Regional Hospital Protects Critical Healthcare Data and Improves Compliance

SandBlast Threat Emulation Service Stops Zero-Day Attacks and Malware

Company

This award-winning hospital is one of the premier healthcare providers in the Northeastern U.S.

Challenge

- Keep critical healthcare operations up and running
- Meet government healthcare regulatory requirements

Solution

- SandBlast Threat Emulation Service
- Check Point IPS Software Blade

Benefits

- Detects and eliminates zero-day and targeted attacks
- Simplifies management and improves visibility

> "Check Point lets us block threats before they can get into our system. It's an ideal way to keep our employee, patient, and business information safe."
>
> — IT Security Engineer

Overview

Delivering Consistently Superior Healthcare

A leading regional hospital in the Northeastern U.S. offers a variety of clinical services, from cardiology, critical care, and oncology, and surgical procedures to fitness, wellness, and education programs. The hospital is proud to be accredited by the Joint Commission, and has received a variety of awards, including recognition by the American Nurses Credentialing Center.

"We are a community-based hospital with about 100 beds, and are highly rated, with numerous certifications and awards," says the healthcare provider's IT security engineer.

Business Challenge

Protect Patient Data in an Evolving Threat Landscape

Like most healthcare providers, the hospital relies on its network to support its most important patient services and business operations. Maintaining maximum security is a top priority. Approximately 1,200 users depend on the network, and the facility is dedicated to complying with the Health Insurance Portability and Accountability Act (HIPAA) and other industry regulations.

"We send and receive a lot of sensitive information through our network and firewall, including payment processing with our business partners," says the IT engineer. "We have concerns about data being breached, patient security, and our own security for our employees and files."

"Our SandBlast Threat Emulation runs in the cloud, and I have to say it's fast," says Ernst. "It examines about 1500 files a day, and you would think that there would be a delay, but we tested it, and the performance is fine."

— IT Security Engineer

The hospital's IT team stays educated on the security landscape, and zero-day malware has emerged as a major threat over the past few years. According to the 2016 Check Point Security Report, the number of unknown malware downloaded per hour in 2015 was nine times greater than the previous year. The stakes are high, since even a brief security lapse could compromise business systems or even impact healthcare services.

"Our patient systems are generally separate from our patient care systems, but we are still in a connected environment," says the engineer. "If a threat gets through, there is the potential that it could impact large parts of the network."

The technology team understands that effective security needs to protect the network not only from external threats, but from issues that originate inside the hospital as well.

"One of our biggest worries is about what happens internally," says the IT engineer. "A problem could arise from something as simple as a user bringing in an infected file on a thumb drive. Research has shown that oftentimes employee behavior can increase risk."

Solution

Preventing New and Unknown Attacks Before They Strike

The hospital has employed Check Point security solutions for years, and depends on redundant 12400 Appliances to provide complete, high availability protection against evolving threats.

To help the organization complement its firewall and IPS solutions, Check Point recommended the cloud-based SandBlast Threat Emulation Service. This convenient, zero-day sandboxing solution not only offers the protection the healthcare provider requires, but is simple to set up and manage.

"I like the cloud-based service because Check Point can take care of it and keep the environment up to date better than we can," says the IT engineer. "That eliminates the worry of having to maintain OS upgrades, patches, and other updates. And we can still configure the rules, so we can control it the way we want to and use it the way we want to."

The Check Point SandBlast Threat Emulation service lets the hospital discover and stop new threats and zero-day attacks using emulation in a virtual sandbox. The solution focuses on email attachments and file downloads, and works smoothly without impacting the hospital's existing environment.

"Our SandBlast Threat Emulation runs in the cloud, and I have to say it's fast," says the engineer. "It examines about 1500 files a day, and you would think that there would be a delay, but we tested it, and the performance is fine."

Next-Generation Prevention, Protection, and Performance

For additional protection against external threats, the regional hospital also relies on the Check Point IPS Software Blade, which combines with the other capabilities on the 12400 Appliances to deliver proactive, best-of-breed security. Its advanced monitoring provides deep insight into attacks, their targets, and their sources.

Simple, Complete Security Management

The healthcare provider has a small technology organization, and making the most of its limited resources is important. The Check Point solution includes central unified management that gives the IT team complete control over their entire security environment from a single, intuitive dashboard.

> "I like the cloud-based service because Check Point can take care of it and keep the environment up to date better than we can," says Ernst. "That eliminates the worry of having to maintain OS upgrades, patches, and other updates. And we can still configure the rules, so we can control it the way we want to and use it the way we want to."
>
> — IT Security Engineer

Benefits

Virtual Sandbox Protects Against Threats in Applications and Files

Check Point's sandboxing solution, SandBlast Threat Emulation service, delivers the advanced protection that the hospital needs to keep its key operations running smoothly and safely, and maintain compliance.

With our cloud-based SandBlast Threat Emulation service, we don't have to bring in another box to prevent malware infections," says the hospital's IT engineer.

With its robust solution in place, Mid Coast Hospital can consistently discover and stop advanced threats that may not have ever been seen before, and therefore could avoid detection by traditional security like antivirus.

"Just recently, the logs showed that we had a spammer trying to send us a file," says the IT engineer. "I noticed I was one of the recipients, so I checked my inbox and spam folder, and confirmed that Check Point prevented it from ever reaching me. The solution is successful at blocking bad files from getting to users in our organization, keeping us secure without any need for us to take action."

Complete, Proactive Intrusion Prevention

The Check Point IPS Software Blade has proven to be an excellent complement to the hospital's cloud-based security service.

"IPS is a really nice tool that we like to use to double check machines that we suspect may have been under attack," says the engineer. "We can go in and check them without having to examine a lot of logs and research."

Single Point of Management Improves Visibility and Saves Time

Controlling operational expenses and streamlining management are always top of mind. With Check Point's comprehensive management tools, the healthcare provider gains network insight while enabling its IT staff to work more efficiently.

"Being able to manage everything through a single pane of glass is great," says the IT engineer. "I can pull up my firewall rules and view the status of our different blades, as well as the cloud operations and events. It's all right there."

The IT team is pleased with the new solution, and continues to keep in touch with Check Point to stay ahead of new security issues.

For more information, visit www.checkpoint.com