CROWDSTRIKE

CrowdStrike Products

Solution Brief

Falcon Seraphic Enterprise Browser: Take Control of Browser Extension Risk

Continuously discover, assess, and enforce policy on browser extensions across managed, unmanaged, and BYOD devices without disrupting the workforce.

The challenge

Browser extensions are deeply embedded in everyday work, but many organizations cannot see every extension employees install. That visibility gap spans managed devices, unmanaged devices, and BYOD, creating a shadow extension estate that can be difficult to inventory or govern consistently.

Marketplace popularity is not a security assessment. Star ratings do not reflect real risk, and manual review cannot provide a consistent view of extension behavior across a changing browser estate. Security teams need evidence-based signals that reflect an extension's reputation, static characteristics, behavior, and history.

At the same time, blanket blocking can interrupt legitimate workflows. Teams need granular controls that distinguish acceptable from risky use, plus event-level visibility when extensions are installed, permissions change, or policy actions occur. Without that context, analysts may be forced to piece together extension activity after the fact.

Key benefits

- Continuously inventory extensions across managed, unmanaged, and BYOD devices
- Surface shadow extensions and close browser visibility gaps
- Assess risk with reputation, static, behavioral, and historical signals
- Use a composite risk score instead of relying on marketplace star ratings
- Block, warn, or allow extensions by permission scope, publisher, or user group
- Track extension installs, permission changes, and policy actions with event-level telemetry
- Accelerate triage with enriched alerts in CrowdStrike Falcon® Next-Gen SIEM

The solution

CrowdStrike Falcon® Seraphic® Enterprise Browser provides continuous browser extension discovery, risk assessment, and policy enforcement across the browser estate. It inventories extensions in use across managed and unmanaged devices, including BYOD, giving security teams a current view of what is installed without disrupting the workforce.

Each extension is assessed using reputation, static, behavioral, and historical signals. These inputs are combined into a composite risk score, helping security teams make decisions based on evidence instead of relying on marketplace star ratings alone.

Policies can block, warn, or allow extensions based on permission scope, publisher, or user group. This makes it possible to apply targeted controls at the browser layer, reducing risk while keeping the extensions employees depend on available for approved work.

Extension activity is also visible through event-level telemetry for installs, permission changes, and policy actions. Enriched alerts can be sent to Falcon Next-Gen SIEM so analysts can investigate and triage extension risk without stitching data together by hand.

Unified extension visibility in the Falcon platform

Extension event telemetry, including installs, permission changes, and policy actions, can flow into Falcon Next-Gen SIEM as enriched alerts, giving analysts a centralized view for faster triage and investigation.

Key capabilities

Discover Extensions Across the Browser Estate

- **Continuous extension inventory:** Continuously identify extensions in use across managed, unmanaged, and BYOD devices to close visibility gaps.
- **Shadow extension visibility:** Surface extensions employees install outside centralized processes before they become security blind spots.
- **Cross-browser, cross-device oversight:** Apply consistent extension visibility across the browser estate while users continue working in their preferred browser workflows.

Assess and Control Extension Risk in Real Time

- **Multi-signal risk assessment:** Evaluate extensions using reputation, static, behavioral, and historical signals rather than marketplace popularity alone.
- **Composite risk scoring:** Combine risk signals into one score so teams can prioritize review and make evidence-based decisions consistently.
- **Granular policy enforcement:** Block, warn, or allow extensions based on permission scope, publisher, or user group at the browser layer.
- **Work-friendly governance:** Apply targeted controls instead of blanket restrictions, helping protect users while keeping approved extensions available for work.

Accelerate Extension Investigations with Falcon

- **Event-level telemetry:** Capture extension installs, permission changes, and policy actions so analysts have a detailed record of extension activity.
- **Enriched next-gen SIEM alerts:** Send extension events into Falcon Next-Gen SIEM to centralize visibility and support faster triage.
- **Faster analyst investigation:** Review extension activity in one place instead of stitching data together by hand when suspicious behavior needs attention.

Schedule 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/

© 2026 CrowdStrike, Inc. All rights reserved.