CrowdStrike Products

Data Sheet

Falcon Exposure Management

The world's leading AI-powered platform for exposure management

Proactive vulnerability and risk management can be a formidable undertaking in the best of times, in no small part due to the maintenance-intensive nature of many traditional vulnerability management (VM) tools. These tools often take weeks or even months to complete a single scan, while also demanding constant upkeep and care.

Adding to that struggle, the proliferation in type and modality of IT assets has created an explosion of new and ever-shifting attack surfaces. For many security teams, merely knowing what they are responsible for protecting can be a serious challenge, not to mention developing a holistic understanding of these assets, the associated exposures and adversary context. Point solutions attempting to address this can themselves represent another source of fragmentation. As many practitioners know, understanding the asset landscape is half of the battle in effective security.

Furthermore, while the ultimate goal for CISOs and boards of directors is to prevent breaches, most VM tools operate in a silo, lacking meaningful integrations with real-time security tools and the associated benefit of insight and mitigation. With the increasing prominence of zero-days and high-profile exploits, this tooling gap often hampers cross-security collaboration, impeding timely and synchronized actions and leaving more opportunity to attackers.

Key challenges

- Legacy VM tools come with a maintenance burden and require slow, disruptive scans
- Security teams struggle to discover and understand overall attack surfaces and adversary context
- Fragmented solutions and lack of visibility impede holistic prioritization and undermine security posture
- Siloed risk management tools stop at understanding risk and are unable to stop breaches

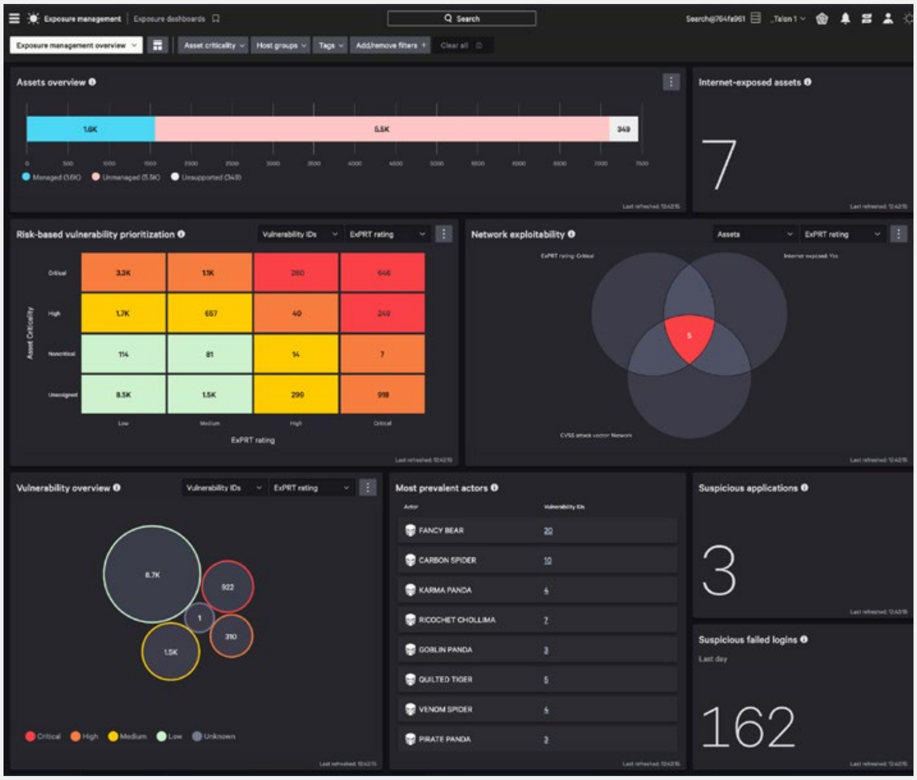
Key benefits

- Unparalleled asset discovery and understanding
- Maintenance-free assessment for a wide variety of exposures
- Native integration with world-class adversary context
- AI-driven vulnerability prioritization
- Attack path visualization to analyze and detect potential for lateral movement
- Consolidated visibility and unified platform facilitating remediation actions

Solution overview

CrowdStrike Falcon® Exposure Management is a powerful groundbreaking product that harnesses the cutting-edge capabilities of the CrowdStrike Falcon® platform. This innovative solution utilizes the unified, lightweight Falcon agent, which enables real-time, maintenance-free vulnerability assessment. Moreover, it integrates the robust, predictive ExPRT.AI prioritization model, trained on world-class threat intelligence and real-life threat detection incidents. These features empower security teams to allocate their limited resources strategically, focusing 95% of resources on the 5% of risk exposures[1] that are most likely to be exploited by threat actors.

In addition, Falcon Exposure Management offers unparalleled real-time asset discovery and understanding, extensive exposure assessment and consolidated visibility across the entire attack surface. This comprehensive suite of capabilities assists organizations in effectively staying on top of their internal and external asset exposures, reducing the external attack surface by 75%,[2] mitigating risks and fostering effective collaboration within the security team. By combining Falcon Exposure Management with CrowdStrike's cutting-edge, real-time security solutions, organizations can safeguard their systems against potential attackers and maintain a strong proactive security posture.



Asset Criticality	Low	Medium	High	Critical
Critical	3.3K	1.1K	260	646
High	1.7K	657	40	249
Noncritical	114	81	14	7
Unassigned	8.5K	1.5K	299	918

ExPRT rating

Actor	Vulnerability IDs
FANCY BEAR	20
CARBON SPIDER	10
KARMA PANDA	4
RICOCHET CHOLLIMA	7
GOBLIN PANDA	3
QUILTED TIGER	5
VENOM SPIDER	4
PIRATE PANDA	3

Falcon Exposure Management unified main dashboard

73%
of organizations are concerned about their growing attack surface[3]

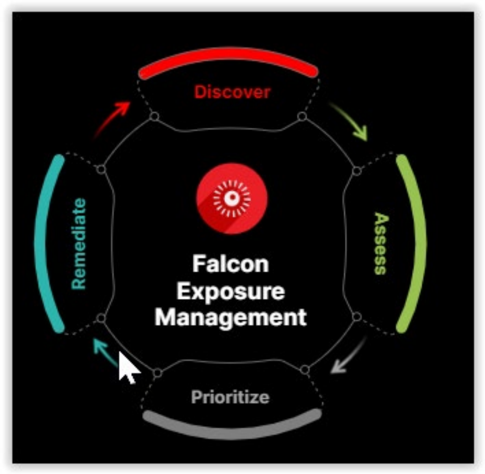
62%
of organizations have blind spots that weaken security posture[4]

76%
of organizations have experienced an attack that started from an unknown asset[5]

[1] CrowdStrike Falcon Spotlight® data
[2] CrowdStrike Falcon Surface® data
[3] Sapio Research & Trend Micro, 2022
[4] Sapio Research & Trend Micro, 2022
[5] CrowdStrike Falcon® Surface data

Key capabilities

Falcon Exposure Management helps security teams fully operationalize vulnerability management programs through the entire lifecycle, from the foundational aspect of asset discovery, to assessment and prioritization of vulnerabilities and exposures, all the way to effective remediation.



Discover

Thoroughly discover all of your assets and blind spots with a variety of advanced methods including active discovery and external attack surface management (EASM). Gain additional context through intelligence such as asset roles, criticality and possible internet exposures.

Active, Passive and API-based Asset Discovery

Effortlessly discover all of the assets in your environment whether they reside on-premises, in the cloud, IT, OT/IoT, endpoint, workloads or applications. Rather than deploying onerous network scanning appliances, the unified CrowdStrike Falcon agent can be designated as a scanner to conduct active asset discovery scans of the network. Passive discovery, on the other hand, utilizes CrowdStrike Falcon® Insight XDR telemetry and local host information such as ARP tables and DNS cache, allowing for automatic understanding of your network segments. API-based discovery allows for asset data ingestion from third-party sources such as ServiceNow, Claroty, Active Directory and many others.

External Attack Surface Management (EASM)

Exposure to the public internet is often an organization's blind spot, and it's frequently the attacker's first stop. Get an outside-in view of the enterprise attack surface and discover internet-connected assets that were previously unknown. Using a proprietary internet mapping technology operating 24/7, the EASM engine can determine location information and see real-time changes. It also automatically provides business discovery, including mapping subsidiaries and other M&A activities.

Application, Account and Identity Intelligence

Track installed applications on each asset. See details of how applications are being utilized and whether unauthorized software is installed. Monitor which accounts are being used, how domain and local credentials are being accessed, when passwords are changed and other potentially suspicious activity.

Asset Roles

In an enterprise environment with tens of thousands of assets, it is not always easy to determine which machine does what, given disparate ownerships and scattered geography. Falcon Exposure Management can automatically determine an asset's role based on its behaviors and activity level, such as when a machine is a DHCP server, email server or a jump server, providing essential context for better understanding risk and exposure.

Assess

Effortlessly assess for a wide variety of exposures. Build compliance using CIS benchmarks. Ingest third-party sources of vulnerability information so you can master your entire exposure surface in one place without needing a separate cyber asset attack surface management (CAASM) tool.

Native Scanless Vulnerability Assessment

Continuous vulnerability assessment using CrowdStrike's single, multi-functional, lightweight Falcon agent provides real-time visibility with no infrastructure overhead or maintenance. Get wide-ranging vulnerability coverage including software CVEs, misconfigurations and end-of-support-life detection on Windows, MacOS, Linux and related applications. Obtain rich vulnerability details, exploit information and attacker context through multitudes of first-party and third-party intelligence feeds.

Secure Configuration Assessment (SCA) against CIS Benchmarks

Weakly configured or misconfigured assets are just as susceptible to threats as those with software vulnerabilities. Assess your assets' configuration settings against user-customizable CIS Benchmarks (a comprehensive set of prescriptive best practice standards), whether for compliance objectives or up-leveled security.

Third-party Vulnerability Data Ingestion

Ingest vulnerability information from third-party scanning solutions and see them alongside CrowdStrike's native vulnerability data to create a single pane of glass for prioritizing and operationalizing all of your exposure information, without the need to pay for a separate integration tool.

Prioritize

Effectively prioritize your exposures based on an AI predictive model with active adversary context. Leverage additional tools and information such as attack path visualization, asset criticality and internet exposure identification to zoom in on the exposures that truly matter to your particular organization.

ExPRT.AI Ratings

Automatically prioritize risks with this dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events. While CVSS scores categorize many CVEs into high-severity brackets — and inundate resource-strapped security teams — the threat-based ExPRT.AI rating narrows down crucial vulnerabilities to a more targeted set so you can confidently prioritize for more impact with less work.

Active Adversary Context

Leveraging industry-leading threat intelligence, Falcon Exposure Management pinpoints and correlates vulnerabilities with adversaries most associated with them and their related tactics so you can better prepare for the types of threats and adversaries that matter most for your particular industry and vertical.

Attack Path Visualization

Visualize intrusion risk across endpoint, cloud and identity assets. Understand lateral movement through critical hosts and user accounts. See exactly how an attacker could potentially navigate their way to your organization's crown jewels. With network relationship and risk exposure highlighted, you gain additional information to evaluate whether a particular risk exposure is an isolated risk or a must-fix.

Asset Criticality

Asset context is an important consideration for advanced prioritization to further optimize limited resources. The powerful rules engine allows you to automatically assign criticality levels to assets based on a wide variety of input parameters so you know which assets to focus on.

Internet Exposure Identification

Not only does Falcon Exposure Management provide an outside-in view of internet-facing IPs, that information is actively correlated against an inside-out view of asset inventory to match and identify exactly which IT assets have an internet exposure. This additional context provides security teams with invaluable information to triage and prioritize risk mitigation.

Remediate

Whether you are trying to orchestrate remediation activities across the organization or deploy immediate mitigating measures, Falcon Exposure Management has you covered, through integration with both native and third-party tools, powerful platform-based actions and the ability to correlate with CrowdStrike's top-notch Falcon Insight XDR solution.

Native Security Orchestration Automation and Response (SOAR) Integration

Automate and orchestrate remediation playbooks through CrowdStrike Falcon® Fusion, the SOAR tool built into the Falcon platform. Customize and flexibly trigger ticket assignments to the right teams based on the right remediation actions.

Third-Party Integrations

Leverage popular ticketing tools such as ServiceNow and Jira to seamlessly create tickets. The powerful two-way integration allows you to actively monitor the status and track the completion of tasks. Additional integration with remediation and patch management tools adds further convenience and flexibility.

Falcon Real Time Response (RTR) Actions

CrowdStrike's proprietary Falcon RTR actions deliver a powerful range of mitigation measures and compensating controls such as:

- **Compute:**
  Kill running process, block file execution, execute patchless config scripts
- **Network:**
  Close ports, restrict IP, restrict DNS, restrict network storage
- **Identity:**
  Restrict accounts, suspend logins
- **Hardware:**
  Restrict USB devices, restrict Bluetooth

Emergency Patching

The Falcon RTR-powered emergency patching capability provides one-click patching convenience for Windows-based systems, delivering surgically targeted, precise, proactive protection.

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.

Sign Up for a Demo →