

WESTINGHOUSE SUPERCHARGES EMAIL SECURITY

GAINS BETTER, MORE ACCURATE PROTECTION WITH PROOFPOINT

CHALLENGE

- Prevent threats from reaching users' mailboxes
- Reduce time and effort spent tracking and remediating malicious emails
- Increase security across 29,000 mailboxes and 30 countries

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

RESULTS

- Increased phishes caught within a two-week period from 23 to 800
- Stopped 100% of incoming emails with invalid addresses
- Streamlined workflow, freeing security and email teams for strategic projects

Since 1886, Westinghouse has transformed people's lives. The company's state-of-the-art products first delivered electricity to the United States, transmitted the first commercial radio broadcast, and captured man's first step on the moon. Today, Westinghouse operates around the world with a product portfolio that includes home appliances, electronics, lighting, and power.

Email keeps Westinghouse employees connected across 30 countries. The messaging team manages multiple email domains and 29,000 mailboxes in a Microsoft Exchange 2013 environment—and has its hands full staying ahead of email-based threats.

"Spam used to be our biggest worry," said John Shepherd, Messaging Engineer at Westinghouse. "But now, we're barraged by threats that are trying to steal valuable company assets. Safety and security are critical to Westinghouse, and we strive to make sure that everything we do supports those goals."

But cyber attackers are sophisticated. They attack constantly, and pose a bigger risk than ever. Phishing campaigns are relentless, trying to induce Westinghouse employees to click on malicious URLs and attachments. Attackers often use impostor emails, spoofing executives' email addresses to trick victims into sending sensitive corporate data (this kind of attack is known as business email compromise, or BEC). And they use malware to breach IT defenses and steal credentials.

Westinghouse had used a McAfee solution, but it wasn't stopping most malicious emails, and it blocked many legitimate senders. Each time it did, Shepherd had to add the sender to a safe list—and that list was getting long. Westinghouse began looking for a replacement.

The email and security teams wanted a better solution for scanning attachments and making sure that URLs embedded in email weren't harmful. They wanted industry-leading protection against spam, phishing, and malware. Looking forward, the teams plan to add services such as Data Leak Prevention (DLP) and encryption, so they wanted a solution that would let them easily add those capabilities.

"We also wanted a solution with one user interface," said Shepherd. "That was huge. With the existing product, we had to sign in to three or four different devices. It wasn't intuitive, and it required jumping through a lot of hoops to find what we were looking for."

SHORT-CIRCUITING THREATS

"I had great experience with Proofpoint Email Protection previously, so we added Proofpoint to our list of solutions to evaluate," said Eric McAnallen, Manager of Messaging Services at Westinghouse. "After we'd seen everything on our list, we chose Proofpoint for its superior capabilities and cost-effectiveness."

Proofpoint Email Protection now defends Westinghouse against unwanted and malicious email with granular visibility. Proofpoint Targeted Attack Protection (TAP) with URL Defense and Attachment Defense stops advanced and zero-day attacks that target users through malicious URLs and email attachments.

“Proofpoint makes a huge difference, because it does so many more things than we had before, and it does them better.”

John Shepherd,
Messaging Engineer,
Westinghouse Electric Corporation

Proofpoint Professional Services worked closely with the email and security teams to implement both solutions.

Because Shepherd and McAnallen were familiar with Proofpoint, they transitioned from the old system to Email Protection and TAP easily. Once the solutions were implemented, they cut over users in less than four weeks. Users never noticed.

“Both the Proofpoint Professional Services and the support teams are awesome,” Shepherd said. “Their commitment to us, product knowledge, and overall good nature were just terrific. I’d give them a 100% recommendation.”

HIGHER ACCURACY

Before, Shepherd had little visibility into what was getting through the McAfee solution. Now, they know that up to 30% of emails are spam, phishing, and malware. Another 20% of mail is bulk email. Westinghouse also gained better protection. For instance, before Proofpoint, the team had applied a phishing rule on the old system that caught 23 phishing messages in two weeks. With Proofpoint, out of the box they caught more than 800 phishing messages in the same timeframe. At the same time, Proofpoint allowed more valid emails through that would have been blocked before.

The team’s safe list dropped from 220 entries to six. It also pared down its block list but is still stopping 100% of emails coming in addressed to people who are not on the Westinghouse system. In just two weeks, Proofpoint stopped more than 200,000 emails with invalid addresses.

“Just today, for example, we’ve had 16 threats but zero users affected,” Shepherd said. “That includes all threats—phishing, malware, and attachments. Our security and incident response teams have lots of positive things to say about Proofpoint because things are getting caught that weren’t being caught before. It’s doing its job.”

MORE EFFICIENT WORKFLOW

TAP log data flows to the security team’s ArcSight software, simplifying data collection and providing more visibility for incident response. The security team also monitors threats in real time via the TAP dashboard.

“Workflow is much more streamlined and at the same time, we have fewer incidents to manage,” McAnallen said. “Having a single interface makes it so much easier to do a search, export the information, and respond quickly.”

Before Proofpoint, Shepherd received one or two requests per day to investigate a suspicious email or pull one from a mailbox. Now he might see one request in a week. The security team spends far less time tweaking rules to improve email catch rates, freeing them to address other strategic security projects.

When Westinghouse does business with organizations that require security certification, Proofpoint has paved the way. Some of the company’s business partners also use Proofpoint, which make it easy to set up communications and get email flowing.

“Proofpoint makes a huge difference, because it does so many more things than we had before, and it does them better,” Shepherd said. “I can work on other things but retain complete visibility into email flow and any impacts that might occur. Proofpoint has supercharged our efforts in keeping Westinghouse safe and secure.”

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.

© 2016 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.