CASE STUDY

proofpoint

HOSPITAL EFFECTIVELY GUARDS ITS 'FRONT DOOR' FROM EMAIL THREATS

DEPLOYS PROOFPOINT, REDUCING RISK AND TIME SPENT FIGHTING THREATS

CHALLENGE

- Block email threats from getting into the organization
- Deploy and manage email protection with a small staff
- Minimize risk to the hospital and maintain HIPAA compliance

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Information Protection, Email Encryption

RESULTS

- Significantly increased accuracy of email threat detection and filtering
- Reduced incident remediation from up to 20 hours to less than 30 minutes
- Enhanced security for sensitive data through automatic encryption
- Gained proactive control over email traffic and defense against email threats

MedStar Montgomery Medical Center is a member of MedStar Health, one of Maryland's most trusted, nonprofit integrated healthcare delivery systems. The hospital treats almost 40,000 patients annually in its emergency department and is also a Joint Commission-certified Primary Stroke Center. Protecting patient data is a top priority, second only to delivering outstanding patient care.

Physicians and care providers at MedStar Montgomery work hard to deliver personalized, compassionate care, and they trust the IT team to ensure that sensitive information is protected. So when MedStar Montgomery migrated from its previous email filtering system, it looked for a solution that not only filtered email effectively, but also could help defend against a rising tide of malicious attacks and advanced threats.

"Email is a huge threat to any network," said Christiane Brown, Assistant Vice President of Information Technology and Telecommunications at MedStar Montgomery Medical Center. "It's a way in the door for threats, and once they're in, they can wreak havoc on the network. You have to focus on email protection."

The hospital was seeing a huge uptick in the volume—and sophistication—of malicious email content and attachments. Malicious Microsoft Word document attachments were common, and carefully crafted JavaScript files disguised as other documents started to appear frequently. Business email compromise (BEC) emails used specific executive and finance staff member's names to try and induce them to pay fake invoices.

"Email attachments are a way of doing business," said Owen Horne, Network Operations Manager at MedStar Montgomery Medical Center. "We have to give people a way to do their jobs but still control that traffic, otherwise we create a 'shadow IT' problem that can open us up to even more threats."

THE RIGHT PRESCRIPTION

The MedStar Montgomery team wanted a solution that guarded the door against email threats. They looked at a number of solutions, which either had to be deployed close to the hospital's servers or on the client devices themselves.

"We chose Proofpoint Email Protection because it was highly recommended in our industry," Brown said. "And we liked the fact that it's cloud-based, so it receives, analyzes, blocks, or quarantines everything before it gets anywhere near our network."

A few months after deploying Proofpoint Email Protection and Proofpoint Information Protection, MedStar Montgomery added Proofpoint Targeted Attack Protection (TAP) in Email, which stops phishing attacks that use malware, weaponized documents, and credential-stealing techniques to access sensitive information.

"The installation was outstanding," Brown said. "We didn't have the time or resources to deploy Proofpoint ourselves, but we didn't need them. Proofpoint managed the whole project, and we were set up and protected right away. That's fantastic in a vendor."

"Proofpoint does a great job of staying updated and continuing to develop new defenses. We were looking for more than a solution—we wanted a business partner. And that's what Proofpoint is for us."

Christiane Brown, Assistant Vice President, Information Technology and Telecommunications, MedStar Montgomery Medical Center

MedStar Montgomery also has called Proofpoint support for help when its team had to quickly resolve an email security-related problem.

"Every time I've called Proofpoint, the issue is not just taken care of, it's addressed down to the last detail," said Horne. "When I ask for help—boom, it's done."

AN EFFECTIVE FIRST LINE OF DEFENSE

"Proofpoint increased detection and filtering accuracy right from the start," Horne said. "It hit that balance of not overwhelming our team with lots of small annoyances while keeping the bad stuff out."

In the past, the team spent hours investigating an incident. Even if only one event happened in a week, it was burdensome to the small staff. "With Proofpoint, what used to require 20 hours of time for event investigation can now be handled in 30 minutes," Horne said.

Before Proofpoint TAP, the IT team had no way of knowing when users received a suspicious email unless they got a call or the user forwarded them the email. If a user clicked on a malicious URL or attachment, then the IT team had to conduct an investigation. Now, Proofpoint notifies them when users receive suspicious emails. When several users recently received a suspicious email, the team was able to delete it before anyone opened it.

"Once malicious emails get in the door, it's too late," Brown said. "Proofpoint gives us proactive protection so that we don't have to rely on users' knowledge of email threats as our primary level of protection."

X-RAY- LIKE VISIBILITY

The team now has its entire email view in one pane—both incoming threats and outgoing emails. Users can encrypt emails with sensitive data simply by marking them 'Confidential' in the header. When the team sees encrypted outgoing emails, they know whether the user encrypted them or whether Proofpoint detected sensitive data and automatically encrypted them.

"It's helpful to know if threats are part of a coordinated campaign or just Internet noise," Horne said. "If you know what the threat is, you can deal with it effectively."

Proofpoint is invisible to users. They're protected and they don't get the spam or threats that they used to see. They can go through their daily digest of emails that have been blocked and release the ones that are safe. Horne said that the transition from the previous solution to Proofpoint was seamless for users.

"What you want is a solution that delivers outstanding defense with nimble administration, so that you don't have to rewrite the email firewall rules every day," Horne said. "One of our favorite things about Proofpoint is that we don't have to do much administration. And that makes a turnkey solution for us."

SECURITY IN PARTNERSHIP

"Proofpoint does a great job of staying updated and continuing to develop new defenses," Brown said. "We were looking for more than a solution—we wanted a business partner. And that's what Proofpoint is for us."

For more information, visit www.proofpoint.com.