Check Point
SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

HARMONY MOBILE AND MICROSOFT INTUNE
SOLUTION BRIEF

Microsoft

Benefits

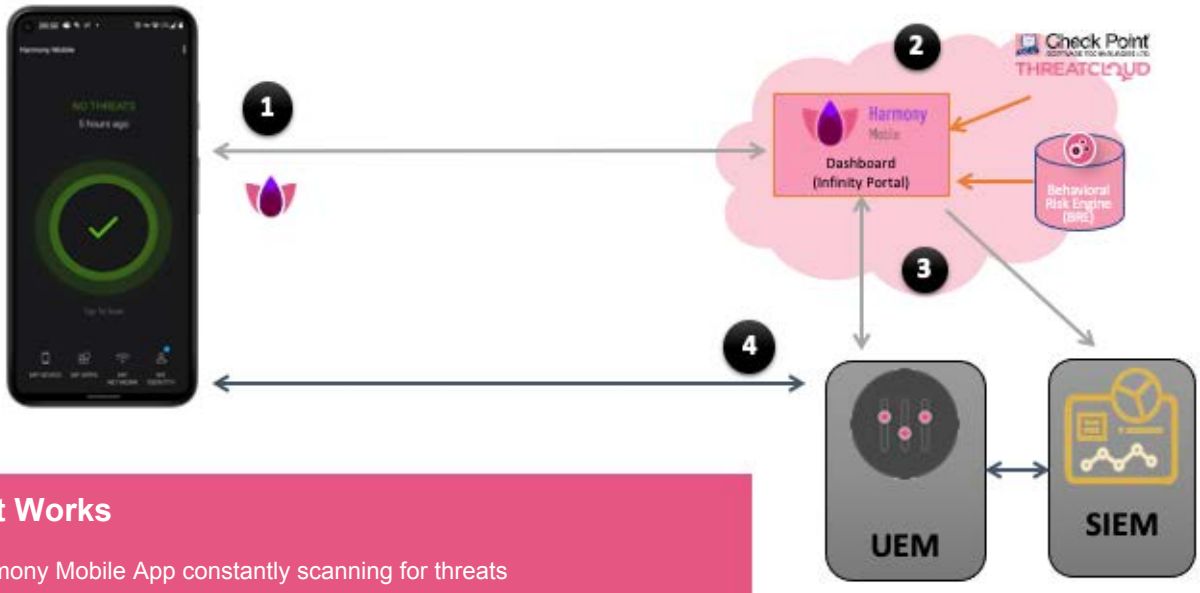
- Complete threat detection and mitigation, the best mobile catch rate, and full visibility.
- Keeps business assets and sensitive data on devices safe from cyber attacks
- Simple deployment and seamless integration with all leading UEM vendors

Check Point Harmony Mobile is an innovative approach to mobile security that detects and stops attacks on iOS and Android mobile devices before they start. Combined with Microsoft Intune®, 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 Microsoft Intune enables automatic threat mitigation by adjusting mobile device policies based on the security posture of a device and your unique security needs. This prevents compromised devices from accessing sensitive corporate information and the enterprise network.

Advanced app analysis
The Behavioral Risk Engine runs downloaded apps in a virtual, cloud-based environment to analyze their behavior and then approve or flag them as malicious.



How it Works

1. Harmony Mobile App constantly scanning for threats
2. Harmony Mobile analyzes the device state, applications & network using indicators from the BRE and ThreatCloud
3. The device security score is sent to the UEM/MDM in real-time
4. The UEM/MDM manages the device and applies mitigation

© 2021 Check Point Software Technologies Ltd. All rights reserved.

Network-based attacks
Harmony Mobile detects malicious network behavior and conditions, and alerts the user to help keep mobile devices and data safe. On-device Network Protection (ONP) allows businesses to stay ahead of emerging threats by extending Check Point's industry-leading network security technologies to mobile devices. Harmony Mobile offers a broad range of network security capabilities, including Anti-Phishing with Zero day Phishing - Blocks phishing attacks across all apps, both from known and unknown zero-day phishing sites, and sites that use SSL, Safe Browsing - Blocks access to malicious sites from any web browser, leveraging the dynamic security intelligence provided by Check Point's ThreatCloud™, Download Prevention, Conditional Access, Anti-Bot, URL Filtering & also Protected DNS are all additional layers of protection that prevents common network attacks and allow the organization to stay ahead of new and emerging Gen V threats.

Device vulnerability assessments
Harmony Mobile analyzes devices to uncover vulnerabilities and behaviors that cyber criminals can use to attack mobile devices and steal valuable, sensitive information.

DEPLOY AND MANAGE MOBILE SECURITY EASILY AND COST EFFECTIVELY

Security and mobility teams have enough to worry about. Therefore, 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. Microsoft Intune UEM and Harmony Mobile deliver strong operational efficiencies for managing mobile security within a broader security infrastructure and allow deployment and management inside your existing Microsoft Intune console.

Automatic App Deployment & Enforcement
Configure Microsoft Intune to enforce enrolled devices to install the Harmony Mobile app by setting it as a required application. Fast deployment is key for the success of protecting the mobile devices fleet. This innovative and unique solution from Check Point allows Harmony Mobile app to be automatically activate by itself without any device end user involvement. With this deployment approach organizations no longer need to wait for users actions and can quickly activate the protection on devices using the MDM/UEM integration. If the app is not installed, the device is blocked from corporate resources using automatic compliance rules and actions configured in Microsoft Intune UEM. Users will receive a Microsoft Intune in-app notification, and clicking it will automatically deploy the Harmony Mobile app. You can also periodically check and enforce device updates with Microsoft Intune UEM and update the Harmony Mobile app on devices accordingly.

Mitigate and eliminate threats right on the device
When a threat is identified, Harmony Mobile automatically mitigates any risk until the threat is eliminated. Integration with your UEM platform allows the solution to restrict secure container access, or make real-time, risk-based policy adjustments on compromised devices that UEMs on their own can't make. Harmony Mobile also activates an on-demand VPN to tunnel data traffic away from cybercriminals and to avoid data exfiltration while still keeping users connected.

Automated Device Management
Automatically protect new devices as soon as they are enrolled in Microsoft Intune. Devices are also automatically deleted from Harmony Mobile once they have been removed or retired within Microsoft Intune.

)RUPRUHLQIRUPDWLRQYLVLWKWWSRLQWRPPRELOHVHFXULW\

© 2021 Check Point Software Technologies Ltd. All rights reserved.
October 10, 2021