CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Exposure Management

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

Challenges

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 represent another source of fragmentation themselves. 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 for attackers.

Key challenges:

- Legacy VM tools with a maintenance burden and slow disruptive scans
- Struggle to discover and understand overall attack surfaces and adversary context
- Fragmented solutions and lack of visibility that impedes holistic prioritization and undermines security posture
- Siloed risk management tools that don't understand 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 Exposure Prioritization Agent that delivers instant, actionable insight
- Attack path visualization to analyze and detect potential for lateral movement
- Consolidated visibility and a unified platform that facilitate remediation actions
- Continuous, authenticated scanning for deeper, always-on visibility

Up to 98% reduction in critical vulnerabilities[1]

Up to 75% reduction in external attack surface[2]

Over 2,000 analyst hours saved annually through continuous assessment and automation[3]

[1] CrowdStrike customer story: https://www.crowdstrike.com/resources/customer-stories/intermex/ Results may not be representative of other customers.

[2] Data from CrowdStrike Falcon® Exposure Management external attack surface management (EASM)

[3] 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 individual customer's module deployment and environment.

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 sensor, which enables real-time, maintenance-free vulnerability assessment. Moreover, it integrates CrowdStrike's 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[4] 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 up to 75%,[5] 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.

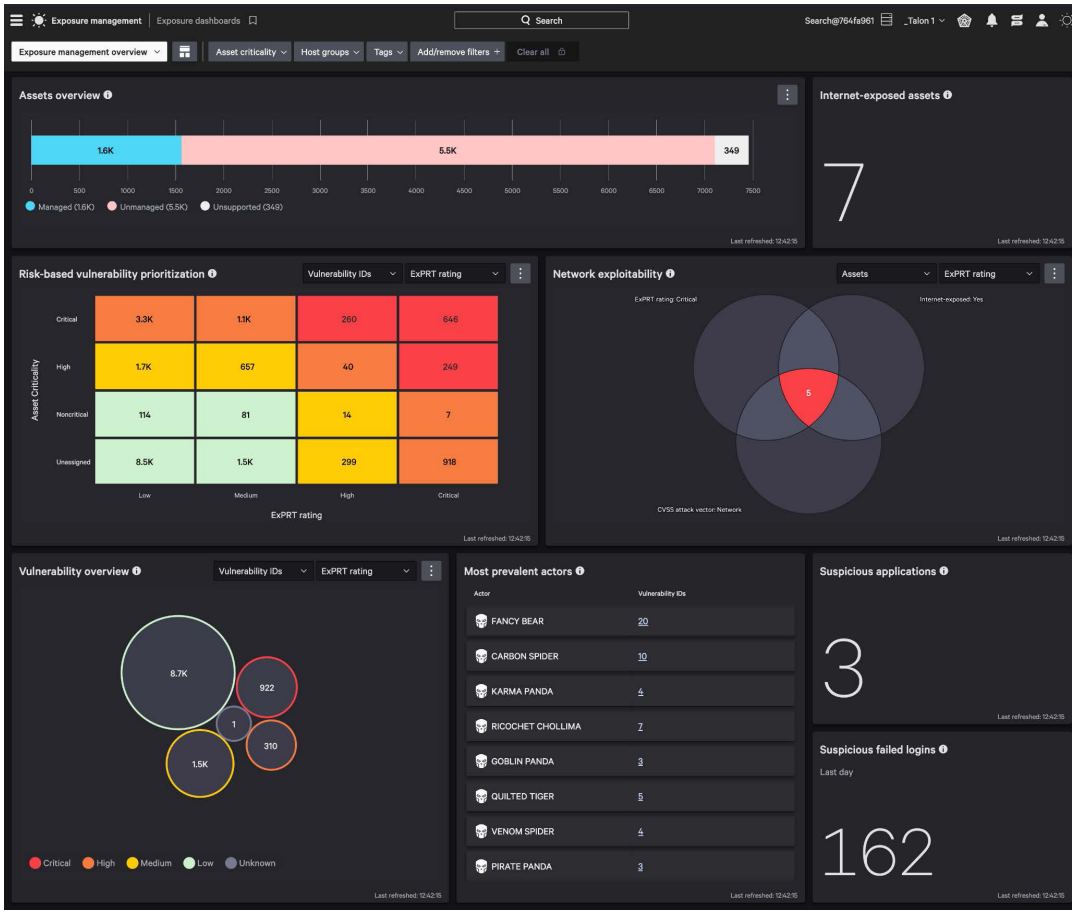

Figure 1. Falcon Exposure Management unified main dashboard

[4] CrowdStrike Falcon® Spotlight data
[5] CrowdStrike Falcon Exposure Management EASM data

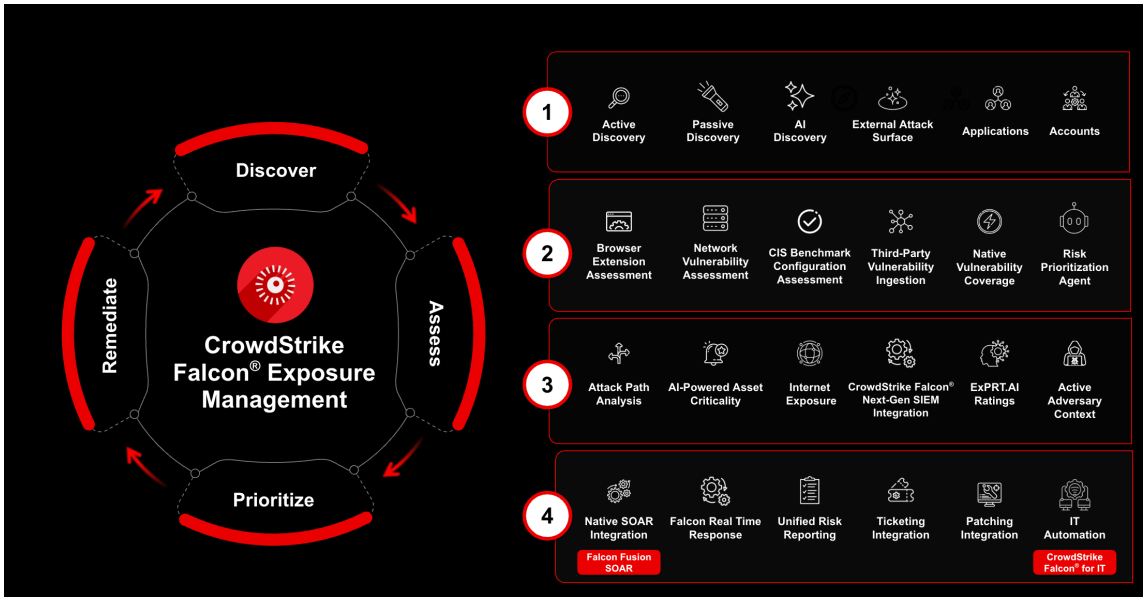

Figure 2. Falcon Exposure Management capabilities

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 assets across your environment — whether on-premises or in the cloud, across IT, OT/IoT, endpoints, workloads, or applications — using a combination of active, passive, and API-based discovery methods. Rather than relying on legacy network scanning appliances, CrowdStrike leverages the Falcon sensor to perform lightweight active discovery directly from endpoints. Passive discovery uses CrowdStrike Falcon® Insight XDR telemetry and local host data such as ARP tables and DNS cache to continuously map the network without intrusive scans. API-based discovery integrates data from third-party platforms such as ServiceNow, Claroty, and Active Directory, providing enriched asset context. This multilayered approach enables security teams to maintain real-time visibility into their entire asset inventory, including cloud workloads and deployed technologies — eliminating blind spots and supporting proactive exposure management.

- **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, and see details of how applications are being utilized or whether unauthorized software is installed. Monitor what accounts are being used, how domain or 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 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 Vulnerability Assessment**
  Continuous vulnerability assessment using CrowdStrike's single, multi-functional, lightweight sensor provides real-time visibility with no infrastructure overhead or maintenance. Gain broad coverage across software CVEs, misconfigurations, and end-of-support detections on Windows, macOS, Linux, and related applications. Access detailed vulnerability insights, exploit information, and adversary context from both first-party and third-party intelligence feeds. This continuous, agent-based assessment delivers a trusted, insider-level view of your environment, validating configurations, patch levels, and vulnerabilities that traditional scanning methods can miss.

- **Continuous Visibility**
  Eliminate the gaps between scans with continuous visibility that keeps your vulnerability data current — automatically. As new CVEs are published, existing asset fingerprints are compared in real time, instantly identifying impacted systems without requiring a new scan. Stay ahead of threats with up-to-date, always-on insight into your exposure.

- **Network Vulnerability Assessment**
  This enables you to identify and prioritize vulnerabilities across your entire network, including sensorless devices like routers, switches, and IoT systems, without requiring any scanning appliances or additional hardware. Authenticated scanning provides deeper, credential-based visibility into networked systems, delivering accurate insights into configurations, patch levels, and vulnerabilities that unauthenticated scans can overlook. Powered by ExPRT.AI, it focuses on the most critical risks by analyzing real-world exploitability, while CrowdStrike threat intelligence provides real-time insights into exploit status. This proactive, intelligence-driven solution helps prevent breaches, reduce the attack surface, and strengthen your security posture.

- **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-leveling security. Available for Windows, Mac, and Linux.

- **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.

- **End-of-Life (EOL) Detection**
  When a software product is no longer receiving support or updates from the manufacturer, it will not get any bug fixes or security updates. It is a crucial form of risk that security teams need to get ahead of. Falcon Exposure Management automatically detects Windows EOL versions so teams can proactively address the exposure with appropriate mitigations.

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 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 — CrowdStrike's 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 industry and vertical.
- **Attack Path Analysis**
  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 risk exposure is an isolated risk or a must-fix.
- **AI-Powered Asset Criticality**
  Asset context is essential for effective prioritization. Falcon Exposure Management uses AI to automatically classify assets as Critical, High, or Non-Critical based on business context, behavior, and peer insights. This ensures security teams focus on the assets that matter most — not just what's vulnerable but what's valuable.
- **Exposure Prioritization Agent**
  Built natively into the platform, the Exposure Prioritization Agent instantly explains each vulnerability in plain language, validates real-world exploitability, and highlights business impact. By combining real-time telemetry, adversary intelligence, and business context, it eliminates hours of manual CVE triage and helps teams focus on what truly matters — reducing risk faster.
- **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 XDR solution.

- **Native Security Orchestration, Automation, and Response (SOAR) Integration**
  Automate and orchestrate remediation playbooks through CrowdStrike Falcon® Fusion SOAR, 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.

Learn more: https://www.crowdstrike.com/

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/