CROWDSTRIKE

eBook

Managed Security Readiness Guide

Four Ways Managed Detection and Response (MDR) Drives Security Success

Table of Contents

Is It Time to Move to MDR?

The Four S's for Security Success

SPEED

The faster security teams can identify a threat, the quicker remediation can take place — reducing risk and decreasing the dwell time of a threat actor.

Adversaries Increase Speed of Relentless Attacks

62 minutes
is the average eCrime breakout time observed in 2023.

2 minutes 7 seconds
is the fastest eCrime breakout time observed in 2023.

Source: CrowdStrike 2024 Global Threat Report

Threats Are Moving from Proof of Concept to Mass Exploitation Faster Than Ever

32% of all Log4j vulnerability scanning occurred in the first 30 days after release.

Source: Verizon 2023 Data Breach Investigations Report

SCALE

Defenders must be able to detect and respond to increasingly sophisticated threats at scale.

75%
increase in cloud intrusions

86%
of hands-on-keyboard attacks were executed by eCrime adversaries

Source: CrowdStrike 2024 Threat Hunting Report

SKILLS

When hiring and retaining in-house talent becomes untenable, security teams must adapt quickly.

The global shortage of cybersecurity professionals is estimated to be **3.4 million**.

Source: ISC2 2022 Cybersecurity Workforce Study

95% of security professionals believe the global cybersecurity skills gap has gotten worse or stayed the same over the past two years.

Source: ESG Complete Survey Results: The Life and Times of Cybersecurity Professionals Volume VI, 2023

SPEND

Cloud adoption, remote working, third-party infrastructure integration and the convergence of IT, operational technology (OT) and the Internet of Things (IoT) are expanding the attack surface, resulting in high costs for organizations.

Cybersecurity **salaries are increasing** as the **talent gap widens.**

Upleveling Security with a Blend of Human Expertise and Technology

The numbers tell a clear story: Adversaries are outpacing defenders as they continuously improve their tradecraft and accelerate the speed and scale of their attacks. Defenders are doing their best to keep up, but slow security that doesn't scale is no match. Breaking free of legacy security operations centers (SOCs) and slow, inefficient security operations doesn't happen overnight. And the realities of limited resources have created an immovable roadblock — until now.

MDR emerged as a market response to security teams needing to become more agile, respond to threats faster and do it all at an unprecedented scale alongside their existing security operations.

Delivered as an always-on managed service, MDR provides a powerful combination of leading security technology and elite, 24/7 expert analysts to address three critical challenges when every second counts:

1. **Drive down risks:** The end game is to be faster than the fastest adversary. MDR reduces mean time to detect (MTTD) and mean time to respond (MTTR) from hours and days down to mere minutes. This ensures organizations minimize their exposure to advanced threats by containing and surgically remediating threats in minutes.

2. **Improve operational efficiency:** Complexity is the enemy of security. Unlike other technologies that get added to complex security stacks, effective MDR brings single platform visibility and managed protection for immediate time-to-value. With no additional build or deployment time, you have an MDR team to start detecting and responding to threats within days.

3. **Augment your team and immediately rightsize security to your business:** MDR scales with the needs of your business. With proactive, hands-on response and remediation, you can easily augment your security team and bridge knowledge gaps. And because expertise is offered as a service, organizations can scale to at-the-moment incident response needs. This allows security team members to focus on higher-value tasks and more strategic projects rather than routine and repetitive work.

Investigation and response take hours to days. With MDR, you can offload full work cycles of your internal security team.

Using MDR to Solve Your "Four S" Pain Points for Robust Security

Establishing more robust security within your environment requires more resources, which are typically costly and complex to manage. That is enough to keep organizations from implementing a fundamental endpoint security program. In reality, what security teams need today to solve speed, scale, skills and spend challenges is a comprehensive endpoint security program and holistic detection and response capabilities for when adversaries strike.

MDR Helps Solve the Four S's Today and Over Time

Optimize

- **Easy deployment:** Remove barriers to upleveling security with simplified deployment and configuration.
- **Rigorous configuration management:** Systematically apply proven, best-practice policies to endpoints, cloud workloads and identities to eliminate security gaps.
- **Open communication:** Dashboards and messaging give security teams the peace of mind to remain as hands-on or hands-off as they wish.
- **Staff augmentation:** Get the benefit of seasoned security professionals with experience in incident handling, incident response, forensics, SOC analysis, identity protection and IT administration without needing an FTE budget.

Detect

- **Deep visibility:** Combine security event observations into a single view to remove silos and catch anomalies that other security approaches miss.
- **24/7 coverage:** Continuous, proactive threat hunting identifies and disrupts novel, hidden and sophisticated adversarial tradecraft, thwarting even the most advanced attacks and avoiding major security incidents altogether.

Respond

- **End-to-end surgical:** Experienced security analysts neutralize and remediate threats to minimize or prevent disruptions to business operations.
- **Decisive response:** Rapid response can scale quickly depending on the severity of the incident, instilling confidence that experts handled it completely and correctly.

Improve

- **Managed investigations:** Respond to threats more effectively without requiring input from security teams while removing overall day-to-day burdens of investigations.
- **Root cause analysis:** Get deep root cause analysis to inform improvements that will harden your organization's security posture and prevent a recurrence of the incident.

Breaking Down Managed Security

You may have pursued security outsourcing options in the past, but times have changed. It is now critically important to reevaluate how you can achieve better, higher-performing security and in what form.

When exploring your MDR options, you may come across managed security service providers (MSSPs) that sound similar or exactly the same. Or you may even wonder if MDR is an MSSP offering with a new name. The short answer: It's not.

The capabilities and benefits of MDR services can vary by vendor and may often overlap with MSSPs. Because the terms "MDR" and "MSSP" are often used imprecisely and interchangeably in the security world, there can be confusion when deciding the right path for your organization. Additionally, many MSSPs employ MDR services for their clients to improve speed, spend and skills — along with the scale they already offer.

Now that we've discussed the value of MDR, let's take a closer look at the key difference between MDR and MSSP services.

Choose the Right Managed Service

MDR: With full response and remediation support, round-the-cloud monitoring and 24/7 operations by proactive threat hunters and security analysts with deep expertise, MDR services solve the need to increase speed, scale and skills for today's organizations. MDR offers additional business value and cost savings by accelerating time to respond, improving operational efficiencies and reducing risk.

MSSP: MSSPs offer a wide array of security, compliance and risk management services but can lack the deep specialization and dedicated focus that an MDR service brings to bear. To compensate, MSSPs often add MDR to improve the speed and skill that today's threat landscape requires.

Is a Legacy SOC Holding Your Team Back?

Legacy SOCs rely on cumbersome operating models with layers of inefficient analyst tiers and error-prone handoffs — increasing exposure time and chances for compromise. Move to a next-gen MDR service to experience outcomes, not more work.

Going Beyond the Endpoint with Unified Threat Data

In an increasingly complex security landscape, organizations need more than isolated tools — they need unified, actionable threat intelligence. A powerful platform that centralizes threat data from endpoints, cloud workloads, network traffic and more is essential for staying ahead of adversaries.

A unified platform with next-gen SIEM technology ingests and normalizes data at scale, applies advanced AI and machine learning to detect stealthy threats, and enables security analysts to prioritize and respond with precision. By breaking down data silos and providing a single console for threat management, organizations can reduce complexity, improve efficiency and enhance their security posture.

The Three Phases of Unified Threat Detection and Response

1. **Ingest:** Ingest and normalize volumes of data from endpoints, cloud workloads, identity, email, network traffic, virtual containers and more.
2. **Detect:** Parse and correlate data to automatically detect stealthy threats with advanced artificial intelligence (AI) and machine learning (ML).
3. **Respond:** Quickly analyze and triage new events, and automate investigation and response activities.

Eliminate Advanced Threats with Visibility Across Your Security Stack

- Email security
- Identity and access management
- Cloud infrastructure security
- Network detection and response (NDR)
- Next-generation firewalls
- Security service edge (SSE)
- And more

Most attacks that occur hit an endpoint, but there is a need to pull in additional telemetry to enhance endpoint detections and surface net-new attacks that might get caught between silos.

Benefits of Consolidated Security

- *Unified threat visibility*
- *Hassle-free detections and investigation*
- *Rapid detection and response*

When MDR Makes Sense

With rising threats and a global shortage of skilled security professionals, teams are under immense pressure. Organizations need solutions that not only offer powerful technology but also integrate with the right processes and strategies to ensure 24/7 effectiveness.

By operationalizing a unified security platform and augmenting internal teams with 24/7 expertise, businesses can immediately enhance their threat detection and response capabilities — regardless of their current security maturity.

This is where MDR factors in: Supercharging an elite 24/7 MDR service with full-stack visibility and powerful, multi-tool response automation enables any and every organization to stay ahead of sophisticated threats. By extending the expertise of MDR services across the entire attack surface, organizations can harness the power of unified threat data without the need for extensive in-house resources.

91% of security pros believe their job is more difficult or the same as it was two years ago.

Source: ESG Complete Survey Results: The Life and Times of Cybersecurity Professionals Volume VI, 2023

Bonus Quiz: Are You Ready for MDR?

Take a quick, 10-question readiness quiz to find out.	Yes	No
SPEED		
1. Have you deployed cloud-native endpoint protection software with real-time visibility and hyper-accurate detections?		
2. Are you tracking your team's MTTR? Is it under 45 minutes?		
3. Are you continuously improving your response playbooks and automation to ensure fast, surgical threat remediation?		
SCALE		
4. Are you monitoring and triaging every new alert 24 hours a day, seven days a week?		
5. Are you equipped to handle attack surges with volatile spikes in adversarial activity whenever they may occur? (e.g., on weekends, holidays, etc.)		
6. Can you detect and investigate multi-domain threat activity occurring across your security stack (e.g., email, identity, network, cloud, etc.) from one unified platform?		
SKILLS		
7. Is your SOC team well-versed in triaging and remediating novel and evolving adversarial tactics and techniques across your environment?		
8. In addition to your detection and response security analysts, do you have specialized threat hunters on staff to exclusively search for advanced, unknown threat activity?		
SPEND		
9. Are you able to build an in-house SOC capable of detecting threats around the clock?		
10. Do you have a breach prevention warranty that improves your risk posture and reduces your cyber insurance premiums?		

Scoring: If you answered "NO" to two or more of the questions above, you're ready to make the move to MDR.

CrowdStrike Does the Work. You Experience the Outcomes.

CrowdStrike Falcon® Complete Next-Gen MDR delivers 24/7 expert management, monitoring and response for the CrowdStrike Falcon® platform and is backed by CrowdStrike's industry-leading Breach Prevention Warranty.* Designed to act as a force multiplier for internal defenses, CrowdStrike's expert-led team monitors your environment, acting as a force multiplier for internal teams to deliver detection and response capabilities able to outpace the speed and sophistication of today's adversaries.

The Advantages of Falcon Complete Next-Gen MDR

4 min. mean time to detect (MTTD)

Source: MITRE Engenuity ATT&CK® Evaluations: Managed Services, Round 2

Immediate Time-to-Value
CrowdStrike Falcon Complete Next-Gen MDR is a service designed to deliver value fast — while enabling organizations to drive down cost and complexity.

Up to **75% reduction in mean-time-to-respond (MTTR)**

Source: CrowdStrike Business Value Assessments (BVAs) conducted in partnership with individual Falcon Complete customers

Active, Hands-on Remediation
CrowdStrike offers the industry's only surgical remediation capable of completing the entire response process, including full cleanup and restoration without costly reimaging or downtime.

+13 million detections resolved annually

Source: Falcon Complete Operations data

Tailored to Your Environment
CrowdStrike delivers continuous platform management, agent maintenance, and rigorous control configurations and optimizations to ensure optimal protection.

> ***"Since shifting to Falcon Complete Next-Gen MDR, alerts have dropped by 20x. It's head-over-heels more mature and effective than what we had in the past."***
>
> DJ Goldworthy, VP of Security Operations at Aflac

* The Breach Prevention Warranty is not available to all customers, in all regions. See FAQ for exclusions.
https://www.crowdstrike.com/products/managed-services/falcon-complete/warranty-faq/

Supercharge Your SOC with CrowdStrike Falcon Complete Next-Gen MDR

Join thousands of customer organizations worldwide that rely daily on the 24/7 elite expertise and comprehensive protection of Falcon Complete Next-Gen MDR.

Whether you need full team MDR protection or simply want to augment a portion of your SOC, CrowdStrike will meet you on your journey with full-cycle, industry-leading managed protection.

Elite 24/7 Expertise

Optimized teams and workflows tailored to the industry-leading CrowdStrike Falcon platform will hunt, disrupt and eradicate advanced threats at speed and scale.

Frictionless Protection

End-to-end detection, investigation and surgical remediation alleviates the burden on in-house security teams and outsourced SOCs and delivers tangible outcomes, not more alerts.

Relentless Adversary Focus

24/7 protection across endpoints, identities and cloud workloads disrupts the most sophisticated adversaries — CrowdStrike Falcon® Adversary OverWatch™ uses advanced AI and unrivaled human expertise to deliver industry-leading threat hunting.

Next-Gen MDR

Unified threat data from CrowdStrike Falcon® Next-Gen SIEM, expanded visibility and cutting-edge generative AI from the Falcon platform enables Falcon Complete Next-Gen MDR to accelerate defense along every point of attack.

Falcon Complete Next-Gen MDR operates as an extension of a customer's security teams — solving your most difficult operational and risk challenges. If you're ready for outcomes without the work, it's time to consider MDR.

For more information, including a demonstration of Falcon Complete Next-Gen MDR, visit https://www.crowdstrike.com/services/falcon-complete-next-gen-mdr/.

About CrowdStrike

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

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

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

CrowdStrike: **We stop breaches.**

Learn more: https://www.crowdstrike.com/

Follow us: Blog | X | LinkedIn | Facebook | Instagram