proofpoint

HEALTH SYSTEM PUTS FAITH IN PROOFPOINT

DEPLOYS PREVENTIVE MEDICINE AGAINST MALICIOUS EMAILS AND ATTACHMENTS

CHALLENGE

- Prevent a growing number of email-based threats from reaching users
- Reduce risk to the healthcare system
- Reduce the amount of time and effort needed to effectively remediate threats

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection with URL Defense and Attachment Defense
- Proofpoint Information Archive

RESULTS

- Immediately stopped thousands of emails containing ransomware and other malicious threats
- Reduced email-related support calls from more than 20 per month to less than three
- Accelerated response with comprehensive, detailed real-time reports
- Greatly increased IT team productivity by redirecting efforts to strategic projects

The Sisters of Charity Health System provides faith-based, high-quality care to people in Ohio and South Carolina. The organization owns St. Vincent Charity Medical Center in Cleveland, Ohio, and Mercy Medical Center in Canton, Ohio. It also provides skilled and assisted living, residential care for homeless men, and resources for families and childcare workers. Like many healthcare organizations, the Sisters of Charity was being barraged by email-based cyber threats, so it turned to Proofpoint for advanced protection.

The Sisters of Charity's primary Microsoft Exchange email system serves 4,600 employees in Ohio. When the health system upgraded its Exchange environment, it also started looking for a better email protection solution. The executive team was keenly aware of rising healthcare cyber threats, and they knew that email is attackers' favorite way to gain access to patient health information, credentials, and financial data.

"It was time to ramp up our protection," said Paul Jones, Chief Technical Officer at Sisters of Charity. "We needed better visibility into the advanced threats that were trying to get in. And we need to detect them quickly, so we can minimize potential damage."

Sisters of Charity was seeing a growing number of spoofed messages, malicious email attachments and URLS, and phishing campaigns. Not only were there more attacks, they were more sophisticated and potentially more dangerous. Users had no way to know if an innocent-looking email message was valid or not, and they often clicked on embedded URLs or opened malicious attachments.

"Our previous system was losing ground against threats," said Ed Wensing,

Information Services, Manager of Customer Service for Sisters of Charity. "We got multiple calls a week from users about suspicious emails, and those were just the ones we know about. The system also was cumbersome to use and manage."

IDENTIFYING A REAL AND PRESENT DANGER

Sisters of Charity initially deployed Proofpoint Email Protection to defend against spam and other unwanted email. They also used Proofpoint Information Archive to preserve, discover, and supervise business-critical information. Now the team conducted a 30-day proof of concept to test Proofpoint Targeted Attack Protection (TAP) with URL Defense and Attachment Defense. TAP helps detect, mitigate, and block advanced threats—whether known or unknown—that use malicious attachments and URLs. In just 21 days of gathering data, TAP flagged more than 11,000 malicious attachments, and 5,000 of those were infected with ransomware.

"We were surprised how many severe threats had been coming through," Wensing said. "TAP showed us how much more we could catch before it was delivered to users."

> "With Proofpoint handling email security, we no longer have to take three steps back in a normal day to work on a security threat. We can just keep moving forward on things that are more strategic."
>
> Ed Wensing, Information Services, Manager of Customer Service

IMMEDIATE RESULTS

As soon as TAP was deployed across the organization, the team saw immediate results. Support calls about suspicious messages dropped drastically. Malicious attachments almost disappeared once TAP Attachment Defense was activated. And Wensing can't remember the last time he saw a support ticket about an infected website, because TAP URL Defense checks suspicious URLs and blocks access to the sites.

"Proofpoint gives us peace of mind knowing that it's watching, checking, and scrubbing all embedded email links," Wensing said. "We haven't had a false positive. Our support calls dropped to maybe two or three per month—and some of those are just user error."

EASY MANAGEABILITY

Wensing finds Proofpoint much easier to manage. A logical screen layout eliminates lots of extra steps that he had been taking to complete simple tasks. He can see exactly what's happening at any time, without having to spend precious time digging through logs. In the past, if something suspicious got through, Wensing's team had to look at every machine to figure out who was targeted, determine if the machine was infected, and assess the damage.

"The data is right in front of us," Jones said. "We can track threats, because TAP reports who received an attachment or malicious URL and who clicked. We can target our resources precisely and avoid wasting time looking for a needle in a haystack."

TWO STEPS FORWARD, NO STEPS BACK

With IT talent at a premium, each IT staff member at Sisters of Charity works on several projects and multiple support cases at the same time. In the past, it took "all hands on deck" to identify a potential threat and remediate the consequences. Meanwhile, work on more important IT and security projects stopped.

"Everyone here is moving at 100 miles an hour," Wensing said. "With Proofpoint handling email security, we no longer have to take three steps back in a normal day to work on a security threat. We can just keep moving forward on things that are more strategic."

For more information, visit www.proofpoint.com.