CUSTOMER CASE STUDY

Regional Bank Gains Security Operations Efficiency While Preventing Advanced Attacks

Bank Secures Network and Endpoints with Check Point SandBlast Network Security and SandBlast Agent

Customer Profile

A regional full-service bank in the United States

Challenge

- Reduce time spent on incident response and remediation
- Prevent unknown malicious web content and email files from entering network and endpoint
- Gain better visibility into incidents and the type and source of malware blocked

Solution

- Check Point SandBlast Network Security
- Check Point SandBlast Agent

Benefits

- Secured both the network and endpoints from malicious content
- Saved significant time previously spent on remediation with automated incident handling
- Gained full visibility into unknown threats and vulnerabilities with granular forensic reports

> "SandBlast Agent has definitely made overall security much better. I feel confident that Check Point is stopping the malware before it gets in."
>
> — Network Security Administrator, U.S. Regional Bank

Overview

U.S. Regional Bank

This is a regional commercial bank that offers financial products and services including, among others, internet banking, commercial, personal checking and savings, business checking and savings, loans, and investing. Since founding the bank has expanded to have over 30 branches in the United States. The bank strives to meet the financial needs of its customers as well as be a business leader within the communities it serves.

Business Challenge

Protecting Users from Malware

Before choosing Check Point, the bank had been expending resources and man-hours every week remediating issues caused by malware entering the network and infecting the endpoints.

The bank's network security was jeopardized when internal users visited websites that were malicious or had been compromised. The websites would download malicious content, some of which they had never seen before, infecting the users' machines.

In addition, spam emails and embedded word documents were getting through the bank's firewall and reaching the end users. When users opened the malicious files, it was already too late. The executable code in them would enable attacks on the endpoints. The IT security team had to engage remediation procedures which could take hours or even days. The bank needed to find a solution that would detect the malicious files before they arrived at the endpoints and reduce the time spent on remediation.

Solution

Zero-Day Protection for both Network and Endpoints

The bank chose Check Point SandBlast Network Security to protect its network as it was the market leader and determined after a detailed process of its own tests to be the best in terms of preventing malware. With SandBlast, the bank secured its network from malicious content accessed by users.

As the bank was satisfied with the performance of SandBlast Network Security, it chose Check Point SandBlast Agent to protect its endpoints.

"We went with SandBlast Agent because it was more effective than the agent we were using; there were things slipping through it," said the network security administrator at the bank.

In order to test SandBlast Agent, Sullivan threw a lot of malware at it, all of which was blocked.

"You couldn't really get anything by it," said the network security administrator.

Since implementation, SandBlast Agent has been immensely effective in protecting the bank's users.

> "We really don't spend a lot of time dealing with information security incidents since we implemented it."
>
> — Network Security Administrator, U.S. Regional Bank

Benefits

Proactively Detecting and Preventing Threats

Check Point SandBlast Zero-Day Protection includes CPU-level detection which proactively identifies advanced Zero-Day threats. This technology is used by the bank for both its network and endpoints.

With their Check Point solutions, the bank is protected even from out-of-band threats such as malware from CD-ROMs and USB drives with access to the machine.

Day-to-Day Efficiency with Simplified Management

With SandBlast Agent, the bank's daily process of incident review has become much more efficient.

"We really don't spend a lot of time dealing with information security incidents since we implemented it. It's easy to manage," says the network security administrator. "Once you get it deployed, it's just a matter of monitoring, running reports, and checking any alerts."

Improving Visibility with Actionable Forensics

A big factor in the success of SandBlast for the bank was the high-granularity of the forensic reports.

"The forensics was definitely a big influence in the reporting and the ability to manage it and push it out. Additionally, the reporting detail and the ease of deployment were factors that affected our decision as well."

For every security incident, SandBlast Agent not only remediates the infection, but also provides a full incident analysis report, allowing the company to identify vulnerabilities and the types of malware they have encountered. The easy-to-understand reports paint a full picture of the incident, providing all the details necessary for a security admin to respond, such as entry point, name of malware, and remediation.

"Our experience with SandBlast has been exceptional," said the network security administrator.

"The forensics was definitely a big influence in the reporting and the ability to manage it and push it out. Additionally, the reporting detail and the ease of deployment were factors that affected our decision as well."

— Network Security Administrator, U.S. Regional Bank

For more information, visit:
www.checkpoint.com/products/sandblast-network-security/
and
www.checkpoint.com/products/endpoint-sandblast-agent/