proofpoint.

CUSTOMER STORY

Whispir Keeps Internal and Customer Communications Data Secure With Proofpoint

whispir

The Challenge

- Stop business email compromise (BEC) targeted attacks on executives
- Detect and stop phishing, and other email attacks
- Strengthen digital reputation for end customers

The Solution

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)

The Results

- Stopped more than 1.2 million email threats—30% of total inbound traffic
- Detected and stopped nearly 460 advanced targeted threats
- Deep content analysis caught 45,000 email threats, including impostor threats

The Organization

Truly connecting with an audience is key to successful communications. For omnichannel messaging leader Whispir, keeping these communications secure isn't just a network issue—it's the heart of the business. Whispir is a global, cloud-based communication platform that handles more than two billion interactions worldwide each year. It provides customers with intelligent automation and effortless workflows to humanize their communications and maximize their engagement.

Since 2001, Whispir has been relentlessly focused on creating human connections in a digital world. Based in Melbourne, Australia, the company extends across three continents, a presence in the United States, New Zealand, Singapore and Indonesia.

The Challenge

Protecting global communications for employees and clients

Like most businesses, Whispir depends on safe communications to enable employees to connect with customers and colleagues. Its cybersecurity team constantly tracks threats and focuses on proactively stopping the latest attacks before they can impact its business or compromise its data.

"We looked at our biggest threats and risks, and determined that phishing, especially against the workforce, was something that we didn't have a lot of controls in place to protect against," said Martin Littlewood, head of information security at Whispir. "A large majority of security incidents start with spear phishing campaigns, malware and harvesting, so we undertook a market assessment of secure email gateway solutions. We were also concerned that our executives were receiving a lot of business email compromise (BEC) emails."

Whispir is growing rapidly in both revenue and staffing, and Littlewood was concerned that his team might not be able to keep pace with the escalating flood of attacks.

"We hired 100 new staff in the last 12 months—a nearly 50% increase for us," said Littlewood. "As a relatively small information security team in a company that's scaling so quickly, coupled with the fact that email messaging is part of our core business, we needed to be able to prevent as much malicious email and spam at the front door as possible."

Whispir needed an enterprise-grade solution. It had to be one that would not only detect and stop the latest email attacks, but would also provide assistance with DMARC deployment to protect against domain spoofing and stop fraudulent emails from using its domain.

"Before we deployed Proofpoint, BEC attacks were fairly common in our organization, and were noted at the board level. Since our investment in a Proofpoint gateway in front of our email, we have substantially reduced them in a way that is visible to our CEO."

Martin Littlewood, head of information security, Whispir

The Solution

Proactive, complete email security

Whispir tested solutions from a variety of leading vendors and determined that Proofpoint Email Protection delivered the strongest combination of features, flexibility and ease of use. This email gateway lets Whispir classify, detect and block suspicious email, including BEC threats.

"The search in the new GUI was really powerful, and the Very Attacked People analyzer was also a key differentiator," said Littlewood. "We had a really good experience during the proof of concept, and Proofpoint effectively passed all of our test cases."

Whispir augmented Proofpoint Email Protection with Proofpoint Targeted Attack Protection (TAP). This solution detects ransomware and other advanced email threats delivered via attachments and URLs. With Proofpoint Threat Response Auto-Pull (TRAP), the organization can analyze emails and quarantine malicious or unwanted emails after they are delivered.

Proofpoint tools also helped Littlewood in his effort to apply a DMARC policy across its sending domains.

"We used Proofpoint Email Fraud Defense to help us achieve DMARC compliance in a short period of time," he said. "And we were able to successfully get a DMARC policy into reject mode across nearly all of our sending domains. This has been a significant achievement for the team."

The Results

Detecting and stopping advanced email threats at scale
Proofpoint Email Protection enabled Whispir to quickly discover and stop email attacks in their tracks—and on a massive scale. It stopped more than 1.2 million email threats spanning phishing, BEC, malware and spam, which represents 30% of its total inbound traffic. The solution also detected and stopped nearly 460 advanced targeted threats.

The company also gained a deep content analysis that has been highly effective, and has caught 45,000 email threats, including impostor threats.

Proofpoint TRAP has proven its success as well, and it has helped Whispir's security team scale its resources to keep pace with a growing array of threats.

"We've got Proofpoint TRAP installed, and we've seen at least three emails that have been successfully delivered to multiple staff, that were then identified as malicious," said Littlewood. "TRAP successfully removed these from the accounts of everyone who received them. That effective automation has been a real positive for us, because our team could not continue to scale and investigate each phishing email manually."

Whispir has also seen measurable benefits from its DMARC implementation. DMARC has enabled the company to strengthen its reputation among end customers.

"Now our customers can identify whether we have DMARC reject policy. And third-party risk management companies have also reflected this capability in their ratings," said Littlewood. "From an external visibility point of view, this has given us clear uplift."

Whispir is continuing to extend and develop its Proofpoint solutions. It's also exploring ways to bring these together with several other security solutions to strengthen trust across its organization.

"We've got a pretty aggressive roadmap with a lot of other implementations. So we're certainly going to look at closely integrating our Proofpoint solution with our other security partners solutions," said Littlewood. "This will allow us to closely coordinate our identity, endpoint and email security together."

With Proofpoint Email Protection in place, Littlewood is confident that his team will continue to stay well ahead of the evolving threat landscape to provide peace of mind to employees as well as Whispir's customers.

LEARN MORE

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