

Zimperium MTD Integration with CrowdStrike Falcon® Next-Gen SIEM

Ultimate Endpoint Security Providing Visibility Across the Unified Threat Landscape

Executive Summary

CrowdStrike users are dedicated to enabling protection and visibility across their enterprise threat landscape, yet many have struggled with visibility into the most vulnerable attack surface: Mobile.

Zimperium's integration with CrowdStrike Falcon Next-Gen SIEM unifies visibility and value across Endpoint, Identity, Cloud & Mobile attack surfaces. Security and SOC teams are provided with mobile alert and correlated incident data, including recommended response actions in real-time within Next-Gen SIEM, alongside every other endpoint they already monitor.

Zimperium, the global leader in AI-empowered mobile security, integrates with CrowdStrike's Falcon Next-Gen SIEM platform to provide organizations with:



Unified Visibility of all Endpoints in Falcon Next-Gen SIEM: Single pane of glass for threat detection and response coupled with risk visibility across the threat landscape.



Mobile alerts and threats mapped into incidents. Using AI to filter out false positives and noise, the integration shares threat and incident data with Falcon Next-Gen SIEM where it can be combined with other endpoint data to speed response.



Ability to Respond to Targeted Campaigns, Not Isolated Events: Zimperium's industry-leading mobile threat intelligence is combined with CrowdStrike's automated security insights, all mapped to the MITRE ATT&CK framework.

The Challenge

Cybercriminals have adopted a "mobile first" attack strategy, using AI-driven phishing, advanced malware and compromised mobile apps to steal credentials, access sensitive data and penetrate enterprise networks.

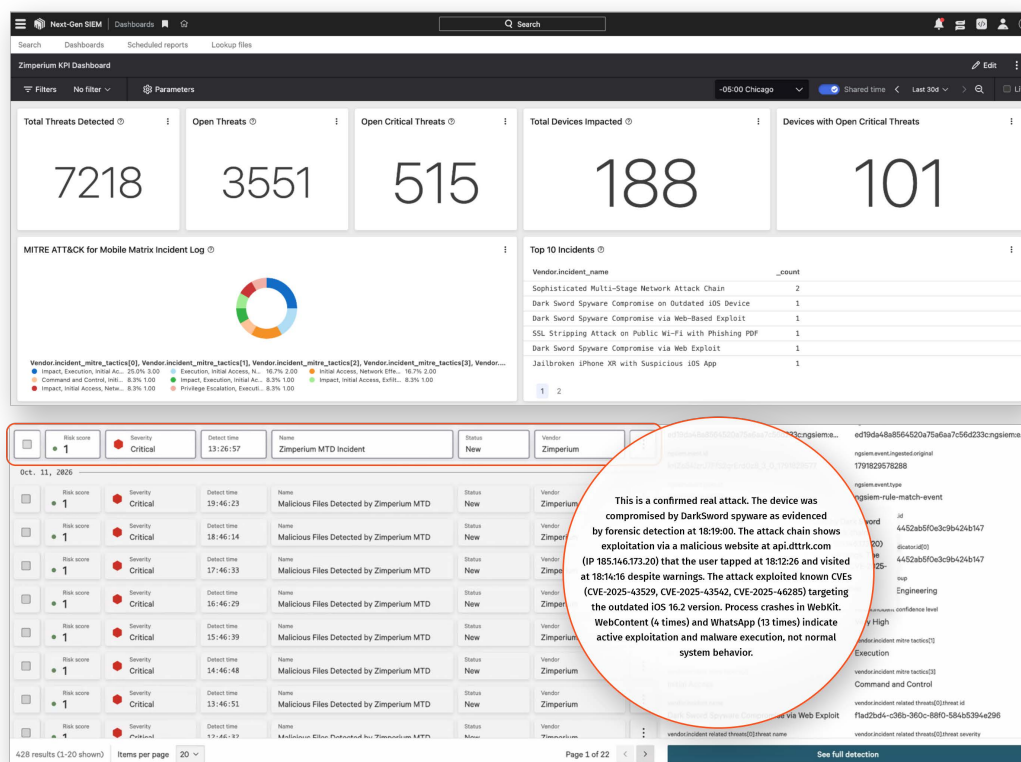
Legacy mobile security solutions often lack key functional capabilities, including the ability to vet mobile applications on the device, which may contain malware or escalated privileges, as well as undisclosed and non-compliant AI that can access sensitive enterprise data. Security teams, which often have limited mobile expertise, are left with little visibility into these mobile threats, slowing the response to multi-vector attacks on the business.

The Zimperium + CrowdStrike Integration Solution

By leveraging Zimperium's AI-Empowered Mobile Threat Defense (MTD) Platform integration with CrowdStrike's Falcon Next-Gen SIEM, organizations can achieve ultimate endpoint security that stops mobile attacks, provides a single pane of glass to see across the entire enterprise threat landscape, and speeds response to multi-vector attacks.

Benefits and Outcomes

- **Seamless Integration with Falcon Next-Gen SIEM** provides visibility into mobile incidents and threats alongside every other endpoint in Next-Gen SIEM.
- **Mobile Security Expertise** enabled for your SOC and Security analysts powered by the world's leading mobile threat intelligence across 500M+ devices and more than 1,000 mobile apps.
- **On-Device and AI-empowered Phishing Defense** protects employee credentials and sensitive enterprise data from AI-enabled social engineering attacks across email, SMS, QR codes and third-party messaging apps.
- **Continuous App Vetting** of every app on the mobile device, identifying non-compliant and malicious apps before they become the entry point.
- **Zero Day Defense** against malware and exploits utilizing on-device AI.
- **AI Governance and Visibility** identifies Shadow AI on mobile devices including unapproved AI app usage and undisclosed, risky AI residing inside of approved apps.
- **Advanced Mobile Forensics & Automated SOC analysis** accelerates detection, investigation and response to security incidents.



DarkSword Mobile Incident Displayed in Falcon Next-Gen SIEM

Use Cases

Use Case	Solution	Benefit
 Phishing attack correlation across mobile and desktop	The SOC is able to correlate any detections across both mobile and traditional desktops to improve visibility of compromises and take action.	Improved phishing attack prevention and response due to expanded threat data that includes phishing attack data on mobile devices.
 High-risk network detection for mobile extending to laptops	SOC teams can now correlate network threats from Zimperium with potential laptop access. Any risky network connections identified by Zimperium can now be used to scan laptop access information to alert on those connections and take further action.	Improved threat awareness and attack surface information due to data from mobile connections to unknown networks that laptops may also have connected to.
 Malicious PDF document detection	Zimperium shares malicious PDF detections from MTD protected devices with the Falcon NG-SIEM to provide SOC teams the ability to correlate the risky PDF with other endpoints throughout the enterprise.	Enterprise reduces risk from malicious PDFs with enhanced visibility from mobile attack surface.
 Zero trust signals from mobile devices	Risk signals from Zimperium protected devices are shared with Falcon NG-SIEM and its rich-set of other zero trust integration partners, such as identity providers, enabling the enterprise to apply dynamic access control policies based on specific threats and threat-types.	Enterprise can require reauthorization by users whose mobile devices risk posture is questionable.

Available Now from the CrowdStrike Marketplace

Implementing the integration is easy. Visit the [CrowdStrike marketplace](#) to get started.

Learn More

Contact your Zimperium representative to learn more about the CrowdStrike integration and how it can benefit your organization.

About Zimperium

Zimperium is the world leader in AI-empowered mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous security that counters evolving threats including phishing, malware, and zero-day attacks.

To learn more about securing your mobile fleet against advanced AI powered messaging threats, visit

www.zimperium.com.



Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc

4055 Valley View, Dallas, TX 75244

© 2026 Zimperium, Inc. All rights reserved.