CROWDSTRIKE

CrowdStrike Products

Solution Brief

Falcon Seraphic Enterprise Browser: Stop Browser Threats Before They Execute

Stop phishing, zero-day exploits, and malicious code in every browser session without replacing the browser or disrupting how users work.

The challenge

The browser has become a primary workspace for modern employees and a growing target for adversaries. Phishing, ClickFix, browser exploits, and malicious JavaScript can unfold inside the browser session, where traditional URL filtering and endpoint controls may have limited context into what a page is doing as it renders and executes.

Modern phishing is designed to evade reputation-based defenses. Zero-hour phishing pages may remain unclassified, while CAPTCHA-gated evasion, reverse-proxy attacks, and browser-in-the-browser techniques can make malicious experiences look legitimate long enough to capture credentials.

Browser vulnerabilities and malicious scripts create a second layer of risk. Zero-day and known-but-unpatched N-day exploits can be weaponized during the patch gap, while threats such as SocGholish, Gootloader, and HTML smuggling can abuse browser scripts to deliver malware. Security teams need prevention at the point of browser execution, plus detailed telemetry when attacks occur.

Key benefits

- Stop zero-hour phishing using runtime signals evaluated as each page renders
- Detect phishing sites, CAPTCHA-gated evasion, reverse-proxy phishing, and browser-in-the-browser attacks
- Disrupt zero-day and unpatched N-day browser exploits during the patch gap
- Block malicious JavaScript before a payload reaches the endpoint
- Protect users in the browsers they already use without forcing a dedicated enterprise browser
- Reduce dependence on signatures, threat feeds, and prior knowledge for browser exploit prevention
- Accelerate investigation with event-level telemetry and enriched alerts in CrowdStrike Falcon® Next-Gen SIEM

The solution

CrowdStrike Falcon® Seraphic® Enterprise Browser adds real-time browser-native protection to the browsers users already know. It evaluates runtime signals as each page renders to help stop zero-hour phishing, CAPTCHA-gated evasion, reverse-proxy phishing, and browser-in-the-browser attacks before credentials are stolen.

But not every attack relies on tricking users into taking the bait. Attackers also exploit vulnerabilities in the browser itself, particularly during the gap between when a vulnerability is discovered and when a patch is deployed. Moving Target Defense, a core feature in Falcon Seraphic Enterprise Browser, helps reduce this risk by randomizing the browser's execution environment to disrupt the assumptions that exploits rely on. This helps zero-day and unpatched N-day exploits fail without waiting for a vendor patch, signature, or prior threat intelligence.

But even a fully patched browser can be targeted by malicious scripts running within webpages. Falcon Seraphic Enterprise Browser addresses this threat by inspecting and controlling JavaScript execution in real time, intercepting malicious scripts before they can deliver a payload to the endpoint. This helps stop browser-based threats such as SocGholish, Gootloader, ClickFix, and HTML smuggling.

Every browser threat can generate event-level telemetry, including the targeted user, URL, attack technique, and signals that are valuable for threat hunting. Enriched alerts can flow to Falcon Next-Gen SIEM or other tools so analysts can investigate quickly without stitching together browser, proxy, and endpoint data by hand.

Key capabilities

Detect and Stop Phishing at Runtime

- **Runtime phishing detection:** Evaluate real-time page signals as content renders to help identify phishing before credentials are entered or stolen.
- **Zero-hour and evasive site protection:** Detect phishing pages that may be unclassified or hidden behind CAPTCHA-gated evasion techniques.
- **Advanced phishing defense:** Help stop reverse-proxy attacks and browser-in-the-browser techniques that can bypass URL-based defenses.

Protect Browser Execution in Real Time

- **Moving Target Defense:** Randomize the browser execution environment so zero-day and unpatched N-day exploits are disrupted without waiting for a vendor patch.
- **Patch-gap protection:** Reduce exposure while browser updates are being developed, tested, and deployed across the organization.
- **Malicious JavaScript prevention:** Inspect and control JavaScript

Runtime browser protection in the Falcon platform

Browser threat telemetry can flow into the CrowdStrike Falcon® platform with user, URL, technique, and detection context, helping analysts move from browser event to investigation and response with less manual correlation.

execution in real time to stop malicious scripts before payloads reach the endpoint.

- **Browser-native threat coverage:** Help stop techniques used by threats such as SocGholish, Gootloader, and HTML smuggling at the point of browser execution.

Accelerate Browser Threat Investigation with Falcon

- **Event-level browser telemetry:** Capture who was targeted, the URL involved, the attack technique, and the runtime signals associated with each browser threat.
- **Enriched next-gen SIEM alerts:** Send browser threat events to Falcon Next-Gen SIEM or other tools to centralize investigation and triage.
- **Faster analyst response:** Give analysts detailed browser context without requiring them to manually correlate separate proxy and endpoint data sources.

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.