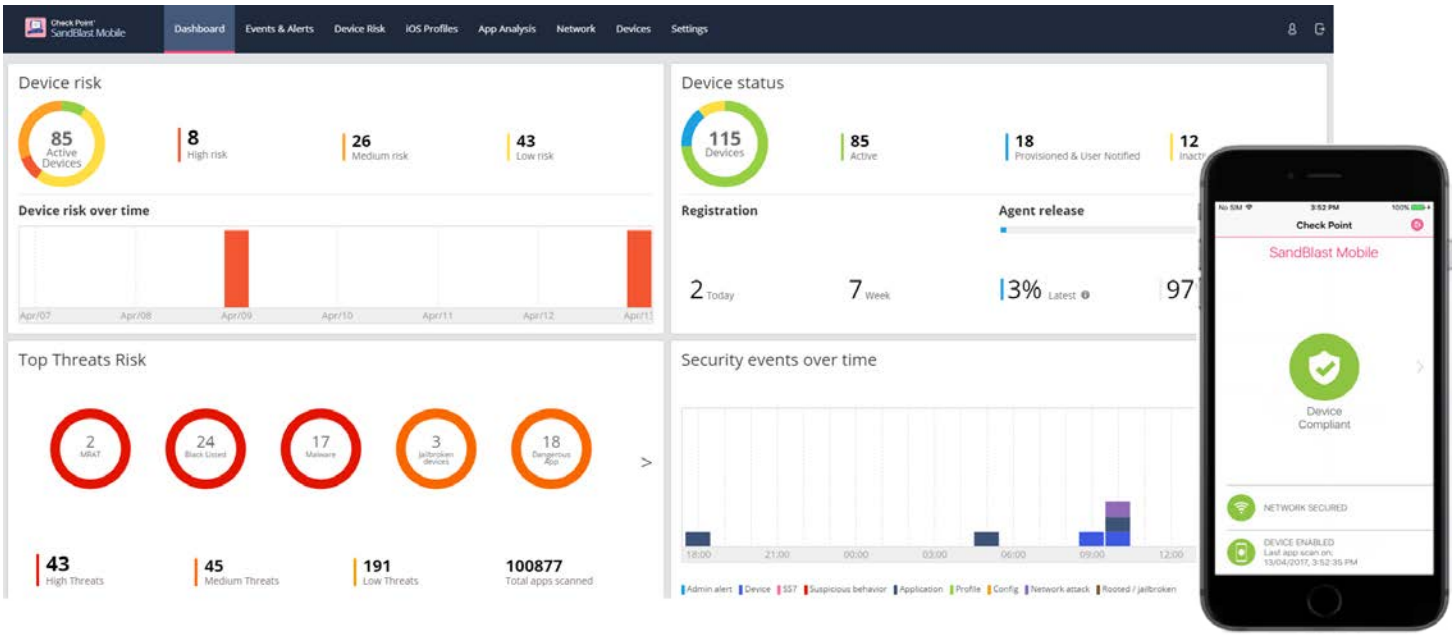
# CHECK POINT SANDBLAST MOBILE BEHAVIORAL RISK ANALYSIS

## AN ADVANCED APPROACH TO COMPREHENSIVE MOBILE SECURITY

Accurate threat detection and efficient response are critical components of preventing advanced attacks on smartphones and tablets. Traditional anti-virus and app reputation solutions can identify known threats, but they can't detect zero-day malware or vulnerabilities in networks, operating systems, SMS messages, and apps.

### It's time to take a new approach.

Only solutions that can analyze behavior across all three vectors for indicators of attack can protect mobile devices effectively to keep them safe from cybercriminals. Check Point SandBlast Mobile identifies threats using on-device, network- and cloud-based algorithms, and triggers automatic defense responses that keep mobile devices and the data on them protected.




SandBlast Mobile Protect app on iOS and Check Point SandBlast Mobile web-based admin console


April 20, 2017

# SANDBLAST MOBILE PROTECT APP

SandBlast Mobile Protect is a lightweight app for iOS and Android™ that gathers data and helps analyze threats to devices in your environment. It monitors operating systems, SMS messages, information about apps, and network connections that Check Point SandBlast Mobile uses to identify suspicious or malicious behavior.

## PRIVACY AND PERFORMANCE

To protect user privacy, SandBlast Mobile Protect never collects or examines content or files. Instead, it examines critical risk indicators found in the anonymized data it collects. Some analysis is performed on the device while other more resource-intensive analysis is performed in the cloud. This approach minimizes any impact to device performance and battery life without changing the end-user experience.

## NETWORK ANALYSIS

Everybody uses public Wi-Fi® hotspots, but they're also an easy way to fool users into joining fake, malicious networks. Cybercriminals can use these man-in-the-middle (MitM) attacks to intercept communication between two or more parties, allowing them to capture or alter data in transit.

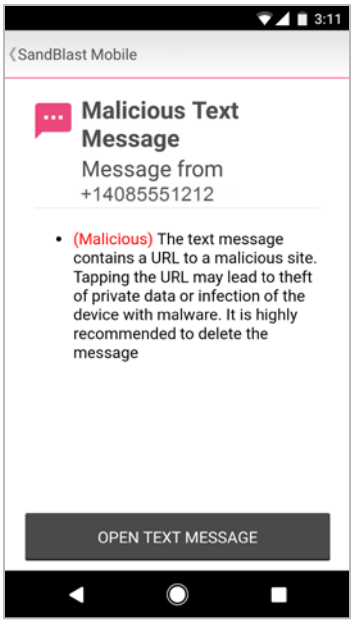
Two common types of MitM attacks are SSL stripping and SSL bumping. SSL stripping circumvents automatic redirection to secure HTTPS connections, and SSL bumping uses fake SSL certificates to fool apps and browsers into believing they're using private web connections.

Check Point SandBlast Mobile detects these types of attacks which can leave sensitive data unprotected and open to the prying eyes of cybercriminals. When a user connects to a Wi-Fi network, the SandBlast Mobile Protect app validates the integrity of SSL connections to detect compromises. It also checks the security of a connection using a cloud-based honeypot that detects if someone is using a MitM attack to break the connection.

## SMS PHISHING ANALYSIS

The Anti-SMS phishing attack feature of SandBlast Mobile detects malicious links, including tiny URLs, in SMS messages and alerts the user through the SandBlast Mobile Protect app notifications. The user is provided with detailed information about the threat in the SandBlast Mobile Protect app, with a recommendation to delete the message. Once the message is deleted, the alert is removed.

Check Point SandBlast Mobile Anti-SMS phishing attack is powered by ThreatCloud™, the industry's largest collaborative network and cloud-driven knowledge base that delivers real-time, dynamic security intelligence.




## THREATCLOUD

Check Point ThreatCloud is the first collaborative network to fight cybercrime. It is a knowledge base that delivers real-time, dynamic security intelligence. That intelligence is used to identify emerging outbreaks and threat trends. ThreatCloud powers the Anti-SMS phishing attack capability for SandBlast Mobile allowing SandBlast Mobile to investigate always-changing IP, URL, and DNS addresses where malicious websites are known.

ThreatCloud's knowledge base is dynamically updated using feeds from a network of global threat sensors, attack information from gateways around the world, Check Point research labs, and the industry's best threat intelligence feeds.

## CONFIGURATION ANALYSIS

Changes to device configurations can happen for a number of reasons. Users might make or accept changes when installing apps, business organizations might require changes to meet policy requirements, or cybercriminals might make changes to carry out an attack. Certain configuration settings, like if an Android device is configured to allow installation of third-party apps from unknown sources, could expose significant security vulnerabilities. SandBlast Mobile Protect monitors all configuration changes on the device. It also performs analysis for weaknesses in device operating systems, like vulnerable versions of Open SSL, which can expose devices to Heartbleed. On iOS, the app checks for CA certificate, proxy, or VPN configurations that could compromise the security of a device.

## ADVANCED ROOTING ANALYSIS

Gaining root access to a smartphone or tablet (also called “rooting” on Android and “jailbreaking” on iOS) is no longer something just gadget enthusiasts do so they can tinker with a device. Root access enables a wide range of customizations, and it gives users more access to do with their devices as they please. It also gives cybercriminals greater access, which exposes devices and data to risk.

Many root detection methods, such as those used by Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions, detect static root indicators like the existence of certain files in a system directory that enable root access. However, there are some free tools like Xposed Framework for Android or xCon for iOS that anyone can use to avoid MDM or EMM root or jailbreak detection.

With root access, cybercriminals can even deny root check requests from the EMM or MDM entirely, giving them the obfuscation they need to carry out undetected attacks on mobile devices. Instead of just looking for static indicators like superuser files, SandBlast Mobile Protect uses advanced techniques to detect if and how root access is granted on a device, including unexpected OS behavior that may indicate rooting or jailbreaks.

## WHAT DO WE ALLOW YOU TO MONITOR?

- Signature and source of apps to determine if an app came from an app store or if it was it side-loaded
- New or updated apps installed on the device
- Acquisition of the app binary from app stores and marketplaces
- Acquisition of app binary from Android devices when an exact hash isn’t available on Google Play
- Wi-Fi connection status
- Operating system integrity, including jailbreak or root checking
- Configuration of the device
- Indication of compromise related to exploits
- SSL integrity information when connected to Wi-Fi
- Malicious SMS phishing message status

# BEHAVIORAL RISK ENGINE

Check Point SandBlast Mobile uses a cloud-based Behavioral Risk Engine (BRE) to perform in-depth threat analysis. In addition to the network, configuration, and root analysis data it collects, SandBlast Mobile Protect sends information about apps on a device to the BRE. It uses this data to analyze and detect suspicious activity, and produces a risk score based on the type and severity of risk. The risk score is then used to determine what automatic mitigation action is needed to keep a device and its data protected.

## APPLICATION-BASED MALWARE DETECTION

Apps are an easy, effective way for cybercriminals to launch sophisticated, targeted attacks.

That's because most users implicitly trust apps they install no matter from where they're downloaded. Making matters worse, most users don't understand or read the permissions they grant during installation. Malicious apps can enable a host of activities like exfiltration of sensitive data, or remotely seizing control of sensors like the camera and microphone to spy on users and their surroundings. The best way to protect devices and data from these risks is to take a multi-layered approach to detecting and stopping app-based threats.

## ANTI-VIRUS (AV) FEEDS

Much like a person can be identified by his or her unique fingerprint, malicious code in apps can be uncovered by looking for unique binary signatures. These scans provide an important first line of defense, but known malware families can be obfuscated, allowing them to bypass signature-based solutions. As part of its behavioral analysis, Check Point SandBlast Mobile immediately detects patterns of known attacks, but it also uses a number advanced detection methods designed to uncover unknown or zero-day threats AV signature scans alone cannot detect.

## DYNAMIC SANDBOX EMULATION

It's difficult to understand how an app behaves in the real world if it sits idle in a sandbox. In fact, malware often waits for certain conditions or user inputs to trigger malicious activity. It may even trigger API calls to detect whether it's running in an emulator.

SandBlast Mobile uncovers obfuscated, polymorphic, and zero-day malware by capturing and installing apps in a dynamic cloud-based sandbox. The sandbox emulates a range of different devices, operating systems, networks, user activities and conditions. This exposes vulnerabilities and exploitations like what apps will do over a period of time and if run under different circumstances including different geolocations and environmental conditions.

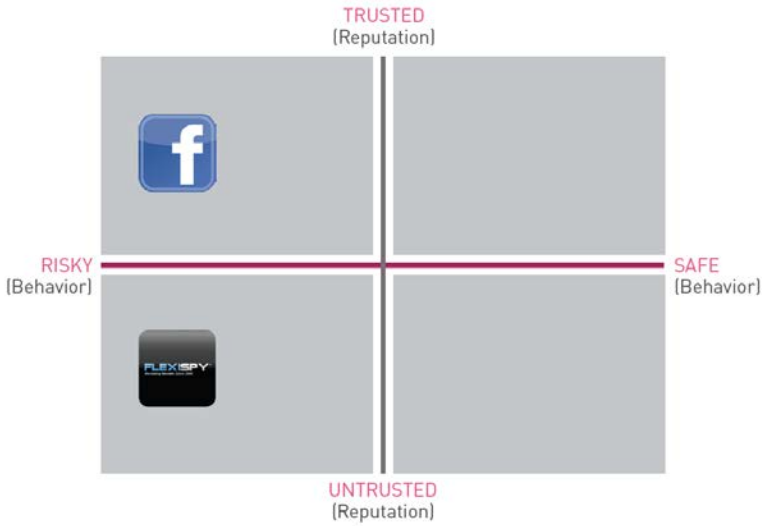
It also simulates user inputs like tapping buttons and settings inside an app, making it harder for cybercriminals to detect if their malicious apps are being analyzed in a sandbox or used by a real person.

## APP REPUTATION AND THREAT INTELLIGENCE

Some trustworthy apps can exhibit risky behavior. This causes false-positive headaches for IT and a poor experience for end users who might be blocked from using completely safe apps. Facebook, for example, syncs and uploads contact details, calendar records and even records voice during status updates.

Although this behavior is associated with the most aggressive types of malware, Facebook isn't malicious. Without a way to determine what apps can and can't be trusted, some app reputation solutions might block users from downloading and using some apps.

SandBlast Mobile whitelists trustworthy apps automatically by correlating risk analysis data with aggregated factors like a developer's reputation, the number of downloads, app source, and the reputation of the server with which an app communicates. This allows end users to download the apps they want without security teams having to worry about these apps compromising devices or data.




## ADVANCED CODE FLOW ANALYSIS

An app's code is like a tremendous map of virtually infinite routes. The logic of one line of code may have dozens or even thousands of touchpoints, all within the same app. This makes it difficult to understand if any of these routes are designed to trigger malicious activity.

Check Point SandBlast Mobile captures apps and reverse-engineers them automatically. This creates a blueprint the solution then uses to expose code and deconstruct flows for semantic analysis that can identify suspicious patterns and behaviors.

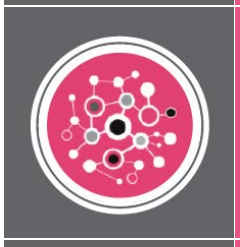
For example, advanced code flow analysis can expose whether hard-coded phone numbers are being used to contact premium SMS services, or if the code is using the device microphone to record sound files it sends to nefarious external servers.

## REMEDIATION AND MITIGATION

Based on the BRE's ongoing analysis, each device is assigned a real-time risk score that correlates with the threat level of that device. The BRE classifies apps and threats to understand the severity of the risks each device poses to the organization. The score for each device is used to determine and execute the best attack mitigation strategy.

### ON-DEVICE MITIGATION

A secure channel can be triggered automatically using a virtual private network (VPN) that protects the privacy and integrity of communications and minimizes the impact of an attack; on-demand, proactive user notifications that contain remediation steps to remove malware and block data exfiltration.



### NETWORK-BASED MITIGATION

Active device protection delivers on-demand blocking of malware to defend against new, emerging and targeted attacks, spyware, drive-by attacks and MitM attacks.

### MDM/EMM ACTIONS

MDM or EMM solutions manage devices and static policies that don't change with the security posture of a device. Through integration with these systems, SandBlast Mobile dynamically changes access privileges to reflect current risk levels, transforming static management policies into active device protection.

### INDIVIDUALIZED RISK SCORE AND THREAT MITIGATION

The risk score for a device is adjusted any time there are new findings from ongoing assessments that represent a change in its risk profile. As a result, organizations always have an accurate picture of the types of threats devices on their network are facing, as well as detailed information about what is being done to mitigate those risks.

The BRE's risk scores determine the mitigation and protection capabilities that will be used, based on pre-defined risk thresholds and policies set by the organization. Once a risk threshold has been reached, Check Point SandBlast Mobile automatically mitigates risks using automated responses on supported devices, in the network, or by triggering dynamic device policy changes on an organization's MDM or EMM solution.

## RISK CATEGORIES AND POTENTIAL MITIGATION OPTIONS

### Informational (Low Risk)

**App and threat classification:**

- Application or configurations have suspicious characteristics but doesn't require immediate action
- Device has vulnerabilities specific to its platform and OS

**Remediation and mitigation:**

- No response required unless malware or a malicious app tries to exploit the device's vulnerabilities
- Dashboard alerts
- Compliance verification
- In-depth forensics, if needed

### Warning (Medium Risk)

**App and threat classification:**

- Potentially contains dangerous capabilities that can be exploited including hacking/rooting tools, unauthorized backup tools, apps downloaded from unofficial stores or marketplaces
- Device has been jailbroken or rooted
- iOS device contains risky or unauthorized configurations or network profiles
- Device has open, unpatched vulnerabilities that could be exploited, putting corporate data at risk

**Remediation and mitigation:**

- Dashboard alerts
- Admin email/SMS notification
- Changes in access privileges (via an MDM or NAC system) to critical corporate resources (email, internal apps, corporate network) to improve enforcement
- Policy violation alerts
- User notification indicates risky behavior and actions to take
- Optional: Triggers Active Protection, which activates a VPN channel to protect privacy and integrity of communications

### Malicious (High Risk)

**App and threat classification:**

- Device infected with malware, exploits, or a malicious app that has malicious intent. Examples include mRATs, info stealers, and premium dialers
- Device demonstrates risky behavior that requires immediate mitigation, such as communicating with an unidentifiable server
- Man-in-the-Middle / Network attack
- Critical vulnerabilities like StageFright and BrainTest

**Remediation and mitigation:**

- Active protection: Blocking traffic to malicious servers to contain the attack. User can continue using the device for legitimate use until remediation is complete
- User notifications: User is informed about the risk and provided steps to remove malware and eliminate the threat
- MDM mitigation: Blocking a device or corporate access, wiping the secure container, etc.

## ADVANCED THREAT DETECTION CAPABILITIES

| Vector | iOS | Android |
|---|---|---|
| Device | • Jailbreaking<br>• Version-specific iOS exploits<br>• Suspicious configuration changes | • Rooting and root kits<br>• Version- or device-specific Android exploits<br>• Suspicious configuration changes<br>• Vulnerable configurations<br>• File system tampering |
| Network | • Man-in-the-middle attacks<br>• Malicious proxy and VPN | • Man-in-the-middle attacks |
| Apps | • Malicious behaviors<br>• Spyphones and RATs<br>• Side-loading of apps using stolen or fake certificates | • Malicious behaviors<br>• Spyphones and RATs<br>• Bots<br>• SMS interception<br>• Keylogging and credential theft<br>• Screen scraping<br>• Malicious SMS URLs |

The Check Point Incident Response Team is available
to investigate and resolve complex security events
that span from malware events, intrusions or denial of service attacks.

For more information, visit checkpoint.com/mobilesecurity

CONTACT US

**Worldwide Headquarters** | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com


April 20, 2017