Network-based attacks
Harmony Mobile detects malicious network behavior and conditions, and alerts the user to help keep mobile devices and data safe. Harmony Mobile's unique network security infrastructure –On-device Network Protection– allows businesses to stay ahead of new and emerging Gen V threats by extending Check Point's industry-leading network security capabilities to mobile devices. The Harmony Mobile application constantly validates traffic on the device itself without routing the data through a corporate gateway. This ensures user and data privacy, allowing for a seamless browsing experience.

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. Google Workspace and Harmony Mobile deliver strong operational efficiencies for managing mobile security within a broader security infrastructure and allow deployment and management inside your existing Google Workspace UEM console.

Automatic App Deployment & Enforcement
Configure Google Workspace to enforce enrolled devices to install the Harmony Mobile 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 Google Workspace UEM. Users will receive a Google Workspace in-app notification, and clicking it will automatically deploy the Harmony Mobile app. You can also periodically check and enforce device updates with MaaS360 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 Google Workspace UEM. Devices are also automatically deleted from Harmony Mobile once they have been removed or retired within Google Workspace.

For more information, visit checkpoint.com/mobilesecurity