proofpoint.

CUSTOMER STORY

US Healthcare Network Protects Email and Cloud Apps with Proofpoint

Proofpoint's People-Centric Solution Secures Critical Patient Information from Cyber Attacks

THE CHALLENGE

- Prevent theft of critical patient information
- Protect company email from phishing, malware attacks
- Defend against cloud account compromise

THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint DLP for email
- Proofpoint Cloud App Security Broker (CASB)

THE RESULTS

- Sharply reduced email-based threats
- Halted cloud account takeover and data breach
- Improved overall efficiency of the IT Security team

The Company

Most physicians enter healthcare because of their passion for medicine and people—not management and paperwork. Running a private healthcare practice offers doctors the freedom to treat patients without the constraints of a large healthcare system. But often, the economics and administrative overhead involved make private practices difficult to manage and grow.

That's where this Proofpoint customer comes in. By providing capital, management services and administrative support, the healthcare network gives private practices the efficiency and scale of a large medical system without giving up their independence.

The company has drawn together independent ObGyn practices and other women's health services into a 600-doctor alliance. Today, it has become one of the country's leading networks of high-quality, low-cost healthcare services for women. But even as it expands, its mission remains the same: blend quality, safety and value through coordinated, integrated medical management programmes and managed-care contracts.

The Challenge: Protecting Patients' Information from Advanced Attacks

As a healthcare company, one of the company's top priorities is protecting patients' private information. In any organisation, the cost of data loss can be high. But in a highly regulated industry such as healthcare, losing patient information can cause serious, lasting harm.

If someone steals private health information, the company doesn't just have to report the breach to its customers and the public. It must also tell regulators and engage an outside forensic analyst to investigate the breach, find the root cause and assess the company's response. If the analyst uncovers systemic problems, the government may impose hefty fines.

Like many healthcare companies, the company was facing a sharp increase in email phishing and malware attacks. Its legacy cybersecurity defences were struggling to keep up.

"We were seeing a constant increase in emails with phishing links or malicious files attached, all designed to get access to patient information," said the company's security manager.

At the same time, the company's shift to cloud-based apps and storage created new opportunities for cyber criminals.

The Solution

The company's first step was bringing in email security specialists for advice on improving email security for employees, member physicians and patients. As part of that process, the company held proof-of-concept trials (PoCs) with several vendors.

Proofpoint stood out because of its high accuracy. It blocked more malicious emails with a much lower number of false positives than other systems tested.

Securing the no. 1 threat vector with a complete email solution

Soon after the PoC, the healthcare network deployed Proofpoint Email Protection. The solution includes Proofpoint Data Loss Prevention (DLP), Targeted Attack Protection (TAP) and Proofpoint Email Encryption to stop email threats and secure sensitive data. And to help automate remediation when something goes wrong, the team installed Proofpoint Threat Response Auto Pull (TRAP).

> "The cost of any breach is high. Our entire reputation is at stake. Proofpoint has given us the tools we need to protect our patients' personal information."
>
> Security Manager

TAP and TRAP are intelligent tools that identify known or suspected malicious messages. TAP blocks or quarantines suspicious emails for further investigation. If the analysis confirms malicious content, TRAP removes it from users' inboxes—even after they've been delivered or forwarded to other users.

DLP, meanwhile, monitors and stops any critical data from being stored or forwarded to any unapproved destination, including cloud-based locations.

Securing the cloud

As more and more employees use cloud-based apps and storage, attackers follow. Cloud-based attacks are especially insidious. If bad actors gain access to a cloud account, they can act as a company insider. That means they can send emails, move client data or even trick other users into wiring money or diverting payments.

These are known as email account compromise attacks, and they often target executives' accounts. By taking over the account of someone in authority, attackers not only have access to the executive's email and data but can trick other employees into taking all sorts of harmful actions.

In a recent six-month study, 97% of companies saw attacks on their cloud accounts. About 60% of companies experienced a compromise. And 11% had executive accounts compromised.[1]

With Email Protection in place, the healthcare company turned to Proofpoint for ideas on how to apply its email DLP policies to cloud-based data.

1 Internal Proofpoint Research

The first step was an easy one. The Proofpoint support team recommended that the healthcare network turn on the included TAP SaaS Defense feature in its Proofpoint solution.

The Results

This feature, which comes included to all TAP customers at no added cost, monitors cloud threats and detects accounts that may have been compromised.

Almost immediately after turning on TAP SaaS Defense, the company uncovered a compromised Microsoft 365 account. An employee's account had been breached. The quick discovery gave the company a chance to react before any confidential data was lost.

"Proofpoint TAP SaaS Defense gave us visibility into a suspicious cloud-based email account," the company's security manager said.

The incident spurred the healthcare company's security team to reassess their overall cloud security posture. The team realised that it would need protection beyond DLP.

After testing several options, the company selected Proofpoint Cloud App Security Broker (CASB) to protect its Microsoft 365 environment. CASB extends Proofpoint's advanced threat protection and DLP capabilities, including Threat Response Auto Pull, to the cloud.

CASB shares DLP classifiers, built-in smart identifiers, dictionaries, rules and templates with other Proofpoint products. This integrated approach allows the security team to protect the personal health information of their clients in cloud-based storage locations with the same DLP rules they use to protect email. By unifying DLP policies, the company reduced risk across email and the cloud without extra management overhead—no need to manually keep policies in sync or recreate rules.

The solution detects critical data stored in the cloud and can halt any transfers of confidential data and hold the files for further analysis. It also protects cloud-based accounts from compromise from phishing emails, stolen credentials and brute-force credential attacks.

CASB works seamlessly with Proofpoint's entire suite of protection tools. By sharing data under a single security "umbrella," it expands Proofpoint's industry-leading email protection to include all cloud-based operations.

By installing CASB, IT teams can detect, investigate and defend against attempts to access sensitive cloud-based data and trusted accounts.

The Results: Far Fewer Malicious Emails, Compromised Cloud Accounts

The results of both Proofpoint deployments were dramatic.

With Proofpoint Email Protection, the number of malicious emails went to almost none—most of them before they reached users' inboxes.

And with CASB, the healthcare company slashed the number of compromised cloud-based accounts from five to 10 per month to just two or three per quarter. The remaining fraction of successful account compromises are detected and quickly mitigated—before they have a chance to cause lasting harm.

According to the company's security manager, the CASB solution has helped heightened the company's overall cloud security.

"CASB gave us the insight and tools we needed to protect our cloud-based accounts and assets," the security manager said.

CASB now monitors all client information sent or stored in the cloud, with access limited to only those who need it. Suspicious login and geofencing rules have helped prevent account takeovers before they occur. And automated, adaptive access policies help verify and remediate suspicious activity that points to a compromise attempt.

More efficient IT, end-user productivity

Beyond keeping the company secure, CASB has also helped IT Team become more productive. In the past, it might spend five to six hours every week checking through security reports. Today, it can investigate an incident in minutes.

CASB is tightly integrated with the company's IT help desk. CASB alerts are prioritised, and when one is triggered, an IT engineer looks into it right away.

The tech first reaches out to the employee to see whether the user is near the location indicated in the alert. If so, the alert is likely a false positive. If the user is not in the same area or can't be located, IT disables their account in Active Directory until they can work with the user to reset the password.

"We have a small staff," the security manager said. "CASB frees up time."

Email Protection comes out-of-the-box with PHI and HIPAA dictionaries that Proofpoint updates, further reducing the company's maintenance load. An open-ended engagement with Proofpoint Professional Services also gives the company access to expertise to help deploy new features as needed—without paying add-on fees.

The combination of Proofpoint features and support gave the healthcare company the confidence it sought to protect its healthcare network from advanced cyber attacks.

The net effect of the Proofpoint installation has been greater data security, fewer compromised accounts and higher productivity for employees, members and the IT Team.

"The value we gain from Proofpoint is tremendous," the security manager said. "In the health industry, the cost of any breach is high. Our entire reputation is at stake. Proofpoint has given us the tools we need to protect our clients' personal information."

LEARN MORE

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