proofpoint.

CUSTOMER STORY

Proofpoint Provides Next-Gen Email DLP for One of Africa's Largest FinServ Groups

The Challenge

- Protect against accidental and intentional data loss over email
- Detect and prevent misdirected emails and misattached files
- Gain visibility with a proactive approach
- Reduce the time it takes to investigate, report and remediate incidents

The Solution

- Proofpoint Adaptive Email DLP

The Results

- Uses behavioural AI to prevent accidental and intentional data loss over email, reducing risk and remediation costs that can't be stopped any other way
- Prevents a significant number of data loss incidents (more than 6,500 in two years)
- Delivers seamless deployment, simplified maintenance and minimal employee disruption

The Organisation

Founded more than 175 years ago, this leading African corporate and investment bank is part of one of the largest financial services groups on the continent. This publicly traded company has nearly $2 billion in revenue and more than 40,000 employees.

The Challenge

Despite having rule-based controls and traditional data loss prevention (DLP) software, data breaches caused by data loss in email were an ongoing concern. The bank's existing security stack was primarily reactive. And instead of preventing data loss incidents or offering visibility into the scope of the problem, the bank's team was only able to analyse incidents after the fact.

When data loss incidents did occur, they became operational events, taking on average days or weeks to investigate, report and remediate. And considering the size of the company, the hours added up quickly and detracted from other areas of the business.

The bank realised the potential for data breaches due to data loss via misdirected emails and misattached files. But the organisation was unable to prevent employees from sending sensitive information to personal email accounts without creating restrictive rules that would impede productivity.

'Before Proofpoint Adaptive Email DLP, we didn't have clear visibility into data loss incidents in email or the true size of the problem,' said the senior manager of information security at the bank. 'We believed it was happening, but we didn't have a solution or strategy in place to help us proactively combat it.'

Adding to its challenges, POPIA—South Africa's version of the GDPR—created urgency and forced the bank to evaluate its DLP strategy and identify more effective ways to prevent data loss incidents in emails.

The Solution

As the bank looked for a solution, its information security team determined several must-have features before moving forward.

They wanted a solution that provided proactive detection and prevention of misdirected emails and misattached files, as well as user education. It also needed to be low maintenance and nondisruptive with a high rate of efficacy.

Enter Proofpoint Adaptive Email DLP

While rules-based DLP plays a critical role in protecting known sensitive data, such as PII, Social Security numbers and payment card data, there are risks it fails to detect. These include sensitive data being sent to the wrong party and employees exfiltrating data to themselves and other unauthorised recipients.

'Adaptive Email DLP does more than just detect and prevent accidental and intentional data loss. We view it as a user awareness tool as well. Employees engage with the warnings and, month-on-month, we see how their behaviour can change. As a result, non-compliant activity has steadily decreased.'

Data loss prevention manager

Proofpoint Adaptive Email DLP uses behavioural AI to automatically prevent accidental and intentional data loss over email. This reduces risk and remediation costs that can't be stopped any other way. By analysing more than 12 months of email data and learning employees' normal email sending behaviours, trusted relationships and how they handle sensitive data, Adaptive Email DLP understands when anomalous email behaviour is occurring. And when an anomaly suggests a misdirected email, misattached file or data exfiltration event is occurring, it notifies admins of potential data loss incidents and warns the user in real time, preventing sensitive data loss through email.

Adaptive Email DLP deployed seamlessly within minutes and began protecting the bank within hours. There was no need to build and test servers. No need to create and update rules. It was easy to set it up and forget about it. The solution works silently in the background, which means employees don't know it's there until they need it. It's helpful, not disruptive and aids the bank in maintaining a strong security culture around trust and enablement.

'Adaptive Email DLP was very easy to deploy and has been incredibly low maintenance,' said the data loss prevention manager at the bank. 'It's not a tool we have to worry about keeping up and running from an infrastructure perspective. It's one less thing the security team has to be concerned about. That was and continues to be a huge selling point for us.'

The Results

'Before we even had our POV, we were able to prove that Adaptive Email DLP would help us improve internal processes, help with risk management and compliance and potentially increase revenue,' said the senior manager of information security. 'The security team was awarded an internal innovation award based on the potential impact Adaptive Email DLP could have.'

With Adaptive Email DLP, the bank is now able to automatically detect and prevent incidents that could have a big impact on the business.

Adaptive Email DLP analyses historical email data to understand normal content, context and communication patterns. This enables a comprehensive mapping of every bank employee's business and non-business email contacts. Relationship graphs are established and continuously updated as email behaviour changes over time after Adaptive Email DLP is deployed.

The tool continually gets smarter and automatically evolves in tandem with changing relationships without any support from security teams. That's how Adaptive Email DLP was able to detect and prevent 4,027 accidental data loss events and 2,427 unauthorised emails in the first two years of the partnership.

'Adaptive Email DLP does more than just detect and prevent data loss incidents,' said the data loss prevention manager. 'We view it as a user awareness tool as well. Employees engage with the warnings and, month-on-month, we see how their behaviour can change. As a result, non-compliant activity has steadily decreased.'

LEARN MORE

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