CrowdStrike Products

CROWDSTRIKE

MANAGED DETECTION AND RESPONSE (MDR) BUYER'S GUIDE

INTRODUCTION

WHAT IS MDR?

A chronic shortage of cybersecurity professionals and expertise is impacting organizations of all sizes across all industry sectors worldwide. The problem is made worse as adversaries improve their tradecraft, enabling them to execute attacks with greater speed and effect. Organizations struggle to move beyond a preventive security stance to address the need for earlier detection, proactive threat hunting and a fast and effective 24/7 response to threats. Staffing and resourcing a dedicated security team that can achieve all of this may be feasible for larger organizations with the budgets to afford it, but most companies will find it a difficult proposition, given their more limited resources.

Managed detection and response (MDR) has emerged in response to this market need. MDR helps an organization by implementing or improving threat detection, response, management and continuous monitoring capabilities — all delivered as a service.

MDR providers leverage endpoint detection and response (EDR) and other technologies to gain visibility into security-related events across the organization to support threat detection and incident investigation. Human analysts monitor for alerts and assist in responding to them. The form of that response includes actions ranging from investigating an alert (triage) to taking practical steps to reduce the impact and risk (mitigation), and finally, completely removing the threat and returning the endpoint to a known good state (remediation).

Look for an MDR solution that owns the outcomes, one that:

- Augments your team with deep expertise
- Eradicates threats in minutes and owns remediation
- Significantly reduces cybersecurity risk and cost

WHY DO ORGANIZATIONS NEED MDR?

Operating an effective endpoint security program can be extremely challenging. The necessary tools can be difficult to use, requiring an abundance of human resources to appropriately implement, support and maintain them. As a result, many organizations fail to take full advantage of the endpoint security technologies they have acquired. The situation is even worse for organizations that want to establish a strong endpoint security posture. Higher levels of security require even more resources, as they can be more costly to maintain and more complex to manage.

The result? Many organizations do not successfully implement a fundamental endpoint security program, let alone a comprehensive one. The situation is exacerbated when serious incidents emerge and the organization has neither the time nor the expertise to properly remediate the situation, potentially endangering the safety of the organization.

The challenges that MDR helps address:

- **They have difficulty fully implementing and properly configuring the technology they have acquired.** Depending on the size and workload of their IT teams, some organizations might not have the tools or bandwidth to quickly and successfully deploy the solution to their endpoints. In addition, they may lack the time and expertise needed to properly configure and tune policies that match their security requirements and keep endpoints protected, as threats and the environment evolve. This situation can lead to an endpoint solution that is only partially deployed and poorly configured — resulting in gaps in protection that leave the organization vulnerable to breaches.

- **There are too many alerts and incidents every day.** Handling the potentially massive number of alerts generated by some endpoint security products can be overwhelming, even for organizations that have a dedicated security team or security operations center (SOC). Managing alerts requires not only manpower but also 67% of IT decision-makers believe that security operations is more difficult today or the same than it was only two years ago.[1] Unfortunately, most organizations suffer from a shortage of both staffing and expertise, leaving alerts unvalidated and opening the door to high-profile breaches.

- **Organizations don't have the resources to properly remediate incidents.** Resource and expertise shortages can lead to organizations struggling to understand the nature and scope of an incident in a timely manner. 80% of IT decision-makers believe security staffing shortages are marking their enterprises more vulnerable.[2] This can mean incidents are not remediated efficiently, not fully addressed or not handled quickly enough, leaving organizations vulnerable or even compromised. It takes skill and experience to know how to properly remediate an incident. Many organizations that lack resources are forced to go through the arduous process of reimaging endpoints. The alternative of surgically combining countermeasures — such as network containment, hash prevention, delete/modify registry key values or stop/disable/restart services — is unrealistic. And reimaging does not ensure full remediation of the incident.

- **It takes time to successfully implement a program.** Even if an organization has sufficient funds to build an internal endpoint security program, implementing a mature security strategy can take a long time. From finding and hiring the right talent and acquiring the appropriate technology, to defining policies and creating an incident response (IR) process, the undertaking can take months if not years. In addition, such programs are often given a lower priority than other urgent IT projects, resulting in long implementation processes that leave organizations vulnerable.

- **Finding and retaining the necessary expertise is difficult.** It can be challenging for an organization to acquire the expert staff needed to efficiently secure its endpoints. According to the International Information System Security Certification Consortium, there are more than 3.4 million unfilled cybersecurity positions worldwide.[3] Even for those who can afford it, recruiting, training and retaining the staff and skills needed to adequately address an advanced and sophisticated threat landscape can be very challenging. This shortage of qualified expertise is an industry-wide problem.

WHAT ARE THE CORE ELEMENTS OF MDR?

Managed detection and response services focus on reducing the time difference between detection and response to effectively reduce risk by decreasing the dwell time of a threat actor. The faster the MDR provider can detect and respond to a threat, the faster remediation can take place.

An MDR that effectively meets this challenge to deliver outcomes for its customers requires a set of core capabilities to enable delivery of rapid detection and response: a strong platform, continuous human threat hunting, 24/7 monitoring and investigation, and surgical remediation. When any one of these core capabilities is missing, it is significantly harder to own the entire lifecycle of the security incident and rapidly return to a known good state.

---

1 *Source:* ESG 2023 SOC Modernization and the Role XDR report. (https://research.esg-global.com/reportaction/515201525/Toc)

2 *Source:* 2023 ESG SOC Modernization and the Role of XDR report. (https://research.esg-global.com/reportaction/515201525/Toc)

3 *Source:* 2023 ESG SOC Modernization and the Role of XDR report. (https://research.esg-global.com/reportaction/515201525/Toc)

A STRONG PLATFORM

A strong technology stack is foundational in delivering MDR that achieves the desired results. The platform must block attacks while simultaneously capturing and recording full endpoint activity as it happens to inform deeper analysis and threat hunting.

A strong platform is built upon:

1. An easy-to-deploy, cloud-native platform that reduces costs and complexities by delivering immediate time-to-value and requiring no hardware, additional software or configuration
2. A machine learning and behavioral analytic engine to provide complete real-time visibility and insight into everything happening throughout your environment
3. A single lightweight sensor to feed the platform detailed telemetry from across your entire environment, including endpoints, cloud workloads and identities

Of course, the technology only provides good protection if it's fully deployed and properly configured. An MDR provider should contribute its experience and best practices to assist in the deployment, configuration and tuning of the platform. This has an immense impact on your security maturity and ensures very fast time-to-value, with onboarding happening in days rather than weeks or longer.

CONTINUOUS HUMAN THREAT HUNTING

Threat detection can uncover many different types of vulnerabilities within your IT environment. Most of the time, detection is driven by algorithms and automation, which are fast, effective and capable of blocking threats at runtime. Some attacks, however, are driven by human adversaries who, knowing well the countermeasures used to detect their activities, work to evade them and remain hidden. Detecting such hidden, advanced attacks requires a more proactive approach.

With threat hunting, expert human analysts continuously sift through the data to look for faint signs of emerging threats and sophisticated attacks. These signs may be the result of attackers using new or novel tactics, techniques and procedures (TTPs); using stolen credentials to impersonate authorized users; or leveraging local tools and software to live off the land and blend in with day-to-day administrative activity.

An MDR service that does not provide both human-based detection and technology-based prevention is missing the opportunity to stop known bad threats at the perimeter and uncover sophisticated threats in the shadows.

24/7 MONITORING AND INVESTIGATION

Once a security alert has been created, it's the role of the security analyst to determine what security measures, if any, must be undertaken. Portions of the threat analysis process can be automated using sandboxing and behavioral analysis techniques, which deliver actionable intelligence and custom indicators of compromise (IOCs) tailored for the threats encountered.

But while many tasks within the analysis phase can be automated, human assessment is required to grasp the outputs of automated workloads and truly understand the veracity, scope and implications of an attack.

Detecting hidden, advanced attacks requires a more proactive approach. With threat hunting, human hunters continuously sift through enterprise security data looking for faint signs of emerging threats and sophisticated attacks.

In addition, an MDR service that filters and focuses its attention on the most severe security alerts while ignoring medium- and low-severity alerts limits its efficacy, because attacks often begin as a long trail of lower-severity security incidents that, when ignored, allow an adversary to gain a foothold and entrench themselves in your network. An MDR service that analyzes all security detections and alerts that were prevented — activity that might indicate the existence of a broader attack — ensures that intrusions are stopped at the earliest stage possible.

SURGICAL REMEDIATION

Alerts for true threats to the organization require a response. The analysis and investigation phases should provide the context necessary to determine the form of that response.

Response can take many forms, such as requiring that an endpoint be removed from the environment and contained, with the objective of reverting back to a known good state. For many organizations, this may require a reimaging of the endpoint. However, with good context, skilled analysts and effective tooling, remediation can return the system to a known good state without reimaging. This is a major benefit of an MDR provider, as the incident can be fully resolved without customer involvement, with less business impact and expense and more speed than entirely reimaging a system.

Remediation provides the final step in responding to an incident — recovery — by restoring systems to their pre-attack state, removing malware, cleaning registry entries, and removing intruders and any persistence mechanisms. This final stage is the most important one to accomplish correctly, for if not done well all of the investment in the other phases of an MDR program is essentially wasted. Attackers leverage countless tricks to maintain access once they establish a foothold in a network. Scheduled tasks, watcher services and redundant backdoors are just a few methods they use to make sure that their intrusion will be resilient against basic quarantine and containment countermeasures.

With a broad range of services falling under the MDR banner, it is critical to have a solid understanding of what capabilities an MDR service should deliver and how those meet your needs as a customer of MDR services.

WHAT METRICS SHOULD YOUR MDR AIM FOR?

CrowdStrike have defined a new cyber metric based on insights gained from helping thousands of organizations defend against threats — "breakout time," or the time it takes for an intruder to begin moving laterally outside of the initial beachhead to other systems in the network. The average breakout time observed for eCrime in 2022 was 1 hour and 38 minutes.[5] Yet this statistic does not tell the complete story: In 36% of those intrusions, the OverWatch team observed that the adversary was able to move laterally to additional hosts in less than 30 minutes.

THE KEY CAPABILITY DRIVING OUTCOMES FOR MDR CUSTOMERS — OWNING THE OUTCOME

"Your MDR should own remediation as part of the response. Stopping an intrusion before it becomes a breach is time-sensitive business. It may require isolating an affected system from the network, killing processes, removing persistence mechanisms from the file system or Windows registry, or carrying out any of a wide variety of actions."[2]

4 Crowdstrike Blog: Does Your MDR Deliver Outcomes — or Homework?
5 CrowdStrike 2023 Global Threat Report

Breakout time spotlights the short window during which an organization can best prevent an incident from turning into a breach. While it's certainly not the only metric by which to judge threat actors' sophistication, ranking breakout time is a valuable way for an organization to evaluate its operational capabilities. It is also useful for defenders who want to benchmark the speed of their average time-to-detect, time-to-investigate and time-to-remediate metrics. CrowdStrike has named this the "1-10-60 rule" and recommends that organizations strive to meet the following performance metrics:

- Detect an intrusion within an average of one minute
- Investigate and understand it in under 10 minutes
- Eject the adversary in under 60 minutes

Organizations operating under this framework are much more likely to eject the adversary before they break out of their initial entry point, thus minimizing the impact of their attack. Of course, organizations can adjust their target response times to meet their individual needs. This could be based in part on which adversary types they are most likely to confront, given the business sector and regional focus of their operations. However, in undertaking an MDR strategy, the 1-10-60 rule provides a framework that allows any organization to align its capabilities against a level of operational effectiveness that should give it confidence in its ability to stop a breach.

WHAT SHOULD YOU LOOK FOR WHEN CHOOSING AN MDR?

Here are some questions to consider when selecting an MDR service.

What is the expertise of the analysts who staff your MDR service?
One key reason to invest in MDR is to augment your own staff with experts, introducing improved skill and maturity without needing to recruit and hire expensive staff. CrowdStrike is uniquely positioned to hire and retain elite threat hunters and security analysts from a wide range of backgrounds, including government, the intelligence community, commercial enterprise and defense. CrowdStrike's team has been proven effective at finding and stopping the most sophisticated threats.

What is the average time for onboarding and tuning the MDR solution to your needs?
Achieving security maturity is not an easy feat. After spending time and effort choosing the right MDR solution for your organization, you want to immediately see value and ensure protection. The gap between decision and protection is often quite large and opens your organization to gaps in protection. Onboarding and operationalizing CrowdStrike Falcon Complete takes a median of only 10 days, shrinking the timeframe for protecting your organization and going from value promised to value realized.

IS MDR THE SAME AS MSSP?

Many organizations ask, "Do I need an MDR service if I have a managed security service provider (MSSP)?" MSSP offerings can vary widely but generally focus on broadly monitoring and managing security tools within an enterprise. This typically includes basic triage of security alerts, along with a variety of other services such as managing technology, upgrades, compliance and vulnerabilities.

MDR services, on the other hand, are much narrower in focus. MDR delivers fast, turnkey integration, typically with a specific technology stack. MDR services are also more mission-focused, aiming to help organizations advance their SOC in specific steps of the detect/response workflow. Because of this narrow focus, MDR can deliver immediate value at a low cost and within a very short time.

What type of automated, preventive technologies are built into your MDR solution?
For a comprehensive MDR solution that can scale appropriately for your organization today and tomorrow, your MDR should enlist the power of automation and preventive technology. Powered by the CrowdStrike Security Cloud and world-class artificial intelligence, the CrowdStrike Falcon platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. This enables the delivery of rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

Does your MDR come standard with managed, cloud-based identity threat protection?
Today, 80% of breaches involve compromised credentials. But despite how prevalent identity-driven attacks are now, they remain extremely hard to detect using traditional approaches. When a valid user's credentials have been compromised and an adversary is masquerading as that user, it's often very difficult to differentiate between the user's typical behavior and that of the hacker. Falcon Complete Identity Threat Protection (ITP) solves this. It's the first and only fully-managed identity protection service that delivers frictionless, real-time identity threat prevention around-the-clock with advanced IT policy enforcement for managed and unmanaged accounts, expert management, monitoring and remediation.

Does your MDR service benefit from integrated, native threat intelligence?
To detect and respond to emerging threats with the greatest efficacy, security analysts must have up-to-date intelligence on the most current TTPs being used by active threat actors. CrowdStrike's MDR services are armed with cyber threat intelligence from CrowdStrike's elite team of threat analysts. CrowdStrike Intelligence brings together security researchers, cultural experts and linguists to add detailed, always-current knowledge of tradecraft into the MDR process, collected from more than 200 adversaries. This intimate knowledge of the latest TTPs in use ensures that CrowdStrike can perform effective and efficient detection and response.

How will the MDR provider communicate with your team?
All MDR services have a stage in their detect/investigate/respond workflow when it's time to hand the reins back to you. Communicating this handoff is a potential point of friction and may introduce new consoles, portals or workflows that slow your team's response. A central hub that enables a seamless delivery of information between the MDR provider and the customer is critical. CrowdStrike's Message Center reduces friction in MDR collaboration and enables frictionless, transparent and secure communication between CrowdStrike managed services analysts and customers. Built within the Falcon platform, the Message Center enables CrowdStrike analysts to deliver real-time updates to customers about in-progress attacks and related activity, so customers are always properly informed about intrusion activity and any mitigation they must undertake. Communications are bidirectional, allowing CrowdStrike and customer analysts to freely communicate and collaborate within the Falcon platform.

What response actions will your MDR take on your behalf, and what actions are left for you to perform?
Response can often be a vague term that causes confusion in the marketplace about what MDR providers will actually do for you and what additional work is left for you to perform after they are done. Your MDR must be able to isolate, contain and eradicate an attacker

Threat remediation services should seamlessly restore systems to their pre-attack states, removing malware, cleaning registries, ejecting intruders, removing persistence mechanisms — avoiding timely reimaging processes altogether whenever possible.

from the environment; eradicating the attacker is usually the line where the responsibility shifts and can create a significant amount of work for the customer beyond isolation and containment. Falcon Complete handles the last stage for you and takes response a step further to perform isolation and containment and, when possible, remediation. This means removing malicious files, artifacts and processes from the environment, immediately returning your organization to a known good state. This delivers outcomes for the customer rather than additional work.

Is your MDR service 24/7?
Attackers don't take a holiday, and neither should your MDR service. Many organizations choose to engage an MDR service in part to achieve around-the-clock threat coverage, especially when their own team may only be staffed during business hours.

Can the MDR provider reduce your risk while also reducing cost?
Understanding the unique outcomes your MDR solution can provide will help you know if it is capable of reducing risk and helping you understand how incidents may impact your business' bottom line. CrowdStrike has one mission: to stop breaches. Falcon Complete manages the entire lifecycle of an incident, ensuring chain of custody on all security incidents to allow CrowdStrike's experts to hyper-focus on stopping breaches 24/7. Further, in 2021, an **economic impact done by Forrester and commissioned by CrowdStrike** showed that Falcon Complete delivers over 400% ROI and saves your organization over 2,500 hours in investigation time per year.

What assurances do you have that demonstrate your MDR will be able to protect your organization?
An MDR service that claims to protect you from cyberattacks is quite common. The question then becomes, "How can I trust you to do what you say?" An MDR that does not confidently demonstrate how it can prove these claims and show its ability to execute creates doubt. That is why CrowdStrike pioneered the **Breach Prevention Warranty**. CrowdStrike stands strongly behind its breach protection capabilities, which cover costs in the event a breach occurs, to demonstrate confidence that the Falcon Complete MDR service won't fail in its mission to stop breaches.

What third-party validation does your MDR service have?
Evaluating MDR solutions is an often cumbersome process that includes conflicting messages about which solution is the right one for you. Many companies claim they offer the same benefits and outcomes. As part of your process, you must ask, "What third-party validation does this MDR have, and how can I use this analysis to support my decision?" CrowdStrike is happy to have been named a leader in both the Forrester Wave for MDR and the IDC Marketscape for MDR, as well as achieving the highest detection coverage in the 2022 MITRE Engenuity ATT&CK® Evaluations for Security Service Providers. Look to these experts when evaluating an MDR solution.

How often does your MDR take part in managing, tuning and optimizing your MDR posture?
Continuous improvement and optimization is critical to defending against today's threats. With adversaries gaining in speed and sophistication every day, it is critical that your MDR service takes a significant and comprehensive role in the management and tuning of the platform, policies and processes for your organization so far as MDR is concerned. This ensures a consistent optimization of the service to deliver outcomes and ultimately stop breaches.

FALCON COMPLETE: A COMPREHENSIVE AND HIGHLY EFFECTIVE MDR SOLUTION

CrowdStrike Falcon® Complete for Managed Detection and Response (MDR) combines the power of the industry-leading, cloud-native Falcon security platform with the efficiency, expertise and 24/7 protection of CrowdStrike's global team of security experts who continuously monitor, triage and respond to every threat targeting customer organizations.

Capabilities	Falcon Complete MDR
24/7 Management, Tuning and Optimization	
Operated by experts	✓
Proactive platform management	✓
Assigned security advisor	✓
Prioritization of asset groups	✓
Cross-disciplinary expertise	✓
Detection and Prevention	
Continuous monitoring with real-time visibility	✓
Investigation of all detections (low/medium/high/critical)	✓
Specialized data, tools and processes	✓
Managed cloud workload protection	✓
Managed identity threat prevention	✓
Threat Hunting and Intelligence	
Native threat intelligence and integrated IOCs	✓
Quarterly threat hunting reports	
Full visibility into the process tree on any endpoint	✓
24/7 proactive human threat hunting	✓
24/7 proactive human threat hunting	
Isolation and containment all threats	✓
Proactive, hands-on surgical remediation	✓

YOUR MDR SHOULD DELIVER OUTCOMES — NOT MORE WORK

Outcomes should be delivered by the MDR provider, not the customer. Falcon Complete commits to owning the results.

A typical customer engages with an MDR service for one simple reason: They want to avoid a damaging breach. Since many MDRs are unable to commit to this outcome, they often break down the requirements into more granular commitments, such as how soon an analyst will respond to a critical alert. Service-level agreements (SLAs) like this are useful in tracking effectiveness over time, and short SLAs for response can reduce risk of a breach, but it's a long way from committing to the primary mission of stopping breaches.

From Day One, Falcon Complete has included its best-in-class Breach Prevention Warranty, designed to provide confidence to customers that CrowdStrike stands strongly behind the team and the results delivered.

There is a wide range of MDR services available today. When choosing one to augment your organization's security team, it's important to first have a good understanding of your team's capabilities to detect, investigate and respond to threats — and also its gaps. Then, you need to assess the MDR's ability to deliver comprehensive coverage across people, process and technology. This will help you determine if your MDR will send you follow-up actions (more work) or simply inform you that the threat has been eradicated and remediated (outcome) — and ultimately stop breaches that threaten your organization.

Schedule a Falcon Complete MDR Demo

Learn more at **www.crowdstrike.com**

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**