ENDPOINT DETECTION AND RESPONSE

Automatic protection against advanced threats

EXECUTIVE SUMMARY

With enough motivation, time and resources, adversaries eventually devise a way to get through an organization's defenses. Unfortunately, when that occurs, most security products "fail silently," unable to detect, let alone alert you on the intrusion. This can allow an attacker to freely roam around your environment for weeks and even months. This situation may be aggravated by a lack of visibility, security resources and expertise. Endpoint detection and response (EDR) is the most promising solution for addressing this challenge. At a primary level, EDR products record the activities and events taking place on endpoints, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible. Even though the basic concept may sound simple, EDR comes in a wide variety of implementations that can vary greatly in scope and efficacy. This is captured in what CrowdStrike ® calls the EDR Maturity Model, a model that encompasses both the evolution and capabilities of EDR solutions. The model, which is outlined in this white paper, can be used as a guide to furthering your understanding of EDR, where it fits in a robust security strategy and ultimately, what is involved in maturing EDR capabilities so that your organization can derive the greatest benefit. Toward that end, it is crucial to find an EDR solution that provides the highest level of protection while requiring the least amount of effort and investment, adding value for the security team without adding additional burden.

For organizations that want total visibility over their endpoints and want to detect and respond to malicious activities before they turn into full blown breaches, Falcon Insight™, CrowdStrike's industry-leading EDR solution, combined with Falcon OverWatch™ a ground-breaking threat hunting service, provides a powerful and comprehensive solution that delivers instant results..

OPERATING IN THE DARK

Past and current breaches have proven time and again that prevention can't ensure 100 percent protection. When prevention fails, an organization can be left in the dark by its current endpoint security solution. Attackers take advantage of this situation to linger and navigate inside the organization for weeks or months, achieving their goals and returning at will. In most cases, the organization learns about the breach from a third party, such as law enforcement or its own customers or suppliers.

When a breach is finally discovered, the victim organization can spend months trying to remediate the incident because it lacks the visibility required to see and understand exactly what happened, how it happened and how to fix it — only to see the attacker return within a matter of days.

Multiple factors contribute to this situation. First, historically, security has put an emphasis on prevention rather than detection. Second, an organization may lack the visibility required to even begin to understand what is happening on its endpoints. This extends from the ability to record what is relevant to security, to the capacity to store and recall the information quickly enough when needed. Third, even when data is available, security teams lack the resources needed to analyze and take full advantage of it. This is why many security teams find that soon after they've deployed an event collection product, such as a SIEM, they are often facing a complex data problem. Challenges around knowing what to look for, speed and scalability begin cropping up and other problems surface before their primary objectives can even be addressed.

THE EDR MATURITY MODEL

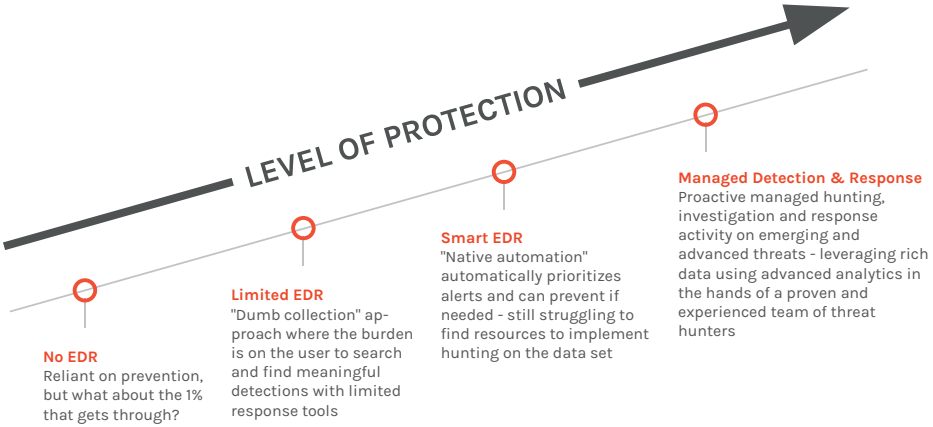
To address incidents not handled appropriately by existing defenses, organizations need solutions that can quickly detect and allow for quick investigation of potentially malicious and suspicious activities.

This is where EDR comes into play. Visibility plays a crucial role in EDR, because while legacy endpoint security products are limited to either blocking or allowing an activity, EDR products add the ability to record endpoint activity and store it for future searches and investigations. This provides security teams with the visibility they need to find incidents that would otherwise remain unseen. But collecting relevant data is only the beginning. Knowing what to do with the data — and what to look for in it — is the next challenge. It requires not only security expertise and the time to perform searches, it means staying up to date on the latest indicators of compromise (IOCs); current adversary tactics, techniques and procedures (TTPs); and security trends. This is why the apparent simplicity of the EDR concept is so deceptive: there are vast differences in the way it may be implemented. Each implementation can vary greatly in scope and efficacy, as illustrated by the EDR maturity model below.

"ENTERPRISES THAT KNOW COMPROMISE IS INEVITABLE AND ARE LOOKING FOR ENDPOINT-BASED APPROACHES FOR ADVANCED THREAT DETECTION, INVESTIGATION AND RESPONSE CAPABILITIES, SHOULD CONSIDER EDR SOLUTIONS."

NEIL MACDONALD,
VP DISTINGUISHED ANALYST,
GARTNER RESEARCH

EDR MATURITY LEVEL



"No EDR." Without EDR, organizations are vulnerable to any threats that manage to get by their existing defenses. This may lead to "silent failure" — the state of being breached without knowing it.

"Limited EDR." This offers an improvement because events that are collected are also visible. However, the burden of analysis rests on the security team. It still needs to know what to look for in the data to which it has access, requiring both time and security expertise.

"Intelligent EDR." In contrast to limited or no EDR, intelligent EDR performs the analysis and automatically detects incidents in real time, while also giving the security team the flexibility of performing its own custom searches.

"Managed Detection & Response." The highest level in EDR maturity, managed detection and response offers the ultimate level of protection, as it enables organizations to proactively and continuously search for threats, rather than passively waiting for detections. A managed implementation provides an immediate and affordable 24/7 solution, offering the requisite skills, expertise and experience found only among seasoned security experts.

FALCON INSIGHT – CROWDSTRIKE EDR SOLUTION

Falcon Insight is the EDR component of the CrowdStrike Falcon® platform. It monitors and records activities taking place on the endpoint, providing the real-time and historical visibility necessary to automatically detect an attacker's activity, while also enabling security teams to investigate and resolve incidents quickly. This stops attackers before they can do damage and eliminates the risk of silent failure.

Falcon Insight is the ideal EDR solution because it not only automatically detects post-breach attacker activity, it grants security teams real-time visibility across their environments. This enables them to engage in proactive threat hunting, incident investigation and timely remediation.

FALCON INSIGHT — THE INDUSTRY LEADER IN EDR

- "Best Behavior Analytics/ Enterprise Threat Detection," **Security Magazine Award 2017**
- "Perfect Detection Score" (5/5) and "Perfect Cost Score" (value for the money) in the 2017 **Forrester Endpoint Security Wave**
- Scored "Strong" (the highest rating possible) in all use cases evaluated in the 2017 Gartner Comparison of Endpoint Detection and Response Technologies and Solutions report

INTELLIGENT EDR

AUTOMATICALLY UNCOVERS STEALTHY ATTACKERS

Pairing full endpoint visibility with indicators of attack (IOAs), Falcon Insight behavioral analytics allows it to analyze billions of events in real time and to automatically detect traces of suspicious behavior. IOAs automate and accelerate the detection of attacker behaviors and pinpoint attacker activities that would otherwise go unnoticed. Thanks to IOAs, it's no longer necessary for security teams to figure out what to look for and then build their own searches.

Understanding individual events as part of a broader sequence allows the Falcon Insight agent to apply security logic derived from CrowdStrike Falcon Intelligence™, CrowdStrike's dedicated threat intelligence offering. If a sequence of events matches a known IOA, the Falcon agent will identify the activity as malicious and automatically send a detection alert.

But Falcon Insight's visibility capabilities are not limited to IOAs. Users can also write their own custom searches, going back up to 90 days, which greatly assists security teams that want to proactively hunt for threats in their environments. Thanks to Falcon Insight's cloud architecture, query results come back in five seconds or less.

INTEGRATION WITH THREAT INTELLIGENCE

Falcon Insight's use of CrowdStrike cyber threat intelligence provides faster detection of the activities and TTPs identified by Falcon Intelligence as malicious. In addition, the integration of threat intelligence brings contextualized information and includes attribution where relevant, providing details on the adversary attributed and any other information known about the attack. Such attributions give Security Operation Centers (SOCs) and security analysts additional context about an attack, providing a detailed narrative that specifies the "who, why and what" of the event. Understanding who might be targeting an organization, and what his capabilities and intentions are, empowers organizations to be better prepared to protect themselves.

THE AUTOMATION OF DETECTION USING THE IOAS, BEHAVIORAL ANALYTICS, BUILT-IN INTELLIGENCE WITHIN **FALCON INSIGHT** AND THE ABILITY TO CONSUME THIRD-PARTY IOCS FROM CUSTOM THREAT FEEDS RESOLVES ONE OF THE BIGGEST CHALLENGES EDR USERS ENCOUNTER: **KNOWING WHAT TO LOOK FOR.**

UNPARALLELED VISIBILITY

REAL-TIME AND HISTORICAL VISIBILITY

Falcon Insight acts like a DVR on the endpoint, recording relevant activity to catch incidents that evaded prevention. It ensures customers have comprehensive visibility into everything that is happening on their endpoints from a security perspective, with contextual information that includes the what, when, why and even "the who" behind an attack.

Its position at the kernel level allows the Falcon agent to track hundreds of different security-related events, such as process creation, drivers loading, registry modifications, disk access, memory access, or network connections. This gives security teams a great deal of useful information, including local and external addresses to which the host is connected; all the user accounts that have logged in, both directly and remotely; a summary of changes to ASP keys, executables and administrative tool usage; process executions; both summary and detailed process-level network activity, including DNS requests, connections, and open ports; archive file creation, including RAR and ZIPS; and even removable media usage.

This complete oversight of security-related endpoint activity allows security teams to "shoulder surf" an adversary's activities in real time, observing which commands he is running and what techniques he is using, even as he tries to breach or move around an environment.

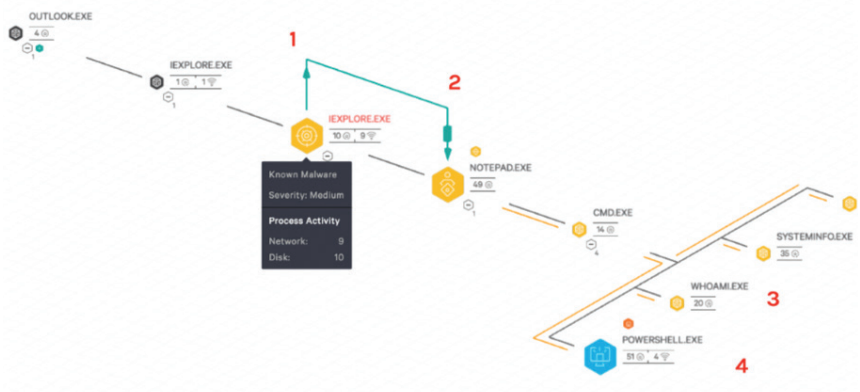
ACCELERATED INVESTIGATION

The information gathered is stored in the CrowdStrike cloud via the Falcon platform, with architecture based on a situational model. The model keeps track of all the relationships and contacts between every endpoint event using a massive, powerful graph database, which provides details and context rapidly and at scale, for both historical and real-time data. This enables security teams to quickly investigate incidents.

That speed and level of visibility, combined with the built-in intelligence of Falcon Insight, provides the context needed to thoroughly understand the data, delivering a level of detail that allows an organization's security team to effectively track even the most sophisticated attacks. This, in turn, allows the security team to promptly uncover incidents, triage and prioritize them, but also to investigate and validate them quickly, leading to faster and more precise remediation.

PROCESS TREE: DETECT THE UNKNOWN, CONNECT THE DOTS AND SEE THE BIG PICTURE

The visibility and ease of investigation is illustrated by the process tree. It automatically unravels entire attacks on just one screen and provides easy-to-read full attack details in context, for faster and easier investigations.



The process tree on the previous page is displaying a spear phishing attack that started with Outlook. In this instance:

1. A user clicked a link in Outlook, which spawned Internet Explorer, which then spawned a tab within Internet Explorer to run an exploit. This is represented by the first Known Malware node, depicted here.

2. Once the exploit was successful, the attacker migrated into notepad.exe to bypass whitelisting (the green line reflects the thread injection from IE to notepad).

3. Then, under notepad's memory space, the adversary used a command shell (cmd.exe) to run whoami, systeminfo, and ping as a part of reconnaissance to get a better understanding of the victim's host and user details.

4. Finally, the adversary ran a PowerShell command, remotely, to dump credentials.

Network containment: Stopping the adversary in his tracks

If the security team faces immediate concerns or if it decides to prevent the victim host from being used as a leverage point for more access (lateral movement) until the compromise can be fully remediated, Falcon Insight can isolate the endpoint. This is called "network containment" and it allows organizations to take swift and instantaneous action by isolating potentially compromised hosts from all network activity. When an endpoint is under containment, it can still send and receive information from the CrowdStrike cloud. Endpoints under network containment will remain contained even if the connection to the cloud is severed and will persist with this state of containment during reboots.

THE CONTINUOUS MONITORING AND UNPARALLELED VISIBILITY PROVIDED BY FALCON INSIGHT SOLVES TWO BIG CHALLENGES FACED BY SECURITY TEAMS USING EDR:

THE ABILITY TO GATHER RELEVANT EVENTS TO DETECT SUSPICIOUS ACTIVITIES, AND BEING ABLE TO VIEW THE ENTIRE ATTACK SEQUENCE AT ONCE.

THE POWER OF THE CLOUD

VISIBILITY IN FIVE SECONDS ACROSS AN ENTIRE ORGANIZATION

With Falcon Insight, relevant endpoint activity is automatically recorded and streamed to the Falcon platform in the cloud, where it is stored in a graph database known as the CrowdStrike Threat Graph™. The Threat Graph is designed to return results for all queries in just five seconds, regardless of the size of the query results or the amount of data in the database.

This approach also guarantees that customers can still search and investigate events and anomalies even if an endpoint is offline, has been reformatted or decommissioned, or even if one is lost or destroyed. This also allows security teams to discover and investigate endpoint activity going back one second, one day, or even across 90 days of activity — putting the information at their fingertips.

Another benefit of having historical analysis enabled in the cloud is that searches performed by analysts have no impact on the endpoints, corporate environment or the network. It also allows for simultaneous queries to be run both in real time and historically. This is critical because the ability to conduct concurrent searches means that analysts don't have to wait for a query to be complete before running another one and obtaining results.

FULLY OPERATIONAL IN HOURS

Since the Falcon agent is both lightweight (20MB footprint) and cloud-enabled, it can be operational — that is deployed, and ready to use — with unprecedented speed. Falcon Insight can be deployed within hours across an entire organization, not weeks or months, and since it requires no hardware or additional software, no tuning or configuration, it has virtually no performance impact on the endpoint. For example, it is not uncommon when responding to a breach for the CrowdStrike Incident Response team to deploy and start using

the Falcon agent within hours across thousands of endpoints, to start monitoring and detecting malicious activities immediately.

The Falcon platform is designed with simplicity in mind. Because customers are already burdened with managing multiple, complex products in their environments, CrowdStrike designed the Falcon platform to integrate seamlessly into an environment without adding complexity. Once deployed, it immediately begins to record activity and enable proactive hunting, offering organizations the fastest time-to-value in the industry.

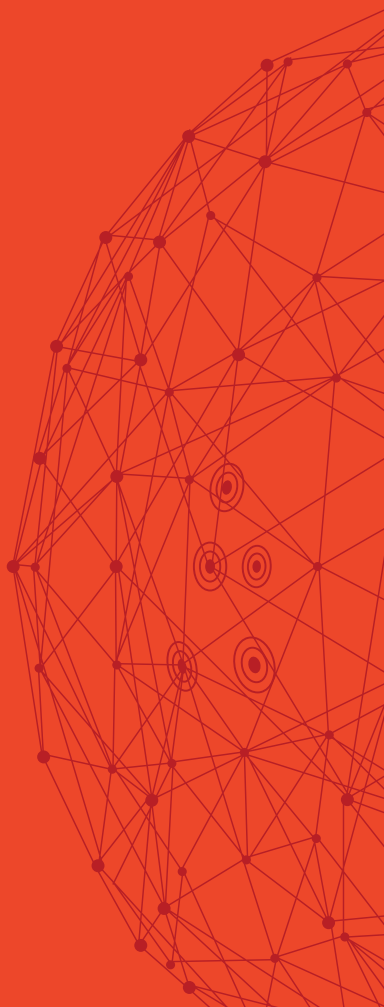
ENABLING PROACTIVE THREAT HUNTING AT UNPRECEDENTED SPEED AND SCALE

The Falcon Insight cloud architecture enables proactive threat hunting on an unprecedented scale. As illustrated in the EDR maturity model discussed previously, threat hunting increases an organization's protection against attackers and plays a critical role in early detection of attacks and adversaries. It does this with a human-led, proactive approach consisting of actively searching for suspicious activities rather than relying on passive technology. Falcon Insight allows security teams to hunt for up to 90 days, returning query results in seconds and easily pivoting from one clue to the next. Additionally, the use of APIs allows customers to "walk the Threat Graph," allowing them to uncover at a glance the relationships between seemingly unrelated events and accelerate the discovery of extremely stealthy attacks.

Organizations that don't currently have the security resources to carry on their own threat hunting can still benefit from it thanks to Falcon OverWatch, the managed threat hunting component of the Falcon platform. The Falcon OverWatch team of experienced security experts works on the customer's behalf 24/7 to proactively hunt for threats and stop breaches.

THE CLOUD ARCHITECTURE OF FALCON INSIGHT SOLVES ANOTHER CHALLENGE FACED BY SECURITY TEAMS USING EDR:

THE NEED FOR SPEED, PERFORMANCE AND SCALABILITY.



The benefits of Falcon OverWatch don't apply only to organizations with small teams, or those with limited proactive hunting skills and experience. Larger, more mature organizations looking for added capabilities and skilled personnel to augment their existing SOC and incident response teams also benefit greatly from OverWatch. In addition, the cloud capabilities of the Falcon platform make it possible for OverWatch to proactively hunt for malicious activities across multiple organizations, allowing it to protect the entire CrowdStrike community. If an attack or threat is uncovered at one CrowdStrike customer, all other customers will immediately benefit from that discovery.

CONCLUSION

Ninety-nine percent prevention means a 100 percent chance of eventually being breached. Once attackers manage to bypass an organization's defenses, they can go unnoticed for weeks or months because security teams lack the visibility and detection tools to identify post-breach activity. This period of silent failure spells success for the attacker and potential disaster for the organization.

Falcon Insight is CrowdStrike's EDR solution. It enables security teams to proactively hunt for threats; investigate and respond to incidents faster; and stop potential breaches before their organizations are compromised. It is the ideal solution for security teams who want to accelerate incident response and gain total visibility and control over their endpoints.

CROWDSTRIKE

crowdstrike.com