

Data Sheet

FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

By using the powerful Falcon platform with its lightweight agent, the continuous monitoring for vulnerability exposures becomes effortless. IT staff will always have access to up-to-date information, with virtually no impact to endpoints across your organization.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

Initiate emergency patching for critical vulnerabilities with native Falcon integrations

FALCON SPOTLIGHT

KEY CAPABILITIES

REDUCE VULNERABILITY PRIORITIZATION EFFORT

Falcon Spotlight is a dynamic vulnerability management solution equipped with intuitive dashboards and powerful filtering capabilities, enabling you to improve your organization's security posture by serving up the most relevant information. Dashboard capabilities include:

- **ExpRT rating:** Immediately prioritize which vulnerabilities are truly relevant to your organization with a dynamic rating that more accurately shows risk levels. The rating is adjusted according to a vast database of source data.
- **Exploit status:** Using integrated vulnerability exploit and threat intelligence, you can easily identify which vulnerabilities in your environment represent the greatest risk, and build reports and dashboards that keep track of these vulnerabilities.
- **Recommended remediations:** Ensure that your remediation efforts are reducing the most risk. Falcon Spotlight intelligently recommends the highest-impact patches to deploy, reducing the chances of deploying a superseded patch.
- **Installed patches:** Use the Installed Patches page to identify which patches are active across your environment, or which patches have been installed but are pending a reboot.

AUTOMATE VULNERABILITY ASSESSMENT

Take advantage of the Falcon platform and lightweight agent to eliminate the burden of lengthy, performance-impacting scans. With scanless technology, automated data collection and a real-time user interface, your IT staff gains a continuous, comprehensive picture of all endpoints in your organization — no more outdated reporting or long scans slowing down regular business processes.

IMPROVE SECURITY OPERATION EFFICIENCY

Streamline your vulnerability management program with custom dashboard features. Create and save custom filters so staff can quickly navigate and research critical issues. Use the custom team dashboards to share insights across your entire team, and set remediation timeframes to speed vulnerability resolution and increase your team's efficiency.

REDUCE OVERALL COMPLEXITY

Falcon Spotlight does not require an additional agent, and endpoints no longer need to use cumbersome hardware or weighty agents, or be on the network to be assessed. Falcon Spotlight is always on, seamlessly bridging the gap between vulnerability management and the rest of the Falcon platform, enriching threat detection and intelligence use cases. Simply select a vulnerability within the dashboard to see a wealth of data around threat actors, including threat intelligence reports and additional insights. Since all data is housed within the same console, analysts can pivot quickly to those vulnerabilities that show the most significant risk to resolve them first.

For hosts with critical vulnerabilities that need remediation instantly, IT staff can take advantage of emergency patching — it's a simple one-click action for Windows patch updates.

Learn more at www.crowdstrike.com

A SINGLE SOLUTION FOR CONTINUOUS VULNERABILITY ASSESSMENT AND MONITORING

Eliminate the need for cobbling together tools to get a complete vulnerability picture — Falcon Spotlight connects the dots, providing immediate visibility of your environment

Tap into the full power of contextual data by using threat intelligence in conjunction with Falcon Spotlight

Maintain business productivity with virtually no impact on any endpoint

Speed up your search results with custom saved searches or universal search to filter results across the entire Falcon console

Utilize the tight integration between the Falcon platform and other Falcon modules for additional in-depth research

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

