proofpoint.

CUSTOMER STORY

Comprehensive Email Data Loss Prevention for a Global Legal and Advisory Services Firm

Taylor Vinters

The Challenge

- Protect sensitive client data and prevent accidental data loss via email
- Prevent misdirected emails and emails to unauthorized accounts and comply with GDPR

The Solution

- Proofpoint Adaptive Email DLP

The Results

- 250 mailboxes protected
- Reputation risk mitigation
- Reduced compliance reporting

The Organization

Taylor Vinters is a global legal and business advisory services firm, with offices throughout the UK and in Singapore. Clients include the Fortune 500, mid-market and startups across the US, UK and Asia. The company has been a Proofpoint Adaptive Email DLP (formerly Tessian) customer for many years.

The Challenge

Every year, organizations with 1,000+ employees send approximately 800 misdirected emails. And Steve Sumner, director of IT at Taylor Vinters, knows that safeguarding your business reputation is of paramount importance, especially in the legal and business advisory services profession.

It only takes one misdirected email or incorrect file attachment to shatter client confidence. It can also result in legal sanction or financial penalty from regulatory authorities. And as a legal and business advisory services provider, Taylor Vinters handles sensitive client data, such as client intellectual property and financial records. So it needed a solution to effectively mitigate the risk of accidental data loss via email.

When the company was evaluating solutions in 2018, the EU's General Data Protection Regulation (GDPR) was coming into force. This motivated the company to look for a solution to address misdirected emails and email data loss risk.

The Solution

Adaptive Email DLP: Misdirected email and reputation risk mitigation
Taylor Vinters uses Adaptive Email DLP to ensure that their client experience is safeguarded by operating with the lowest possible risk of sending misdirected emails or attaching incorrect attachments. This is made possible through cutting-edge Proofpoint technology and the industry's broadest email datasets to analyze working relationships and understand the difference between misdirected email, wrong-file attachments, data exfiltration attempts and regular business.

In-the-moment contextual security warnings provide an additional layer of security, explaining anomalies detected in the emails about to be sent and coaching employees toward safer email behavior.

"The effectiveness of Adaptive Email DLP's in-the-moment security warnings is the equivalent to us giving our employees a security awareness training session," said Steve Sumner, director of IT, Taylor Vinters.

"What I was conscious of in deciding to select Proofpoint Adaptive Email DLP (formerly Tessian) was that we don't have something that pops up every 5 minutes with an alert. It had to be an efficiency gain, so the employees could feel confident that they were protected, but not be so onerous that it makes them less and less efficient, or negatively impacts their working day."

Steve Sumner, director of IT, Taylor Vinters

The Results

Taylor Vinters sees the ROI of Adaptive Email DLP on a daily basis, and Sumner and his security operations team value the ability to triage and drill down into the types of emails blocked to better understand how data loss risks are evolving over time.

Communicating that ROI to the executive leadership is another bonus, and is made easy with Adaptive Email DLP's extremely user-friendly reporting feature.

In fact, requests to Sumner for reporting metrics are happening less and less frequently, demonstrating the level of confidence the Board has in the platform and its ability to improve the firm's cybersecurity posture.

The low cost of effort of having Adaptive Email DLP running passively, with advanced protection and a low false positive rate, is a big plus for Sumner, who couldn't imagine a possibility of not having Adaptive Email DLP deployed in his environment.

Reducing the cost of compliance

The cost of compliance is set to increase as more countries implement data privacy legislation. When it comes to GDPR, 88% of organizations spend more $1 million on compliance annually, with 40% spending over $10 million. Misdirected emails are the top GDPR-reported cybersecurity incident in the UK. Not having to file reports for misdirected emails to the regulatory authority is a significant efficiency gain for Taylor Vinters, allowing them to focus on their core business, without interruption.

According to Sumner, the relevance of Adaptive Email DLP is only increasing as the global regulatory landscape becomes more complex. And data security and privacy regulations similar to the GDPR are being adopted in multiple jurisdictions where Taylor Vinters operates. With comprehensive email data loss protection in place, Sumner knows the company is protected now and into the future.

LEARN MORE

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