SOLUTION BRIEF
MICROSOFT ENTERPRISE MOBILITY + SECURITY AND CHECK POINT SANDBLAST MOBILE

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

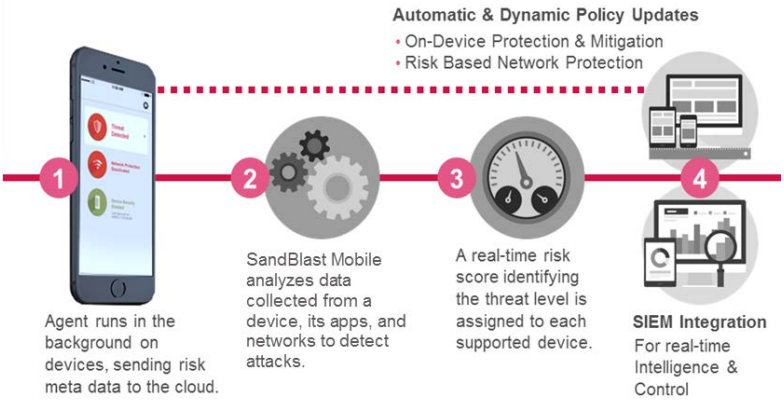
Check Point SandBlast Mobile is an innovative approach to mobile security that detects and stops attacks on iOS and Android mobile devices before they start. Combined with Microsoft Enterprise Mobility + Security (EMS), the solution provides dynamic security that helps keep assets and sensitive data 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, in the network, and in SMS messages, and delivers the industry's highest threat catch rate for iOS and Android. Integration with Microsoft EMS enables automatic threat mitigation by adjusting mobile device conditional access 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.

SMS Phishing attacks

Detect malicious SMS Phishing messages, also known as SMiShing, to block when malicious links are sent to mobile devices through SMS messaging.

April 20, 2017

DETECT AND MITIGATE ADVANCED THREATS AUTOMATICALLY

When a threat is identified, the integrated SandBlast Mobile and Microsoft EMS 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, disconnecting from compromised networks, or blocking malicious links in SMS messages. Integration with your Microsoft EMS allows SandBlast Mobile to make real-time, risk-based policy adjustments on compromised devices, such as blocking access to email and other corporate applications.

Threat-Based Mitigation Actions

When a high-risk, malicious application is identified on a device, SandBlast Mobile triggers Microsoft EMS to take action, such as block access from that device to email and other corporate applications, to keep data safe until the application is removed and the threat eliminated. The user is notified by SandBlast Mobile through the SandBlast Mobile Protect app with information on why the device is at high risk and instructions on how the user can mitigate the issue. 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 Microsoft EMS portal via Azure AD Management portal.

Automatic App Deployment & Enforcement

Configure Microsoft EMS to enforce enrolled devices to install the SandBlast Mobile Protect 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 Microsoft EMS. Users will receive a Microsoft EMS pop-up message, and clicking it will automatically deploy the SandBlast Mobile Protect app. You can also periodically check and enforce device updates with Microsoft EMS and update the SandBlast Mobile Protect app on devices accordingly.

Automated Device Management

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

LEARN MORE

FORTIFY24x7.COM/MOBILESECURITY

CONTACT US **Fortify 24x7** | 2067 Apa Road, Point Roberts, WA 98281 USA | Tel: (800) 989-2647 | Fax: 650-362-2121 | Email: info@fortify24x7.com

April 20, 2017