proofpoint.

CUSTOMER STORY

Proofpoint Helps Groupe Pasteur Mutualité Insurance Protect Its Brand and Customers

GROUPE PASTEUR MUTUALITÉ

The Challenge

- Mitigate business email compromise, phishing and other attacks
- Safeguard interaction with third-party partners
- Protect brand integrity

The Solution

- Proofpoint Email Fraud Defense

The Results

- Decreased unauthorized email attempts with Email Fraud Defense and DMARC reject
- Identified and blocked 2,000 spoofed messages per domain, and email risks in 65 countries
- Improved visibility to minimize shadow IT

The Organization

In the insurance business, building trusted relationships are a key to success. Groupe Pasteur Mutualité (GPM) has been doing this for more than 160 years. This global player in the protection, support and well-being of caregivers provides healthcare professionals with insurance coverage and services that facilitate their professional practices. With 500 employees and 138,000 protected people, the company understands the importance of protecting its highly respected brand and reputation. It also knows the importance of making sure its email communications are secure.

The Challenge

Protecting a global insurance brand through security best practices

Like other insurance organizations, GPM is relentlessly focused on mitigating security threats. When the global pandemic emerged in 2020, the company shifted its operations to remote work. It also redoubled its efforts to protect its brands and reduce risk from email threats. The organization decided to implement Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect its email traffic against phishing and other fraudulent activity.

"When the COVID-19 lockdowns occurred, we decided to start a DMARC initiative," says Paloma Gouin, chief information security officer at GPM. "We wanted to reduce domain spoofing, and implement and enforce a reject policy for our ten domains. But this was challenging because our small IT team was stretched, and we had limited resources."

With DMARC, organizations can verify that legitimate email is authenticating properly, and that fraudulent activity that appears to come from its domains will be blocked before it can reach customers and business partners. However, putting DMARC in place can be complex. The company needed a partner that could help streamline deployment and strengthen email security and visibility.

The Solution

Minimizing business email risk and streamlining best practices

While attending a training event focused on security best practices, the GPM team was extremely impressed with Proofpoint solutions for implementing DMARC. The company also evaluated other vendors from the Gartner Magic Quadrant before choosing Proofpoint Email Fraud Defense. This solution protects organizations against business email compromise (BEC) scams and authenticates all emails delivered to and sent from the organization. It also mitigates the risk of inbound impostor threats. And it helps GPM simplify its DMARC implementation by providing guidance through each step of its rollout.

> "Proofpoint helps us ensure that our business email communication is protected, and that bad actors cannot spoof our domain names. It gives us confidence knowing that our organization, clients and partners are protected."
>
> **Paloma Gouin**, chief information security officer, Groupe Pasteur Mutualité

GPM worked closely with the Proofpoint Professional Services team to set up DMARC protection with a step-by-step approach. They started with its most critical domain and gradually extending across a total of ten domains.

"Once we partnered with Proofpoint, the first phase focused on gaining visibility into our environment," says Paloma. "Then after five months, we implemented an email reject policy. The Proofpoint consulting team provided us with great support throughout the process."

The Results

Stopping threats worldwide across multiple domains
Proofpoint Email Fraud Defense quickly delivered on its promise to stop email fraud and help GPM protect its trusted domains.

"After installing Email Fraud Defense, we identified more than 2,000 messages blocked for each of our domains," explains Paloma. "We also discovered and identified 65 countries that were spoofing our domain names, using the solution's geographical heat map that examines imposter domains. I was amazed at the sheer number of countries that were sending out these messages from lookalike domains."

GPM is also implementing DMARC to help provide protection for its inbound traffic, and is asking its vendors and partners to put best practices in place as well. Proofpoint also helped GPM minimize risk and strengthen compliance within its own organization, by improving insight into the state of its IT environment.

"Using the domain discover tool helped us greatly. We found a lot of misconfiguration and several shadow IT activities that were underway within our organization," says Paloma.

DMARC is now in place and operating smoothly, backed by Proofpoint Email Fraud Defense. This means GPM can continue to extend its services to leading healthcare providers, and remain assured that its brand will not be compromised by BEC or other security threats.

LEARN MORE

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