CROWDSTRIKE

CrowdStrike Products
Solution Brief

Falcon for Defender

Detect and respond to attacks that bypass Microsoft Defender with the unrivaled leader in detection and response

Challenges

As the velocity and sophistication of cyberattacks continue to increase, security teams need to work faster and more efficiently to outpace the adversary and stop breaches. For organizations relying on Microsoft Defender, managing complex policies, signature updates and multiple consoles places significant operational burden on security teams.

This complexity leads to protection gaps that can create an opportunity for adversaries. The larger or more diverse the environment that organizations have to secure, the more difficult it can be to stay ahead of attackers. This onerous complexity can often lead to visibility and protection gaps that modern fileless malware and ransomware can exploit. In the event that one of these sophisticated threats evades Microsoft Defender, the consequences for the organization could be substantial.

Solution

As a global cybersecurity leader, CrowdStrike brings over a decade of expertise building the world's most advanced cloud-native platform and the industry's most dominant endpoint detection and response (EDR). CrowdStrike combines the world's best threat intelligence with innovative detection and response technology to better understand and stay ahead of adversaries.

CrowdStrike Falcon® for Defender makes market-leading detection and response technology available to organizations to run alongside Microsoft Defender, delivering the protection needed to defend against tradecraft from today's relentless adversaries.* This provides customers with extra protection and additional peace of mind from the trusted industry leader amid a rapidly evolving threat landscape. Customers can also opt to include managed threat hunting and leverage CrowdStrike's 24/7 team of cybersecurity experts to proactively monitor their environment around the clock.

Key benefits

» Seamlessly deploy Falcon for Defender across the enterprise alongside Microsoft Defender

» Reduce risk with CrowdStrike's market-leading detection and response capabilities

» Upgrade to 24/7 expert threat hunting for added peace of mind

*Microsoft and Defender are registered trademarks of Microsoft Corporation. CrowdStrike Falcon for Defender is not affiliated with or endorsed by Microsoft. Falcon for Defender may not be combined with any other CrowdStrike Offerings and this offer is only valid as long as the customer remains an active Microsoft Defender user.

Key advantages

Demand more from your cybersecurity with CrowdStrike Falcon for Defender. See what Microsoft misses and stop the breach with the world's leading detection and response platform. Falcon for Defender is designed to deploy seamlessly alongside Microsoft Defender for additional peace of mind at a lower total cost of ownership.

Deploy instantly, secure confidently

Microsoft products can be top adversary targets. Falcon for Defender deploys quickly and silently alongside Microsoft Defender, giving you independent protection delivered by the leader in stopping breaches.

- **Quick and seamless deployment:** The lightweight Falcon agent deploys in minutes for instant protection, with no reboots needed and zero interoperability issues when running alongside Microsoft Defender.
- **Independent, market-leading protection:** Don't settle for cybersecurity tied to the operating system that changes with each edition and version. Trust the unrivaled leader in EDR to spot the threats that bypass Microsoft Defender.
- **Low total cost of ownership:** Falcon for Defender delivers unmatched cybersecurity peace of mind at a lower total cost of ownership to ensure that cost does not create compromise.

Find missed attacks with trusted detections

See threats that Microsoft Defender misses with CrowdStrike's proven, AI-driven detections powered by the world's best threat intelligence.

- **Superior threat detection:** Stop the adversary with AI-powered detection enriched with the world's best threat intelligence and expert insight. CrowdStrike's unique adversary-driven approach uncovers the most elusive threats with tactical precision, setting the industry standard for the most trusted detections with the fewest false positives.
- **Streamlined data ingest:** Falcon for Defender deploys quickly and seamlessly ingests endpoint alert data directly from Microsoft Defender via a prebuilt connector. Instantly gain unwavering endpoint visibility across your entire enterprise without leaving the Falcon console.**
- **Unified alert experience:** Review endpoint alerts from both CrowdStrike and Microsoft Defender together within the Falcon console to reduce triage time and quickly uncover evasive threats.

Get peace of mind with 24/7 expert hunting

CrowdStrike's expertise is your expertise. Harness the power of elite threat hunters working 24/7 to proactively detect threats that Microsoft technology missed.

- **Upgrade to 24/7 hunting:** CrowdStrike's 24/7 team of world-class threat hunters relentlessly pursues adversaries targeting your endpoints. Fortify your defenses against advanced attacks with around-the-clock, real-time protection.
- **AI-powered expertise:** CrowdStrike's team of cyber experts is armed with cutting-edge technology — including the latest AI-driven cybersecurity — to stop even the most sophisticated adversaries on your behalf.
- **Peace of mind, maximum productivity:** CrowdStrike's 24/7 expertise frees up your security team to spend less time hunting the same threats over and over again and spend more time on what matters most to your security operations.

**This section includes forward-looking statements including, but not limited to, statements concerning the expected timing of product and feature availability, the benefits and capabilities of our current and future products and services, and our strategic plans and objectives. Such statements are subject to numerous risks and uncertainties and actual results could differ from those statements. Any future products, functionality and services may be abandoned or delayed, and customers should make decisions to purchase products and services based on features that are currently available.

CrowdStrike: Best-of-breed security

Leader in Endpoint Security[1]

Leader in EDR[2]

Best EDR Three Years Running[3]

100% Detection Coverage[4]

[1] Named a Leader in the 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms

[2] Named a Leader in The Forrester Wave™: Endpoint Detection and Response Providers, Q2 2022

[3] SE Labs Annual Best Endpoint Detection and Response Award — 2024

[4] MITRE Engenuity ATT&CK® Evaluations: Enterprise — Round 5

Stop the breach with surgical response

Respond rapidly and eradicate sophisticated threats found by either Microsoft Defender or CrowdStrike directly from the Falcon platform. Take direct endpoint action, respond across the fleet and leverage native no-code workflow automation to shut down attacks at scale.

- **Actionable insights:** Detailed CrowdStrike detection information, from impacted hosts and root cause to indicators and timelines, helps rapidly remediate threats.
- **Surgical precision:** Eliminate stealthy threats with Falcon Real Time Response (RTR) for direct system access to contain threats. Kill processes and run commands, executables and scripts to shut down threats from anywhere in the world.
- **Enterprise-scale automation:** Streamline and automate complex tasks at scale with native CrowdStrike Falcon® Fusion SOAR to dramatically improve SOC team efficiency and shut down attacks.

Contact us → **Try a free demo** →

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/