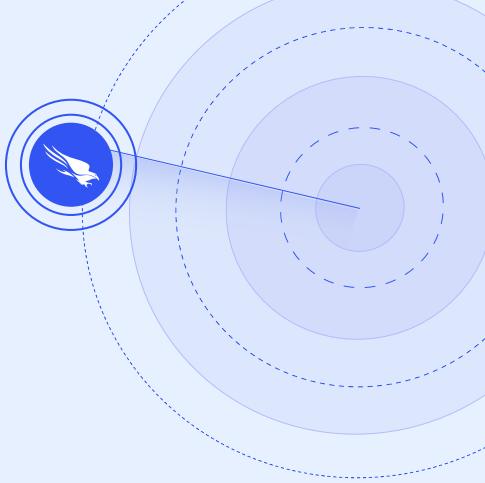
XM Cyber | INTEGRATION SOLUTION BRIEF

XM Cyber x Crowdstrike

Accelerating Threat Response by Enriching CrowdStrike Falcon with Attack Path Intelligence



Executive Summary

Modern SOC teams are often caught in a cycle of reactive response, buried under a high volume of alerts that lack business context. While those that use the CrowdStrike Falcon platform benefit from industry-leading endpoint protection capabilities, many teams still struggle to quickly and accurately triage alerts and efficiently investigate threats.

The integration between XM Cyber and CrowdStrike addresses this challenge by injecting real-time exposure intelligence seamlessly into the Falcon platform. Bi-directional enrichment shifts the SOC from "fire-fighting" to proactive prevention, as analysts gain the clarity needed to understand not just what happened on an endpoint, but where an attacker could go next.

The Need for Continuous Exposure Management

The primary hurdle in modern security operations is a lack of context. SOC teams often see a detection in isolation without understanding the broader attack surface or the business criticality of the involved assets. To move faster, teams need to know if an alert represents a localized event or a critical step in a multi-stage breach leading to "crown jewel" assets.

The integration between XM Cyber and CrowdStrike Falcon creates a continuous loop between risk management and security operations. By enriching Falcon incidents with exposure data, XM Cyber allows teams to prioritize their response based on verified reachability. This ensures that the most dangerous attack paths are neutralized before they can be exploited.

Introducing

CROWDSTRIKE

Secure the Endpoint. Stop the Breach

AI-powered protection, detection, and response - backed by world-class adversary intelligence.

XM Cyber

Prevent Attacks That Put Your Business At Risk

Get ahead of attackers by continuously discovering, prioritizing, and fixing every validated exposure in YOUR environment before it's exploited.

Solution Benefits by Use Case

Assess Your Defenses Against Validated Exposures and Real-World Threats

Align on what matters most to the business and what's truly possible.

Spot Gaps in Detection Coverage

Automatically identify unmanaged assets or "shadow IT" where Falcon sensors are missing or inactive, ensuring 100% security hygiene across the environment.

Validate Where Attackers Can Go Next

Instantly visualize if a detection in Falcon represents a direct path to a critical asset. See the full "blast radius" from the breach point to your crown jewels.

Context-Aware Detection Engineering and Incident Response

Empower SOC teams with business context directly within their EDR workflow.

Move from Triaging to Acting

Equip analysts with reachability context the moment an alert fires, allowing them to filter out noise and accurately disposition alerts with certainty.

Automate Context Enrichment

Automatically tag Falcon agents as critical assets or choke points, providing instant visibility into the business stakes of a detected event.

Operationalize Exposure Intelligence

Ensure continuous alignment between proactive and reactive security teams.

Optimize Attack Scenarios

Improve your security posture by running attack simulations from devices that were actually attacked, using their CrowdStrike incident score as the baseline.

Reduce Mean Time to Respond (MTTR)

Bypass manual evidence gathering by seeing exactly how an attacker could move toward your domain controllers or sensitive data.

Access Control and IAM	**Endpoint Security**	Data Protection	Network Security	Config Management
Email Security	Remote Access	Vuln Management	Device Management	Web Services
Virtualization	Security Rating	SSPM Cloud Services	SIEM / SOC	IT Management

XM Cyber

As the pioneer of exposure management, XM Cyber delivers a continuous and actionable understanding of cyber risk across the entire attack surface, including hybrid, cloud, on-prem, OT, legacy, AI, and container environments. Powered by proprietary Attack Graph Analysis™, the platform continuously validates exploitable exposures against a digital twin of your production environment, applying nearly a decade of offensive security expertise. By revealing the critical choke points where multiple attack scenarios converge, XM Cyber directs security teams to the remediation actions that eliminate the most risk with the least effort. The result is measurable improvement in security posture through prioritized, high-impact remediation, along with clear, business-contextual reporting that enables leaders to communicate risk effectively and demonstrate security ROI.