proofpoint.

CUSTOMER STORY

Health System Protects Against Email-Based Threats

Prevents Advanced Attacks While Simplifying Security Operations

WellSpan Health

The Challenge

- Better detect and stop email threats to protect sensitive data
- Reduce the amount of time spent managing incidents
- Gain better visibility into potential exposure

The Solution

- Proofpoint Email Protection

The Results

- Prevented thousands of phishing attempts from being successful
- Gained valuable time back for team to focus on strategic security projects
- Became more proactive through granular insight and reporting

The Organization

Residents of South Central Pennsylvania and northern Maryland have a fierce advocate for their health with WellSpan Health. The integrated health system is comprised of a multispecialty medical group of more than 1,200 physicians and advanced practice clinicians, six respected hospitals, five cancer centers, a regional behavioral health organization, a regional home care organization, more than 15,000 employees and 140 patient care locations. The organization is just as fierce about protecting its email traffic from infection as it is about protecting and caring for its patients and local communities. That's why it recently engaged Proofpoint—to protect and defend against email cyber attacks.

The Challenge

WellSpan Health has grown rapidly over the past four years, with three new health care organizations joining the system since 2013. As WellSpan expanded its reach, its email security landscape became complicated. Each of the newly joined organizations had its own email security solution. It wasn't long before the security operations team was trying to manage, support and gain visibility from a mix of products.

"Many of the products we were using weren't completely focused on email, and they just weren't catching things that posed significant threats," said Mike Shrader, manager, IS security operations, at WellSpan Health. "Phishing emails were a particular problem, but general spam and malware were still getting through to end-user mailboxes."

The team received trouble tickets every day from users reporting spam or phishing messages. But how many weren't being reported? What were users clicking on? If one user got a phishing email, did two—or 100—other users also get it? Finding and dealing with those messages was time consuming.

"It was really hard to determine our exposure," Shrader said. "We'd spend half a day of work for just one email incident—and we treated every incident as important because it might be."

That diligence paid off, to a point—WellSpan didn't experience any major breaches. But the cost in time and human resources was high, and the volume of malicious email was only increasing and becoming more sophisticated.

"Email protection is critical, because it is one of the biggest potential risks to the organization," said Shrader. "All it takes is one email to create huge impact on our ability to maintain operational efficiency and the security of patient data."

"Proofpoint just works. We see it work every day, and therefore, our caregivers don't ever have to wonder if their email is going to work or not. Most importantly, we're effectively protecting the patient data within our system against email-based threats."

Mike Shrader, manager, IS security operations, WellSpan Health

The Solution

Tests come back positive

Shrader had previous experience with Proofpoint solutions, so WellSpan decided to test Proofpoint Email Protection as a potential solution. Proofpoint Email Protection defends against unwanted and malicious email with granular visibility and business continuity. It uses a combination of machine learning technology and composite reputation analysis to continuously safeguard end users from threats. WellSpan's test results were positive—and eye-opening.

"It was a no-brainer to see how many spam, virus-infected, and phishing messages Proofpoint caught compared to the previous solutions we had," Shrader said. "When we deployed it, we just changed the MX (mail exchanger) record and cut it over. The implementation went very well."

The Results

Maximizing team talent

These days, the security operations team is spending far less time on email administration issues. Instead, they can create policy routes, write rules to have Proofpoint look for specific types of threats, and get more granular insight into the threat landscape.

"We're spending less time tracking down malicious emails and we're able to be more proactive in protecting against threats, now that this solution is in place," Shrader said. "We can keep threats from getting in the door and use our security team for their security expertise."

Protecting sensitive data

The healthcare environment is seeing huge increases in ransomware attacks, and WellSpan is no exception. Since deploying Proofpoint, Shrader's team has seen many instances of CryptoLocker variants. Proofpoint has caught more than 12,000 emails carrying this and other ransomware threats.

"The product has been effective, and most importantly, we're effectively protecting the patient data within our system against email-based threats."

Taking the pulse of threats

WellSpan has also found the Proofpoint reporting tools to be useful, Shrader said, noting: "Our monthly reports to management show trends in virus and phishing activity and enable us to keep an eye on mail flow. The metrics are important for us."

For example, before Proofpoint, users received high volumes of bulk emails in their inboxes. After Proofpoint was deployed, bulk messages were put in users' digests, reducing email volumes by half. Users can review their digest and release any email that they want to receive, but now up to 50% of email coming into the organization is stopped. The team is also using the Proofpoint Syslog feature to send real-time email data directly to its SIEM system. From the SIEM, the team can correlate data from multiple systems and have a detailed view in a single "pane of glass"— one familiar interface. This kind of correlation ability will help WellSpan be even more proactive and improve incident response processes.

The fix for protection

"Email is a significant threat to any organization and its data," said Shrader. "When someone asks my advice, I say take email security seriously. Really do the research, gather your requirements, and compare solutions to pick the best one."

LEARN MORE

For more information, visit **proofpoint.com**.