Mississippi Secretary of State's Office Secures Mobile Devices, Gaining Peace of Mind and Significant Savings

Check Point SandBlast Mobile Prevents Advanced Attacks on Mobile Devices

"SandBlast Mobile gives us so much more protection with so much less management effort. Instead of taking up to 30 minutes to install on a device, it now takes two or three minutes, and we get consistent protection across Android and iOS platforms."

— Russell Walker, Chief Technology Officer, Mississippi Secretary of State's Office

Customer Profile

The Mississippi Secretary of State's Office provides information through eight different divisions.

Challenge

- Provide enterprise-grade protection for Android and iOS mobile devices and users
- Make security transparent to mobile users
- Simplify management

Solution

- Check Point SandBlast Mobile

Benefits

- Prevented known and unknown malware from infecting mobile devices
- Reduced installation time per device from 30 minutes to 3 minutes
- Regained hours of productivity through effortless management, achieving a 50% cost savings over the previous solution

Overview

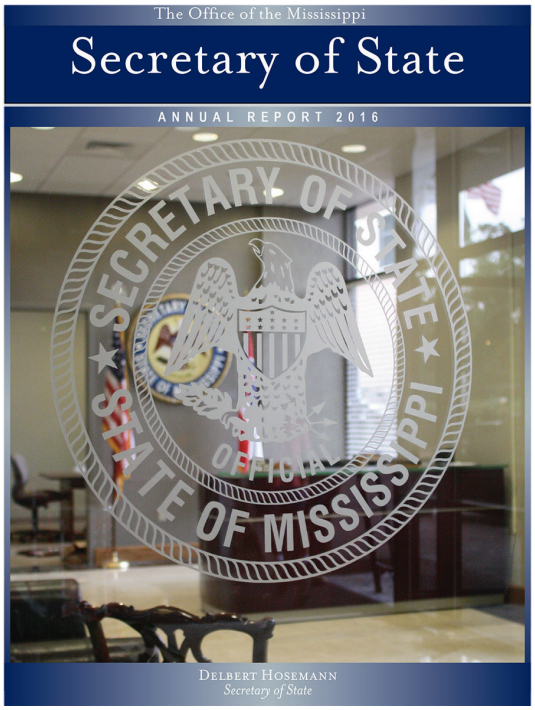
Mississippi Secretary of State's Office

The Mississippi Secretary of State's Office oversees business formation and services; charities; public lands; elections and voting; regulation and enforcement; securities; education and publications; and policy and research for the state. Check Point's SandBlast Mobile solution provides protection to employees' devices to carry out those responsibilities.

Business Challenges

Delivering Better Protection for Mobile Users

The Mississippi Secretary of State's Office supports approximately 100 state executives, department heads, and directors who use their own mobile devices for business. These "high-value targets" usually have access to more sensitive information than lower-ranking employees and travel more often. For determined cybercriminals, they represent the fastest path to valuable data, systems, and assets.



"Mobile users represent a moving attack surface," said Russell Walker, Chief Technology Officer in the Mississippi Secretary of State's Office. "Even though we had recently upgraded our security infrastructure, I still wasn't comfortable with these devices being able to directly access the network, because the antivirus solution on them wasn't really enterprise-grade."

The previous solution couldn't ensure secure connections for mobile devices to the state's network, which increases the risk of an attacker breaching the device. The antivirus solution also took up space and processing power on the device, which was a nuisance to users. Finally, the entire solution was difficult to manage. It wasn't integrated with the rest of the network or security infrastructure, and there were different processes required for Android and iOS platforms.

"Just managing 100 devices required a substantial investment of staff time and system resources," said Walker. "For instance, it took up to 30 minutes just to load it correctly on one mobile device. We needed a more powerful solution that was truly cross-platform and didn't require any user interaction."

> "SandBlast Mobile worked great. Users didn't even know it was there. It took so little effort and worked so well that we took it straight to production."
>
> — Russell Walker, Chief Technology Officer, Mississippi Secretary of State's Office

Solution

From Pilot to Production

The Secretary of State's Office identified three possible solutions, including Check Point SandBlast Mobile, and conducted proof-of-concept testing. Walker's team initially deployed SandBlast Mobile on a small number of devices to see how it worked.

"SandBlast Mobile worked great," said Walker. "Users didn't even know it was there. It took so little effort and worked so well that we took it straight to production."

Benefits

Extra Assurance

Walker and his team gained peace of mind knowing that all mobile devices in their diverse BYOD environment now have an extra layer of protection. They don't have to worry about infected devices connecting to the network or cybercriminals gaining unauthorized access to sensitive data through a compromised mobile device.

SandBlast Mobile has already stopped Man-in-the-Middle (MitM) attacks that targeted state executives over public Wi-Fi networks, which are often unsecured. Users are unaware of connecting to vulnerable networks that allow cybercriminals to compromise data on smartphones and tablets. SandBlast Mobile safeguards data at rest on devices or in motion through the cloud, preventing it from being intercepted by cybercriminals through public Wi-Fi attacks. SandBlast Mobile also detects malicious network behavior and conditions—disabling suspicious networks and preventing the device from accessing the corporate network when a threat is detected.

Through advanced app analysis, SandBlast Mobile captures apps as they are downloaded to devices, and runs each in a virtual, cloud-based environment to analyze its behavior. Approved apps are installed while malicious apps are prevented. SandBlast Mobile continually analyzes devices to find weaknesses that other security solutions don't detect to keep devices as secure as possible.

"When we first deployed SandBlast Mobile, it immediately identified risky apps and operating system vulnerabilities that existed on users' devices," said Walker. "Having advanced app analysis allows us to notify users and remove risky apps or remediate issues. It gives us even more confidence in our protection."

SandBlast Mobile also delivered quantifiable savings to the Secretary of State's Office. Walker said that it is an affordable solution, and when they account for productivity regained, they achieved a 50% savings over the previous solution.

> "Check Point is a trusted vendor. With SandBlast Mobile, we have that same level of trust in our mobile devices, their connections to our network, and their safety over public Wi-Fi networks. That lets us sleep at night."
>
> — Russell Walker, Chief Technology Officer, Mississippi Secretary of State's Office

More Protection with Far Less Effort

"SandBlast Mobile gives us so much more protection with so much less management effort," said Walker. "Instead of taking up to 30 minutes to install on a device, it now takes two or three minutes, and we get consistent protection across Android and iOS platforms."

Additionally, SandBlast Mobile delivers a stream of real-time, detailed threat intelligence to the Check Point SmartEvent platform. Data is correlated with Check Point's ThreatCloud™, providing broad threat intelligence that can be used to prevent cyberattacks. The team correlates SandBlast Mobile data with other security system alerts for enhancing security event monitoring, incident response, and risk analysis.

"Check Point is a trusted vendor," said Walker. "With SandBlast Mobile, we have that same level of trust in our mobile devices, their connections to our network, and their safety over public Wi-Fi networks. That lets us sleep at night."

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