# A COMMUNITY HOSPITAL IN THE WESTERN UNITED STATES PROACTIVELY DEFENDS ASSETS AGAINST CYBER THREATS

Check Point stops spam, spoofing, and advanced threats while simplifying management.

### Customer Profile

Anonymous – Community Hospital in the Western United States

### Challenge

- Simplify security management
- Protect end users from email-based threats
- Prevent crypto-threats from disrupting operations

### Solution

- Check Point SandBlast Network
- Check Point R80 security management

### Results

- Gained visibility into security infrastructure from edge to core in a single pane of glass
- Eliminated spam and email spoofing
- Prevented crypto locker from affecting systems

"Check Point does everything well. Spam and email spoofing are gone. My depth of knowledge and insight into our security environment quintupled. I save at least three to four hours each week simply being able to see everything in one place."

- CIO, Community Hospital in Western United States

## Overview

### Community Hospital in the Western United States

The hospital is a critical-access facility that provides robust care services to more than 10,000 patients per year. Based in the Western United States, it supports several clinics and home health, hospice, and assisted living care services.

## Business Challenges

### Prescribing a Change

Protecting patient data and healthcare infrastructure from cyber threats is increasingly time consuming and resource-intensive for healthcare providers. At the hospital, high volumes of phishing, spam, and a crypto locker incident had become significantly disruptive. When a user clicked on a malicious email link on his remote laptop, it encrypted files on the laptop and spread onto the hospital network when he reconnected. It took almost nine days to restore systems and files to normal.

Until recently, the hospital used Cisco security appliances for network security. At renewal time, the hospital considered the cost increases to be unacceptable. Not only was the equipment expensive, it required extraordinarily high levels of certification and expertise to use and maintain. The Community Hospital needed a security solution that was more effective, easier to use, and less costly.

"The hospital had chosen Check Point to replace Cisco prior to my arrival," said the hospital's Chief Information Officer. "After consulting peers and reviewing products, the team chose Check Point for its reputation, robust solutions, and cost-effectiveness."

The CIO is also the hospital's HIPAA Security Officer—responsible for developing and implementing policies and procedures to ensure the integrity of electronic Protected Health Information (ePHI). When he joined the hospital, he quickly upgraded the Check Point appliances to ensure the latest protection.

"I like that Check Point is aggressive in its ability to detect threats, provide analysis, and disseminate that data to its customers," said the CIO and HIPPA Security Officer. "We have a security solution in place equal to those of institutions many times our size."

> "I like that Check Point is aggressive in its ability to detect threats, provide analysis, and disseminate that data to its customers"
>
> - CIO, Community Hospital in Western United States

## Solution

### Security from Cloud to Ground

Check Point Security Gateway Appliances provide edge security and secure connection between all locations. Check Point Next Generation Threat Prevention & SandBlast™ (NGTX) software provides multi-layered protection from known threats and zero-day attacks using SandBlast Threat Emulation, SandBlast Threat Extraction, Antivirus, Anti-bot, IPS, App Control, URL Filtering, and Identity Awareness.

Check Point SandBlast Network secures the hospital's Microsoft 365 email traffic from threats and malware, preventing it from reaching end-users' mailboxes. Antivirus and URL Reputation protections within SandBlast Network use real-time intelligence from the Check Point ThreatCloud database to defend against the latest threats from known sources.

Check Point R80 security management oversees the hospital's security infrastructure. With the SmartConsole, the hospital gained policy, logging, monitoring, event correlation, and reporting in a single system. Multiple administrators can work simultaneously on the same server and policy without conflict.

> "We have peace of mind knowing that the Check Point solutions are working well. In addition to our own security and technical teams, we have the Check Point experts standing behind us to work on cyber security issues with us. It's a huge relief."
>
> - CIO, Community Hospital in Western United States

# Results

## Simple and Comprehensive

"Check Point R80 security management is simply huge for us," said the community hospital's CIO. "We can manage security from our organization's edge to core, and I can launch everything in a single pane of glass."

The hospital's CIO can now manage all of the blades on the Security Gateway Appliances. He can view the results of email heuristic analyses and know which threats are trying to enter the network via email. Geo policy makes it easy to exclude traffic coming from locations where the hospital does not do business. Application control enables him to create granular policies that allow, block, or limit usage of web applications.

"Check Point does everything well," said the CIO. "Spam and email spoofing are gone. My depth of knowledge and insight into our security environment quintupled. I save three to four hours each week simply being able to see everything in one place."

## Proactive, Trusted Protection

Having a single dashboard enables the team to be proactive about the hospital's security. They no longer have to wait for alerts, field calls from users, or comb through log files to detect or respond to threats. They can see exactly what's going on.

After deploying Check Point SandBlast, an onsite user clicked on a malicious link, and her files became inaccessible. This time, Check Point was there to stop the threat from entering the network. The IT team saw that the files were encrypted and coached her through restoring them. When Check Point asked her if she wanted to revert her files back to a known good state, all she had to do was click "yes."

"In one instance of encrypted files, Check Point paid for itself," said the CIO. "If the threat had propagated through the network, it would have cost tens of thousands of dollars in remediation. Now if a screen from Check Point pops up, we tell users to just click 'yes.' We trust Check Point implicitly."When CHEC needs assistance, the Check Point team is right there.

"We have peace of mind knowing that the Check Point solutions are working well," she said. "In addition to our own security and technical teams, we have the Check Point experts standing behind us to work on cyber security issues with us. It's a huge relief."

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