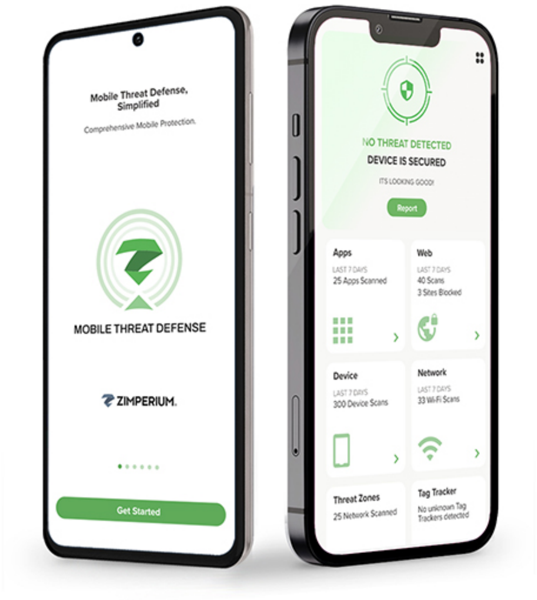
ZIMPERIUM®

Enterprises and Government Agencies Choose Zimperium Over Crowdstrike Falcon for Mobile

As enterprises and government agencies remain prime targets for attacks, mobile protection that only meets the minimum security requirements or “checks the box” is not enough to secure critical infrastructures and sensitive data. Organizations must adopt a platform like Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - to strengthen their cybersecurity, especially when enabling remote data access and productivity toolsets on mobile devices. Zimperium’s conditional access integration allows organizations to verify if the device is safe and protected before allowing access to mobile productivity tools like Microsoft Office 365, reducing friction with zero-touch activation.

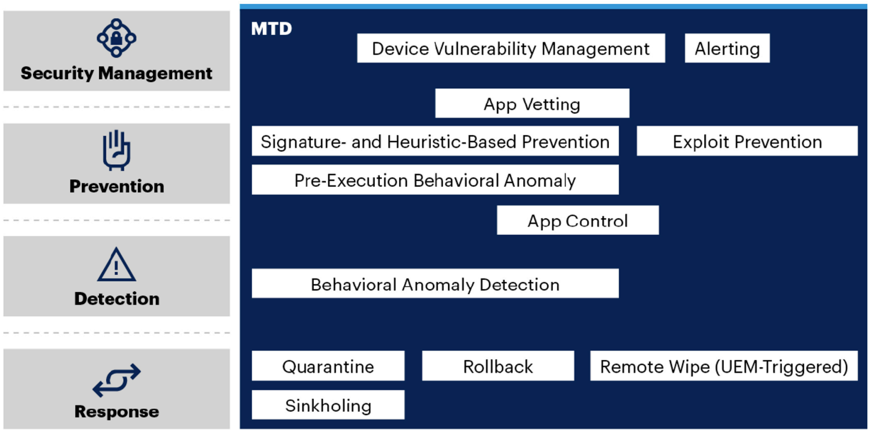


Gartner defines mobile threat defense solutions as having features like OS and application risks, threat forensics, zero-day detection capabilities, network attack detection and prevention, and agnostic EMM integration support. Organizations considering Crowdstrike Falcon for Mobile for mobile security should analyze key technical capabilities that Gartner considers fundamental to a mobile threat defense solution., along with third-party integrations into UEM, SIEM, and other management consoles.

Mobile Threat Defense According to Gartner

When compared to the Gartner definition of mobile threat defense, Falcon for Mobile fails to meet the Gartner definition in many ways, including the lack of these fundamental and foundational requirements:

- Device vulnerability management
- App vetting
- Mobile phishing protection
- Device attack protection
- Web content filtering
- Network attack protection
- Agnostic integrations with third-party systems



Security Management

Prevention

Detection

Response

MTD

Device Vulnerability Management

Alerting

App Vetting

Signature- and Heuristic-Based Prevention

Exploit Prevention

Pre-Execution Behavioral Anomaly

App Control

Behavioral Anomaly Detection

Quarantine

Rollback

Remote Wipe (UEM-Triggered)

Sinkholing

Source: Gartner (2022)

> ***"Mobile threat defense products not only prevent attacks but also detect and remediate them. Mobile threat defense focuses on identifying and thwarting malicious threats, rather than relying on device management configuration to protect against simple user mistakes. Mobile threat defense products offer protection beyond the device and app restrictions that UEM tools offer."***
>
> **– Gartner**

Did you know?

- **100% of Zimperium customers use device OS upgrades, PIN enforcements, and Data Access Controls.**
- **90% of Zimperium customers have reported a rooted or jailbroken device in the last 12 months.**
- **Zimperium console and APIs provide detailed forensics enabling SOC teams to consumer rich telemetry, improving visibility, threat hunting, and overall posture of security.**
- **One customer reported: Zimperium MTD blocked multiple Android users with multiple malicious apps, saving them hours of remediation and potential fines.**

Don’t Just Check the Box, Secure the Box

Productivity, management, and security are top concerns that organizations have when deciding whether to leverage Falcon for Mobile. Security teams need a comprehensive mobile security platform to secure critical infrastructure and sensitive data.

			Zimperium	CrowdStrike
Mobile Endpoints – iOS, Android, ChromeOS	**Phishing**	On-Device mobile phishing detection	**Yes**	**No**
		Cloud-based mobile phishing detection	**Yes**	**Yes**
		Known phishing URLs	**Yes**	**Yes**
		Unknown phishing URLs (Zero-days)	**Yes**	**No**
	Apps	Sideloaded app detection	**Yes**	**Yes**
		Enterprise app compliance and detection policies	**Yes**	**No**
		Known malware	**Yes**	**Android Only**
		Unknown malware (Zero-days)	**Yes**	**No**
		Offline malware detection	**Yes**	**No**

			Zimperium	CrowdStrike
Mobile Endpoints – iOS, Android, ChromeOS	**Network**	Provide detailed app risk and privacy analysis	**Yes**	**No**
		Fine grained privacy controls (e.g., GDPR,BYOD)	**Yes**	**No**
		Network attack detection (e.g. MITM)	**Yes**	**No**
		Reconnaissance scan detection	**Yes**	**No**
		Insecure/Risky/Networks/Rogue Access Point Detections	**Yes**	**No**
	Device	Offline Remediation w/o MDM/UEM	**Yes**	**No**
		Remediation with MDM/UEM integration	**Yes**	**No**
		Advanced compromised / Elevation of privilege detection	**Yes**	**No**
		Detailed mobile threat intelligence and forensics	**Yes**	**Limited**
		Device risks (e.g. PIN, OS, Encryption, etc)	**Yes**	**Yes**
		Malicious profile detection	**Yes**	**No**
		Protect devices across multiple UEMs in a single tenant	**Yes**	**No**
		Provide advanced protection for Samsung KNOX devices (DLP)	**Yes**	**No**
		Personal info does not need to be pulled from the device and transferred to the cloud for analysis	**Yes**	**No**

About Zimperium

Founded upon the premise that mobile security requires an entirely novel approach, Zimperium secures both mobile devices and applications so they can safely and securely access data. Zimperium provides the only mobile security platform purpose-built for enterprise environments. With machine learning-based protection and a unified platform that secures everything from applications to endpoints, Zimperium's solutions provide on-device mobile threat defense and comprehensive in-app protection to protect growing and evolving mobile environments. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank Corp.

Find additional information or contact us at zimperium.com.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244