U.S. Public Health Services Provider Safeguards Network Ensuring Quality Health Care Delivery to Millions

Check Point SandBlast Zero-Day Protection Secures Network and Prevents Downtime

Customer Profile

This public health services provider treats 2 million patients a year.

Challenge

- Secure patients' vital information
- Prevent downtime to critical internet-connected medical devices
- Improve visibility into attacks on the network

Solution

- Check Point SandBlast Zero-Day Protection with Threat Extraction and Threat Emulation

Benefits

- Ensured timely, quality patient care to millions
- Reduced time and resources expended on remediation
- Gained instant visibility into threats and vulnerabilities previously unseen

> "I believe in the Check Point product, SandBlast, because we believe in prevention and not just monitoring. So we use it in line, and it works really well."
>
> — Information Security Manager, U.S. Public Health Services Provider

Overview

U.S. Public Health Services Provider

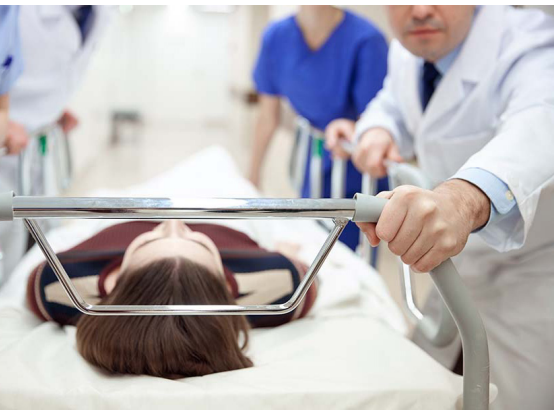
As a leading West Coast provider of emergency health services, this organization has over two million patients and runs over 90 locations, with two major trauma and rehabilitation centers. The organization provides critical, life-saving services in emergency cases.

Business Challenge

Protecting Patients

Being a large-scale healthcare provider, the organization is responsible for securing its patients' highly sensitive data. Information such as patients' medical information, social security numbers, and personal addresses makes the organization a prime target for malicious actors. Entry of any bad actor could have disastrous results for patients and the hospital including identity theft, insurance fraud, data manipulation leading to mistreatment and more.

With important medical devices that require internet connectivity, it is absolutely crucial that the organizations' network is protected. If an attack compromises connectivity, downtime to life-saving devices could result in serious repercussions to patients receiving emergency care. This could lead to delays in treatments, patients getting sicker or even death.



To ensure patients receive the emergency services they need, the organization needed a solution that would not just detect advanced threats to its network, but ultimately prevent them from coming in.

"I believe in the Check Point product, SandBlast, because we believe in prevention and not just monitoring. So we use it in line, and it works really well," said the Information Security Manager at the Public Health Service Provider.

Solution

Advanced Threat Prevention

To protect its network, the health services provider chose Check Point SandBlast with Zero-Day Protection. The organization uses Check Point Firewall IPS, App Control, Anti-Bot, and Anti-Spam capabilities, as well as Threat Emulation and Threat Extraction technologies. Check Point's unique CPU-level exploit detection capability enables Threat Emulation to block malware designed to bypass regular sandboxing technologies, ensuring security against advanced threats such as WannaCry.

With Check Point SandBlast, the organization has been able to prevent countless attacks through email and web thanks to the Threat Emulation technologies. According to the organization's Information Security team, event logs show that CPU-level evasion detection has been highly effective in catching malware.

The team also found Threat Extraction to be highly useful.

"Threat Extraction was very promising, as we could deliver a cleansed document while the file actually gets checked in the background to see if it's malicious," said the Information Security Manager.

> "Threat Extraction was very promising, as we could deliver a cleansed document while the file actually gets checked in the background to see if it's malicious."
>
> — Information Security Manager, U.S. Public Health Services Provider

Benefits

Greater Efficiency with Simple Management

Before SandBlast, the organization's Information Security team would normally have to do a full forensics investigation into a threat, or wipe the box entirely and rebuild it, usually taking four to five hours. The ability of SandBlast to prevent malware from ever getting onto the machine has been enormously beneficial to the team, significantly reducing time spent on remediation.

"One of the benefits that we have seen using SandBlast is that we don't have to go back and clean the machine. We see it preventing malware," said the IT Security Manager

Especially valuable to such a small team has been the "single-pane-of-glass" dashboard, which has allowed them to see, manage, and upgrade everything in one place.

When the team encounters an issue, they contact Check Point support for assistance and have had good results.

"Check Point support is quick to respond and have helped us resolve several issues fairly quickly, so we've had a positive experience with them," said the Information Security Manager.

Enhanced Visibility into Security Incidents

One of the features the organization's team has most appreciated is the log in abilities. With SmartEvent, the team can get a clear overview of what's going on in the network from the application layer as well as a threat layer. If malicious activity is detected, the team is quickly alerted to it and the threat is blocked.

"SandBlast gives us visibility into threats that we wouldn't normally see without it," explained the Information Security Manager.

For the small team, the simple management and instant visibility of Check Point SandBlast are a big help, enabling them to know exactly what's going on in the environment without expending more resources.

"SandBlast does give us a sense that we have more advanced protection, so it helps us trust that we're prepared for a more advanced attack," explained the manager.

> "SandBlast gives us visibility into threats that we wouldn't normally see without it."
>
> — Information Security Manager, U.S. Public Health Services Provider

Next Step

Protecting Endpoints

Seeing the success of SandBlast Network Solution, the organization is now looking to implement the same capabilities on their endpoints using Check Point SandBlast Agent. SandBlast Agent not only includes Threat Emulation and Threat Extraction, but also automated forensic incident review, a great benefit to the health provider.

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