# CHECK POINT
# MOBILE THREAT PREVENTION

## BENEFITS

- Deploy any iOS or Android mobile device on your organization's network with confidence.
- Protect sensitive information on mobile devices from cyber espionage
- Improve visibility and protection against the latest mobile threats with mobile security that integrates easily into your existing mobility and security infrastructures (MDM, MAM, NAC, SIEM, etc.)
- Augment the security measures of Microsoft Exchange and container/wrapper solutions
- Enable rapid response to cross-platform advanced persistent threat (APT) attacks
- Enable contractors to access corporate data safely from unmanaged devices
- Preserve user experience and privacy, while adding the protection required by organizational or regulatory mandates.

## DETECT AND STOP ATTACKS BEFORE THEY START

Smartphones and tablets give us unprecedented access to the critical business information we need to work faster and more accurately. Providing your employees with access to that information on the mobile devices they choose has many benefits, but it also exposes your business to risk.

Check Point Mobile Threat Prevention, an innovative approach to mobile security for iOS and Android devices that detects and stops mobile threats before they start. Whether your data's at rest on a device or in flight through the cloud, Mobile Threat Prevention helps protect you from vulnerabilities and attacks that put data at risk.

## HIGHEST LEVEL OF MOBILE SECURITY FOR THE ENTERPRISE

Only Check Point provides a complete mobile security solution that protects devices from threats on the device (OS), in applications, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. Mobile Threat Prevention uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning.

It safeguards devices from unprotected Wi-Fi® network access and Man-in-the-Middle attacks and stops access to the corporate network when a threat is detected. It uses real-time risk assessments at the device-level (OS) to reduce the attack surface by detecting attacks, vulnerabilities, changes in configurations, and advanced rooting and jailbreaking. Its dynamic threat response prevents compromised devices from accessing an organization's network, and allows organizations to set adaptive policy controls based on unique thresholds for mitigation and elimination of threats on the device.

### Advanced app analysis

You can trust your employees to access your sensitive business assets, but can you trust their apps? Our solution captures apps as they are downloaded to devices, and runs each in a virtual, cloud-based environment to analyze its behavior before being approved or flagged as malicious. Our easy to understand, exportable analysis reports helps your security teams ensure apps employees use are safe.

### Network-based attacks

Public places are filled with open Wi-Fi networks, making it difficult to know which networks are safe and which aren't. Cybercriminals can use these networks to hijack smartphones and tablets, assuming control of devices and valuable data like messages, files, and network credentials. Our solution detects malicious network behavior and conditions, and automatically disables suspicious networks to keep devices and your data safe.


August 6, 2015

### Device vulnerability assessments

Cyber criminals make it their business to know the weakest link in your security before you do. That often includes weaknesses in operating systems and apps that other security solutions may not detect. Our solution continuously analyzes devices to uncover vulnerabilities and behaviors cyber criminals use to attack devices and steal information. With better visibility into the threats mobile devices face, you can reduce your overall attack surface and your risk.

## FULL MOBILE THREAT VISIBILITY AND INTELLIGENCE

Mobile Threat Prevention's cloud-based dashboard makes managing supported devices and controlling mobile threats fast and easy. It provides security and mobility teams with real-time threat intelligence and visibility into the quantity and types of mobile threats that could impact their business or users.

### Integrate intelligence with existing systems

Mobile Threat Prevention's stream of real-time threat intelligence pushes to Check Point SmartEvent automatically for monitoring of security events and for correlation with attacks on internal networks. There, this information is shared and correlated in Check Point's Threat Cloud, providing the broadest set of threat intelligence that can be used within network environments to prevent cyber attacks from occurring. Threat intelligence can also be fed into existing enterprise systems like your security information and event management (SIEM) platform. This includes detailed logs and other indicators of compromise that can be filtered to trigger response actions that help your security team take action quickly to control and eliminate risk.

## DEPLOYING MOBILE SECURITY HAS NEVER BEEN EASIER

Security and mobility teams have enough to worry about. That's why Mobile Threat Prevention is designed to help them secure mobile devices quickly and confidently through integration and cooperation with MDM or EMM solutions. That helps make the solution highly scalable, and delivers strong operational and deployment efficiencies for managing mobile security within a broader security infrastructure.

### Deploy advanced mobile security with ease

Whether you support 300 or 300,000 devices, integrating our solution with your MDM is fast and easy. Deployment and management can be done through your MDM automatically, accelerating adoption and reducing overall operational costs. Our solution scales with your MDM, seamlessly protecting mobile devices you enroll and removing capabilities for those you delete. As a result, you can rest assured you have the layers of security you need to both manage and protect mobile devices, even in a highly dynamic environment.

### Mitigate and eliminate threats right on the device

When a threat is identified, our solution automatically mitigates any risk until the threat is eliminated. If a threat can be eliminated on a device immediately, users are notified about and prompted to take action, like deleting malicious apps or disconnecting from hostile networks. Integration with your MDM allows the solution to restrict secure container access, or make real-time, risk-based policy adjustments on compromised devices that MDMs on their own can't make. Our solution can also activate an on-demand VPN to tunnel data traffic away from cyber criminals and to avoid data exfiltration while still keeping users connected.

### Respect user privacy and device performance

End-user privacy is critical, so we never analyze files, browser histories, or application data. Our solution uses state and context metadata from operating systems, apps, and networks to determine if a device is compromised. It anonymizes the data it uses for analysis to keep it and security intelligence information separated. Our analysis is performed in the cloud to avoid impacting device performance, and since protection runs in the background, so users are stay protected without having to learn anything new.

## For more information, visit checkpoint.com/mobilesecurity.

CONTACT US

**Worldwide Headquarters** | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com


August 6, 2015