SOLUTION BRIEF
MAAS360 AND CHECK POINT MOBILE THREAT PREVENTION

BENEFITS

- Keep business assets and sensitive information on iOS and Android smartphones and tablets safe from cyber attacks
- Automate threat detection and mitigation on mobile devices employees use for work
- Simplify and lower the operational costs of deploying and managing comprehensive security for mobile devices

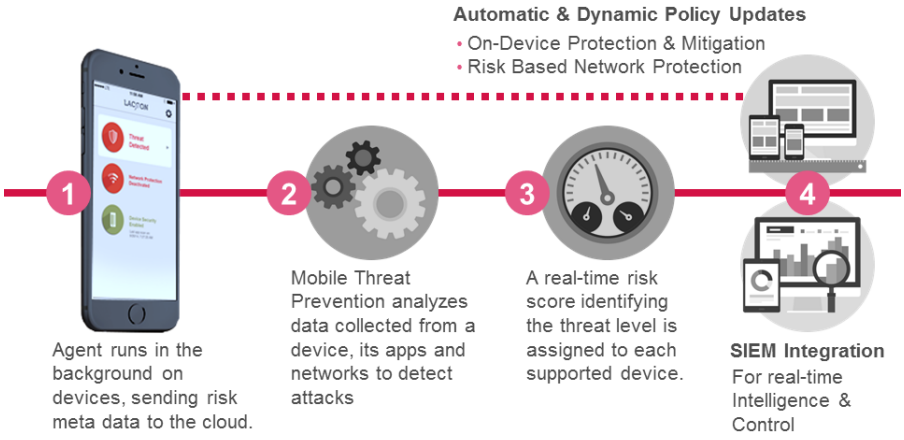
Check Point Mobile Threat Prevention is an innovative approach to mobile security that detects and stops attacks on iOS and Android mobile devices before they start. Combined with IBM MaaS360® Enterprise Mobile Management, the solution provides dynamic security that helps keep assets and sensitive data secure.

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 apps, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. Integration with MaaS360 enables automatic threat mitigation by adjusting mobile device policies based on the risk to a device and your unique security needs. This prevents compromised devices from accessing sensitive corporate information and the enterprise network.

HOW IT WORKS

DELIVERING COMPREHENSIVE THREAT PREVENTION FOR iOS AND ANDROID



Advanced app analysis

Capture and run apps downloaded on mobile devices in a virtual, cloud-based environment to analyze their behavior then approve or flag them as malicious.

Network-based attacks

Detect malicious network behavior and conditions, and automatically disable suspicious networks to help keep mobile devices and data safe.

Device vulnerability assessments

Analyze devices to uncover vulnerabilities and behaviors that cyber criminals can. use to attack mobile devices and steal valuable, sensitive information

February 18, 2016

DETECT AND MITIGATE ADVANCED THREATS AUTOMATICALLY

When a threat is identified, the integrated Check Point and MaaS360 solution automatically mitigates 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 compromised networks. Integration with your MaaS360 MDM allows Mobile Threat Prevention to make real-time, risk-based policy adjustments on compromised devices, like blocking access to a secure container.

Threat-Based Mitigation Actions

When a high-risk, malicious application is identified on a device, Mobile Threat Prevention triggers Maas360 to block access from that device to email and other corporate applications to keep data safe until the application is removed and the threat eliminated. Once removed, the profile(s) will automatically be re-activated so that the device will regain normal access to email and other apps.

DEPLOY AND MANAGE MOBILE SECURITY EASILY AND COST EFFECTIVELY

Security and mobility teams have enough to worry about. So whether you support 300 or 300,000 devices, this integrated and highly-scalable solution was designed to help teams secure mobile devices quickly and confidently. 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. It delivers strong operational efficiencies for managing mobile security within a broader security infrastructure and allows deployment and management inside your existing MaaS360 console.

Automatic App Deployment & Enforcement

Configure MaaS360 to enforce enrolled devices to install the Mobile Threat Prevention app by setting it as a required application. The app is pushed to the device along with registration details, allowing for easy one-click installation for the end-user. If the app is not installed, the device is blocked from corporate resources using automatic compliance rules and actions configured in MaaS360. Users will receive a MaaS360 pop-up message, and clicking it will automatically deploy the Mobile Threat Prevention app. You can also periodically check and enforce device updates with MaaS360 and update the Mobile Threat Prevention app on devices accordingly.

Automated Device Management

Automatically protect new devices as soon as they are in enrolled in MaaS360. Devices are also automatically deleted once they have been removed or retired from MaaS360.

LEARN MORE

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

February 18, 2016