

Falcon OverWatch for Defender

Add 24/7 managed threat hunting to Microsoft Defender to uncover post-exploit activity and hands-on-keyboard intrusions

Challenges

Modern attacks are designed to evade automated detection. Adversaries increasingly use stolen identities, legitimate tools, and AI-assisted tradecraft to blend in and move fast. In 2025, 82% of detections were malware-free, and breakout times dropped to as low as 27 seconds.¹ Automated alerts alone can't catch sophisticated intrusions before they spread.

Microsoft Defender² plays an important role in endpoint protection, but organizations need continuous, expert-led hunting to identify real adversary behavior and novel tradecraft that isn't fully detectable by security tools to stop attacks earlier.

Solution

CrowdStrike Falcon® OverWatch for Defender brings industry-leading managed threat hunting to Microsoft endpoint customers. It adds continuous expert monitoring to uncover sophisticated threats that evade automated detection, while Microsoft Defender continues to be operated as the primary endpoint security tool. A lightweight CrowdStrike Falcon® sensor runs alongside Microsoft Defender to collect the rich telemetry necessary for detecting novel and evasive threats while not disrupting current protections or operations.

Key benefits

- Get peace of mind with 24/7 expert threat hunting
- Detect hands-on-keyboard post-exploit activity that automated tools can miss
- Improve security outcomes without replacing existing Microsoft Defender protections

¹ CrowdStrike 2026 Global Threat Report

² Microsoft and Defender are registered trademarks of Microsoft Corporation. CrowdStrike Falcon OverWatch for Defender is not affiliated with or endorsed by Microsoft.

Powered by the AI-native CrowdStrike Falcon® platform and CrowdStrike's patented threat hunting engine and threat intelligence, Falcon OverWatch for Defender augments Microsoft Defender deployments in two distinct ways:

1. It proactively detects hands-on-keyboard activity, credential abuse, misuse of legitimate tools, in-memory attacks, and other evasive interactive intrusion techniques. Elite hunters investigate and escalate real threats, helping security teams respond before an intrusion becomes a breach.
2. It dynamically adapts detection posture with new threat discovery across the entirety of the CrowdStrike ecosystem. As new techniques are identified from incident response and hunting operations across over 40,000 customers, Falcon OverWatch hunting patterns are developed and deployed to improve detection of future intrusions and retroactively identify indications of prior adversary activity.

Falcon OverWatch: Proven at scale

- Operationalizes the latest threat intelligence to improve detection
- Analyzes 14 million detection leads annually
- Adds 1,800+ new detection patterns developed annually
- Detects 100 high- to critical-severity intrusions every day

Key advantages

24/7 expert hunting, always on

Falcon OverWatch for Defender gives Microsoft customers around-the-clock access to elite threat hunters focused on identifying sophisticated attacks that may never generate an automated alert.

- **Continuous hunting:** CrowdStrike threat hunters work 24/7 to identify stealthy adversary behavior that blends into normal operations.
- **Dynamic posture improvement based on new intelligence:** Falcon OverWatch threat hunters develop new hunting patterns and retroactively hunt based on real-time intelligence from incident response, hunting operations, and knowledge of adversary tactics, techniques, and procedures (TTPs).
- **High-confidence outcomes:** Analysts validate suspicious activity before escalation, helping teams act faster with greater confidence.

Finds what automated detection can miss

Falcon OverWatch for Defender is built to uncover the types of threats that security tools can overlook.

- **Disrupt adversaries earlier in the attack lifecycle:** Threat hunting focuses on adversary behavior, not just triggered alerts.
- **Reveal stealthy post-exploit activity:** CrowdStrike identifies subtle attack patterns that may otherwise remain hidden.
- **Strengthen your Microsoft Defender security outcome:** Falcon OverWatch for Defender adds an expert hunting layer that helps close visibility and detection gaps.

Human expertise, powered by AI

Falcon OverWatch for Defender combines human judgment with AI-driven analytics to hunt at speed and scale.

- **AI-powered hunting at scale:** Falcon OverWatch uses a patented AI-enabled hunting engine, proprietary detection patterns, and deep adversary expertise to analyze up to 6.2 trillion events per day.
- **Adversary-informed precision:** CrowdStrike tracks more than 280 sophisticated nation-state, eCrime, and hacktivist adversaries, helping hunters recognize real-world tradecraft faster.
- **Less noise, better signal:** Expert validation helps defenders focus on the threats that matter most and require immediate response action.

Stronger protection through the power of the crowd

CrowdStrike hunts across a broad global customer base, giving Falcon OverWatch visibility and insight that no single environment can match.

- **Shared intelligence at speed:** When Falcon OverWatch uncovers a new technique in one environment, that knowledge is operationalized across all others.
- **Global scale reveals what others miss:** With visibility across a broad range of customer environments in a single view, Falcon OverWatch can identify activity that is truly uncommon at scale. This perspective helps CrowdStrike uncover emerging threat patterns, identify new adversary tradecraft earlier, and strengthen hunting across customer environments.
- **Stronger outcomes over time:** Each investigation improves future hunting, detection, and response.

[Contact us](#)

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/>

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

