CROWDSTRIKE

CrowdStrike Products

Solution Brief

Falcon Seraphic Enterprise Browser: Secure Mobile Work Across iOS and Android

Extend enterprise browser security, Zero Trust access, data protection, and SaaS governance to smartphones and tablets across managed and unmanaged devices

The Challenge

Mobile devices are now a routine part of enterprise work. Employees, contractors, and partners use phones and tablets to access SaaS applications, internal web apps, and sensitive corporate data wherever they are. Yet many security and access controls were designed around managed laptops and workstations, leaving mobile browser sessions with inconsistent visibility, policy enforcement, and protection.

That gap creates both security and data risk. Mobile users can encounter sophisticated phishing, malicious web content, and credential theft. Sensitive information can also leave the organization through clipboard actions, screenshots, downloads, or the use of unsanctioned services, especially when work happens on personal devices outside traditional endpoint controls.

Full-device enrollment and virtual desktop infrastructure (VDI) can add cost, complexity, friction, and privacy concerns on personal devices. Security teams need a way to secure mobile work without taking control of the entire device.

Key benefits

- **Secure corporate work on iOS and Android across managed and personal devices**
- **Extend browser security, access, and data loss prevention to mobile**
- **Keep corporate browsing and data separate from personal activity**
- **Access SaaS and private applications without traditional VPN or VDI**
- **Control clipboard, screenshots, downloads, and watermarking in the browser**
- **Help stop phishing, credential theft, and web threats**

The Solution

CrowdStrike Falcon® Seraphic® Enterprise Browser extends enterprise browser security to mobile through a dedicated secure browser for iOS and Android. It supports managed and unmanaged devices while keeping corporate browsing logically separate from personal activity and applying consistent security and access policy.

Mobile users can access SaaS, private web apps, and internal resources through the browser without relying on traditional VPN or VDI workflows. Identity and device context help govern access based on risk.

Browser-level data controls govern clipboard actions, screenshots, downloads, and watermarking so sensitive information stays inside approved mobile workflows. The same browser-layer approach can extend SaaS governance to mobile, helping control access to SaaS and reduce sensitive data exposure when used in a secure browser.

Browser protections help stop modern web threats, while phishing defenses reduce the risk of credential theft and browser-based compromise. Together, secure access, data loss prevention (DLP), identity policy, and SaaS governance create a protected mobile work experience.

One browser security strategy from desktop to mobile

Falcon Seraphic Enterprise Browser extends a consistent security model across laptops, smartphones, and tablets. On mobile devices, a dedicated secure browser brings protected access, DLP, identity policy, SaaS governance, and web threat protection to iOS and Android while helping preserve privacy on personal devices.

Key capabilities

Secure Mobile Work Without Managing the Whole Device

- **Dedicated mobile workspace:** Deliver a protected enterprise browsing experience through a secure mobile browser for iOS and Android, with corporate activity logically separated from personal use.
- **Managed and unmanaged device support:** Protect corporate mobile sessions across company-owned phones and tablets as well as BYOD and contractor devices without requiring full-device management for every user.
- **Granular mobile policy:** Apply policy by user, group, device type, or domain, and use mobile device management (MDM) and identity-provider integrations to support enterprise deployment and access governance.

Protect Access and Data at the Point of Use

- **Browser-native private access:** Connect users to approved SaaS applications, self-hosted web apps, and internal resources through the protected browser without making VPN or VDI the default access path.
- **Mobile DLP controls:** Govern clipboard actions, screenshots, downloads, and watermarking to reduce data leakage and keep sensitive information inside approved workflows.
- **Identity-based access:** Use identity context to allow access to enterprise assets.
- **SaaS governance:** Extend browser-level policy enforcement to SaaS applications accessed through the dedicated secure mobile browser.

Stop Browser Threats Across Mobile Sessions

- **Web threat prevention:** Help block malicious web content before it can lead to compromise.
- **Mobile visibility and auditability:** Maintain visibility into protected browser activity across the mobile fleet so security teams can investigate events and enforce policy consistently across devices.

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.