CROWDSTRIKE

Redefining MDR with Cross-Domain Visibility

Outpace adversaries with managed detection and response built to defeat cross-domain threats

In this eBook

Managed detection and response (MDR) is entering a new era. As adversaries evolve, so must the security operations built to stop them. Attacks are no longer operating in a single domain, and organizations need to detect and respond across the entire attack surface. What once worked now falls short in the face of fast-moving, multi-vector threats.

This eBook explores how unified data, real-time correlation, and expert-led operations are enhancing and upleveling what MDR can deliver:

- How cross-domain attacks expose the limits of traditional MDR
- How unified data on a single platform drives earlier, higher-fidelity detection
- Where expert analysis adds speed, clarity, and confidence to response
- The role of next-gen SIEM technology in powering this new model
- What sets CrowdStrike apart in delivering outcomes, not just alerts

Table of Contents

The Modern Threat Landscape

Today's threat landscape is defined by speed, scale, and attack sophistication. Adversaries are executing targeted campaigns and move stealthily across domains. According to the CrowdStrike 2026 Global Threat Report, the average eCrime breakout time — the period between initial compromise and lateral movement — dropped to just 29 minutes in 2025. This compressed timeline often gives security teams only minutes to detect, investigate, and respond before attackers can take critical steps toward compromise.

Cross-domain attacks add more complexity. Adversaries pivot between cloud, identity, endpoint, email, and network layers, exploiting blind spots between siloed tools and disconnected teams. Increasingly, intrusions involve hands-on-keyboard techniques that mimic legitimate user behavior.

In 2025, **82% of detections were malware-free**, a clear sign that adversaries are relying on valid credentials and native tools to stay hidden.[1]

Fragmented defenses are no match for today's faster, stealthier attacks.

Real-world cases show how quickly attacks can escalate. In August 2025, CrowdStrike responded to pre-ransomware activity at a North American organization. The adversary gained access via a compromised VPN appliance service account that led to lateral movement to a host without CrowdStrike Falcon® Insight XDR as a staging point to attempt deployment of Sinobi ransomware. Defenses that focus on the endpoint often miss this kind of activity, especially when adversaries operate in identity, cloud, and network layers where visibility is traditionally limited.

Fragmented defenses can't keep pace with multi-vector threats, and monitoring one domain at a time is no longer enough. Today's threat landscape demands a new kind of MDR — one that's unified, expert-led, and built to outpace even the most sophisticated adversaries.

[1] CrowdStrike 2026 Global Threat Report

The Limits of Traditional MDR

Traditional MDR was created to reduce the burden on SOC teams by handling alert triage and response. But most services haven't evolved beyond basic detection, and instead of delivering action, they operate as alert-forwarding services, pushing large volumes of raw alerts without correlation, context, or resolution.

Data ingestion adds to the problem. Many providers integrate with legacy security information and event management (SIEM) tools that collect high volumes of telemetry without alignment to detection goals. Data is ingested broadly, not strategically, which drives up cost, delays outcomes, and floods analysts with undifferentiated signals.

At the heart of traditional MDR operations is a flawed assumption that more rules means better protection. But without intelligent filtering, more rules simply create more noise. Traditional MDR providers rely on static, out-of-the-box correlation rules that are rarely tuned to reflect an organization's environment or the behavior of modern adversaries. These rules generate low-fidelity alerts, often triggered by weak indicators, offering little context or confidence.

Without a focused detection strategy, MDR delivers visibility without action, and analysts are left to chase alerts instead of stopping threats.

Unified Data Is the MDR Detection Advantage

Full Attack Surface Visibility

Stopping breaches requires more than round-the-clock monitoring. It requires real-time correlation, intelligent prioritization, and the ability to respond across every layer of the enterprise. This is possible with a unified, platform-native MDR approach that consolidates telemetry from endpoints, identities, cloud workloads, network activity, and email into a single console. Unified data enables faster detection, deeper investigation, and more decisive response.

This level of integration is critical as modern threats navigate beyond endpoints. Next-gen SIEM technology plays a key role by ingesting prioritized third-party data across identity providers, cloud platforms, email security tools, and network infrastructure. This gives MDR teams complete visibility across the attack surface.

AI-powered Technology

AI-native next-gen SIEM technology enhances security operations by analyzing vast volumes of telemetry in real time and automatically correlating events across multiple data sources to surface genuine threats. Advanced machine learning models learn from historical attack patterns to distinguish between benign anomalies and legitimate adversary behavior, while intelligent automation helps prioritize high-risk activities that require immediate attention. This AI-driven approach significantly improves detection accuracy by reducing false positives and accelerating investigation workflows, enabling analysts to focus their expertise on validating and responding to the most critical threats.

Adaptive Defense

The combination of native and third-party telemetry enables true detection in depth. High-fidelity signals from the unified platform reveal early indicators such as initial compromise, privilege escalation, and behavioral anomalies. Third-party telemetry adds external context to track attacker movement across domains and throughout the kill chain. MDR providers that leverage unified data from a single platform do more than scale operations — they deliver adaptive defense. Each detection, analyst action, and response feeds back into the platform, continuously improving detection fidelity and reducing time to detect and respond.

This is the future of MDR: a unified platform that brings together native visibility, third-party integration, AI-driven insight, and the expert-led response required to stop breaches with speed and precision. It delivers more than alerts by turning detection into decisive action, giving defenders the upper hand before adversaries can execute actions on objectives.

CrowdStrike Falcon Complete Next-Gen MDR: Built for What's Next

CrowdStrike Falcon® Complete Next-Gen MDR combines elite security expertise with AI-powered automation to detect, disrupt, and defeat threats with unmatched speed and precision.

Delivered on a Unified Platform

Traditional MDR providers often operate at a distance from the technology they rely on. They detect threats on platforms they don't control, creating a gap between alerts and action when seconds matter. Falcon Complete Next-Gen MDR takes a different approach. Built on the AI-native CrowdStrike Falcon® platform and backed by full ownership of the detection pipeline and remediation process, Falcon Complete Next-Gen MDR doesn't just triage alerts, it delivers outcomes. This deep integration enables earlier, more comprehensive response and better security across the entire attack lifecycle.

With unified telemetry across domains, the Falcon Complete team accelerates detection and streamlines investigations. The service is fully operationalized through the Falcon platform and CrowdStrike Falcon® Next-Gen SIEM, which serves as the engine behind real-time threat correlation and cross-domain visibility.

Falcon Next-Gen SIEM is optimized for speed and scale. It ingests and correlates data quickly, avoiding the bottlenecks common in legacy SIEMs. Natively integrated with threat intelligence, endpoint, identity, and cloud data from the Falcon platform and enhanced with security orchestration, automation, and response (SOAR) capabilities, Falcon Next-Gen SIEM enables Falcon Complete analysts to respond to threats earlier in the kill chain.

Smarter, Faster Defense Powered by AI

Falcon Complete analysts harness purpose-built generative and agentic AI from CrowdStrike® Charlotte AI™ alongside proprietary tooling to revolutionize their investigative workflows. Through intelligent incident tagging, triage automation, and orchestrated playbook execution, these experts rapidly analyze and contextualize threats across diverse data sources. This native integration of AI technologies accelerates routine tasks and enriches investigations, enabling analysts to make faster, more informed decisions with real-time containment capabilities. By combining expert judgment with AI-powered automation, Falcon Complete analysts detect, disrupt, and defeat threats at machine speed.

Prioritized Telemetry

Falcon Complete Next-Gen MDR takes a strategic approach to data onboarding by focusing on what matters most. Starting with the endpoint, analysts get high-fidelity visibility into host activity and early-stage attacker behavior. They then extend that coverage with CrowdStrike Falcon® Identity Threat Protection to expose credential misuse and lateral movement, and CrowdStrike Falcon® Cloud Security to detect threats in cloud environments.

Falcon Next-Gen SIEM brings this data together, correlating signals in real time and layering in prioritized third-party telemetry. This includes network perimeter traffic, identity security data, cloud user workspace activity, infrastructure telemetry, and email security data, all critical for uncovering cross-domain attacks.

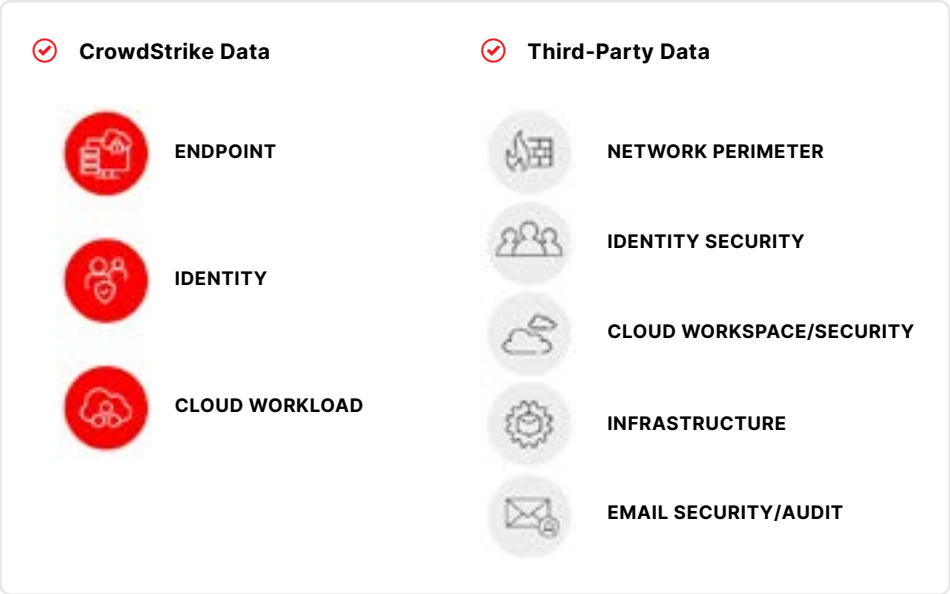

Figure 1. Falcon Complete Next-Gen MDR delivers visibility across key CrowdStrike and third-party data sources (shown here as examples, not a full list)

Detection That Powers Effective Threat Response

The Falcon Complete detection engineering team plays a critical role in delivering high-fidelity, scalable detections. Their strategy centers on developing and continuously refining detection logic that aligns closely with real-world adversary behavior. By leveraging threat intelligence, analyzing attack patterns, and using the capabilities of Falcon Next-Gen SIEM, the team creates detection rules designed to identify both known and emerging threats.

Detection development is tightly integrated with front-line operations at CrowdStrike. Engineers collaborate directly with analysts, threat hunters, and incident responders to incorporate insights from active investigations, ensuring each detection is actionable and relevant. This real-time feedback loop improves coverage and reduces false positives.

The team also works closely with product and engineering to inform platform enhancements that support detection accuracy, data coverage, and workflow efficiency. Ongoing performance evaluation and research into evolving attack techniques help ensure Falcon Complete Next-Gen MDR stays ahead of adversary tradecraft and continues to deliver effective, expert-led protection.

Expert-Driven Protection, 24/7

Falcon Complete Next-Gen MDR delivers expert-led protection around the clock, provided by a global team of expert analysts trained to stop breaches and combat today's toughest threats. The service operates on a follow-the-sun model, staffed by regionally distributed "fire teams" that provide continuous threat detection, investigation, and response.

Each fire team functions as a cohesive unit, owning the full response lifecycle, from detection to remediation. This model not only enables real-time decision-making but also eliminates gaps and delays that often occur in traditional SOCs. All analysts hold advanced certifications — including CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) — and bring deep expertise in adversary tradecraft, incident handling, and security operations. By combining deep technical expertise with operational precision, Falcon Complete fire teams handle every threat with urgency and expertise 24/7.

Purpose-built detections, real-time feedback from the front lines, and full platform integration mean Falcon Complete Next-Gen MDR doesn't just identify threats — it stops them.

While technology surfaces threats at speed, it's the Falcon Complete team that determines scope, severity, and the right course of action. By continuously adapting to evolving tactics and operating directly on the AI-native Falcon platform, they deliver rapid investigation, full-cycle remediation, and operational insight that reduces risk and drives better outcomes.

Elite Threat Hunting That Stops Breaches

Threat hunting is a core function of Falcon Complete Next-Gen MDR, and the service leverages CrowdStrike Falcon® Adversary OverWatch™ — CrowdStrike's 24/7 managed threat hunting team — to proactively hunt across trillions of security events each week. Armed with deep adversary intelligence and real-time telemetry from CrowdStrike's first-party endpoint, identity, and cloud data, combined with third-party data from Falcon Next-Gen SIEM, Falcon Adversary OverWatch's AI-powered threat hunting experts rapidly uncover emerging tradecraft and disrupt adversaries before they can achieve their objectives.

Full-Cycle Remediation

Falcon Complete Next-Gen MDR delivers more than detection and alerting — it delivers full-cycle remediation. When threats emerge, CrowdStrike experts take direct, hands-on action to disrupt malicious activity, all without waiting on customer intervention.

Using CrowdStrike Falcon® Real Time Response (RTR) capabilities, the team can isolate systems, remove persistence mechanisms, and delete malicious files across endpoints and cloud workloads. Falcon Identity Threat Protection extends countermeasures to Active Directory, allowing for immediate account blocking or identity verification. CrowdStrike Falcon® Fusion SOAR automates further response, integrating with third-party tools to block senders, add users to restricted user groups, force password resets, and more.

Even in the face of sophisticated attacks, the Falcon Complete team is able to take action to remediate quickly, without operational disruption.

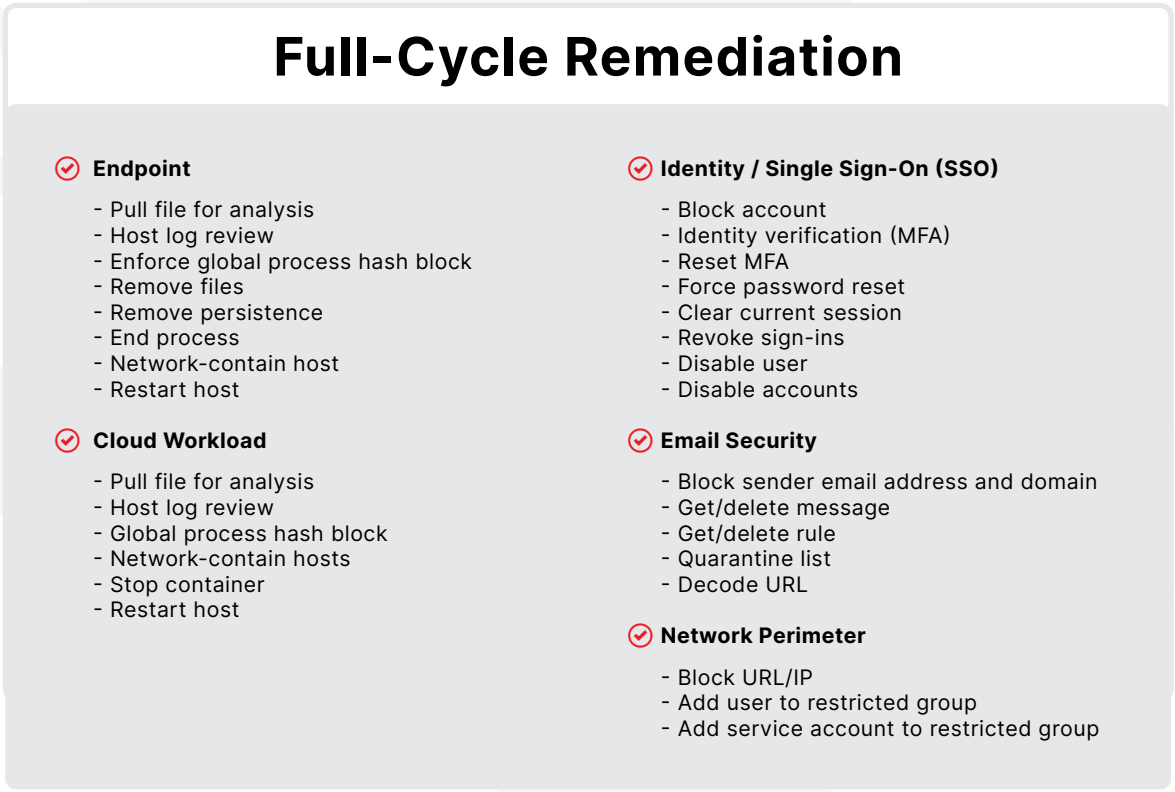

Figure 2. Full-cycle remediation delivered by the Falcon Complete team

Next Steps

Falcon Complete Next-Gen MDR transforms traditional security operations by combining cross-domain visibility, precision detection, and expert-led response into a unified service. Operating on the AI-native Falcon platform, CrowdStrike's global analyst team leverages advanced SIEM capabilities and proactive threat hunting to identify and neutralize threats before they impact your business.

Beyond traditional approaches to MDR, the Falcon Complete Next-Gen MDR service delivers operational excellence through measurable security outcomes. By combining human expertise with advanced technology, the Falcon Complete team helps organizations stay ahead of evolving threats while reducing security complexity and risk.

With Falcon Complete Next-Gen MDR, customers are already prepared and protected against what's next.

Ready to Outpace Adversaries?

Discover how Falcon Complete Next-Gen MDR delivers unmatched visibility, speed, and outcomes.

Schedule a Demo **Get the Data Sheet**

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

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/