Hospital Immunizes Against Data Breaches While Improving Patient Care

Forcepoint provided this regional health provider with a holistic solution to train and continuously preventing workers from accidentally creating data vulnerabilities or falling victim to outside manipulation

Achieving patient satisfaction is one of this hospital's top priorities. But employees' commitment to serving patients—indispensable when delivering quality patient care—can also be exploited, as hackers attempt to steal valuable medical data for their own financial gain. The hospital knew it needed a holistic solution to safeguard sensitive and protected information by protecting against costly human-based vulnerabilities. That's why it turned to Forcepoint.

Customer Profile
This 200-bed acute care hospital facility serves patients in several counties across Mississippi and Tennessee.

Industry
Healthcare

HQ Country
United States

Products
Forcepoint Web Security
Forcepoint Email Security
Forcepoint Data Loss Prevention

The sensitive information stored by medical service providers can be even more valuable to hackers than financial data and, if leaked, cause more harm than just an empty bank account. With information like patient personal data, physician credentials, and Drug Enforcement Agency license numbers, hackers can create fake identities, pose as a medical professional online, or even file fraudulent insurance claims.

For breached organizations, the impact is much greater than an already critical loss of patient and community trust. In addition to regulatory fines, add the costs of customer notification, identity protection, customer help lines, and in-depth incident forensics—and the total financial impact can slam the brakes on operations and growth.

The best of intentions can endanger sensitive information

At this 200-bed acute care facility, the IT security manager says that his colleagues are dedicated to serving their patients and the surrounding community. "People in healthcare are generally in the business to help people, and they want to be as accommodating as they can to patients and visitors," he said. But that helpfulness can be exploited by hackers and other bad actors seeking financial gain.

Some of the most dangerous vulnerability points in any environment exist at the interaction points between humans and data. While advanced technologies can predict system behavior, humans remain, to a certain degree, the wild card. "Every social engineering person I've talked with says that they may not get past the technology, but they can get past the people. And to me, that's alarming," said the IT security manager.

> "Every social engineering person I've talked with says that they may not get past the technology, but they can get past the people. And to me, that's alarming."
>
> **IT SECURITY MANAGER,** Regional Health Provider

Maintaining data health with a holistic, human-centric solution

With web browsing and email communications such integral parts of users' daily work, the hospital knew it needed a cybersecurity solution that could address human vulnerability without impacting the ability to provide care for its patients. That's why Forcepoint's robust, flexible approach to security would turn out to be just the right fit.

To meet the need for a customizable solution to safeguard its users, data, and environments, Forcepoint worked with the hospital to implement a solution that unified web and email protection with data loss prevention to block malware, risky content, spam, and phishing attempts, while increasing data visibility as it moves on and off the network. This suite of Forcepoint products is highly customizable, so policies can be fine-tuned to work most effectively for the organization—protecting users without getting in the way of patient care and legitimate business, and finding opportunities to educate them on proper security practices.

Blocking spam to boost productivity

One of the hospital's most powerful results with Forcepoint Email Security is the sheer amount of spam blocked before it ever reaches its intended destination. 87% of all email is blocked as spam before it can enter users' mailboxes, saving staff valuable time—even just the time it takes to delete irrelevant emails has made a difference in productivity. And labeling emails from outside the organizations with "External" helps to combat spoofing and phishing attacks. Attempts to spoof an organization's high-level executives can be thwarted when it's obvious that an email has come from off the network.

The hospital's security team further customized the Email Security solution to block mail from all foreign servers. Because external email originating outside the U.S. is extremely rare for this rural hospital, this was an easy way to eliminate potential problems even earlier. "A few months back, there was a lot of talk about a particular strain of malware that was being propagated, but the emails were coming from Russian servers, so we were able to block that on our end. They never made it into our organization," the security manager said.

Challenges

Needed to protect data from human-based vulnerabilities from social engineering attempts

Fully locking down web use or data access wasn't feasible to optimizing patient care delivery

Approach

Protect web browsing and email use with Forcepoint Web and Email Security; sensitive information sent via email is encrypted

Add a comprehensive layer of data protection with Forcepoint Data Loss Prevention

Educate employees on proper handling of sensitive data with employee coaching pop-ups for self-remediation of risk; staff are notified if sensitive information is unsecured

Customized and seamlessly integrated for comprehensive protection that keeps business moving

Customization is a big advantage of Forcepoint Web Security. The hospital's team uses categorization to block sites with high instances of malware (e.g., shopping sites). But if a specific shopping site is needed as a legitimate part of the organization's work, the team can reclassify it to make it accessible without unlocking the whole category. The IT security manager sees this as a good learning opportunity as well—when users attempt to visit blocked sites, they are alerted as to the category of site to help them self-regulate future browsing activities.

Forcepoint DLP ties into both Web and Email Security to provide an extra layer of data protection. The security team receives an alert detecting protected information entered into an unsecured website. "We've found some pretty amazing things, like some big-name companies that were having sensitive patient information entered into an unencrypted website. So, we were able to work with other organizations and alert them that this was going on, and they were able to get it resolved," said the IT security manager.

For email, DLP ensures that any sensitive information sent via email is encrypted. Though the hospital has a third-party encryption tool, there have been several instances in which Forcepoint DLP identified unencrypted sensitive information slipping through the cracks. This information was then used to further fine-tune the separate encryption tool to make it more effective.

Building a team of security-aware professionals and maintaining peace of mind

Informing users of why a website was blocked, correcting processes around confidential information, and providing additional information about an email's origin all serve as opportunities for employee education, which the IT security manager and his team know is critically important. And the results of annual security tests are showing progress. "We bring an assessor on site and one of the things they do is try to gain access to sensitive areas. Year after year, as we educate our users, it gets harder [for assessors to compromise users]." Not only is the solution working—it is facilitating and empowering better education of users along the way.

But, the manager says, the real measure of value is the solution's quiet efficacy. "I think this is largely one of those products that sort of sits behind the scenes, and people don't really appreciate all that it's doing. We don't hear a lot about it, which tells us that it's doing a good job."

> "We bring an assessor on site and one of the things they do is try to gain access to sensitive areas. Year after year, as we educate our users, it gets harder [for assessors to compromise users]."
>
> **IT SECURITY MANAGER,** Regional Health Provider

Results

87% reduction in email volume just based on spam blocking

Avoided malware infection that affected several peer institutions

Staff are less likely to fall for social engineering attempts, better protecting data and systems

FORCEPOINT

Contact: forcepoint.com/contact