

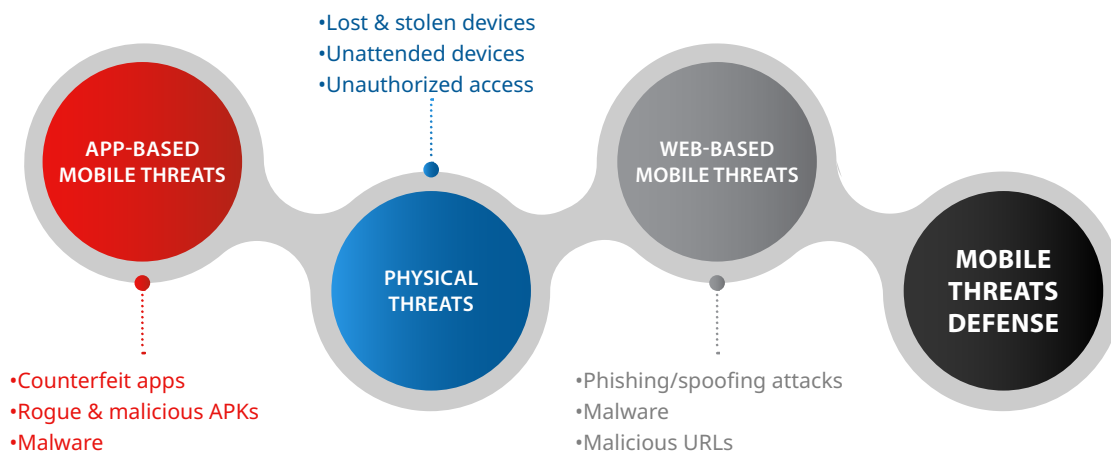
WATCHGUARD MOBILE SECURITY



SMALL DEVICES CAN CAUSE BIG PROBLEMS

With the large and diverse mobile threat landscape, businesses require enterprise mobile security solutions. This is especially true as the new hybrid workplace, with remote and work-from-home options, makes these mobile devices a more common and critical component of an organization's IT infrastructure.

It's more critical than ever for organizations to secure endpoints and their data to prevent suffering data breaches and unauthorized access to sensitive information.

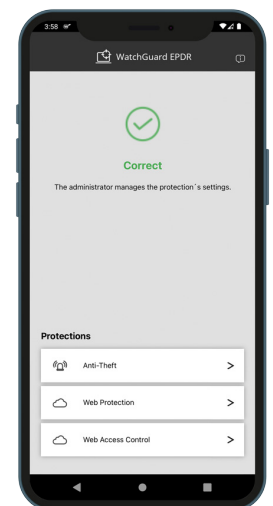


WHY MOBILE SECURITY?

WatchGuard Mobile Security allows organizations to centrally manage the security and confidentiality of the data stored on their Android and iOS smartphones and tablets without requiring specific technical knowledge or dedicated on-premises security servers. Additionally, they provide tools available anytime, anywhere to protect mobile devices against malware, loss and theft.

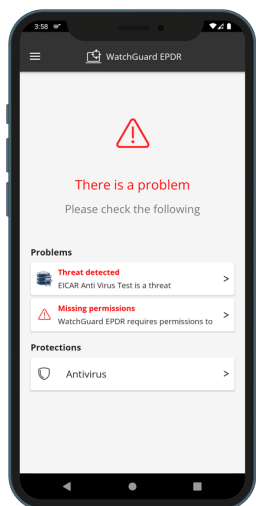
Productivity Has Gone Mobile

- Corporate data is being increasingly accessed on mobile outside the corporate perimeter and employees working remotely have hastened the pace of mobile adoption within enterprises.
- Securing mobile devices in the enterprise is just half the challenge. The other is ensuring that employees are able to work productively.
- Make employees feel confident about the security of their mobile devices and provide a modern workplace where security and productivity play an equal role.



Potential Mobile Cyber Threats

- Physical threats to mobile devices most commonly refer to the loss or theft of a device, enabling hackers to have direct access to the hardware where private data is stored.
- Application-based threats: users download apps that look legitimate but actually skim data from their device.
- Web-based threats: users visit affected sites that seem fine on the front-end but, in reality, automatically download malicious content onto devices. Mobile phishing attempts continue to grow each year.



Mobile Device Management (MDM) Isn't Enough

- MDM is a management tool for the administration of mobile devices, not for security. MDM matters, but it's just one piece.
- Bring your own device (BYOD) policies are a real challenge for security professionals since the impact of a wrong click from the user can bring serious consequences. As malware advances and evolves, it's harder to spot a threat once it's inside the network.
- WatchGuard Mobile Security can detect and block mobile cybersecurity threats from harming your organization.

IMPROVING ENTERPRISE MOBILE SECURITY

CATEGORIES	FEATURES	ANDROID	iOS
Security Policy	Network Access Enforcement	✓	
Malware Scan	Malicious APKs scan	✓	
	Malware URLs*		✓
	On-demand scans	✓	
	Scheduled scans	✓	
	Real-time antivirus protection	✓	
Web Protection	URL filtering*		✓
	Anti-phishing*		✓
Anti-Theft	Remote locking	✓	✓
	Remote wipe	✓	✓
	Geolocation	✓	✓
	Snap the thief	✓	
	Remote alarm	✓	✓
Unified Security Reporting	Alerts for malware	✓	✓
	Alerts for unprotected devices	✓	✓
	Centralized reports	✓	✓
Deployment	Without MDM	✓	✓
	WatchGuard in-house MDM		✓
	3rd party MDM	✓	✓
	Supervised/ unsupervised devices		✓
	Protection upgrades	Google Play	Apple Store

*The iOS Supervised mode allows admins to use these additional features, while the unsupervised will only allow the basic ones.

Compatible solutions within the Endpoint Security Platform for Android and iOS:



[System Requirements for Android](#)

[System Requirements for iOS](#)