proofpoint

CUSTOMER STORY

Global Auto Parts Manufacturer Benefits From Managed Security Awareness Training

End-to-End Proofpoint Solution Slashes Targeted Phishing Attacks

THE CHALLENGE

- Reduce fraudulent email and directed phishing attacks
- Increase employee awareness of email-based scams and engage them in the security effort
- Improve productivity of the cybersecurity team by automating the triage process

THE SOLUTION

- Proofpoint Email Protection with Targeted Attack Protection (TAP) and Threat Response Auto-Pull (TRAP)
- Proofpoint Managed Security Awareness Training (mPSAT)
- Proofpoint Closed-Loop Email Analysis and Response (CLEAR)

THE RESULTS

- Blocked virtually all malicious email attacks against employees
- Engaged employees as active defenders of company security
- Significantly improved productivity of cybersecurity team

The Company

This U.S.-based public company is a leading manufacturer and distributor of replacement parts for motor vehicles. Over the decades, the company has built its reputation on quality and reliability. As a result, it has gained the trust and loyalty of partners and customers worldwide.

The Challenge

Staying ahead in an ever-changing cybersecurity landscape

One of the greatest frustrations of cybersecurity experts charged with protecting their companies from email-based attacks is their inability to get ahead of the criminals who try to break through their many layers of security. As soon as a security team identifies, analyzes, and can block one type of malicious phishing or malware vehicle, criminals have designed a new "phish" specifically designed to avoid the existing detection methods. Leveraging the shared libraries of recent attacks provided by Proofpoint and others can help companies reduce the response time to new threats. But by definition, this process is reactive, rather than proactive.

This automotive parts manufacturer—a Proofpoint customer for almost seven years—knows this frustration well.

"It's like a game of "Whack-a-Mole," said the information security officer. "Every time one new phishing attack pops up, we find it and stop it. But right away, something new comes along and occasionally slips through."

The company first started working with Proofpoint in response to the deluge of spam their employees received each day. Discussions with Proofpoint engineers convinced the information security team that they needed broader email protection than a spam filter could provide. Over time, the company has implemented a range of Proofpoint products in a constant effort to stay ahead of attackers. In addition to Proofpoint Email Protection,

the company installed Proofpoint Targeted Attack Protection (TAP), Threat Response Auto-Pull (TRAP), Encryption, and Email Data Loss Prevention (DLP). These solutions successfully blocked almost all phishing and malware attacks, significantly increasing IT and employee productivity.

To further protect the company from phishing attacks, the security team realized they needed to train their employees to identify potentially-malicious messages. Their goal was to engage all email users as active participants in company security. The security team sought to provide their users with the tools they needed to respond correctly in such situations.

> "We've been a Proofpoint customer for about seven years now. We've put a lot of eggs in the Proofpoint basket, and it's been rock solid. We've never regretted any purchase we've made from Proofpoint."
>
> Information Security Officer

The company had initially engaged another vendor to provide phishing awareness training. While the security team saw the benefits of a managed training program, over the course of a year they found critical holes in the solution that impacted not just employees but demanded additional time and effort from the security team. The "suspected phishing mailbox" received as many as 45 "suspicious" emails daily, with each one requiring fifteen minutes to an hour of manual analysis to resolve. Also, the incompleteness or inconsistency of the information employees forwarded increased the difficulty of the investigation. Soon the team required a full-time resource to handle the load.

The Solution

Managed Proofpoint Security Awareness Training with CLEAR

The security team met with Proofpoint to discuss the issues they faced. They were committed to a managed security training model but required a more efficient, automated solution. The team also wanted a seamless integration with their existing Proofpoint investment.

Proofpoint proposed a solution: Managed Proofpoint Security Awareness Training (mPSAT), coupled with Proofpoint Closed-Loop Email Analysis and Response (CLEAR). This combination would not only expand their employee-educational efforts but automate the process of reporting suspicious emails, the analysis of those emails, and the remediation process once the investigation is complete.

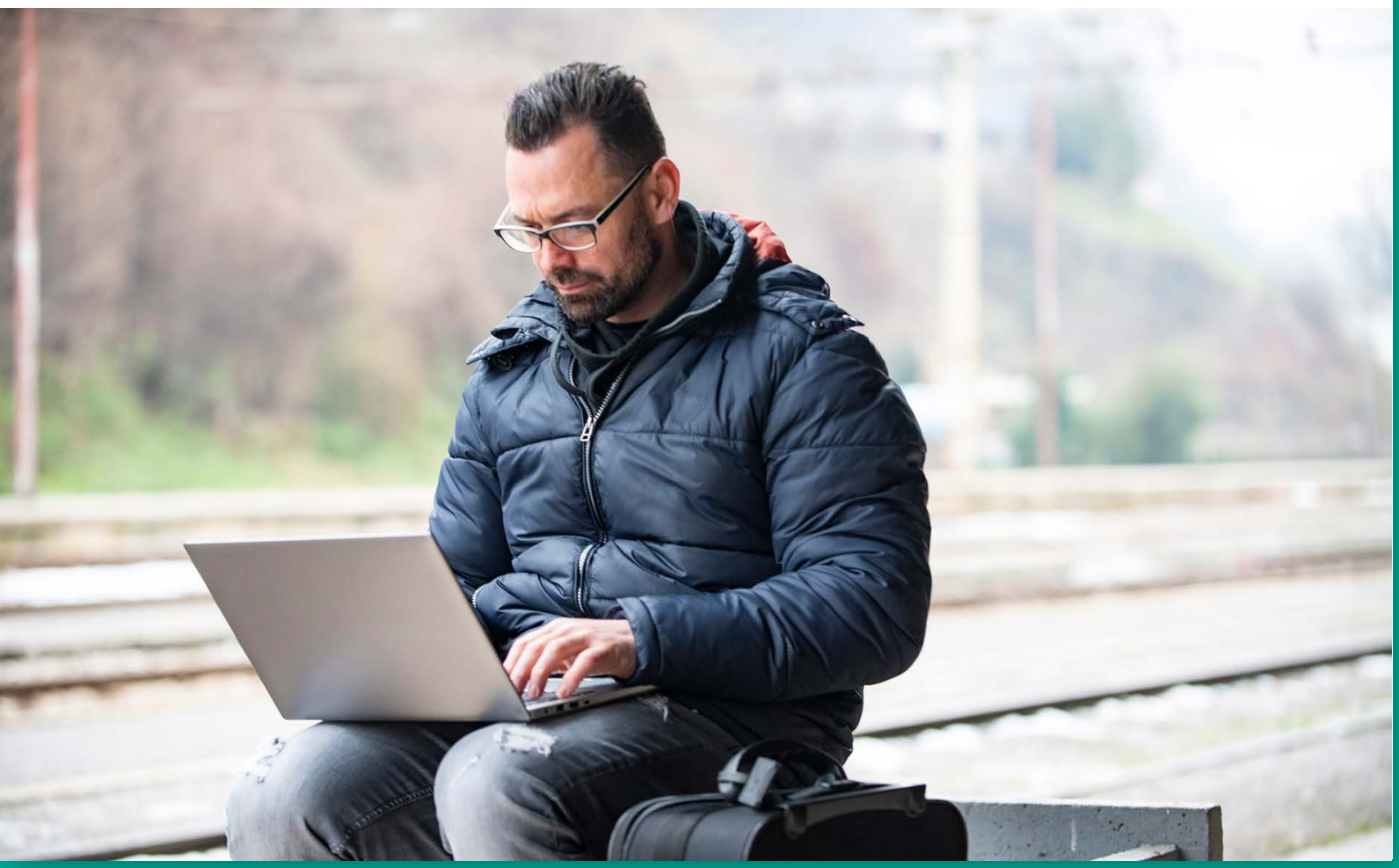
Given their experience with Proofpoint, the security team felt confident that mPSAT could meet their training needs. However, CLEAR turned out to be a critical factor in the company's decision to switch from their existing vendor to Proofpoint. The integrated solution provided a far broader managed training and awareness program than their initial vendor provided.

CLEAR is composed of three key pieces. First, a PhishAlarm "button"—embedded in all desktop and mobile email clients—allows users to send suspected phishing emails directly to an abuse box with all headers and attachments intact, providing consistent information for analysis. Second, a module called the PhishAlarm Analyzer receives the suspect messages, analyzes them based on various risk factors, and categorizes them based on their likelihood of containing malicious content. This intelligent process reduces the triage time required each day from hours to minutes. And third, PhishAlarm Analyzer passes the information on to TRAP for manual or automated remediation.

TRAP analyzes the reported messages against multiple intelligence and reputation systems and shares the results with the message security team. TRAP can automatically delete or quarantine messages above a certain risk threshold, or it can provide the security team with the information needed to make a determination manually. A security engineer can execute the proper decision with a single click. Once analysis determines a message to be malicious, TRAP automatically removes all harmful content, wherever it is. TRAP can follow forwarded mail or distribution lists to their end recipients. Even if an employee clicks on a malicious link and later realizes they have made a mistake, they need only hit the PhishAlarm. PhishAnalyzer and TRAP will then take all of the actions necessary to purge the malicious content from the system.

Also, CLEAR was included with the company's existing TRAP license and thus required no additional investment. The combination of these factors made the decision to move to an end-to-end Proofpoint solution an easy one.

As part of the overall mPSAT effort, the information security officer also wanted an administrator who could oversee and coordinate the company's entire security awareness and education program. The mPSAT administrator takes on the challenges of designing, running and reporting—all necessary for a security-education program to succeed. A dedicated administrator is an experienced resource who can free up the information security officer, as well as the security team, to focus on new projects and other priorities. This novel training program gives employees the knowledge, training and tools they need to take an active role in protecting themselves and the company. The result is fewer "clicks" on phishing emails and earlier identification and reporting of suspicious messages.



The Results

mPSAT with CLEAR brought immediate improvement in employee awareness and participation

According to the information security officer, the transition from the company's previous training vendor to Proofpoint mPSAT was completely seamless. "The mPSAT administrator has been excellent and has taken a load of administrative work off of my plate. And Proofpoint's managed training model has shown us the benefits of using a single vendor to protect our employee communications."

The mPSAT team began with monthly tests, sending out emails to all employees using the latest attack methods. If a test pointed out specific areas for improvement, the administrator designed a targeted campaign to address the issue, working with both teams and individuals to provide additional education as needed. The results have been measurable and significant, dramatically reducing the number of "clicks" on malicious links embedded in the test emails.

CLEAR has exceeded the security team's expectations. When an employee clicks on the PhishAlarm button, they receive instant feedback that their message has been received, making them active participants in the company's security. Within less than six months, the number of employees who clicked PhishAlarm in a test case has increased five-fold, from 5% to 25%. The information security officer credits the improved performance in tests to the use of positive reinforcement.

"PSAT is an educational program," explained the information security officer. "We want to reward people for taking the correct action, not criticize them for making a mistake. We want our employees to become part of the solution. They are not just our last line of defense, but our first line of defense against the newest types of malicious email."

The automated CLEAR process has also reduced the amount of time required to receive, analyze and remediate suspect emails. What used to take a full-time resource to address the daily volume of suspicious messages can now be handled in a few minutes by anyone on the security team, increasing the team's productivity.

"We've been a Proofpoint customer for about seven years now," summarized the information security officer. "We've put a lot of eggs in the Proofpoint basket, and it's been rock solid. We've never regretted any purchase we've made from Proofpoint."

LEARN MORE

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