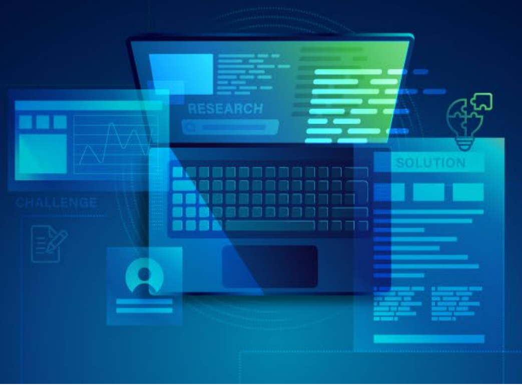
Netsurion



Case Study

Co-managed SIEM/SOC for a Healthcare Company

This healthcare organization has over 70 years of experience assisting hospitals and health systems. With healthcare organizations often targeted by hackers, safeguarding PHI (Protected Health Information) data and maintaining HIPAA (Health Insurance Portability and Accountability Act) compliance are crucial to this U.S.-based healthcare organization and consortium with over 95 member hospitals. They sought a comprehensive security solution to augment their small IT team.

Industry
Healthcare

Size
100 employees

> Trust is everything in the healthcare community. Netsurion's co-managed SIEM/SOC solution addresses our staff challenges with comprehensive 24/7 visibility, deep SOC expertise, and actionable threat intelligence.

VP of IT Operations
Healthcare Organization

Challenge

Healthcare is changing with increased challenges in IT modernization, privacy, and cyber threats. The healthcare customer realized that the IT landscape was shifting along with the importance of healthcare analytics to identify process improvements and opportunities to improve healthcare delivery costs. Although they do not directly provide clinical or patient care, healthcare analytics and "big data" involve ingesting large volumes of data with health indicators. The healthcare organization engaged a consultant who conducted a third-party assessment that provided IT and security recommendations. "This assessment some years ago outlined the policies, procedures, technology, and controls needed to increase cybersecurity visibility and vigilance," said the vice president. This assessment led the healthcare customer to evaluate Security Information and Event Management (SIEM) from Netsurion with their three-person team.

Prior to a co-managed SIEM, their team faced:

- Limited visibility into advanced threats and threat actors
- Increased cyber threats with fewer IT staff compared to larger organizations
- Complex HIPAA compliance reporting and audit requirements
- Challenges in extending security controls to new areas like the cloud
- Lack of a Security Operations Center (SOC)

One of the healthcare organization's goals centered on agility and continuous quality improvement. "We want the member hospitals in our consortium to know that we are good stewards of their patient and hospital data. Our team places a high priority on vigilant data security to protect against internal and external threats," states the IT vice president.

Solution

Why Netsurion's Co-Managed SIEM

"We didn't previously have a SIEM solution, but knew it was a useful and important tool/capability following our third-party assessment. We considered several alternatives in addition to Netsurion's solution. After an evaluation phase, we realized that we did not have the dedicated staff to implement and operate a SIEM internally - we saw the benefits of a managed SIEM. We selected Netsurion because their solutions are purpose-built for small-to-medium-sized businesses (SMBs), like ourselves who require simplicity and affordability."

Data breaches, malware infections, and ransomware attacks that can disrupt operations and even patient safety continue to challenge healthcare communities. However, the demand for cybersecurity professionals far outpaces the available supply. A co-managed service from Netsurion enables organizations to leverage a team of highly skilled experts while retaining responsibility for incident response. Netsurion has built deep familiarity with their security operations, network architecture, and IT processes.

Onboarding and Rapid Time to Value

The healthcare organization started with Netsurion in 2016. They were impressed with the trusted relationship, personal touch, and ability to tailor to their requirements. An operational runbook was created and maintained that documented each engagement and standard operating procedures to follow that optimize outcomes.

"Our goal was to mobilize quickly, and given our limited staff, the Netsurion SOC team was a big factor in our decision. We had a great onboarding experience that covered many moving pieces. The Netsurion SOC was there to walk us through the process. We had a short implementation window, and the onboarding and implementation helped ensure a fast return on investment," said the VP.

Full Cloud and On-Premises Coverage

Netsurion simplifies security across cloud and on-premises environments, providing comprehensive visibility to rapidly detect threats wherever they arise. This unified single-paneof-glass view of the healthcare organization's environment increases productivity, enhances compliance, and accelerates time to respond for cyber threats. "We started with Netsurion on-premises and layered on cloud coverage," stated the IT executive. "This allowed us to protect both our business information and healthcare data, across our network and in the cloud. We now have a holistic view into suspicious actions and potential threats by insiders and external threat actors alike."

Comprehensive Monitoring and Alerting

HIPAA outlines requirements for healthcare organizations to follow in risk management, log monitoring, security incident handling and investigation, and encryption. "We wanted a SIEM solution that was easy to deploy, included a managed SOC with 24/7 analysts, and offered actionable security intelligence and reporting," said the healthcare IT leader. Netsurion's met all their needs:

- Maintain the trust of member hospitals
- Minimize risk involving data leakage
- Respond faster to emerging threats and vulnerabilities
- Simplify HIPAA compliance and reduce security costs
- Remediate threats while minimizing false positives

Reports and Dashboards

Netsurion conducts regular assessments and planning sessions with key members of our co-managed customer team through Executive Dashboard Reviews of the Critical Observation Report (COR). Process suggestions based on customer input during these review meetings assist Netsurion in improving operations and outcomes.

"Netsurion's SOC coverage is very reassuring. We immediately learn about potentially suspicious activities and act quickly, knowing false positives have been filtered out makes us more productive. The reporting is comprehensive with monitoring guidance and vulnerability assessment scanning recommendations all together, which saves us time. I try to attend the monthly assessment meetings as often as I can," said the vice president.

Results

Netsurion provides solutions for the healthcare community to help improve security, simplify compliance, and protect sensitive patient data. Risk management relies on continuous data management and protection; satisfying compliance mandates is merely the starting point to a mature security posture. Just as this healthcare organization has done, ensure a holistic approach with end-to-end security from on-premises to the cloud. Combine people, processes, and technology to remain vigilant given the healthcare sector's ever-increasing threats.

> “With Netsurion's co-managed service and 24/7 monitoring and alerting, our security maturity has continued to evolve, allowing our internal IT team to focus on core business responsibilities.
>
> VP of IT Operations
> Healthcare Organization

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Extended Detection and Response (MXDR). Learn more at www.netsurion.com.