Northwest U.S. Health Provider Uses Forcepoint Security to Free Up Resources for Business Improvements

The mid-sized, northwest U.S. healthcare provider was sacrificing too many IT resources to protect vital patient data from ransomware scams, so the company turned to Forcepoint for a better solution.

This regional healthcare provider's IT team had its hands full protecting sensitive patient data from phishing threats pushing ransomware scams. Manually dealing with such incidents was taxing the team's time and resources, preventing it from focusing on more business growth-focused projects. The healthcare provider—with facilities in Idaho, Washington, Montana, and the inland northwest—turned to Forcepoint for an integrated security solution that greatly streamlined and automated the safeguarding of data against both external threats and internal risks.

CUSTOMER PROFILE:
Regional medical referral center providing a comprehensive range of medical services to patients throughout the inland northwest.

INDUSTRY:
Healthcare

HQ COUNTRY:
United States

PRODUCTS:
- Forcepoint Web Security
- Forcepoint Email Security
- Forcepoint DLP

This regional health care provider faces many of the same challenges as many in the United States: the hospital must maintain rock-solid IT security to comply with HIPAA regulations and other patient privacy and data protection standards. Slipping up in this area could result in hefty fines and other penalties, as well as a loss of customer trust.

But it is also under pressure to invest in other technologies—like digitizing records, leveraging data analytics, and using cloud-based applications—to maintain a competitive edge and thrive in its market. The bottom line: that can drive business improvements in other areas.

Manually identifying risky end-user behavior

When the provider's Director of Data Security came onboard a few years ago, he discovered that the hospital network had a phishing problem. 2,600-plus employees were poorly trained on how to identify and report phishing attempts they received via email. What's more, a decidedly unhealthy number of them were clicking on suspicious links in such emails, exposing the organization to the threat of being compromised by malware. According to Verizon, about 30% of phishing messages get opened by targeted users and 12% of those users click on malicious attachments or links in those messages.

The good news was that patient data hadn't been compromised by the attacks. The not-so-good news was that the team was spending a substantial amount of money, time, and resources to manually analyze and report all accounts of suspicious activity. It was time to get smarter about web and email security.

Building a better malware trap

The provider needed a solution that would streamline and largely automate the tedious process of identifying and recording risky end-user behavior. It wanted to better educate employees on how to respond to phishing attempts and reduce the organization's exposure to ransomware and other advanced malware threats, while also greatly decreasing the amount of time the team spent responding to such incidents.

The provider and Forcepoint deployed an integrated IT security solution that included Forcepoint Web Security, Email Security, and Data Loss Prevention (DLP). The solution was designed to achieve four security goals:

- → Protect against external threats like phishing attempts
- → Identify and prevent accidental or intentional data exfiltration
- → Train staff to be more responsible IT users
- → Maintain HIPAA compliance

Forcepoint worked with the team on a Proof of Concept (POC) in which they were able to demonstrate a streamlined solution which combined protection against external and internal threats and worked seamlessly within the network infrastructure.

The director of data security wasn't surprised by the success of the POC.

"As a security consultant, I used to travel around and do a ton of pen testing and vulnerability assessments. The companies that had Forcepoint in place were highly successful. So, with the previous knowledge I had about Forcepoint, I was confident that it was the best choice for us," he said.

Smarter end users, immediate ROI

The Forcepoint solution delivered immediate ROI in the form of reducing staff hours responding to various external threats, the director said. The integration of DLP provided a new protective shield against potential internal threats, which also doubled as compliance with HIPAA and other regulations and standards. Employees have become assets to the hospital's security posture.

Challenges

Protect against external threats like phishing attempts.

Identify and prevent accidental or intentional data exfiltration.

Train staff to be more responsible IT users.

Maintain HIPAA compliance.

Approach

Integrated IT security solution including Forcepoint Web Security, Email Security, and Data Loss Prevention (DLP).

"They used to click on anything that they received. Now we've done extensive training to help them understand when not to click on emails or links in emails," he said.

"If a phishing email does come through, within two minutes I have end users reporting it. We can then use the Forcepoint solution to block the attacks, identify potential victims, and help our employees do their job properly and safely, preventing sensitive medical records from leaving the organization."

Meanwhile, Forcepoint's advanced reporting functions have enabled the IT team to easily report to management key details about the threat environment and how much ROI the Forcepoint solution is delivering.

For example, after just 30 days, Forcepoint Email Security and Web Security had actively filtered out 726 viruses and identified 722,331 cases of phishing and spam messages. The IT team went from seeing malicious threats on a daily basis and having to quarantine them manually, to almost never seeing them get past the Forcepoint filter.

"Within a couple of weeks of implementation, our executives were praising the solution. We went from seeing only 10% of malicious activity filtered out with the previous solution to averaging about 60-80% with Forcepoint in place. Our false positive rate is less than 0.1%," the director said.

The sky's the limit

Now that the hospital's IT resources are freed up to pursue other, more growth-oriented projects, the provider is accelerating plans to complete its digital transformation, take advantage of the cloud, and even look at more cutting-edge technology investments.

As the provider decides where best to invest for its own future, the director of data security is confident that Forcepoint will help keep the hospital's IT operations safe and secure.

"The relationship with Forcepoint is only going to grow. I'm really impressed with the capabilities and level of protection the solution provides. I'm a Forcepoint customer because I choose to be. I don't know of another solution that does the job better," he said.

Filtered out

726
viruses

60-80%
of malicious activity

Identified

722,331
cases of phishing and spam

Results

Filtered out 726 viruses and identified 722,331 cases of phishing and spam.

60-80% of malicious activity filtered out.

Less than 0.1% false positive rate.

"I'm a Forcepoint customer because I choose to be. I don't know of another solution that does the job better."

DIRECTOR OF DATA SECURITY

Forcepoint