Check Point
SOFTWARE TECHNOLOGIES LTD

SOLUTION BRIEF

CHECK POINT SANDBLAST MOBILE AND ANDROID ENTERPRISE

OVERVIEW

Check Point SandBlast Mobile is an innovative approach to mobile security that detects and stops attacks on mobile devices before they start. Combined with Android Enterprise, the solution protects against mobile threats like malware, web, and network attacks on both corporate-owned Android devices and personally-own Android devices. The combined solution offers the best protection while respecting the employee's privacy.

BENEFITS

- Secure corporate data while respecting employee's privacy
- Secure all Android Enterprise deployment types
- Protect against mobile threats on both work and personal profile
- Separate policy for work and personal profiles

MOBILE THREATS ARE RELEVANT IN ALL DEPLOYMENT OPTIONS

Android devices support a data separation model called a work profile (from Android 5.1.1 Lollipop and later). The work profile contains all corporate applications and data and ensures that the data is separated from any personal apps and data a user may have.

While data segregation is very important, it doesn't remove mobile threats. All known mobile attack vectors are still relevant. For example, malware installed on a personal profile may take advantage of Android's Accessibility Services (AAS) and read sensitive date from the work profile's screen. It can passively collect anything the user types in, including credentials and passwords, two-factor authentication data, fill forms on behalf of the user and even grant itself additional permissions without user assistance. The AAS permissions can't be revoked by UEM solutions; however, SandBlast Mobile prevents all kinds of known mobile malware on both work and personal profiles, including AAS-based attacks.

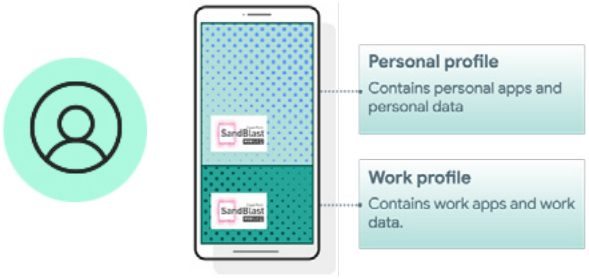
Phishing attacks are another type of threat that is still relevant in secure containers. The mobile phishing vectors include corporate emails, personal emails, SMS messages, messaging applications and web browsing in both work and personal profile. Malicious websites can exploit vulnerabilities in the browser to gain access to both work and personal profiles, install malware on the device, change the device's configuration and take over the device remotely. SandBlast Mobile detects both known and unknown phishing attacks and blocks them on both work and personal profiles.

SANDBLAST MOBILE SECURES IN EVERY DEPLOYMENT SCENARIO

Personally-owned devices

Personally-owned devices that are also used for work (BYOD) can be set up with a work profile that allows work apps and data to be stored in a fully managed separate, self-contained space within a device. In this deployment, the organization has no visibility or access to a device's personal profile. However, malware on the personal space can still compromise corporate data on the work profile.

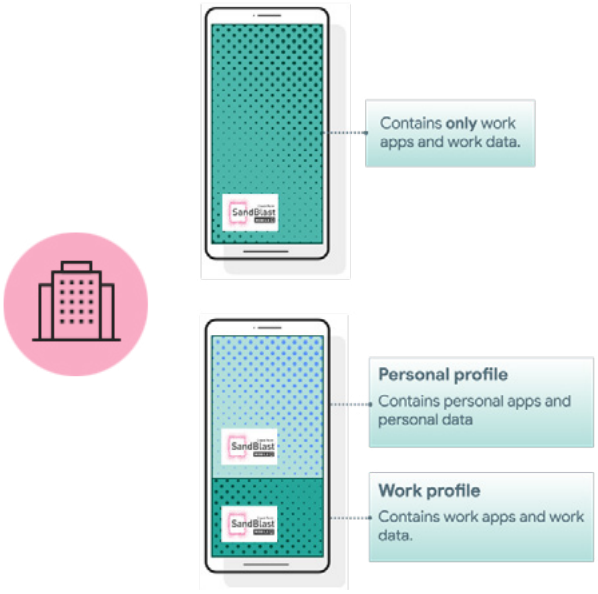
For example, it can record calls or collect messages from the work profile. Therefore, Check Point recommends protecting the entire device. SandBlast Mobile can protect both the personal data and corporate data and enforce different policies for each.



Corporate-owned devices

Organizations can exercise full management control over the Android devices they own and issue to employees. There are three deployment options available for these types of company-owned devices: fully managed, fully managed with a work profile that allows organizations to enforce two separate sets of policies for work and personal profiles, and fully-managed devices dedicated to a set of apps.

SandBlast Mobile supports all possible Android Enterprise deployment modes. The solution can be deployed on both profiles with a dedicated entity that allows using different policies for each profile. Since malware on the personal profile can compromise data on the work profile, Check Point recommends protecting both profiles.



Summary

SandBlast Mobile provides full protection for all Android Enterprise deployment use cases. To prevent corporate data loss, compromise of sensitive information, and attempts to access the corporate's network, Check Point recommends protecting both the work profile and the personal profile. SandBlast Mobile protects both types of profiles using a single license.

Learn more: https://www.checkpoint.com/products/mobile-security