proofpoint.

CUSTOMER STORY

Colonial Companies Defends Data and Migrates to Cloud With Proofpoint

COLONIAL
Banking | Home Loans | Insurance

The Challenge

- Protect employees and operations from email fraud
- Stop loss of intellectual property
- Safeguard brand reputation
- Streamline administration

The Solution

- Proofpoint URL Isolation
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull
- Proofpoint Security Awareness
- Proofpoint Data Loss Prevention
- Proofpoint Insider Threat Management

The Results

- Secures email against business email compromise
- Streamlines insider investigations
- Prevents sensitive data loss from departing employees
- Saves small IT team time with automation

The Organization

Founded in 1952 as Fort Worth Mortgage Corporation, Colonial Companies is now a national, multiservice financial institution headquartered in Fort Worth, Texas. Servicing more than $23 billion in residential mortgage loans, Colonial Companies understands that there's a lot riding on its network infrastructure. The company trusts Proofpoint to keep its operations—and its reputation—safe from cyber threats.

The Challenge

Preventing sensitive data loss from departing employees

In the financial services industry, smooth, secure communication is key. And it's the foundation for high-stakes business processes. But not all threats come from outside the organization, so Colonial deployed Proofpoint Insider Threat Management (ITM). This cloud solution helps the organization protect sensitive data from insider threats and data loss at the endpoint. Colonial's primary use case is departing employees, which has been particularly useful during a time of flux in the industry. Proofpoint ITM's consolidated view of alert data, screen shots for context, and out-of the box threat library have helped the organization safeguard sensitive company data in a way that aligns with their business needs.

"In the past year, we've had some employee attrition for a variety of reasons," said Dakota Reynolds, information security threat analyst at Colonial Companies. "Proofpoint ITM helps us detect data exfiltration and risky behavior of people who are leaving."

> “This ITM cloud solution has substantially streamlined what I do, especially when investigating alerts.”
>
> **Dakota Reynolds**, information security threat analyst, Colonial Companies

Migrating email to the cloud, securely

Like all financial services organizations, Colonial relies on email to move applications and business transactions forward. The company uses a mixed email environment, with some emails going through Microsoft Exchange Cloud, and others being handled on-premises. So protecting this hybrid environment is challenging, especially as new threats evolve and change.

“Most of what I see in the traffic on a daily basis is business email compromise attacks (BEC), and phishing attempts for credentials,” said Dakota Reynolds, information security threat analyst at Colonial Companies. “Bad actors send mass emails to our employees, trying to phish their credentials to gain a foothold, or use a compromised account to send attacks to other people. And we can see up to 40 of these types of attacks each day.”

Colonial Companies was looking for an easy-to-manage, multilayered solution that could protect the organization from the latest cyber threats. It also wanted to provide best practices training to its employees to strengthen its effectiveness.

The Solution

Gaining visibility into risky behavior

To help safeguard its organization, Colonial deployed a wide range of Proofpoint solutions. For protection against insider threats, Colonial uses Proofpoint ITM to gain visibility into its riskiest users to quickly detect suspicious behavior. The screen shots provide context into unusual activity, which helps Colonial determine the best response.

“We have 35 different alerts set up in Proofpoint ITM for different conditions, such as uploading a file to a website that exceeds a certain size,” said Reynolds. “We also use ITM for our users who may be leaving the organization. When that rule gets triggered, they are placed in a special Active Directory group for closer monitoring and the alert severity increases.” Reynolds adds: “This ITM cloud solution has substantially streamlined what I do, especially when investigating alerts.”

Taking full control of a trusted domain

For protection against BEC threats, Proofpoint Email Fraud Defense helps Colonial secure its email channel to maximize trust in business communications. To minimize the risk of inbound imposter attacks, phishing and malware, it automatically identifies the company’s business partners and suppliers. Then it validates their DMARC records and uncovers the risk they pose.

Proofpoint Email Fraud Defense has also helped Colonial simplify its DMARC authentication, through guided workflows and support from consultants. To protect its brand, Colonial is employing a DMARC policy set to p=reject. This instructs email receivers to refuse to accept email that fails the DMARC check.

“Enforcing DMARC and going to p=reject was a way for us to keep people from spoofing our address and trying to cause some reputational harm to our company,” said Reynolds.

Reynolds and his team also use Proofpoint Domain Discover within Proofpoint Email Fraud Defense. This feature automatically identifies lookalike domains that could be used to impact its brand. And it enables the team to take action against them.

To extend its email security strategy beyond technology alone, Colonial uses Proofpoint Security Awareness to help foster a culture of security.

“We use Proofpoint Security Awareness Pro to give all our employees comprehensive training on phishing awareness,” said Reynolds. “When our users come on board, they get the training. And then we have them repeat it annually. So they’re pretty good at using Proofpoint for Microsoft Outlook to report emails that they would consider to be suspicious.”

If a user reports a suspicious email, it is sent to the organization’s Closed-Loop Email Analysis and Response (CLEAR) mailbox. This accelerates user reporting and security response to phishing attacks.

“Most of what our users are reporting is pretty accurate, which speaks to the quality of the Proofpoint Security Awareness training that we’re providing,” said Reynolds.

The Results

Securing the organization and saving time
Colonial recently migrated from Proofpoint ITM on-premises to ITM SaaS, a cloud-native solution that is part of the Sigma Information Protection platform. Now, instead of clicking from screen to screen, Colonial is able to see alert metadata in a single view.

Reynolds sees a lot of value from the migration. “The ITM SaaS solution has substantially streamlined what I do, especially when investigating alerts. The dashboard is a lot more useful. The screen shots work so easily in ITM SaaS and provide the context needed to determine a user’s intent.”

To empower its security team with more proactive capabilities, Colonial also deployed Proofpoint Threat Response Auto-Pull (TRAP). This threat management platform lets Reynolds and his team streamline the incident response process. When a potentially malicious email is detected, TRAP automatically removes it. The solution can also quarantine emails after they have reached user email boxes, which lets the security team sidestep slow, repetitive manual processes.

“When you quarantine an email in TRAP, you can also set it to quarantine anyone else copied on the message,” said Reynolds. “Using these products makes my life a lot easier. I no longer have to go in to pull every single email myself—and possibly not even recognize that something has happened until after the fact. Knowing that TRAP is acting on a threat on our behalf is extremely helpful, because then I can take actions to make sure that every recipient is protected. I can pull that specific email from their inbox before they can accidentally click on something.”

Proofpoint Targeted Attack Protection (TAP) has also helped the organization strengthen its security. Its built-in URL Isolation feature analyzes and isolates select URLs based on security policies. This means users can access websites from their email with confidence.

“If an email is from an external sender, every link goes through URL Isolation,” said Reynolds. “So if Proofpoint has identified a domain that is malicious, our users can’t engage with it, because it’s blocked automatically. That’s an additional layer of security that really is helpful.”

For Colonial Companies, the comprehensive Proofpoint portfolio of security offerings has given the security team a multifaceted approach to protecting the organization.

“Proofpoint solutions give us a range of protection, so if one product doesn’t cover a threat, something else will,” said Reynolds. “That’s a huge benefit to us. From time to time, one of our executives will ask about a particular security solution, such as URL isolation or security training. And in a lot of cases, we can let them know that we already have a solution in place for the issue.”

LEARN MORE

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