CUSTOMER CASE STUDY

Health Care Insurance Company Boosts Its Defenses While Minimizing Complexity

Check Point SandBlast Delivers Superb Zero-Day Protection and Better Visibility

Company

This company is a large U.S. health insurance carrier.

Challenge

- Consolidate security capabilities and close gaps in coverage
- Keep pace against evolving threats with advanced protection
- Simplify support and management of security infrastructure

Solution

- Check Point SandBlast Zero-Day Protection

Benefits

- Increased malware catch rate, blocking malicious files and ransomware attacks from infiltrating the network
- Gained a single dashboard for environment-wide visibility and higher team productivity
- Built foundation for adding protection without adding complexity

> "SandBlast is a great addition. It blocked more than 30,000 malicious emails and downloads in its first six months and prevented them from ending up in users' inboxes. It has delivered great performance."
>
> — Chief Information Security Officer, Independent Health Care Insurance Carrier

Overview

Health Care Insurance Company

This company is an independent, not-for-profit organization that has provided health care services in its state for more than 30 years. When it experienced a growing number of cyber-attacks, it quickly moved to add another layer of security.

Business Challenge

Protecting Patient Data

Like other organizations in the health care sector, insurance companies have experienced intensified cyber-attacks within the past 12 to 18 months. Patient care data and financial data are at stake, so the company took decisive steps early in 2015 to boost its defenses. Over time, it had acquired multiple point solutions, each with its own set of capabilities. Now the company wanted to add layers of security and new features to close some gaps, such as improving Data Loss Prevention (DLP) coverage.

"We were seeing high volumes of zero-day and other advanced threats," said the Chief Executive Security Officer (CISO) for the company. "We needed to increase our capabilities and reduce our security infrastructure support and maintenance burden at the same time."

"Check Point met our requirements of being able to consolidate capabilities into one solution. We also liked the fact that we can deploy it on premises for more control."

— Chief Information Security Officer, Independent Health Care Insurance Carrier

The company had multiple, separate firewalls for web filtering, content filtering, and Intrusion Prevention System (IPS) protection. As the CISO and his team evaluated their options, they looked at Palo Alto Networks, F5, FireEye, and several niche solutions. However, none of them offered the unique combination of comprehensive features, high scalability, centralized threat visibility, and low IT overhead that they wanted.

"We have a small team supporting a large number of technologies and programs," the CISO said. "It was important to simplify as much as possible so that we can focus on strategic security projects instead of multiple, point solutions.

Solution

Proof of Protection

After conducting a proof-of-concept evaluation with one other vendor, the company chose Check Point's SandBlast Zero-Day Protection solution. Check Point SandBlast protects networks from even the most sophisticated malware and zero-day threats, using Threat Emulation sandboxing and Threat Extraction technologies.

"Check Point met our requirements of being able to consolidate capabilities into one solution," the CISO said. "We also liked the fact that we can deploy it on premises for more control."

The health insurance company migrated to SandBlast over several months to avoid disrupting its existing environment. It gained consolidated Check Point firewall, IPS, Virtual Private Network (VPN), DLP, zero-day protection, web filtering, and anti-bot protection capabilities in a single, easily manageable solution.

Benefits

Turning the Tables on Malicious Email

Before SandBlast, other parts of the infrastructure had missed a significant number of malicious emails, attachments, and zero-day malware. As soon as SandBlast was deployed, the CISO and his team saw a much higher catch rate. In early 2016, when ransomware proliferated, the company was able to prevent a successful attack.

"SandBlast is a great addition," he said. "It blocked more than 30,000 malicious emails and downloads in just the first six months and prevented them from ending up in users' inboxes. It has delivered great performance."

Proactive Threat Prevention for Safer Users

Check Point SandBlast's Threat Emulation engine detects malware before hackers can evade it. It quickly quarantines and inspects suspicious files before they enter the network. The Threat Extraction capability within SandBlast complements Threat Emulation by eliminating risky content, such as macros or embedded links and reconstructing the document to quickly deliver a safe version of the content to users. The company's employees are better protected, which enables them to better protect policyholder data.

"I love the visibility we have with SandBlast and the Check Point Next-Generation SmartEvent appliances. With one dashboard, we can manage our Check Point devices across the company, and it's extremely valuable to see the lifecycles of threats trying to enter or leave the environment."

— Chief Information Security Officer, Independent Health Care Insurance Carrier

One Dashboard, Less Complexity

"I love the visibility we have with SandBlast and the Check Point Next-Generation SmartEvent appliances," said the CISO. "With one dashboard, we can manage our Check Point devices across the company, and it's extremely valuable to see the lifecycles of threats trying to enter or leave the environment."

High-quality graphs and visualization capabilities give the CISO and his team real-time cyber threat visibility. They can move from high-level views to detailed views in a click to quickly understand how threats are behaving. This enables them to fine-tune policies or other security measures if necessary to continuously enhance the security.

Next Steps

"We plan to add Check Point SandBlast Agent to our endpoints, which will give us additional protection from zero-day attacks on our endpoints, as well as deeper data and forensic analysis," the CISO said. "We're also considering Check Point vSEC to extend security to our virtualized VMware environment. Check Point will enable us to continue to build on our foundation with high visibility and manageability."

For more information, visit www.checkpoint.com