

Falcon Exposure Management

Know what is actually exploitable, see exposure in real time, and reduce risk faster.

Challenges

Frontier AI is changing how attacks happen. Attackers can now identify weaknesses, generate exploit paths, and move from exposure to exploitation faster than ever. The exploit window is collapsing from weeks to hours, and increasingly to minutes.

At the same time, vulnerability discovery is accelerating. More than 48,000 new CVEs were published in 2025 alone,¹ flooding security teams with findings without giving them the clarity needed to prioritize real risk.

Most organizations still rely on:

- **Periodic scans** that create outdated snapshots
- **Static severity scoring** that measures theoretical risk
- **Manual workflows** that cannot keep pace with modern threats

Many organizations also need a way to modernize exposure management without replacing their existing endpoint security tools. The result: Attackers exploit what works, while defenders struggle to identify what matters most.

Solution overview

CrowdStrike Falcon® Exposure Management operates across any third-party endpoint environment, including those in organizations that do not use CrowdStrike endpoint solutions today. Organizations can get started immediately without replacing their existing endpoint security stack and expand into the CrowdStrike Falcon® platform over time.

Key benefits

- Identify what attackers will actually exploit
- Continuously understand exposure in real time
- Reduce noise with exploitability-driven prioritization
- Start without replacing your existing endpoint security tools
- Act faster with integrated response workflows
- Unify CrowdStrike and third-party exposure data

¹ CVE Program

Falcon Exposure Management helps organizations answer the three questions that now define security in the frontier AI era:

1. **What is actually exploitable in my environment?**
2. **Where am I exposed right now?**
3. **How do I reduce risk before adversaries attack?**

Built on the AI-native CrowdStrike Falcon platform, Falcon Exposure Management combines CrowdStrike telemetry with third-party asset and vulnerability data to create a unified, real-time view of exposure.

Unlike legacy approaches that rely on periodic scans and static severity scoring, Falcon Exposure Management continuously prioritizes risk based on exploitability, adversary behavior, attack paths, and business context, helping teams focus on the exposures most likely to lead to a breach.

1. What is actually exploitable in my environment?

Falcon Exposure Management helps organizations cut through vulnerability overload by identifying the exposures attackers are most likely to exploit. By combining exploitability analysis, adversary intelligence, attack path analysis, and business context, it enables teams to prioritize real risk instead of chasing thousands of findings.

Exposure Prioritization Agent

Built natively into the Falcon platform, the Exposure Prioritization Agent explains vulnerabilities in plain language, validates exploitability using real-time telemetry, and highlights business impact. This helps teams eliminate manual triage and make faster, higher-confidence remediation decisions.

ExPRT.AI Prioritization

CrowdStrike's ExPRT.AI uses AI trained on real-world adversary intelligence and Falcon telemetry to predict which vulnerabilities attackers are most likely to exploit. Unlike static CVSS scoring, it prioritizes exposures based on exploitability, attacker behavior, and environmental context.

Active Adversary Context

Falcon Exposure Management maps vulnerabilities to active adversaries, tactics, and real-world attack activity, helping teams understand which threats matter most to their industry and organization.

Attack Path Analysis

Visualize how attackers could move across endpoint, identity, cloud, and network environments to reach critical assets. Attack Path Analysis highlights reachable and chainable exposures so teams can focus on the risks most likely to lead to a breach.

AI-Powered Asset Criticality

Automatically identify business-critical assets using AI-driven analysis of asset behavior, activity, and organizational context. This helps security teams prioritize based on business impact, not just exposure severity.

Internet Exposure Identification

Correlate internet-facing assets with internal systems to identify externally reachable exposures and prioritize the risks attackers can target immediately.

Up to
98%
reduction in critical
vulnerabilities²

Up to
75%
reduction in external attack
surface³

More than
2,000
analyst hours saved annually⁴

² CrowdStrike customer story: <https://www.crowdstrike.com/resources/customer-stories/intermex/>. Results may not be representative of other customers.

³ Data from Falcon Exposure Management external attack surface management (EASM)

⁴ These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on an individual customer's module deployment and environment.

2. Where am I exposed right now?

Falcon Exposure Management provides continuous, real-time visibility across internal and external attack surfaces, helping organizations understand exposure as environments change. By combining CrowdStrike telemetry with third-party asset and vulnerability data, it creates a unified, real-time view of exposure across the environment.

Continuous Exposure Visibility

Continuously surface exposure across endpoints, configurations, identities, and internet-facing assets without relying on periodic scan windows or scanning infrastructure.

Active, Passive, and API-Based Asset Discovery

Discover assets across on-premises, cloud, endpoint, IoT/OT, and application environments using active, passive, and API-based discovery methods. This multilayered approach helps eliminate blind spots and maintain an up-to-date inventory across hybrid environments.

External Attack Surface Management (EASM)

Gain continuous visibility into internet-facing assets, shadow IT, unknown exposures, and external attack paths using real-time internet mapping technology operating 24/7.

Third-Party Asset and Vulnerability Data Ingestion

Ingest and unify third-party asset and vulnerability data alongside CrowdStrike telemetry to create a single source of truth across the attack surface.

AI Application Inventory and Shadow AI Discovery

Continuously identify sanctioned and unsanctioned AI applications and services across the environment, helping organizations detect shadow AI, unmanaged usage, and emerging exposure risks.

Browser Extension Assessment and Control

Identify risky, malicious, or unauthorized browser extensions that increase exposure and create potential paths for credential theft, SaaS abuse, and data exfiltration.

Secure Configuration Assessment (SCA)

Continuously assess endpoint configurations against CIS Benchmarks across Windows, macOS, and Linux systems to identify misconfigurations and strengthen security posture.

Network Vulnerability Assessment (NVA)

Continuously identify exposure across unmanaged infrastructure, including routers, switches, firewalls, and IoT systems, without requiring scanning appliances or additional infrastructure.

3. How do I reduce risk before adversaries act?

Falcon Exposure Management connects visibility directly to action, helping organizations reduce exposure before attackers can exploit it. Integrated workflows, automation, and real-time response capabilities accelerate remediation and help shrink the exploit window.

Falcon Fusion SOAR

Automate remediation workflows and orchestrate response actions across security and IT teams using CrowdStrike Falcon® Fusion SOAR, built natively into the Falcon platform.

Falcon Real Time Response (requires CrowdStrike Falcon® Insight XDR)

Take immediate mitigation actions, including network isolation, compensating controls, process termination, and emergency response, directly from the Falcon platform.

Third-Party IT Service Management (ITSM) and Patching Integrations

Integrate with ServiceNow, Jira, and patch management solutions to streamline ticketing, workflow orchestration, remediation tracking, and operational collaboration.

Emergency Patching

Enable fast, targeted patching for Windows systems to reduce exposure during active threats and zero-day events.

Automated Remediation Workflows

Connect prioritization directly to remediation through integrated workflows that accelerate response, reduce manual effort, and help teams act faster.

Unified Response Across the Attack Surface

Correlate exposure, adversary activity, and response actions across endpoint, cloud, identity, and network environments to reduce risk before attackers can move laterally or escalate access.

Start anywhere, expand everywhere

Falcon Exposure Management gives organizations a practical path to modern exposure management without replacing existing endpoint security tools.

Organizations can:

- Start with Falcon Exposure Management in any third-party endpoint environment
- Unify CrowdStrike and third-party exposure data
- Correlate assets into a single, real-time view
- Reduce risk without disrupting existing tools
- Expand into the Falcon platform over time

No rip and replace required.

[Learn more](#)[Sign up for a 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/>