



How to confidently and cost-effectively, meet **HIPPA** regulation utilizing **MSSP**

Faster breach response with automated identification and notification

Overview

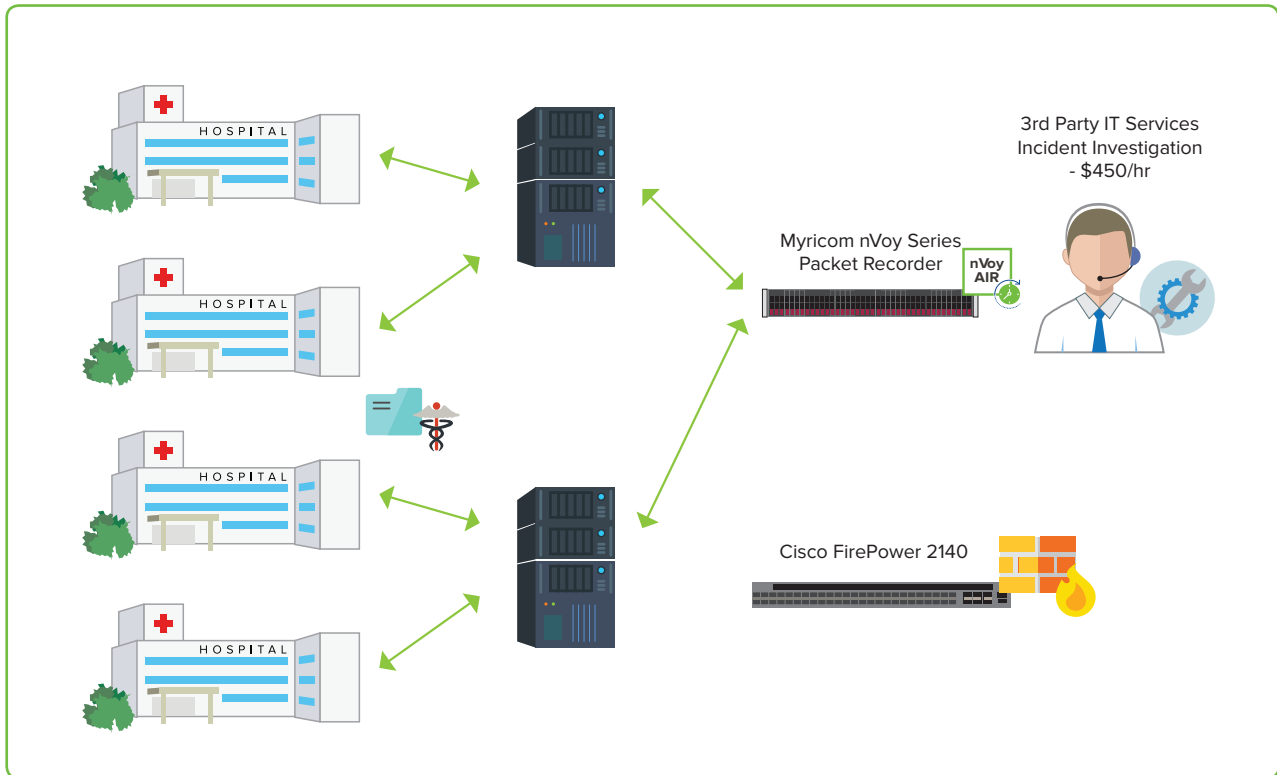
A large metro healthcare clinic is assessing its level of risk and breach response competencies. Given its requirement to secure patient health records in compliance with HIPPA data privacy regulation it is paramount that it have a robust plan to detect, react and contain a breach as quickly as possible.

Due budget constraints the clinic has limited internal IT and InfoSec resources and therefore chooses to outsource to an managed service provider (MSP) a number of IT responsibilities. For example, the clinic's critical data, including PII patient records records, are stored off-premise at a third-party data center spread across 20 servers. Additionally, network maintenance and monitoring is provided by the MSP through remote access to the data center. In the event of a potential data breach, a cyber-security firm is available to investigate any potential security incidents at an additional cost of \$450/hour.

Challenges

Given that industry research reports that data breaches are often not discovered well after the fact and that breach response could take weeks, if not months, the clinic executives and board were extremely concerned about breach preparedness and that they could face serious HIPPA compliance issues. While their reliance on outside resources are a necessity it creates several vulnerabilities that must be addressed:

- The length of time required to investigate potential breaches (weeks, even months)
- Lack of internal visibility into true breaches and their impact
- The high cost of breach investigation
- Difficulty – and expense – complying with data-privacy regulations



The Solution

CSPi's Myricom® nVoy Packet Recorder and Automated Investigation Response (AIR) application.

How it Works

The Myricom® nVoy solution was the perfect solution for the healthcare clinic needs. It is easy to set-up and with just a few steps nVoy can be instructed to monitor and capture user selected data – like PII healthcare records. This drastically reduces the scope of network traffic that needs to be investigated during a potential breach. The nVoy packet broker can tap into any network environment, either inside the clinic and/or at the data center, and provide remote access for real-time reporting. The nVoy solution continually captures and records specified data while the AIR application ingests intrusion alerts generated by the clinic's firewall. Working automatically in the background the AIR application compares these intrusion alerts against critical assets looking for a match which verifying a breach while it is ongoing.

If there is a verified breach, the Myricom solution immediately dispatches an email, to the internal IT resource and the MSP, containing a detailed report that pinpoints any records that were exposed or potentially impacted. Armed with this information, early in the response process the team can immediately kick-off the breach response process. With the already provided detailed data breach investigation can be completed in hours, not days, weeks, or months.

Benefits

- **Reduced costs:** The healthcare clinic significantly reduced the amount of time it once spent on incident response, leading to a 36.2% return on investment. Additionally, the clinic realized three times its investment after the first breach incident.
- **Dramatic reduction of breach reponse time:** The near immediate notification of a verified breach the investigation process can begin immediately, and the allows the investigation to be completed in a fraction of the time – in hours versus days.
- **Highly effective forensic analysis:** With the reduced scope of data to investigate it enables the investigation to be highly focused and with immediate access to all recorded data which allows for retrieval of prior conversations between malicious agents and devices
- **Meet compliance regulations:** With the exact details on impacted records the clinic can confidently meet notification and reporting requirements of HIPAA and other data privacy regulations.



Better security starts now. To learn now CSPI is ready to help you improve security and achieve better business results, contact us at myricom.sales@cspi.com

About CSPI

CSPI (NASDAQ: CSPI) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPI Corporate Headquarters

175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPI High Performance Products

800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPI Technology Solutions

800.940.1111
us-ts-sales@cspi.com



www.linkedin.com/company/csp-inc



[@ThisIsCSPI](https://twitter.com/ThisIsCSPI)



us-hpp-sales@cspi.com



www.cspi.com

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.