proofpoint.

CUSTOMER STORY

Proofpoint Helps Nonprofit Health System Strengthen Its Overall Email Security Posture

The Challenge

- Protect brand from abuse and strengthen security posture
- Stop business email compromise (BEC) people-targeted attacks
- Support migration to cloud-based email platform

The Solution

- Proofpoint Email Fraud Defense
- Proofpoint Secure Email Relay

The Results

- Stopped more than 1.2 million email threats—30% of total inbound traffic
- Detected and stopped nearly 460 advanced targeted threats
- Deep content analysis caught 45,000 email threats, including impostor threats

The Organization

Today more than ever, it is important to build a nation of healthy communities. Helping to lead that effort is one of the largest nonprofit health systems in the U.S. This organization has a mission of compassion and healthcare equity. It advocates for those who are poor and vulnerable and provides innovative approaches to how and where healing can happen. And with more than 1,000 care facilities, the organization serves millions of patients in states across the U.S. But with its extensive reach and the sensitive nature of its information, the health system team knows how critical it is to have the highest level of protection for its communications.

The Challenge

Keeping healthcare available for underserved communities

Like other healthcare providers, the organization is committed to maintaining the security of its patients and its business data. When it was formed several years ago through a merger, this large provider saw an opportunity to not only strengthen security but streamline processes for its IT team.

"We have a really active cybersecurity function, and we have protections of every nature that we can think of for the organization," said the system director, cybersecurity engineering. "Prior to our merger, our two organizations had their own tools in place for email filtering and authentication. But coming together gave us the opportunity to decide what really made the most sense for the combined organization."

Throughout the healthcare industry, there has been a sharp uptick in business email compromise (BEC) scams. So protecting the organization from these people-centric attacks was a top priority. The team focused on implementing Proofpoint Email Fraud Defense, and cleaning up email authentication for the more than one thousand registered domains that the organization's parent companies had accumulated over the years.

"It's a huge, complex issue to go verify, validate and tune email authentication for over a thousand domains," said the system director. "If you do it poorly, then email messages that should be delivered will not be, and email messages that are potentially fraudulent will get through."

As the health system team evaluated areas to shore up in its email security strategy, they focused on three key areas: sender policy framework (SPF) records, DomainKeys Identified Mail (DKIM) records, and Domain-based Message Authentication, Reporting & Conformance (DMARC). And to optimize and align these elements for maximum security, the organization deployed Email Fraud Defense from Proofpoint.

"We found the expertise offered by Proofpoint consultants to be very valuable. Having someone who has implemented DMARC for a variety of different businesses and has already worked with and understands various email marketing vendors was key to putting email fraud defense in place at scale."

System director, cybersecurity engineering

The Solution

Streamlining email authentication and security

Proofpoint Email Fraud Defense helps the organization simplify its DMARC implementation journey. It also provides protection against fraud attacks like BEC scams, across all of its domains.

To let good emails in and keep bad ones out, the health system team took an inventory of all the organization's domains. They determined what level of email authentication had already been implemented for those domains and whether it was still valid.

"Suppose you had a domain that was used for marketing purposes, but it was deprecated, allowing vendors you no longer work with to send emails on your behalf," said the system director. "Before you start using it for marketing again, you need to validate that all the SPF information that is associated with that domain is accurate. You also have to coordinate with the vendors that will send mail on your behalf with regard to DKIM, to be sure that you're publishing the correct public key associated with the private key that they're using on their outbound server. And once you have all of that aligned, you implement DMARC to ensure that aggregate reports come back to be sure that things are working as you expected them to and give you a heads up if a bad actor attempts to send email impersonating you."

Proofpoint Email Fraud Defense gave the team access to consultants who provided best practices recommendations throughout every step of the configuration and DMARC implementation. And to keep attackers from exploiting issues like SPF vulnerabilities, the organization uses the hosted SPF feature in Email Fraud Defense. This improves SPF security by preventing attackers from easily using a publicly discoverable SPF record to abuse its domain.

The organization also deployed Proofpoint Secure Email Relay to help support the process of migrating its on-premises Microsoft Exchange email platform to a cloud solution.

"The intent was to no longer have exchange servers on premise, so we needed to retire our email relay solution," said the system director. "We could have deployed our own mail servers, but we would still need to build the staff to maintain it and develop expertise around it. We chose to deploy Proofpoint Secure Email Relay because it gives us the functionality that we need, and it's a cloud application."

The Results

Personalized consultation helps scale email defense

Proofpoint Email Fraud Defense has helped the organization simplify its DMARC implementation, and the alignment of SPF and DKIM records, for better protection against top email fraud attacks. As part of the solution, Proofpoint consultants made it easier to achieve the updates and configuration the organization needed, to provide protection on a massive scale.

"We found Proofpoint consulting to be valuable, due to the sheer volume of DNS domains we're working with," said the system director. "If you don't have access to someone who possesses all that knowledge, you have to develop it internally. That adds time and distracts staff from doing other things."

Proofpoint Secure Email Relay has also enabled the organization to move forward with its cloud strategy. At the same time, it provides centralized control—and the ability to easily stop emails from a mail provider if security threats emerge.

"If a cloud services provider is compromised and all of a sudden there are a lot of illegitimate messages coming out of them, we can go into Secure Email Relay and turn them off," said the system director. "That is a completely separate function from our primary email, so it helps us maintain the separation between user email and more transactional types of emails from applications or third-party partners."

With its Proofpoint solutions in place, the organization has upleveled its protection against today's more advanced cybersecurity threats, and unlocked a new level of flexibility and scalability through cloud services.

LEARN MORE

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