CUSTOMER STORY

Global Wine Company Controls Business Email Compromise Scams With Proofpoint

The Challenge

- Protect business processes from business email compromise (BEC) and ransomware
- Develop a risk-focused workplace culture and awareness of cybersecurity threats
- Accelerate response time to day-zero threats

The Solution

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection
- Proofpoint Threat Response Auto-Pull
- Proofpoint Security Awareness Training

The Results

- Dynamic security protects wine maker from emerging threats
- Threat response time reduced from days to minutes
- Automated solution helps cybersecurity team save time and focus on more strategic tasks

The Company

For this global wine company, world-class winemaking and brand marketing make a successful pairing. It serves customers in more than 70 countries, making it one of the largest wine companies in the world. And with more than 3,000 employees worldwide, the company focuses on growing and sourcing grapes, and making and promoting its wine. But with such a large organization, protecting against growing threats in email became a very real concern.

The Challenge

Taking critical email protection beyond the basics

The wine company is truly a global enterprise. It has over 65 brands and nearly 13,000 hectares of vineyards. But its IT team faced increased pressure to protect the company from emerging new threats, which were targeting their steadily evolving infrastructure.

“We have a fairly small, distributed security team,” said the global head of information security at the wine company. “Over the years, our organization has become more complex. And we have acquired some new wineries and other properties. So securely integrating the systems and data from those acquisitions has been among our biggest challenges.”

Like most organizations, the company relies on email and internet access to support its most important business operations and its supply chain. The company uses Microsoft 365 productivity applications with E3 licenses that provide a variety of security services. But as the threat landscape evolved, the company needed to strengthen its cybersecurity to proactively protect the organization against potential gaps.

“There was a discomfort with visibility and protection around email,” said the global head of information security. “As we evaluated our security posture, we also started to see a bit more in the press about the escalation of business email compromise threats. We were concerned about accounting fraud, where threat actors stand up a spoof domain and ask our organization to make banking changes. We were also worried about users simply clicking on links that they should not, potentially placing malware or ransomware on their workstations.”

> “Proofpoint has enabled us to get ahead of some threat campaigns very early and thwart them before they could go any further. Our lead SOC analyst just told me how glad he was that we were able to catch a recent threat early, because we could have easily been among the many victims of a ransomware attack.”
>
> Global Head of Information Security, Global Wine Company

The Solution

Strengthening security awareness with Proofpoint

The team realized that it needed not only technology solutions to augment its email security, but stronger best practices. It also needed better awareness of security and trust throughout the company culture.

“We’re a wine company, and that means our workforce primarily thinks about the business of wine production,” said the global head of information security. “Like many organizations, our employees tended to take email protection for granted. But our annual testing exercises and phishing exercises revealed that we weren’t quite where we needed to be in terms of email handling and hygiene. That was one of the catalysts that drove us to ensure that we were properly protecting our business.”

To improve its email security, the company deployed the Proofpoint Enterprise Protection Suite. This cloud-based platform accurately classifies and blocks threats. And it combines sophisticated threat intelligence with phishing detection, anti-spam and antivirus technologies. To help educate its workforce about the new solution and arm them with best practices for safer behavior, the company also signed up for Proofpoint Security Awareness Training.

“We’ve initially been using Proofpoint Security Awareness Training to determine our baseline. We also want to establish a multi-tiered awareness strategy around phishing and other threats,” said the global head of information security. “That’s a real benefit of the platform. It also helps our employees know that there’s a security function in place that provides these types of training services, which is much more than just background security activities.”

The company also deployed Proofpoint Threat Response Auto-Pull (TRAP). TRAP can automatically quarantine malicious emails that are able to bypass the company’s perimeter. And to streamline the email incident response process, TRAP uses Proofpoint Threat Intelligence to classify messages. This helps correlate threat data across email, cloud, network and social media. What’s more, this automation and intelligence saves the team time with email analysis and clean up, and reduces their threat exposure and limit potential damages.

The Results

A smarter, faster approach to discovering and stopping threats
Deployment of the new solution has been smooth, and the Proofpoint team worked closely with the global head of information security and his team to help increase awareness of the capabilities of the solution—and configure it to deliver the strongest outcomes.

"The engagement and responsiveness of the Proofpoint team have been stellar," said the global head of information security. "They are persistent and knowledgeable, and have really helped us educate our IT leadership team. This is also helpful as we work to gain approval for the Proofpoint Security Awareness and Training Platform."

The Proofpoint Enterprise Protection Suite has been highly effective at stopping malicious emails before they could make their way to the company's employees and its business processes. According a recent service review, approximately 76% of inbound messages were discovered to be malicious and blocked. And fewer than 5% of all email threats were imposter threats. Proofpoint Emerging Threat (ET) Intelligence has been extremely successful in accurately detecting potentially harmful communications, with a tiny 0.01% of all inbound email turning malicious after delivery.

The team especially appreciates the solution's threat intelligence, which keeps the organization informed of emerging issues. This helps his team take a more proactive approach to avoiding potential attacks. In a recent service review, the solution determined that 3,150 email addresses were targeted with 10,777 individual credential phishing emails over 90 days. And over the same period, it detected and stopped 185 imposter threats. These include BEC attacks that were based on fraudulent invoices with false banking details from a bottling supplier.

"Proofpoint has been very timely in alerting us to the global threats that have unfolded over the course of the last couple of years that we could potentially have been at risk for," said the global head of information security. "That's something I can't get from all of my security partners, and Proofpoint has been very consistent."

Proofpoint has also provided powerful automation that saves time in responding to issues. This allows the team to stop malicious activity before it can impact employees or business processes.

"My team has told me in the last six months that the URL defense has been a real benefit and they've been very thankful for having that capability in place," said the global head of information security. "In situations where someone might have clicked on something, they generated an alert. We were able to turn around response times much faster than we were able to in the past, especially enabling some of the automated responses with TRAP. That has been really beneficial for us. With a small team, we need to enable as much automation as we can without disrupting the business."

As the company continues to build out its security solution, the team is confident that it can protect the organization. Now not only do they have the latest technologies, but they have a corporate culture that's focused on minimizing risk.

"We've gotten big benefits from the Proofpoint Security Awareness and Training Platform. Now we're advising our employees that we're expanding our security capabilities, along with the education available to them," said the global head of information security. "It's been really well received, and we're moving in the right direction to address email as one of our biggest attack vectors."

LEARN MORE

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

ABOUT PROOFPOINT
Proofpoint, Inc. is a leading cybersecurity company that protects organizations' 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 organizations of all sizes, including more than half of the Fortune 1000, 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**.