Check Point
SOFTWARE TECHNOLOGIES LTD

AVIZENT
Network Solutions

SandBlast Mobile

Mobile Security: Robust, Agile, Transparent

Mobile security is a top concern for every company these days — and for a good reason. In the new normal, your remote workers increasingly access corporate data from their mobile devices, and that means you're exposed to data breaches more than ever.

SandBlast Mobile is the market-leading Mobile Threat Defense solution. It keeps your corporate data safe by securing employees' mobile devices across all attack vectors: apps, network and OS. Designed to reduce admins' overhead and increase user adoption, it perfectly fits into your existing mobile environment, deploys and scales quickly, and protects devices without impacting user experience nor privacy.

KEY PRODUCT BENEFITS

Complete Protection: Protect corporate data across all mobile attack surfaces

Simple Management: Scalable and easy-to-manage security for any type of mobile workforce

User Friendly: Quick user adoption with zero impact on user experience or privacy

UNIQUE PRODUCT CAPABILITIES

- Prevents malicious app downloads
- Prevents phishing across all apps
- Prevents Man-in-the-Middle attacks
- Blocks infected devices from accessing corporate apps
- Detects advanced jailbreaking and rooting techniques and OS exploits

The Market-Leading Mobile Threat Defense Solution

IDC ANALYZE THE FUTURE

For the third consecutive year, Sandblast Mobile named a leader in the IDC MarketScape for Mobile Threat Management (MTM)

LEARN MORE

FROST & SULLIVAN

Frost Radar Best Practices Award for Growth, Innovation & Leadership

LEARN MORE

Gartner

2019 Gartner Market Guide for Mobile Threat Defense

LEARN MORE

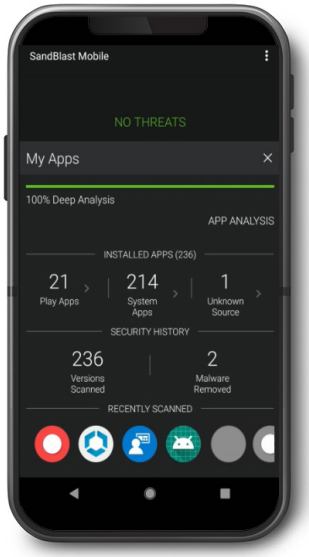
Miercom

SandBlast Mobile designated as Certified Secure, scoring the highest in competitive testing

LEARN MORE

Complete Protection

Protecting Corporate Data Across All Mobile Attack Surfaces



1. App Protection

SandBlast Mobile prevents malware from infiltrating employees' devices by detecting and blocking the download of malicious apps in real-time.

Check Point's unique Behavioral Risk Engine runs applications in a cloud-based environment to determine if an app is malicious, leveraging machine learning and AI, sandboxing, advanced static code flow analysis, anomaly detection, and app reputation among other techniques.

2. Network Protection

SandBlast Mobile's unique network security infrastructure – **On-device Network Protection** – allows businesses to stay ahead of emerging threats by extending Check Point's industry-leading network security technologies to mobile devices.

SandBlast Mobile offers a broad range of network security capabilities, including:

- **Anti-Phishing with Zero-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 ThreatCloud™
- **Conditional Access:** Blocks infected devices from accessing corporate applications and data, independent of UEM solutions
- **Anti-Bot:** Detects bot-infected devices and automatically blocks communication to command and control servers
- **URL Filtering:** Mark websites as "blocked" or "allowed", preventing access on any browser to websites deemed inappropriate by an organization's corporate policies
- **Protected DNS:** Allows administrator to manage and control all mobile device's DNS preferences. The service protects end-users privacy and prevents MiTM attacks & DNS Spoofing of plain text DNS messages.
- **Wi-Fi Network Security:** Detects malicious network behavior and Man-in-the-Middle attacks, and automatically disables connections to malicious networks.

3. OS and Device Protection

Ensures devices are not exposed to compromise with real-time risk assessments detecting attacks, vulnerabilities, configuration changes, and advanced rooting and jailbreaking.

Simple Management

Scalable And Easy-to-Manage Security For Any Type of Mobile Workforce

SandBlast Mobile **integrates with any mobile management solution (MDM/UEM) and supports any device-ownership program** (BYOD, COPE). This makes the solution **highly scalable**, delivering operational and deployment efficiencies for managing mobile security within a broader security infrastructure.

Zero-touch deployment: The on-device app installs on employees' devices with a single click and without their interaction, leveraging your existing MDM/UEM. Learn more

Tailored protection for all Android Enterprise deployment models: SandBlast Mobile protects both work and personal profiles to ensure comprehensive threat prevention. Learn more

Easy to manage: a cloud-based and intuitive management console provides the ability to oversee mobile risk posture and set granular policies. SandBlast Mobile also expands your mobile application deployment security by giving administrators an application vetting service, allowing them to upload or link applications (both Android or iOS) into the SandBlast Mobile Dashboard and receive a full app analysis report within a few minutes.

Integration

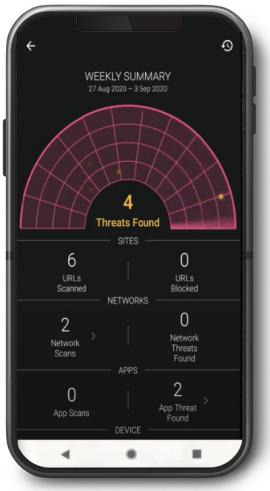
SandBlast Mobile provides out-of-the-box integration with the largest mobility technology ecosystem on the market

SandBlast Mobile Management Console

User Friendly

Quick User Adoption with Zero Impact on User Experience or Privacy

Privacy by design: user and corporate data kept completely private; no personal information is collected or analyzed at any point. SandBlast Mobile never analyzes files, browser histories, or application data. The solution uses state and context metadata from operating systems, apps, and networks to determine if a device is compromised. It anonymizes the data it uses for analysis in order to keep it protected.



Elegant user experience: no impact on device usability and browsing experience; the on-device app performs without draining battery life or data consumption.

User education: Employees become increasingly aware of mobile security risks with detailed threat real-time notifications and weekly summaries.

> *"Check Point SandBlast Mobile is incredibly easy to administer. We wanted a solution that didn't overwhelm us or require too much resource to manage."*
>
> David Wright, Head of IT Service Management, National Health Service (NHS) England

Why SandBlast Mobile?

Mobile security is no longer optional. With remote workers constantly accessing corporate data, companies are looking for a solution to keep their data protected, easily managed and without causing any disruption to their employees performance and productivity.

SandBlast Mobile addresses all those concerns providing advanced protection from all kinds of mobile threats and across all attack vectors (apps, network and OS). By using the innovative zero-touch deployment, organizations can swiftly extend their secured devices from zero to tens of thousands. Scalable to support any type of mobile workforce, the solution makes its deployment, adoption and easy to provide end-to-end threat protection without impacting user privacy.

> *"Undoubtedly the biggest benefit has been visibility. This translates into greater confidence in the security of mobile devices, and the assurance that important corporate information is accessible, yet protected. Check Point SandBlast Mobile has very user-friendly protection."*
>
> Pedro Pablo Peréz, CEO, ElevenPaths (Telefonica Group)

United Kingdom Headquarters
104 Kidmore Road, Reading RG4 7NB Tel | WhatsApp +44 7858 929 008
www.avizent.com

AVIZENT Network Solutions