV still adds tremendous value by eliminating the obvious threats. However, it can't be your only answer to endpoint security. Traditional AV simply doesn't provide an adequate level of protection.

Next-generation AV expands beyond simply identifying and addressing known malware — an approach that leaves vulnerability gaps that can be exploited by attackers. Next-generation AV goes beyond identifying known signatures to block exploits that leverage vulnerabilities, providing an additional line of defense.

In addition, next-generation AV should be able to fully leverage behavioral analytics and machine learning to identify unknown malicious files, stepping beyond a focus only on malware to look for signs of attack as they are occurring, rather than after the fact. This approach entails seeking out indicators of attack (IOAs) to identify active attacks, rather than solely relying on indicators of compromise (IOCs), which are only present after an attack has taken place. To achieve this, the solution must gather enough endpoint activity data throughout the environment to contextualize each IOA with other pieces of information, ultimately forming the most complete picture of activity possible.

TIP: IT decision-makers evaluating so-called "next-generation" AV products should look closely at those that claim to offer behavioral analytics or machine learning. The litmus test should be the quality and relevance of the data being analyzed. If the data is limited to a few seconds of execution, or only looks at questionable files to extract information, there won't be enough context to determine if an activity in progress is malicious.



Next-generation AV solutions should be able to look across both legitimate activity and malicious activity, and make use of algorithms that don't overwhelm analysts with false positives, while at the same time detecting a chain of activities that indicate attacks. For example, the solution should look not only at files and code being executed to determine if they are malicious. It should also look for behaviors that reveal IOAs, such as:

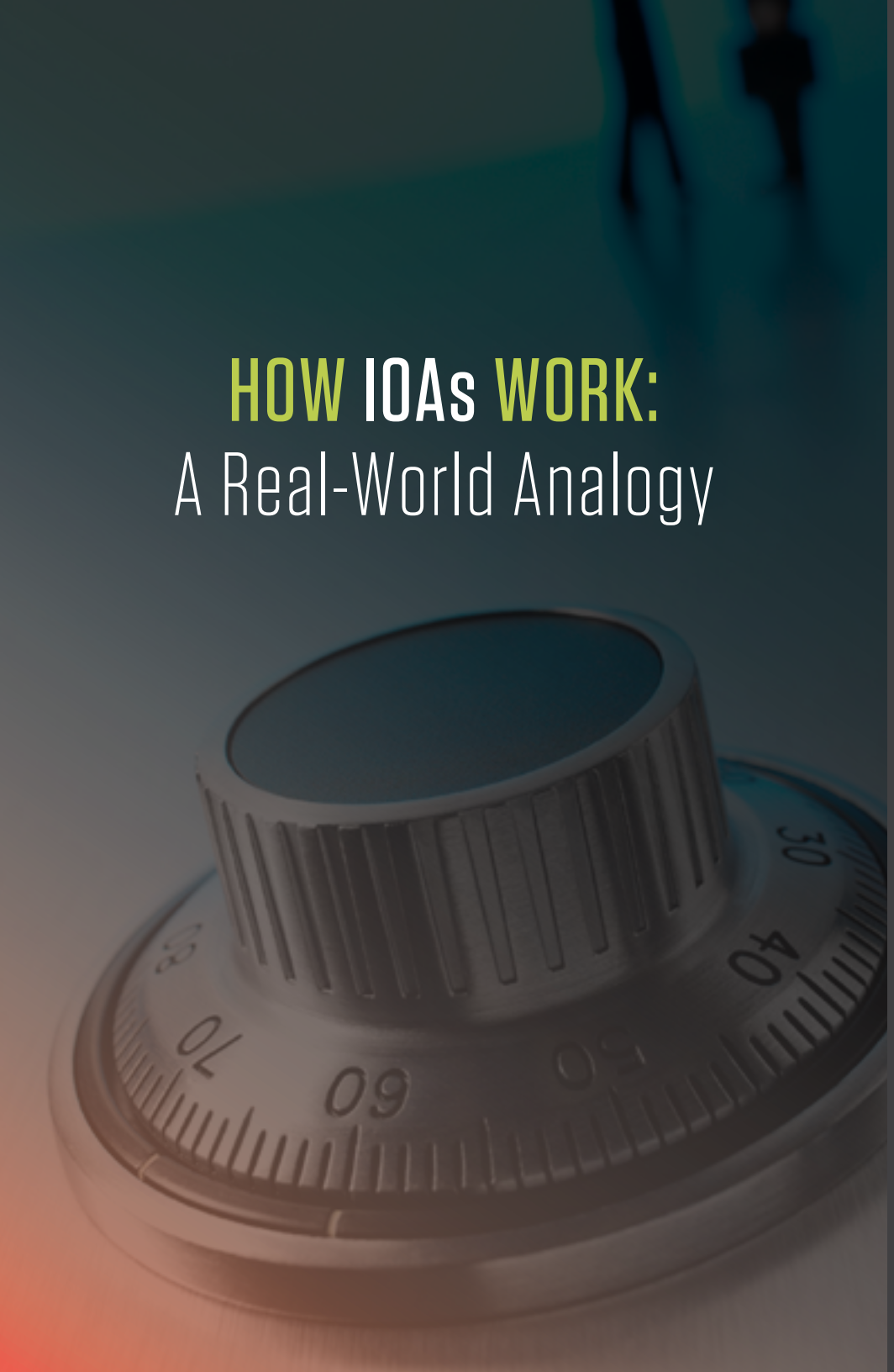
- If the attacker is trying to hide his presence and activities
- If credentials are being dumped from memory or disk
- If privileges are being escalated
- If lateral movement is taking place within the network

Individually, any one of these behaviors may not indicate a threat, but when they're examined in context with one another it becomes apparent an attack is in progress.

In order to collect this much data and analyze it swiftly and accurately, next-generation AV requires a level of computational power and scalability that can't be accomplished using old-school on-premises architecture and conventional database methods. Such feats can only be achieved via a purpose-built cloud platform capable of supporting cutting-edge data modeling technology, such as a graph database. To that end, CrowdStrike created the cloud-based Falcon platform, which is capable of collecting and storing billions of discrete endpoint execution events, and examining them in real time using the CrowdStrike Threat Graph™ data model. Built on a graph database, CrowdStrike Threat Graph can analyze and correlate data collected from endpoint sensors located in over 175 countries in seconds, spotting patterns to determine if an attack is underway.

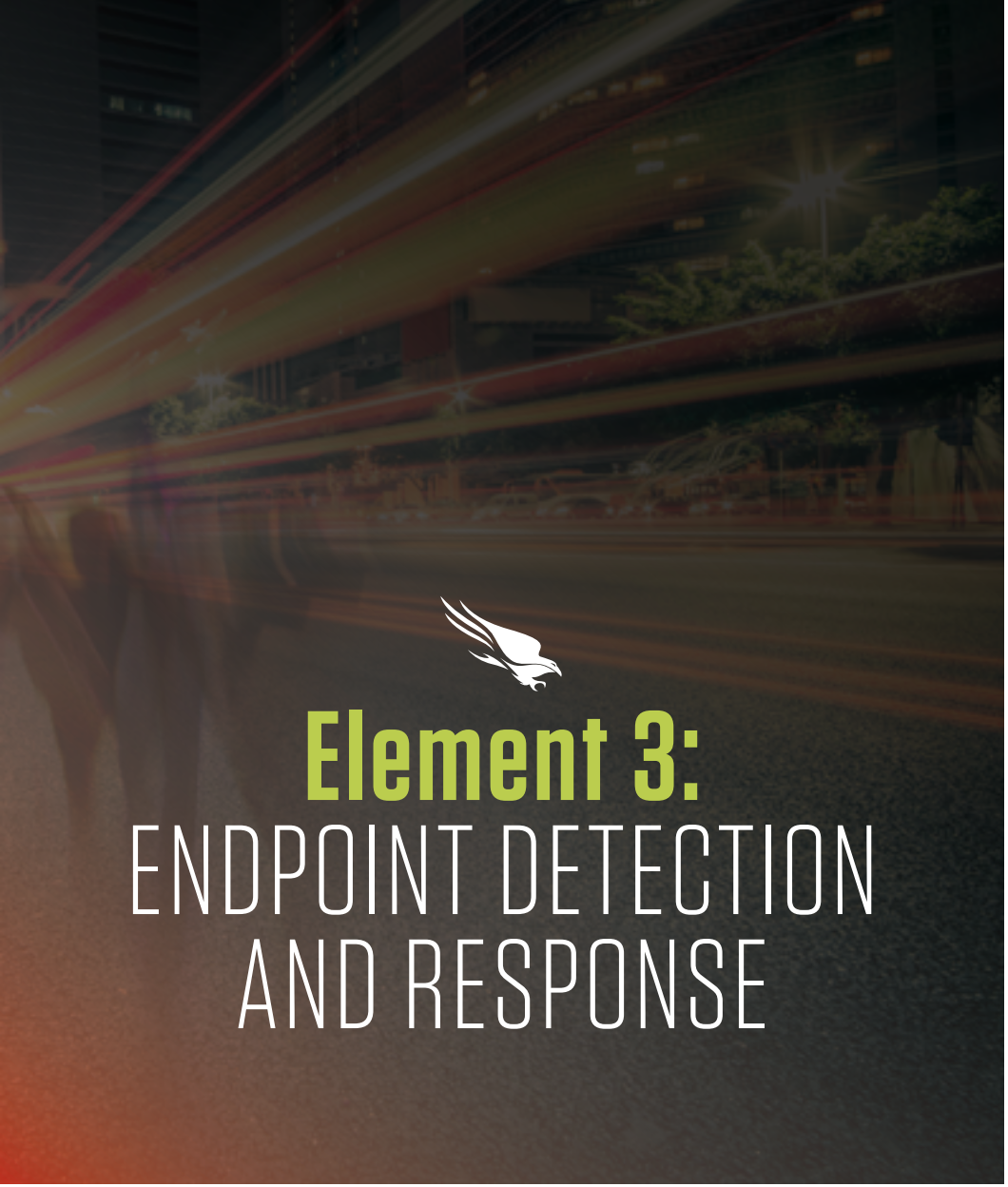
This architecture, where the heavy lifting is performed in the cloud, allows Falcon to provide endpoints with maximum protection and negligible endpoint impact, keeping the endpoint safe while ensuring optimal performance. Falcon's next-generation AV capabilities are uniquely designed to offer the visibility and speed necessary to find and block unknown threats before they cause a breach.

HOW IOAs WORK:
A Real-World Analogy



To illustrate how IOAs work, let's look at how a criminal might plan and carry out a bank robbery in the physical world. A smart thief begins by "casing" the location, performing reconnaissance to identify and understand any potential vulnerabilities. Once he determines the best time and tactics for success, he proceeds with the crime. A stealthy robber chooses a time when he's less likely to be observed. He then breaks in, disables the security system, finds the vault, and attempts to crack its combination. If he succeeds, he grabs the loot and makes an uneventful getaway, successfully completing his mission.

In this example, IOA's represent the series of behaviors a bank robber displays as he progresses toward his objective of robbing the bank and getting away with it. These behaviors might include driving around the bank (identifying the target), parking and entering the building, disabling the security system, and so on. Of course, any of these activities on their own wouldn't necessarily indicate an attack is imminent. It is only when these events are observed occurring in specific combinations that a potential threat can be identified and eliminated.



Element 3: ENDPOINT DETECTION AND RESPONSE

A fully functioning endpoint detection and response (EDR) system should record all activities of interest on an endpoint for deeper inspection, both in real time and after the fact.

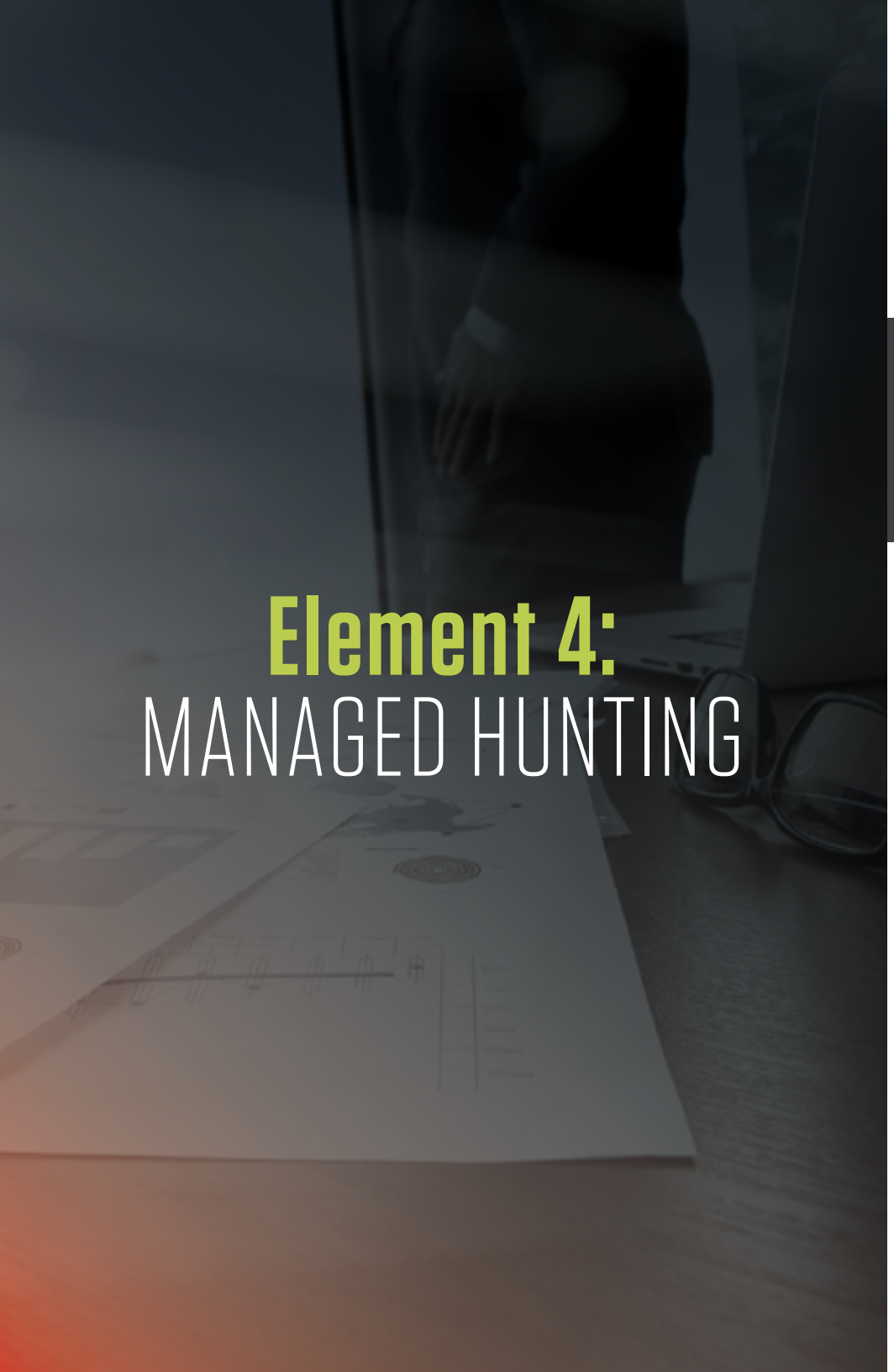
Such a solution can be compared to a surveillance camera that starts recording when it detects movement: The product should record all activities, starting when the system does anything that might indicate the beginning of an attack, such as:

- Running an application
- Connecting to a network
- Visiting a website
- Writing a file to disk

This gives the system the power to proactively hunt through large volumes of data to find malicious patterns of activity that may not have been detected otherwise.

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

The solution can only collect and keep all the necessary data if it takes advantage of the scalability offered by the cloud. In addition, cloud deployment is crucial for protecting remote systems that may be off the network or outside the VPN. And cloud capabilities make it possible to analyze this kind of behavior across numerous organizations to take advantage of the collective knowledge of a crowdsource community where threat intelligence is aggregated anonymously.



Element 4:
MANAGED HUNTING

At the end of the day, attackers are people, and people are adaptive and creative. Defenders are at a major disadvantage if they rely on technology alone to counter every attack.

TIP: An effective next-generation endpoint solution must be augmented by a team of security experts hunting through the available data and proactively looking for threats.

An elite hunting team not only finds things that may have been missed by automated response systems, they can learn from incidents that have taken place, leverage the aggregated crowdsource data, analyze it thoroughly, and provide customers with response guidelines when malicious activity is discovered..

This kind of managed hunting is at the heart of next-generation endpoint security. Without it, customers have no one but their often understaffed internal teams to watch 24/7 for adversary activity, and no guidance on how to respond to extremely sophisticated attacks. Managed hunting pits the brainpower of expert human defense teams against the ingenuity of determined adversaries.

The CrowdStrike Falcon® platform provides an unparalleled team of dedicated threat hunters who, when paired with the robustness of the data collected by Falcon, are able to thwart attacks that would never be detected by any other system or technology.

Element 5:
THREAT INTELLIGENCE

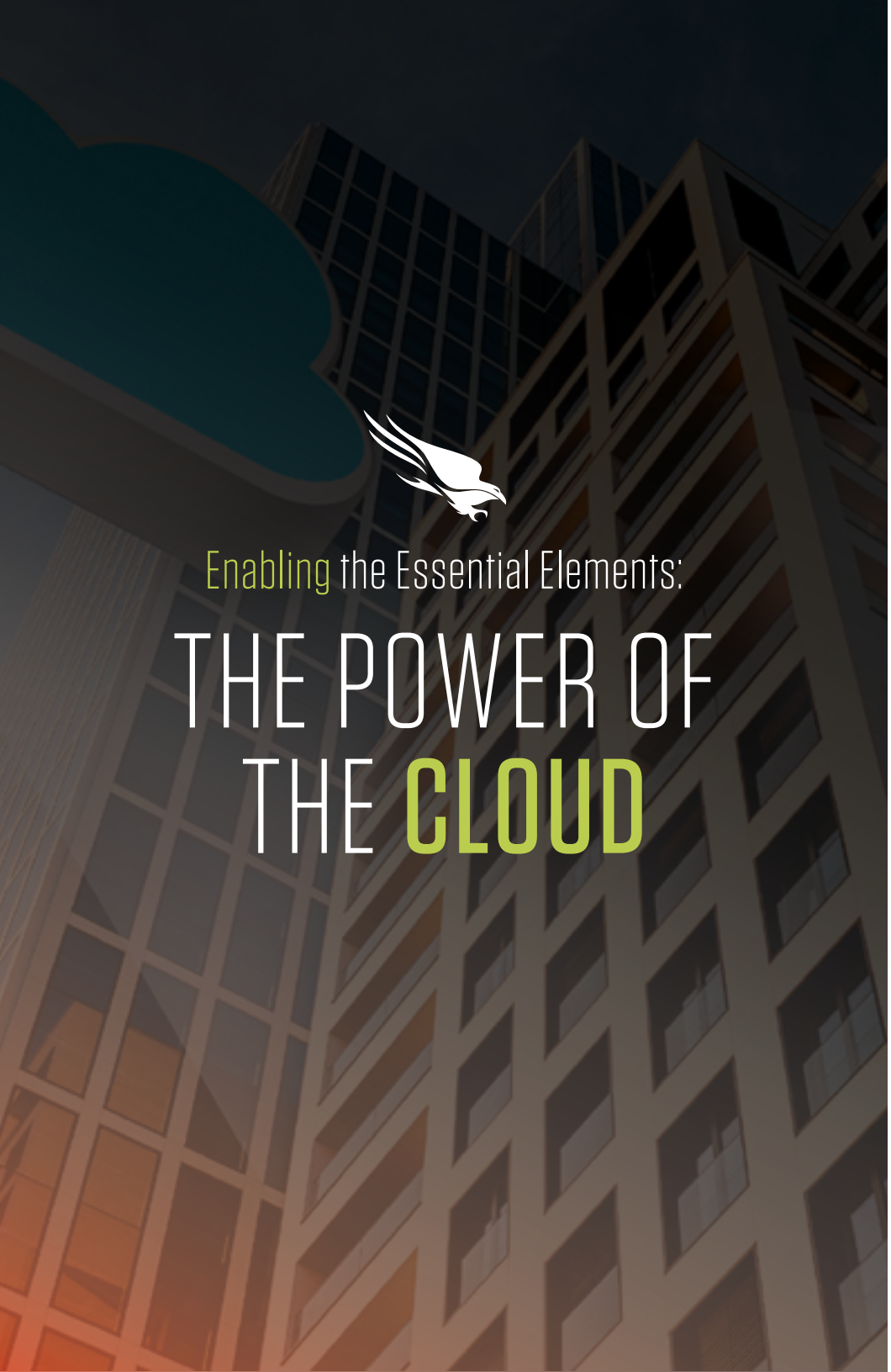
To fully support a next-generation approach to endpoint protection, threat intelligence needs to provide more than the tactical advantages of understanding, responding and resolving incidents faster. It also needs to offer the proactive alerts and reports that security experts need to prioritize their resources at an operational level. Truly insightful threat intelligence doesn't stop there: It must also provide the information that helps security leaders make the right decisions and define a security strategy best adapted to their very unique risks.

TIP: The value of threat intelligence lies in its ability to offer the most accurate, actionable and up-to-date information needed to proactively protect organizations from breaches, through a deep understanding of threats and adversaries, and what it takes to stop them.

No single product or service can stop a breach on its own. It takes people, process, technology and intelligence – all working in concert – to stop breaches.

Because sophisticated adversaries can move so quickly and stealthily, it is essential that security teams receive the intelligence required for all defenses to be automatically and precisely instrumented throughout the enterprise, to stop breaches with minimal impact and maximum protection.

This is why security professionals looking at next-generation endpoint protection must ensure that they don't focus solely on the security infrastructure but include threat intelligence as part of a total solution.



Enabling the Essential Elements:

THE POWER OF THE CLOUD

The only way to effectively deliver these five essential elements that constitute next-generation endpoint protection is via a purpose-built cloud architecture. The on-premises model isn't suited to extremely arduous tasks such as collecting a rich data set in real time, storing it for long periods, and thoroughly analyzing this volume of data in a timely manner to prevent breaches. With the cloud, it is possible to store petabytes of data for months on end, to gain historical context on any activity running on any managed system. With the CrowdStrike Threat Graph, these massive data stores can be analyzed in seconds, allowing immediate blocking of an attack in progress as IOAs are observed, and providing the ability to look back and see whether these activities took place in an organization's environment at any previous point in time. The cloud also enables aggregation of data across environments to fully leverage the knowledge and intelligence of the crowd.

At present, many endpoint security products claim to be cloud-delivered, but are actually based on architectures developed primarily for on-premises systems. This "bolt-on" cloud model can never match the performance of a purpose-built, cloud-native system. Even when connected via the cloud, an isolated appliance placed in a vendor data center cannot take advantage of the fundamental benefits of crowdsourcing.This ability to leverage the "power of the crowd" requires a true cloud model capable of correlating data streams across numerous customers.

NEXT GENERATION ENDPOINT SECURITY FROM **DAY ONE**

Each of these five elemental components of next-generation endpoint security are being tested and rolled out in a piecemeal fashion by numerous vendors across the industry. Some companies focus solely on prevention, while others may concentrate on machine learning. Many fixate on one or two very specific detection techniques, but none can offer all of the elements that next-generation endpoint security requires in a single integrated solution — none except CrowdStrike.

CrowdStrike's holistic design philosophy demonstrates that the efficacy of next-generation endpoint security can only be achieved when each of the five elements is present. Without all of them working together in concert, a system can't be labeled next-generation endpoint protection.

Unlike the fragmented, bolt-on approach other security vendors take, CrowdStrike's purpose-built cloud architecture delivers its powerful combination of IT hygiene, next-generation AV, endpoint detection and response, 24/7 managed hunting services and threat intelligence to proactively search for hidden attacks — in one unified platform.

In addition to offering the greatest capacity for blocking and detecting attacks and uncovering previously undiscovered threats, the cloud-based Falcon platform enables lightweight, lightning-fast deployment. Without hardware and additional software to procure, deploy, manage and update, rolling out endpoint security becomes quick and simple. While on-premises systems can take up to a year to fully roll out, CrowdStrike has been successfully deployed in environments with tens of thousands of endpoints in a matter of hours. The nature of CrowdStrike's cloud architecture allows it to be easily deployed side-by-side with existing security solutions, offering a seamless transition.

CrowdStrike's ultimate goal is to help its customers stop breaches immediately, with minimal time, effort and impact on their business processes. Ultimately, that is the definition of next-generation endpoint protection.

PROTECTING AGAINST BREACHES IS AN ONGOING BATTLE.

To be truly effective, a next-generation endpoint protection solution must provide continuous breach protection. This means providing constant prevention, detection, visibility and intelligence, so you can be protected before, during and even after a breach.

CrowdStrike next-generation endpoint protection integrates all those elements in one tiny agent, supported by the cloud, that can be deployed in hours with no impact on your endpoints or their users. Its ability to continuously stop breaches makes it a true and proven next-generation endpoint protection solution.

NEXT GENERATION ENDPOINT EVALUATION CRITERIA

To help you measure and compare different solutions, use the following set of criteria, which CrowdStrike security experts consider critical to the success of an effective next-generation endpoint protection solution.

(Place checkmarks in all the boxes that apply.)

Evaluation Criteria for Next-Gen Endpoint Protection

PREVENTIVE SECURITY and IT HYGIENE	CROWDSTRIKE FALCON ENDPOINT PROTECTION	SOLUTION 2	SOLUTION 3
Shows who is on your network at all times	X		
Shows what applications your users are running in real time and historically	X		
Shows where and how user accounts are being used	X		
PROTECTION AND PREVENTION			
Protects against both known and zero-day malware with ML on endpoint	X		
Protects against ransomware	X		
Protects beyond malware and against fileless attacks *(that don't use portable executables and/or files)*	X		
Protects against known and unknown exploits	X		
Dynamically stops attacks in progress *(stops attacker activity, such as privilege escalation, lateral movement, credential theft, etc., if the attacker succeeds in earlier steps of the Attack Chain)*	X		
Protects online, offline, on-premises and off-premises	X		
DETECTION AND RESPONSE			
Operates in kernel mode for complete visibility	X		
Ensures network containment of compromised systems	X		
Provides 24/7 monitoring and proactive hunting	X		
Provides instant search capabilities *(query results in 5 second or less)*	X		
FORENSICS			
Captures the data necessary to conduct efficient and fast forensic analysis	X		
Can determine what data was exfiltrated	X		
Offers long-term data retention	X		
Provides forensics data even if the compromised system is inaccessible or destroyed	X		

PRODUCT COMPLETENESS	CROWDSTRIKE FALCON ENDPOINT PROTECTION	SOLUTION 2	SOLUTION 3
Provides protection before, during and after attacks	X		
Provides 24/7 managed hunting and actionable alerting by security experts	X		
Is self-sufficient *(doesn't require additional products, agents or modules to offer full next-gen capabilities)*	X		
Supports Windows, Mac and Linux	X		
DEPLOYMENT, MANAGEABILITY AND USABILITY			
Offers a fully cloud-based management and deployment option	X		
Installation and updates don't require reboots	X		
Fully deployed and operational in days vs. weeks or months	X		
Has imperceptible footprint on endpoint *(less than one percent CPU usage at all times, even when queries are performed)*	X		
Doesn't require tuning or expert-level configuration	X		
INTELLIGENCE AND INTEGRATION			
Automatic IOC ingestion from third-party SIEM integrations	X		
Supplies its own intelligence *(doesn't depend on other sources for intelligence)*; offers APIs for integration and expansion	X		
Provides tactical, operational and strategic threat intelligence	X		
Provides attribution	X		

QUESTIONS TO ASK

The following questions will help you gain insight into how a next-generation endpoint protection solution works, so you can asses the type of experience you can expect from it.

1. Can the product help me before, during and after an attack?
2. What can the product do if we are already breached and it's deployed after the breach?
3. Can the product tell me how attackers are accessing my environment? How does it accomplish that?
4. Can the product tell me who is attacking me? How does it accomplish that?
5. How does the product help me protect against, detect and manage future breaches?
6. How long does it take for the product to be fully operational?
7. Will I be alerted and receive your assistance if my team misses something important?
8. Can the product tell me what files have been exfiltrated?
9. For attacks that don't use malware, how do you detect the attack?
10. How many technologies does it use to detect malware?
11. Can the product detect if someone is using stolen credentials, or abusing privileges?
12. How many distinct products/modules/agents/appliances do I need to cover all prevention, detection and response needs?
13. What additional hardware and software (servers, appliances, database licenses, components on the endpoints) are required to implement the product? Are they provided as part of the next-generation endpoint protection solution, or is there an additional cost?
14. What is the impact of the solution on endpoint performance? What is the footprint on disk, memory and CPU?
15. What security controls does the solution use to protect itself?
16. Does the solution integrate with other security and enterprise tools?

ABOUT **CROWDSTRIKE**

CrowdStrike® is the leader in cloud-delivered endpoint protection. 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. Falcon 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 cyber attack types, using sophisticated signatureless artificial intelligence/ machine learning 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 60 billion security events from across the globe to immediately prevent and detect threats.

CROWDSTRIKE

www.crowdstrike.com