proofpoint.

PARTNERSHIP STORY

Global Food Packaging and Processing Company Secures Email with Proofpoint

The Challenge

- Reduce message-based phishing and malware attacks
- Increase IT efficiency with automated analysis and remediation
- Secure communications with partners across the supply chain
- Develop risk-related metrics and reporting to help guide security strategy

The Solution

- Proofpoint Enterprise Protection with Targeted Attack Protection and Threat Response Auto-Pull
- Proofpoint Internal Mail Defense and Proofpoint Email Fraud Defense
- Proofpoint Nexus People Risk Explorer
- Proofpoint Security Awareness Training with CLEAR

The Results

- Significantly reduced the number of malicious emails reaching employees
- Reduced resources dedicated to analysing suspicious emails
- Empowered CISO with metrics showing decrease in phishing delivery rate by 5% and click rates by 88%
- Improved employee awareness and increased employee reporting of phishing attempts

The Company

Global food packaging and processing company seeks email security

A package should save more than it costs. That's the belief of this global food packaging brand that produces almost 200 billion food and beverage containers each year. The company works closely with its customers and suppliers to provide safe, innovative and environmentally sound products. Each day, these products meet the needs of hundreds of millions of people in more than 160 countries. With more than 25,000 employees worldwide, the company has built a reputation for innovation, industry leadership, and sustainable business practices. But with so much on the line, the company needed a better approach to securely protecting its email communications.

The Challenge

Building a secure email infrastructure for a global business

Cyber criminals may use various tools to breach a company's network, but message-based attacks are far and away their most effective weapon. The company has been long aware of this fact. And it has tried to prevent phishing and other malware attacks on its employees and partners for many years. But as cyber criminals have become more sophisticated in their targeting and methodology, the company's chosen solution began to show its limitations.

"We had several issues with our previous supplier," explained the company's lead IT security analyst. "And with our support contract expiring, we decided it was time to bring on another vendor."

To start, the team needed to increase the number of phishing messages stopped by their email security gateway. More than 40% of malicious emails were slipping past it. And even after they educated employees on identifying phishing emails, the team found far too many genuine attacks getting through and tricking their employees into clicking on malicious links. The team soon reached their turning point. The company was hit by an attack that slowed down email delivery for close to 12 hours, which significantly impacted everyone's productivity. The team knew they had to quickly find a better solution.

"Proofpoint has been incredibly effective in identifying and stopping malicious attacks. Now we have full visibility into our email environment. We've been able to streamline our analysis and remediation. And in turn, we've increased our overall company security."

Lead IT security analyst

The Solution

Proofpoint delivers on all counts

With a complex, global environment, the company sought a single partner to work with to protect the company from message-based attacks. The security team invited several vendors to participate in an extensive RFP process across a wide range of requirements. Proofpoint beat the competition on all counts. And the selection of Proofpoint as the Gartner Magic Quadrant leader in the space gave senior managers the confidence they sought in moving forward with Proofpoint.

The security team started by laying a strong foundation for their email security architecture. They implemented a multi-tiered approach to meet their requirements. This began with Proofpoint Email Protection with Targeted Attack Protection (TAP) and Threat Response Auto-Pull (TRAP). TAP uses static and dynamic techniques to continually adapt and detect new cyber-attack patterns. And it analyses potential threats by using multiple approaches to examine behaviour, code and protocol. TAP also detects threats and risks in cloud-based applications and connects email attacks related to credential theft or other attacks. And it uses machine learning to observe patterns, behaviours and techniques used in each episode. TRAP analyses messages against multiple intelligence systems and shares the results with the message security team. It can automatically delete or quarantine messages above a certain risk threshold. Or it can provide the security team with the information needed to decide manually. And that decision can be executed with a single click. Once it's determined that a message is malicious, TRAP automatically removes all harmful content. What's more, it can follow forwarded mail or distribution lists to their end recipients.

"The automated analysis and remediation we gained from TAP and TRAP was a game changer for us. Not only did they stop more malicious emails from getting in, but they significantly reduced the amount of manual analysis we had to do with our previous supplier," explained the lead IT security analyst.

To fully align its solution to users' specific risks, as well as track the success of its solution, the company used Proofpoint Nexus People Risk Explorer (NPRE). This cybersecurity risk model provides a people-centric view into the risks that the organisation is exposed to. NPRE gathers threat data across Proofpoint products and translates it into risk models. It also identifies and segments employees within the organisation into risk groups. And then it recommends customised security controls based on the risk group profile.

The team now had a strong foundation in place. Next they set out to prevent threats from attackers using business email compromise (BEC) and email account compromise (EAC). EAC and BEC attacks share the same goal: to fool the recipient into believing a message originates from a legitimate source to access company information. To address these problems, the team implemented Proofpoint Internal Mail Defense (IMD) and Email Fraud Defense (EFD), respectively. IMD examines internal traffic and identifies BEC and EAC signatures. And then it automatically diverts malicious traffic into a secure location for further analysis. EFD uses DMARC to verify the identity of the sender. DMARC establishes end-to-end email authenticity by keeping a list of approved users, credentials and valid domains at each endpoint. This extends email protection to the company's many partners around the globe. And it significantly reduces security risk in their supply chain.

The company's security team has long known that company employees are the last line of defence against email fraud. With a security awareness training programme already in place, the team chose to expand their efforts in this area. They chose Proofpoint Security Awareness Training with Closed-Loop Email Analysis and Response (CLEAR). With these solutions, they get the ability to automate the employee reporting process, analysis and remediation for suspicious emails.

"CLEAR has been a huge success for us," said the manager of information security education and awareness. "With our previous solution, if employees suspected a possible phish, they had to fill out a form and email it to IT for analysis. Now they press a button on their email toolbar. CLEAR forwards the suspect message, along with all of its details, to TAP and TRAP for analysis and remediation."

The Results

Moving to Proofpoint yields tangible results

With Proofpoint Email Protection with TAP and TRAP, the company has seen concrete results. The team saw 30% more malicious emails blocked than their previous solution. Combined with TRAP's automated analysis and remediation, the Proofpoint solution freed up precious IT resources. And the team went from two full-time people dedicated to analysing potential malware to a single engineer who spends less than half a day on analysis.

The security awareness team has also seen a significant increase in the number of employees who report suspected phishing attacks. This includes both external messages and those generated by the team's regular test campaigns. And using CLEAR, 42% of employees reported the test phish during their latest test, with the percentage increasing every month.

The advanced reporting provided by Proofpoint NPRE gives the team strategic insights that help the organisation map out and prioritise its security budget. For example, a recent report showed an increase in year-on-year credential phishing threats by 54%, but a decrease in both the phishing delivery rate of 5% and click rates of 88% by employees. Using NPRE and TAP to further investigate the finding, the team was able to credit the achievement to PSAT training internally for employees. It also helped them better justify the budget to the CISO and board.

The company has been delighted with the results. Summarised the lead IT security analyst: "Proofpoint has been super to work with. The product is effective and reliable, and the support team made installation straightforward. Proofpoint has not only stopped more attacks, but we now have visibility into our entire email environment. We've been able to streamline our analysis and remediation. And in turn, we've increased our overall company security."

LEARN MORE

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

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.