# RCB BANK PROTECTS ITS MOBILE FLEET WITH REAL- TIME PREVENTION FROM CHECK POINT

Check Point SandBlast Mobile flawlessly protects users and mobile devices from mobile malware and sophisticated network attacks, ensuring sensitive data is safe.

RCB BANK
That's my bank!

### Customer Profile

RCB Bank is a community bank across Oklahoma and Kansas

### Challenge

- Increase security of business and customer information on mobile devices
- Enable consisten protection across bank-owned and BYOD devices
- Ensure effectiveness and granular risk assessments

### Solution

- Check Point Harmony Mobile

### Results

- Immediately identified, blocked, and notified of cyber threats and non compliant devices
- Delivered visibility into specific threats, potential impact, and remediation tips
- Simplified mobile security ad-ministration with customizable dashboard, ease of use, and rapid deployment

"SandBlast Mobile proved itself. It's an effective, affordable solution that protects us in ways that our container solution alone could not accomplish."

— Stacy Dunn, Information Security Analyst RCB Bank

## Overview

### RCB Bank

RCB Bank is a community bank, headquartered in Claremore, OK, with locations across Oklahoma and Kansas. Founded in 1936 as Rogers County Bank, RCB Bank serves its communities with conservative banking practices and progressive banking products. RCB Bank provides a full range of banking, lending, investing, business, and education services.

### Protecting Information While on Mobile

RCB Bank heavily relies on mobile devices for exchanging information. Employees use specialized banking apps, as well as email, on these platforms. Their entire mobile fleet consists of iOS devices: most of them are provided by the bank, but if employees wish to access their email from their personal phones, they must have an iPhone in order to do so.

As a financial institution, RCB Bank is subject to numerous compliance requirements and audits. It has built its security infrastructure on NIST guidelines and follows Center for Internet Security (CIS) Controls and CIS Benchmarks best practices. Its layered approach to security includes Check Point firewalls and Check Point endpoint security solutions.

Now that the bank has included mobile as part of their strategy, it needed to ensure that mobility didn't come at the expense of security. They did their research, and found out that statistics on mobile device security are not encouraging. According to various US sources, including the Pew Research Center, although 95% of Americans own mobile devices, only 7% deploy any type of security application. When a business allows employees to use their personal devices, it has no way of knowing if the employee's children spouse, friends, or family also use them. At the same time, if business-owned devices can be used off-network, there's no telling where they go or how they are used outside of business, hence opening a potential backdoor to the organization.

RCB Bank wanted consistent defenses across its IT architecture, including mobile devices. Because they are frequently used for collaboration, devices are interconnected with the network and each other, information is shared, and data is often daisy-chained between multiple channels.

"Our customers trust us with their information," said Stacy Dunn, Information Security Analyst for RCB Bank. "Devices, apps, on-network use, and WiFi or cell use of business data must be secure. We require our employees to have a passphrase and/or biometric lock, but we needed more protection."

> "We designed our proof of concept to identify any exploitable vulnerabilities and see if SandBlast Mobile was successful and accurate," said Dunn. "We put it through a series of tests, which it passed with flying colors."
>
> — Stacy Dunn, Information Security Analyst RCB Bank

## Solution

### Check Point SandBlast Mobile Passes the Test

The bank turned again to Check Point for a security solution suited to its mobile fleet. They decided to conduct a proof of concept with Check Point SandBlast Mobile—the leading enterprise mobile security and mobile threat defense solution. SandBlast Mobile protects employees using mobile devices from known and unknown malware, Man-in-the-Middle attacks, and OS exploits and misconfigurations. It also blocks phishing on all apps, prevents infected devices from accessing corporate data, and blocks devices from sending data to Command and Control servers in the case of a bot infection. A cloud-based dashboard provides real-time threat intelligence and visibility into the types of threats that could affect the business.

"We designed our proof of concept to identify any exploitable vulnerabilities and see if SandBlast Mobile was successful and accurate," said Dunn. "We put it through a series of tests, which it passed with flying colors."

Dunn first installed a network scanner from the App Store on her mobile device. Check Point SandBlast Mobile immediately flagged her iPhone as non-compliant, correctly identified the app as a high-risk "hacking tool," and issued a compliance warning. Next, she and her team installed other compromising apps, such as device trackers, which also were quickly detected and the user was provided with remediation options.

To assess the solution's ability to detect and stops exploits, the team set up a " compromised network" to hijack WiFi traffic. As soon as a phone connected to the WiFi network, SandBlast detected the attack and identified it as a Man-in-the-Middle attack that was able to break SSL encryption. At the same time, the phone's internet browser was stopped from sending or receiving any information. The team added an Android device to the testing, pitting it against a malicious Linux-based threat. SandBlast also immediately detected the threat, asked the user to delete the file, and simultaneously notified the admin account.

# Results

### Fast Time to Value

Deployment was fast and easy. Dunn quickly configured settings in the Policy Settings Tab and then set Device, Application, WiFi Network, and the On-device Network Protection policies. When SandBlast Mobile detects non-compliance, the device user is immediately notified. The dashboard makes it easy to see which applications pose specific levels of risk, so that the team can make decisions about access privileges and usage.

"Deployment was fast and painless," said Dunn. "We just pushed SandBlast Mobile to all devices using our MDM tool. It was easy for users, too. They simply allowed SandBlast Mobile to initialize and perform a scan, and they could optimize their individual settings. SandBlast Mobile is lightweight and most users won't even notice the application."

### At-A-Glance Visibility

Dunn and her team count on the customizable SandBlast Mobile dashboard for at-a-glance activity status checks as well as granular, deep-dive views into specific user and application usage. Real-time alerts enable the team to quickly respond and remediate any incidents.

"SandBlast Mobile proved itself," said Dunn. "It's an effective, affordable solution that protects us in ways that our container solution alone could not accomplish."

For more information, visit:
https://www.checkpoint.com/products/