PREMIER U.S. HOSPITAL PROVIDES ONGOING, LIFE-CRITICAL CARE WITH CHECK POINT NEXT GENERATION FIREWALLS AND CYBERSECURITY MANAGEMENT

Check Point R80 SmartConsole for firewalls and management protect hospital networks, devices and data.

Customer Profile

This organization is one of the premier hospitals in the United States.

Challenge

- Defend healthcare users, systems and data against targeted threats such as ransomware
- Improve security manageability across tens of thousands of devices
- Ensure high availability and performance for life-critical systems

Solution

- Check Point 23800 Next Generation Firewalls
- Check Point 3200 Next Generation Firewall
- Check Point R80 Cyber Security Management

Benefits

- Gained world-class cybersecurity protection across its global infrastructure
- Consolidated policy, log, event, system, and reporting management to a single pane of glass
- Improved performance and increased overall system uptime

> "Check Point's R80 displays what's happening in our network live, right from the console. It saves us time in dozens of ways, enabling us to better protect our network."
>
> —Security Engineer, Premier U.S. Hospital

Overview

Premier U.S. Hospital

This nonprofit medical center treats more than two million patients each year across multiple campuses. Its IT and security team faces the massive task of securing thousands of desktops, laptops, mobile devices, medical devices, and Internet-connected systems. It relies on Check Point to ensure healthcare delivery 24×7.

Business Challenges

Securing Its Digital Footprint

The hospital's digital footprint is huge and critical to saving people's lives. Securing large numbers of computing devices is just the beginning. The network must provide formidable barriers to cyber threats targeting connected medical devices, such as telemetry and bio-robotic systems. Building controls, including heating, lighting, and refrigeration are also digitally connected and require protection.

In addition, data privacy and security are critical to the hospital's mission as a healthcare provider. It supports research generating biomedical knowledge and intellectual property (IP) that must be protected. The hospital also must comply with Payment Card Industry (PCI) regulations governing payment transactions and with HIPAA regulations protecting patient data and personal privacy.

"Cyber attacks on healthcare organizations like ours can have devastating consequences," said the Security Engineer for the hospital. "Ransomware is always a major concern, because physicians, caregivers, and researchers need access to the network and data around the clock. Strong security at our network edge is crucial for our organization."

Solution

Next Generation Cyber threat Monitoring for a Life–Critical Environment

For primary sites, the hospital chose Check Point 23800 Next Generation Security firewalls with consolidated Gen V security, gaining the highest level of threat prevention against large-scale and multi-vector attacks. High-availability clusters ensure maximum uptime of connected systems. High performance enables adding advanced threat prevention and the ability to inspect within encrypted traffic. Unified security management makes it easier to maintain compliance while protecting the hospital's wide range of sensitive information. Smaller internal

networks are protected with Check Point 3200 Next Generation Security firewalls.

"Check Point security firewalls protect our inbound and outbound traffic, as well as traffic over VPNs that are established with partnering organizations," said the Security Engineer. "Check Point R80 brings everything together for granular visibility and simplified management in a single pane of glass."

The security team uses Check Point R80 cyber security management to manage their entire security environment from a centralized dashboard. Check Point SmartEvent provides full threat visibility with a single view into security risks. Real-time forensic and event investigation, compliance, and reporting capabilities give the team control over any security events that arise.

SmartLog provides centralized tracking of log records and security activity with instant visibility over billions of log records. The intuitive search box delivers real-time search results, saving security administrators valuable time.

"We also engaged Check Point Professional Services, which have been wonderful," said the Security Engineer. "The Check Point team helped us with deployment, provided step-by-step migration processes, and were always available and responsive."

"Check Point R80 brings everything together for granular visibility and simplified management in a single pane of glass."

—Security Engineer, Premier U.S. Hospital

Results

Granular Cyber Visibility

The security team now has visibility into policies, logs, events, systems, and reporting from a single R80 SmartConsole dashboard. Check Point R80 also provides a command line interface and REST APIs, which enable them to simplify daily management. For example, they can easily make bulk changes and add rules directly from a command line.

"Check Point R80 displays what's happening in our network live, right from the console," said the Security Engineer. "It saves us time in dozens of ways, enabling us to better protect our network."

Exceptional Operational Advantages

Prior to using R80 cyber security management, it was difficult for multiple administrators to work on different security tasks simultaneously. With the R80 SmartConsole, Check Point introduced concurrent administration capabilities that allow multiple security administrators to be logged into the system and accomplish different goals quickly and more efficiently. The ability to simply log in and work without disrupting other administrators has been invaluable.

Check Point next generation firewalls, together with the R80 SmartConsole, have delivered exceptional performance from day one. Teams can work at full speed without delays from performance bottlenecks, as well as have full visibility across their entire infrastructure.

The hospital plans to activate IPS and SandBlast Network Zero-day Threat Protection, as well as investigate Check Point CloudGuard Dome9 capabilities to assess its public cloud security posture. As the hospital expands Check Point usage, it also increases overall cyber defense—and that's good for everyone's health.

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