CROWDSTRIKE
Investor Relations

# CrowdStrike Falcon OverWatch for Defender Extends Managed Threat Hunting to Microsoft Endpoint Customers

May 5, 2026

*CrowdStrike's expert-led threat hunting augments Microsoft Defender by identifying and stopping threats that would otherwise go undetected*

AUSTIN, Texas--(BUSINESS WIRE)--May 5, 2026-- CrowdStrike (NASDAQ: CRWD) today announced Falcon OverWatch for Defender, extending industry-leading managed threat hunting to Microsoft endpoint customers. Falcon OverWatch for Defender strengthens security outcomes for Microsoft Defender with enhanced visibility, real-time detection and response, and continuous expert monitoring to identify and stop sophisticated threats that would otherwise go undetected, extending the value of existing endpoint deployments.

For organizations standardized on Microsoft Defender, automated detections alone leave gaps that today's AI-accelerated adversaries are built to exploit. Falcon OverWatch for Defender closes those gaps with continuous, expert-led hunting that identifies and stops threats before they escalate. The announcement builds on CrowdStrike's continued support for Microsoft environments, following the launch of Falcon Next-Gen SIEM for Defender.

“Today's attacks are stealthy, fast-moving, and designed to evade detection, making expert-led threat hunting essential," said Adam Meyers, head of counter adversary operations at CrowdStrike. "OverWatch for Defender extends proven threat hunting to Microsoft environments, delivering the security outcome customers need most: stopping the breach.”

**Proactively Hunting Stealthy Adversaries**

According to the CrowdStrike 2026 Global Threat Report, 82% of detections in 2025 were malware-free. Adversaries are increasingly using AI, trusted identities, and legitimate tools to accelerate attacks, blend into normal activity, and evade detection. At the same time, frontier AI models are surfacing a surge of new vulnerabilities adversaries can exploit. With breakout times as fast as 27 seconds, alert-driven approaches alone cannot keep pace. Identifying and stopping stealthy threats requires continuous, intelligence-driven threat hunting. Powered by the AI-native Falcon® platform and deep adversary expertise, Falcon Adversary OverWatch's elite threat hunters rapidly uncover and disrupt evasive threats.

**Falcon OverWatch for Defender**

Falcon OverWatch for Defender uncovers subtle patterns of attack, escalates high-confidence threats, and guides response to disrupt sophisticated threats that might otherwise go undetected, without impacting existing protections.

Key features and benefits include:

- **Adversary Intelligence-Driven Hunting:** CrowdStrike tracks over 280 of the world’s most sophisticated nation-state, eCrime, and hacktivist groups. The industry’s top threat hunters leverage this intelligence to identify real threat actor behavior, deliver high-confidence detections, and stop sophisticated attacks.
- **AI-Powered Threat Hunting at Machine Speed and Scale:** The OverWatch team leverages patented AI, proprietary detection patterns, and deep adversary expertise to analyze up to 6.2 trillion events per day, uncovering stealthy and novel threats.
- **Power of the Crowd:** With visibility across CrowdStrike's vast global customer base, OverWatch rapidly applies new techniques identified in one environment across others, enabling earlier detection and response. No single-customer deployment can replicate this advantage.

Customer results show Falcon OverWatch can reduce alert volume up to 500x, with 98% true positives, and up to 95% reduction in threat hunting staffing costs. OverWatch for Defender brings these proven outcomes to Microsoft Defender customers.

To learn more about Falcon OverWatch for Defender, read our blog.

*Microsoft and Defender are registered trademarks of Microsoft Corporation. CrowdStrike is not affiliated with, endorsed, or sponsored by Microsoft.

**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 | Instagram
Start a free trial today: https://www.crowdstrike.com/trial



View source version on businesswire.com: https://www.businesswire.com/news/home/20260505531987/en/

**Media Contact**
Jake Schuster
CrowdStrike Corporate Communications
press@crowdstrike.com

Source: CrowdStrike