Samsung Research America Secures Intellectual Property from Advanced Mobile Threats

Mobile Workforce Protected with Multi-Vector Security from Check Point

SAMSUNG RESEARCH AMERICA

Customer Profile

Samsung Research America researches and builds innovative electronics for consumers and businesses worldwide.

Challenge

- Prevent compromised devices from accessing the network or enterprise data
- Defend clean devices on the network
- Protect both iOS and Android mobile devices with single solution

Solution

- SandBlast Mobile
- Integration with VMware AirWatch
- Integration with Splunk SIEM

Benefits

- Gain 100% protection for iOS and Android devices
- Achieve high user adoption
- Simplify management and free IT resources

> "Check Point SandBlast Mobile is the best zero-day malware protection possible for mobile devices. There's nothing else out there with multiple layers of protection. Our IP is secure, and that's peace of mind."
>
> — Steven Lentz, CISSP, CIPP/US
> Director Information Security at Samsung Research America

Overview

Gaining In-Depth Threat Defense—and Peace of Mind

Samsung Research America is a wholly owned subsidiary of Samsung Electronics Company. The organization researches and builds new core technologies to enhance the competitive edge of Samsung products. Headquartered in Silicon Valley, Samsung Research occupies locations in key technology centers across North America.

Business Challenge

Securing Devices In the Wild

As an industry-leading manufacturer of consumer electronics, Samsung is committed to forward-looking innovation and bringing new products to market ahead of competitors. An extensive portfolio of patented intellectual property forms the core of Samsung innovation. Human resources, legal, and research and development employees routinely work with confidential product plans and proprietary information. The last thing Samsung needs is leaked confidential information, which could significantly compromise its market advantage and the company's bottom line.

Like many organizations, Samsung employees increasingly work on smartphones, tablets, and their own devices. The IT team must support approximately 800 corporate-owned and 400 employee-owned devices. A couple of years ago, Steven Lentz, CISSP, CIPP/US, Director Information Security at Samsung Research America, recognized the potential security threat to sensitive information on mobile devices.

"Mobile devices don't operate behind a security infrastructure like corporate PCs, laptops, and servers do," said Lentz. "Mobile devices are out in the wild, creating potential security issues and enabling malware to enter the network. There's no mobile firewall to prevent cyber threats from getting in through emails and apps."

Lentz viewed the problem from two sides. First, he wanted to proactively prevent data leaks from mobile users. Second, he wanted to defend against cybercriminals trying to break in from the outside via phishing emails and other tactics. He set out to find a solution that would meet rigorous requirements.

A new solution had to guarantee that no compromised device could get on the corporate network to begin with, nor could any compromised device access company applications and sensitive data. Once a clean device is allowed on the network, it must be defended. Lentz also needed to protect devices with multiple operating systems, and he needed a way to integrate protection with Samsung's existing AirWatch by VMWare mobile device management (MDM) and Splunk security information and event management (SIEM) platforms. Integration was essential to enabling full visibility of mobile threats and automatically enforcing security policy across the enterprise.

"Defense in depth is needed because traditional antivirus is not enough for advanced threats," explained Lentz. "We needed multiple layers of protection and critical features like application-based malware coverage, enterprise integration, and zero-day malware firewall protection for mobile devices."

> "Check Point had more up-to-date information and automated delivery of the latest malware-related intelligence."
>
> — Steven Lentz, CISSP, CIPP/US, Director Information Security at Samsung Research America

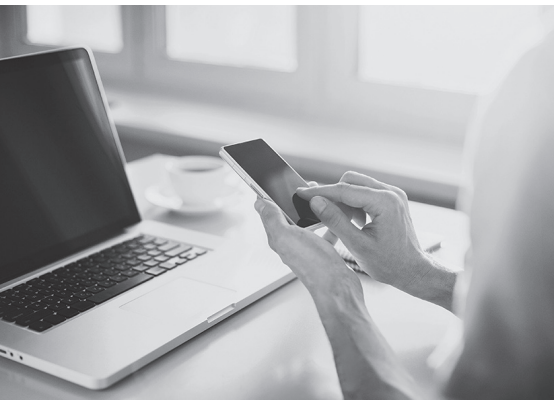
Solution

New In-Depth Protection

Lentz and his team considered numerous consumer and enterprise antivirus products, but they all fell short. Next, they talked to peers and began evaluating vendors that provided solutions for advanced threats, one of which was Check Point. During a demo, Check Point SandBlast Mobile quickly identified several mobile devices that had malware infections. SandBlast Mobile provides multiple layers of defense against exploits, targeted network attacks, mobile malware, and commercially available mobile remote access Trojans (mRATs) that enable spyware and data theft. Samsung chose SandBlast Mobile for its ability to protect devices from app-based zero-day malware and other threats.

"Check Point had more up-to-date information and automated delivery of the latest malware-related intelligence," said Lentz. "Check Point SandBlast Mobile offers the closest thing to zero-day detection on mobile devices. I like it when a product does what it is supposed to do—and more. Check Point did exactly that."

SandBlast Mobile also integrated seamlessly with VMware AirWatch, enterprise mobile management (EMM) and Splunk security information and event management (SIEM) platforms. Now Samsung gained comprehensive visibility into mobile threats and automated enterprise-wide security policy enforcement.



Protection in Action

Check Point SandBlast Mobile defends against threats on devices, in apps, and in the network, many of which use phishing emails, text messages, and browser downloads to attempt entry. It correlates and analyzes device, application, and network information in the cloud to deliver real-time threat intelligence.

The Check Point solution runs a copy of the mobile app without data in a sandbox environment to see if it operates suspiciously. It performs advanced code analysis on the network communication link without actually inspecting the data. Check Point also applies behavioral heuristics for advanced rooting and jailbreak protection. If a user downloads something malicious and Check Point identifies it as malware, it notifies the MDM system to quarantine the device, removes the security profile from the infected device, and prevents the device from accessing the corporate network.

Fast, Straightforward Deployment

"The deployment took just 3 weeks," said Lentz. "We deployed SandBlast Mobile on the network and automatically activated it on devices using our MDM. It's easy for administrators to manage."

Business Impact

It Just Works

On its first day in service, SandBlast Mobile identified three embedded pieces of malware on employee devices. Next, it caught more than 20 different kinds of malware. Each time the solution identified a new threat, it notified security administrators immediately and offending devices were quarantined from the company network. After the threats were eliminated, the Check Point solution reestablished connectivity with corporate networks and assets.

Once the Check Point solution was fully deployed, IT found that five percent of the company's enrolled devices were infected with multiple types of malware, including credential stealers, keyloggers, mRATS, and unauthorized root kits. All devices were quarantined from company networks and assets until the users could be informed and the threats removed.

"So far, we have been 100 percent protected with coverage for both iOS and Android devices," said Lentz. "Because it's difficult to track down mobile users in order to remediate their devices, automating protection was critical. Devices were immediately quarantined, which is our number-one defense."

High User Adoption

After users were informed about the new software being deployed, they didn't have to do anything different. The AirWatch MDM containerizes business information separately from personal information on users' mobile devices, and Check Point secures both. The app runs in the background, using minimal system resources. Users didn't have to learn anything new and are only alerted if SandBlast Mobile quarantines the device.

"Our users don't have to worry about it because it's invisible," said Lentz. "We've seen high adoption and satisfaction from employees and contractors because it's easy to register for the software, it respects their privacy, and it runs quietly in the background."

> "The Check Point solution has given us back one full-time resource of man hours. We're freed up to get more done."
>
> — Steven Lentz, CISSP, CIPP/US, Director Information Security at Samsung Research America

Mobile Threat Visibility

Check Point integrates threat intelligence with Samsung's Splunk SIEM, delivering better visibility into mobile device compliance with security policies. It enables IT to manage threats proactively while simplifying security management. A cloud-based dashboard provides real-time intelligence and visibility into the number and types of mobile threats trying to gain entry.

"Integration with our AirWatch MDM and Splunk SIEM automated real-time intervention," said Lentz. "Now, quarantines keep threats off the network and enable us to better protect sensitive information."

According to Lentz, maintenance of the SandBlast Mobile is minimal. It might take an hour a week, which usually occurs when the software identifies malware on a phone and the team waits for the user to respond before cleaning the device. Otherwise, the software sits in the background, silently protecting Samsung's mobile devices.

"The Check Point solution has given us back one full-time resource of man hours," he said. "We're freed up to get more done."

Confidence to Expand Mobile Deployment

SandBlast Mobile has proven itself to be highly effective, identifying dozens of threats with no false positives. Proven success gave Samsung significant confidence to allow unknown, employee-owned devices onto its network. The solution finds malware on a daily basis from compromised links, downloads, or applications on new, user-owned phones. When the team installs the Check Point software on a new phone, it makes sure that the phone and all pre-existing apps are clean.

Peace of Mind

Proactive security and multiple layers of defense now protect Samsung's corporate data and intellectual property, and Lentz recommends the solution to peers.

"Check Point SandBlast Mobile is the best zero-day malware protection possible for mobile devices," he said. "There's nothing else out there with multiple layers of protection. Our IP is secure, and that's peace of mind."

For more information, visit
www.checkpoint.com/mobilesecurity