CASE STUDY

proofpoint.

# KELSEY-SEYBOLD FIGHTS FRAUD WITH EMAIL FRAUD DEFENSE AND CLOSES THE GAP ON ADVANCED THREATS WITH INTEGRATED PROTECTION

## COMPREHENSIVE PROOFPOINT CAPABILITIES INTEGRATE WITH PALO ALTO NETWORKS TO INCREASE CYBER SECURITY PROTECTION

### CHALLENGE

- Stop spam and malicious threats from reaching users' mailboxes
- Streamline incident response
- Protect health and patient data
- Ensure that all email sent under the clinic's name is authorized

### SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection with URL Defense and Attachment Defense, integrated with Palo Alto Networks Wildfire
- Proofpoint Threat Response
- Proofpoint Email Fraud Defense
- Proofpoint Email Encryption
- Proofpoint Email DLP

### RESULTS

- Stopped spam, malicious attachments, and blocked malicious URL links
- Automated incident response steps to save hours of time and enhance user productivity
- Improved visibility and forensics to potential malicious threats when combined with Palo Alto Networks API
- Regained control over email domains to block fraudulent email
- Strengthened data protection with encryption and DLP

When you're a patient at Kelsey-Seybold Clinic, an entire team of physicians, nurses, and specialists coordinates your care—from evidence-based medicine and disease management to preventive practices. Likewise, Kelsey-Seybold Clinic takes a comprehensive approach to email security. That's why it relies on Proofpoint to defend against everything from advanced email threats to email fraud.

As the first National Committee for Quality Assurance (NCQA) Accountable Care Organization in the United States, Kelsey-Seybold has always taken a proactive approach to improving patient care. Kelsey-Seybold operates 20 multispecialty care centers across the greater Houston area. To coordinate care across multiple specialties and locations, the clinic uses centralized electronic medical records, digital imaging and archiving.

The clinic is just as proactive about security. For years, the security team has blocked adware, stringently filtered malicious websites, and inspected network activity, including Secure Socket Layer (SSL) traffic. Kelsey-Seybold also uses geographic tools to block traffic and network connections from outside of its target market. For example, the team blocks more than 30,000 attempted connections per hour from China alone. Filtering has slashed overall network traffic and the volume of potential threats. When Kelsey-Seybold redesigned its network edge and moved to Office 365, it upgraded network defenses, which also has helped.

But the healthcare provider knew that most threats still arrive through email. So Kelsey-Seybold's earliest security efforts focused on closing that gap.

"We've successfully limited our exposure, but email is still the number-one vector for introducing malware into an organization," said Martin Littmann, CTO/CISO for Kelsey-Seybold Clinic. "That's where Proofpoint has proven to be immensely valuable."

### COORDINATED DEFENSES PROTECT USERS

Kelsey-Seybold initially purchased Proofpoint Email Protection to block spam and viruses. The clinic soon added Proofpoint Targeted Attack Protection (TAP) to protect against advanced threats that arrive in malicious URLs and attachments.

**Proofpoint gives us an end-to-end email solution. Our users know that what they send is protected. What they receive is filtered and has the Kelsey-Seybold stamp of approval. Proofpoint is a tremendous asset for our email system and an effective, time-saving solution for us.**

Martin Littmann,
Chief Information Security Officer,
Kelsey-Seybold Clinic

Today, every URL embedded in an email is sandboxed and rewritten. That enables the security team to vet the links and see who has clicked on them.

Proofpoint Threat Response automates and accelerates incident response. Threat Response is integrated with Proofpoint TAP and the clinic's Palo Alto Networks firewall with a network security solution. If a user clicks a malicious link or opens an attachment, TAP notifies Threat Response and then runs scripted responses. For example, a TAP alert signals Threat Response to automatically remove suspicious email from the user's inbox.

The clinic uses virtual desktops. When an alert is generated in Threat Response, Proofpoint collects the alert data, antivirus data, and application logs. Then it shuts down the virtual desktop and directs the user to log into a fresh virtual desktop. If suspicious network or web activity occurs, the Palo Alto Networks solution analyzes it.

Protected health information must be encrypted when sent in email. Proofpoint Email Encryption makes this easy for employees. Users are instructed to insert key words in subject lines or use sensitivity settings to force email encryption. Additionally, using opportunistic Transport Layer Security (TLS), Proofpoint automatically encrypts the message if the recipient server also supports TLS. Several times, Proofpoint logs have verified that certain emails were sent and received as encrypted—even though the users hadn't done anything to encrypt them. This kind of automatic encryption helps the clinic avoid a reportable breach. The clinic also uses Proofpoint Email DLP to monitor emails and block any that expose Social Security numbers.

Kelsey-Seybold deployed Proofpoint Email Fraud Defense to stop unauthorized emails being sent from Kelsey-Seybold domains. Email Fraud Defense also blocks incoming messages that spoof trusted domains.

## PREVENTING WASTED TIME

"Proofpoint's flexibility and ability to set custom rules and automate workflows save invaluable time," said Frank Patterson, Information Security Architect at Kelsey-Seybold. "Our environment is highly virtualized, and Proofpoint orchestrates steps that we would otherwise have to do manually."

When the team receives a malware alert on a virtual desktop, Threat Response automatically lets affected users know that the machine will restart in 90 seconds. That gives users a chance to finish up what they were doing. Then the virtual machine reboots as a new machine. For physical machines, the security team handles alerts itself. That process includes contacting the user, removing the machine from the network, and reimaging it.

"The thing that gives us the most time savings is Proofpoint's ability to weed out spam and malware," said John Morgan, Information Security Analyst at Kelsey-Seybold. "Spam filtering is not sexy, compared to malware detection, but saving 3,000 employees from spending 10 minutes each day handling spam adds up to real time savings."

## STOPPING FRAUDULENT EMAIL

"When we first tried Proofpoint Email Fraud Defense, we were amazed," Littmann said. "We didn't realize how popular 'we' were in Russia as a purveyor of vanity pharmaceutical products. We wanted to wrest back control over our domains and make sure that emails sent from 'us' are authorized."

Kelsey-Seybold tracks four primary domains and a number of internal "vanity" domains. The team is reviewing all mail sent by third-party business partners and marketing services. It plans to turn on full blocking after completing those reviews.

"I'm just amazed at the number of countries and types of messages being sent under Kelsey-Seybold's name," said Patterson. "For example, in the last 30 days, there would have been 350,000 messages blocked."

## A TREMENDOUS ASSET

Kelsey-Seybold has tried other email solutions running alongside Proofpoint. But none provides Proofpoint's full range of capabilities.

"Proofpoint gives us an end-to-end email solution," said Littmann. "Our users know that what they send is protected. What they receive is filtered and has the Kelsey-Seybold stamp of approval. Proofpoint is a tremendous asset for our email system and an effective, time-saving solution for us."

For more information, visit www.proofpoint.com.

**ABOUT PROOFPOINT**
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

© 2017 Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.