proofpoint.

CUSTOMER STORY

Major US Financial Institution Ensures Email Integrity with Proofpoint

Proofpoint people-centric email security solution halts directed email attacks

THE CHALLENGE

- Reduce cybersecurity risk from fraudulent email, targeted phishing attacks
- Prevent attackers from spoofing the company's domain name
- Maintain the trust of customers and partners; reduce financial exposure

THE SOLUTION

- Proofpoint Email Protection and Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)
- Proofpoint Cloud App Security Broker

THE RESULTS

- Blocked or quarantined over 6.6 million unwanted messages in 30 days
- Achieved 100% rejection of fraudulent email to reduce risk
- Protected employees' email and cloud accounts from BEC and EAC attacks
- Stopped domain-based spoofing and protected the integrity of the company brand

The Company

This leading U.S. financial services company has served its clients faithfully for more than 150 years. With more than 6,500 financial advisers serving approximately five million clients, the company provides the full spectrum of financial services. These include consultation on wealth and asset income protection, education and retirement planning, and investment advice. The company's financial performance and long-standing reputation of trust have kept it growing steadily. And over the years it's become one of the most highly valued companies in its sector.

The Challenge

Battling for secure communications

The company has a reputation for integrity and safety that is every bit as important as the returns it generates or its assets under management. As the company transitioned into the Digital Age, it invested heavily in becoming a technology leader. And it had a particular focus in the area of security. Over time, the company has become very adept at leveraging new technologies to help battle attackers who were attempting to defraud their clients, employees and partners. And one of the forefronts of this battle has been in the area of personal communications, particularly in the areas of business email compromise (BEC) and email account compromise (EAC).

According to the company's senior engineer for email security, "Our biggest challenges from a cybersecurity standpoint were either through spoofed emails getting through or hacked accounts. We also saw a lot more domain spoofing, with bad actors using our domains to send out fraudulent messages. And as we migrated more functionality to the cloud, we saw more and more cloud email accounts attacked."

The team also had limited visibility into their email traffic, as well as its contents. They had implemented rules on their previous email gateway. And they had deployed filters to block incoming spoofed traffic. However, it was impossible to see all incoming and outgoing email messages. This lack of detail limited their ability to block all suspicious traffic.

The Solution

Creating multiple layers of intelligent protection for 100% coverage

The company turned to Proofpoint to address these issues. And it found its solution in Proofpoint Email Protection and Email Fraud Defense. The email security team also implemented Targeted Attack Protection (TAP) and Threat Response Auto Pull (TRAP). These protect them against messages carrying advanced malware, ransomware or dangerous links. These intelligent tools identify known or suspected malicious senders. And they either block or quarantine any suspect messages for further analysis, even after delivery. If the analysis determines a message to be malicious, TRAP follows forwarded mail or distribution lists. And it removes all dangerous content from the system. These features gave the company a foundation of protection against advanced malware, ransomware and dangerous URL links.

> "Proofpoint provides us with a multilayered approach to preventing email-based attacks and ensuring email authenticity. This gives our employees, customers and partners the confidence they need to trust their communications and know that the assets we manage are safe."
>
> Senior Cybersecurity Engineer, Email Security

Proofpoint also helped the company address their BEC and EAC attacks. BEC, in particular, had become increasingly common. Display-name spoofing, domain spoofing, and lookalike domains can "trick" the receiver of a message into believing a message is coming from a known and trusted source. As an example, the team described one attempted attack during which more than 500,000 messages arrived from a spoofed domain during a single 16-day window.

The email security team was able to block this massive attack, and many others of lesser magnitude. To do this, they used Proofpoint Email Fraud Defense to implement DMARC (Domain-based Message Authentication Reporting and Conformance). Email Fraud Defense gave the team visibility into the details of domain-based attacks targeting employees, customers and business partners. And it provided them with the ability to quarantine or block any messages from suspicious domains. When team members first implemented the solution, they found many cases where up to thousands of spoofed emails arrived over a brief period, often from multiple spoofed domains. This detailed visibility allowed them to create rules to identify, quarantine and block any domain-based fraudulent messages.

"The email security team is responsible for making sure that our employees and our financial reps are safe. Impostors or bad actors often try to fool someone into authorizing a fund transfer or sending out gift cards by sending a fake email from our CEO," said the company's senior engineer for email security. "These bad actors are increasingly sophisticated: sometimes 50% of the message is legitimate and the other 50% is not."

The team then turned to its cloud-based communications. As the use of cloud email services has increased, attacks on cloud-based accounts have skyrocketed. Once attackers have hacked a remote account, they gain complete control over that account. They can cause severe damage, as any email recipient believes a received message is "genuine" because it originated from a trusted source. To protect their cloud-based communications, the company installed Proofpoint Cloud App Security Broker (CASB). CASB extends advanced threat protection to the cloud, allowing the IT team as a whole to detect, investigate and defend against bad actors attempting to access sensitive data and trusted accounts. For example, any suspect file uploaded to a cloud-based collaboration app is quarantined and analyzed for potential risks in real time. CASB also interoperates seamlessly with the Proofpoint suite of protection tools, sharing data, and effectively expanding the area of protection to include all cloud-based operations.

The Results

Layered, people-centric approach delivers secure communications

With the automated threat detection and remediation provided by Proofpoint, there was an immediate impact. During a recent 30-day window, for example, the company received over 18 million inbound messages. Of those, 37%—some 6.6 million messages—were blocked or quarantined. The email security team credited Proofpoint Email Protection and Email Fraud Defense—in particular TAP and TRAP—for catching the vast majority of malware directed at their employees.

"At first glance, some emails can look legitimate," explained the email security team's senior engineer. "But TAP examines everything. And it can either block a suspicious email or quarantine it and notify us that we need to investigate further. Even if a malicious message has already been delivered, TRAP automatically pulls it from every mailbox. This saves our team a lot of manual work."

With DMARC, the email security team added another robust layer of protection around their communications system. When they first implemented DMARC, they found regular instances of massive domain-based attacks. There were up to thousands of spoofed emails received over brief periods, often from multiple spoofed domains. DMARC also allowed them to prevent malefactors from using the company's valuable domain names for attacks on third parties. This helped them protect the integrity of their brand.

The final piece the team put in place came in response to the increasing use of cloud-based tools. EAC attacks, in particular, have increased as more users turn to cloud-based applications for collaboration and communication. The email security team installed CASB to protect their employees' cloud activities from attack. According to the email security team lead, the company hasn't had a single cloud account compromised since CASB began to monitor and protect their cloud-based users.

"Once attackers have hacked a remote account, they gain complete control over that account," said the senior email security engineer. "They can then cause severe damage, since email recipients believe a received message is 'genuine' because it originated from a trusted source."

Through its seamless integration across all points of attack, Proofpoint provided the email security team with a single, unified view of their communications security system. Proofpoint allows them to make modifications, add new rules, or implement additional features as new threats emerge.

"With Email Protection and Email Fraud Defense, combined with DMARC and CASB, Proofpoint gave us the closest thing there is to a 'silver bullet' against email fraud," the company's email security team leader concluded.

LEARN MORE

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

0601-005-01-01 6/20