# HEALTHCARE: Mobile Security

## Protecting enterprise patient mobile applications

## Mobile Threat Defense Sandblast Mobile

## HEALTHCARE – MOBILE APPLICATION CHALLENGES

The heavily regulated healthcare industry is implementing innovative solutions to improve patient care while keeping up with government mandates. Many of the changes evolved over time and were initiated by the Affordable Care Act (ACA) of 2010 that brought about comprehensive health care reform. At the center of this evolution was the implementation of the electronic health records (EHR) system that has reached a new phase. Today, hospitals are entering a transitional period of their initial rollout and expanding the bridge between healthcare and new technology as part of their strategy. Some of them are mobile centric solutions. As a result, more patient mobile applications are being introduced and implemented to provide extended care. These solutions are part of the EHR system architecture with complex integration to backend APIs and modules. As such, the challenge to provide cyber security protection for these devices against today’s next generation cyber security threats are also on the rise.

## INTRODUCTION OF MOBILE DEVICES IN HEALTHCARE

Delivering mobile solutions is expanding in various areas of the hospital. Part of this strategy is to stay competitive, improve the patient experience, and leverage the mobile technology that can improve patient care.  As a result, mobile application solutions are an integral part of patient care. They can be found in the following:

- Patient Portals
- Care Centers
- Physician Devices
- Nurse stations
- Patient Wait Rooms

## Prevent Mobile Threats

- ✓ Blocks devices from sending data to botnets
- ✓ Blocks phishing attacks in all apps
- ✓ Blocks infected devices from accessing corporate data
- ✓ URL filtering
- ✓ Safe Browsing
- ✓ On-Device Network Protection
- ✓ Multi-layer protection for OS, Application, & Network

## Full Threat Visibility

## ELECTRONIC HEALTH RECORDS - EVOLUTION

The introduction of EHR systems was a digital transformation. Consequently, it enabled a broader expansion of electronic information management. By implementing these changes, organizations are now positioned to provide better security for patient care and introduce new technology. Patients are now able to manage a variety of tasks related to their health: view their medical records, communicate with their physician, schedule appointments, obtain results, request medications, review their medical history, etc. The growth is expanding to mobile tablets, medical devices, internet of medical things (IoMT), applications, and integrating with various systems; they are linking research development and patient care.

## HEALTHCARE – ENTERPRISE MOBILE APPLICATIONS

As mobile internet usage exceeds personal computers, so does the growth of applications on the devices. Major health system vendors are aware of this growth and continue to heavily invest in mobile development solutions. They are utilizing them to expand interoperable platforms, improve patient communication, and reduce cost in workflows. Here are some of the top mobile applications by health systems:

- Airstrip, AirStripOB/Cardiology
- Aetna, ITriage
- Cerner, CareAware Connect
- DSS Inc.
- Epic Systems, MyChart Mobile
- GetWellNetwork, Marbella
- MEDITECH, Ambulatory EHR
- PatientKeeper
- Patient Safe, PatientTouch System
- Spok, Spoke Mobile

Larger organizations are exploring further and increasing mobile development by creating customized solutions. In turn, they are expanding their mobile application footprint. Thus, improving patient care while exposing themselves to cyber-attacks.

## INFORMATION TECHNOLOGY - STRUGGLE

As the digital transformation of healthcare over the years matures, many challenges still remain for the IT security teams. In large part, they are left with more work as they implement a security strategy for their EHR systems. For many, this infrastructure can be very complex to manage because it introduces new applications, integrated systems, and backend databases that require specific skills.

Those organizations operating more efficiently often are implementing new solutions in Endpoint, Cloud, Mobile and Network/Firewall which increases demand for specific skill sets and resources to sustain those areas of growth. Moreover, as mobile devices expand in the hospital, so does the applications for both clinical and patient areas. Many support teams are left scrambling to find the right solution for mobile security. This is quite a task because these corporate applications are on premise or in the cloud. To further complex matters, protection is required for the applications on both business and personal devices. Ultimately, presenting a very challenging platform to secure.

## MODERN SOLUTION – SANDBLAST MOBILE

Protection for mobile devices that have patient care applications requires a modern solution to prevent an attack. Providing continuous enhancements to the product is also essential because of the rapid nature of modern cyber-attacks. It needs to evolve over time to incorporate new features yet remain flexible to manage.

Check Point offers a unique product in Sandblast Mobile (SBM) to meet the specific requirements (HIPPA) for the healthcare industry and protects mobile devices from next generation cyber-attacks. It is built with the latest, cutting-edge technology in the industry for both Android and Apple devices delivering on network, OS and application layer protection. It offers a 100% cloud infrastructure. With this architecture healthcare IT teams are able to onboard customers faster. Organizations with existing MDM / EMM solutions are able to integrate with SBM for easy deployment. Thus, enhancing their security posture without disrupting the current on premise protection. With a built-in Check Point VPN there is no disruption to hospital workflows. An incident will automatically trigger the system by directing traffic to a secure path.  Therefore, it does not disrupt the patient experience. It also provides protection on phishing SMS attacks on all applications. Additionally, it delivers granular policy segmentation to protect various satellites sites and hospitals under the organization. This allows easier management over the course of time. Distributed patient devices are also protected with location tracking and safe browsing to meet the organization’s standards.

**Application Protection**

Mobile applications remain the most vulnerable attack vector to mobile devices. SBM provides total protection by encapsulating enterprise applications from such malicious network, application, and OS level attacks. Because patients utilize their personal device to access their EHR applications, healthcare providers need to prevent malicious attacks. SBM sandbox technology obtains insights to every application in the cloud and reduces resources on the device. During the analysis it will reverse engineers the application and inspects it for any malicious code that might compromise the device. For further support, certain applications can be blacklisted to prevent them to be installed on the devices. Thus, it protects enterprise EHR applications from today's modern attacks.

| MOBILE APPLICATION THREATS | |
|---|---|
| • Various malware | • Eaves dropping |
| • Ransomware | • Grayware |
| • Spyware | • Trojan SMS (phishing) |
| • Fake Apps | • Adware |

## SANDBLAST MOBILE - OVERVIEW

Sandblast Mobile (SBM) is an innovative approach to mobile security that detects and blocks attacks on iOS and Android mobile devices before they start. It monitors operating systems, SMS messages, information about apps, and network connections to identify suspicious or malicious behavior. It fully integrates with the Managed Device Management solutions (MDM): Airewatch, MobileIron Core, BlackBerry Enterprise Server, IBM Maas360, Good Dynamics (Blackberry Dynamics), MS Intune & Citrix ZenMobile.

## MDM (“Police”) vs SBM (“Detective”)

Introducing SBM requires understanding the current environment and formulating a couple of questions:

1. What do you use to protect your mobile devices?
2. Do you have an enterprise solution like an MDM?
3. How you protect applications, O/S & network on BYOD?

For simplicity, the MDM can be considered your “**Police**” solution that pushes corporate ***static*** policies (“**laws**”) and provides a container. That work in the past but not today with the sophisticated attacks. That’s why it’s important to combine it with an advanced security protection, SBM (the “**Detective**”). SBM dynamically changes access privileges to reflect current risk levels, transforming static management policies into active device protection. For a complete solution you combine both: “**Police & Detective**”

## MDM Key Functions

- Enforce & Pushes policies (“**laws**”) to devices
- Control – provide **control** for known attacks and some security to smartphones and tablets
- Container - provides a container in device to protect corporate files: email, apps etc.
- Other, track inventory, perform real-time monitoring and reporting

## What’s happening to mobile security?

- Usage - 90% attacks start with phishing; increase in mobile phone usage; more traffic / data
- Targets - Call Tapping (SS7), track location, emails, contacts, microphone, photos, account’s credentials, messaging apps (messenger, WhatsApp, Slack etc.)
- Damages- Corporate espionage, executive tracking, spear phishing, privacy invasion, account takeover, eaves dropping on meetings, impersonating contacts

## PRODUCT STRENGTH

1. **Best catch-rate** in the industry for known and unknown attacks
2. **Multi-layer detection / protection** : O/S, App & Network
3. **Visibility & Intelligence** – cloud infrastructure
4. **Attractive Pricing –** competitive pricing
5. **Maturity & Vision –** long term history of cyber security
6. **Flexible Architecture –** cloud infrastructure

## KEY FEATURES – On-Device Network Protection

### DETECTION

**Network Attacks** – detects suspicious network; fake WI-FI and SSL stripping; SMS attacks, cellular network attacks (SS7)
**OS Exploits –** detects, vulnerability, configuration changes, rooting and jailbreaking
**Apps –** detects known and unknown malicious and risky apps (e.g. rooting apps)
**Real-time risk assessments –** assign risk levels to devices

### DYNAMIC THREAT RESPONSE

**User & MDM notification**
**Integration w/MDM –** allows solution to make real-time risk based policy adjustment
**Activate an on-demand VPN –** tunnel data traffic away from cyber criminals
**Threat Cloud –** collaborative network knowledge base; real time protection

### PREVENTION

**On-Device Network Protection –** inspects all traffic to validate URL
**Anti-phishing –** prevents phishing attacks on email, or social media
**Safe Browsing –** prevents access to malicious websites and blocks them; thru ThreatCloud
**Conditional Access** – control access to corporate resources when device is compromised
**Anti-bot –** detects bot-infected devices and blocks communication
**URL filtering –** blocks access to websites based on corporate policies

### OTHER

**Multi-layered application analysis –** cloud based behavioral risk engine (BRE)
**Dynamic Sandboxing**
**Anti-virus (AV) Feeds**
**Application-based malware**
**App reputation & threat intelligence**
**Advanced code flow analysis**

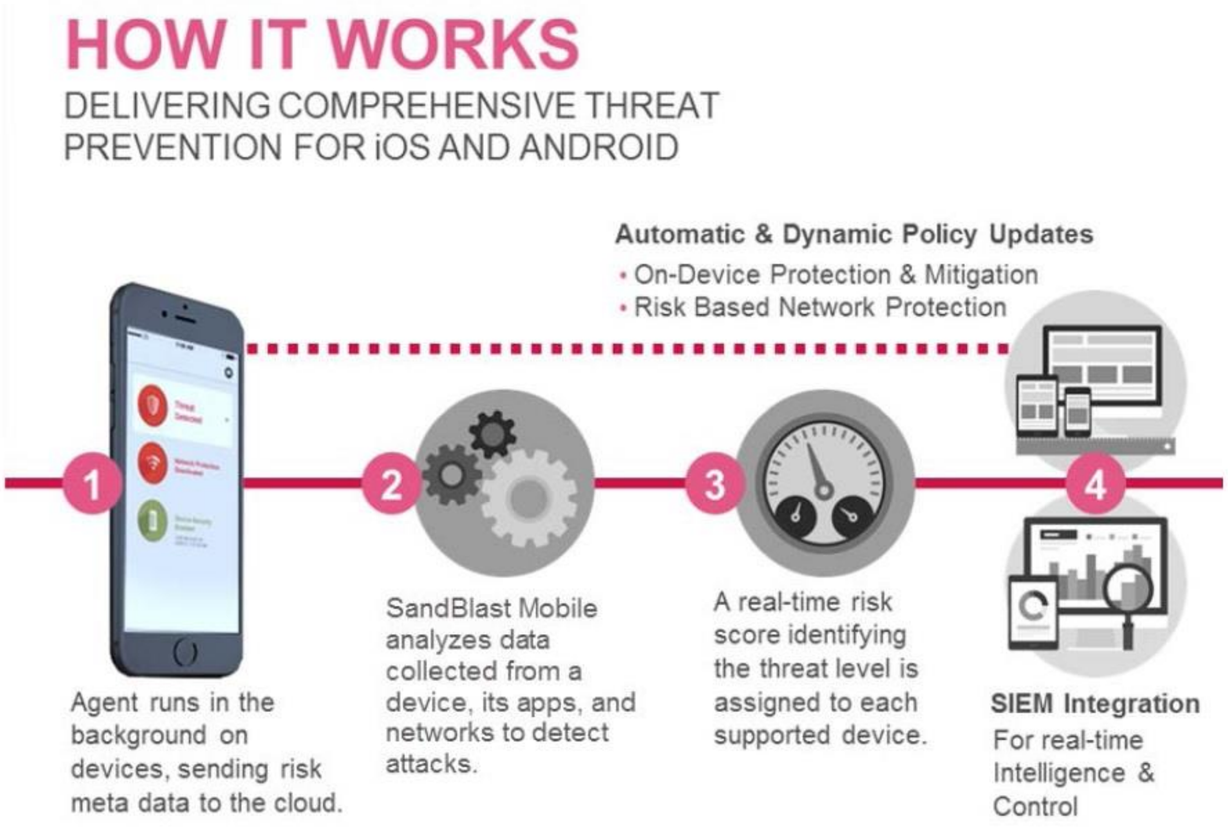
## 5 Mobile Security Myths Debunked

1. **Mobile isn't a big problem** – study found 39% downloaded mobile malware and 24% connected to a malicious Wi-Fi network when compromised; estimated 5%- 20% of devices already compromised
2. **MDM is enough –** reactive solution to infected devices and just "control" damage; hygiene policy security. Free jail break or "rooting" tools are available to bypass MDM & EMM systems
3. **Secure containers are safe** – most often container access systems and apps (Dropbox, Box, Oracle, Salesforce or SAP) outside the parameter; network spoofs, or man-in-the-middle attacks eavesdrop, intercept and alter traffic. Users fall trap to fake Wi-Fi hotspots that lead to such attacks
4. **IOS is Immune –** Check Point found vulnerability in apple developer enterprise program. The program lets organizations develop and distribute apps without publishing on Apple's App store. Malicious apps can hide behind man-in-middle attack do the same by hijacking traffic between device and MDM
5. **Mobile Antivirus is all I need –** limited to unknown attacks when signatures are not available for "zero-day" (newly created) malware

## Competitors

**Poor Visibility** – lack data visibility in dashboard
**Poor catch-rate** – poor catch rate for unknown attacks
**High Cost –** some are up to 40%+ higher
**Security limitation** – can't protect corporate data & email; lack enhanced solution (container)
**Limited Support** – lack multiple layer protection and don't protect key areas (e.g. SS7)
**False Positives** – often time produce many false positives

## How it Works?



HOW IT WORKS

DELIVERING COMPREHENSIVE THREAT PREVENTION FOR iOS AND ANDROID

Automatic & Dynamic Policy Updates

- On-Device Protection & Mitigation
- Risk Based Network Protection

1 Agent runs in the background on devices, sending risk meta data to the cloud.

2 SandBlast Mobile analyzes data collected from a device, its apps, and networks to detect attacks.

3 A real-time risk score identifying the threat level is assigned to each supported device.

4 SIEM Integration For real-time Intelligence & Control

## On-Device Network Protection - Glance

**PROTECTION METHODOLGY**
All traffic inspected locally on device.
Cellular traffic data is not routed through an external gateway or proxy.
Checks for threats against ThreatCloud.
Negligible impact on latency or battery.

**PRIVACY**
No PII inspected on device.
No PII sent to external gateway or proxy.
Configurable option to allow user to disable inspection for specific categories.

**PHISHING PROTECTION**
Blocks access to phishing sites on browser apps.
Blocks access to phishing sites on all nonbrowser specific apps (Facebook Messenger, Slack, WhatsApp).
Blocks access to known and unknown phishing sites.

**MALICIOUS SITE PROTECTION**
Blocks access to malicious sites on all browsers.
Types of malicious sites that are blocked (i.e. only botnets or spyware) can be defined.

**CONDITIONAL ACCESS**
Blocks access to company resources if device is at risk
Blocks access to cloud and on-premise apps.

**ANTI-BOT**
Blocks communications between malware and command and control servers.
Blocks all communications by malware.

**URL FILTERING**
Over 60 site-based URL categories (e.g. gambling, adult, violence, etc.).
Blocks access to restricted sites on all browsers and non-browser apps.
Extend policies from endpoints to mobile.