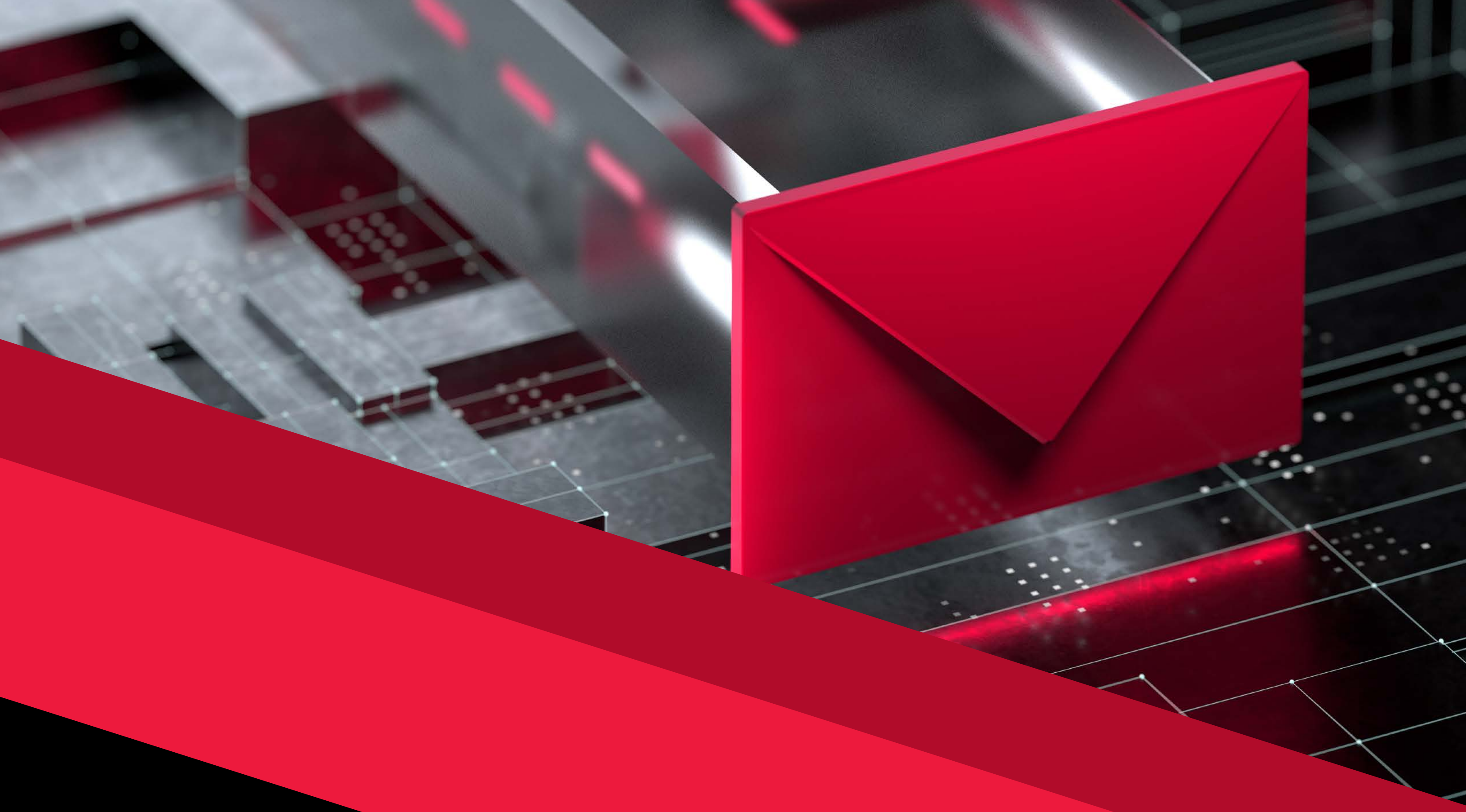

CASE STUDY

Avoiding Business Email Compromise

Industry data is pretty consistent – on average 80% of organisations experience of some type of data breach, targeted email attack, successful phishing attack or other security incident in a given 12 months. Whether it's sensitive information leaked through email, business email compromise (BEC) or phishing attacks, the attacker's goal is to steal credentials and move through the network to obtain desirable rewards including customer data and interference with business processes.

Trustwave®

Client Spotlight

The company is manufacturer and sales organisation with headquarters in New Zealand and business in 18 countries. A leader in the high-performance sporting industry, they have a large investment in technology research and pride themselves on customer service.

The Challenge

The client has almost 200 users on the Microsoft 365 Outlook email environment with Advanced Threat Protection (ATP). Most of their users access their email while on the road, using their mobile devices and phones as business demands. The ability to act with agility is essential to their business.

The staff were becoming overwhelmed with large amounts of spam and phishing attempts. Many phishing attacks were very sophisticated and played to the human psyche by targeting urgency of a request. This made it difficult for staff to distinguish if requests were coming from potentially risky or valid sources.

> *"With Trustwave, we were able to achieve better protection from email attacks while reducing total cost of ownership"*
>
> – IT Manager

Disaster struck when the organisation experienced a breach of an email account which resulted in financial damage to the business.

A director's email account was compromised using a phishing attack. The email account and password were now in the hands of the attacker. Manipulating the banking details on an invoice sent to the client, the invoice had been mistakenly paid into the attacker's account. The IT manager was alerted only after the incident occurred. In fact, the alert was raised by the client themselves, alerting the management team of the payment and asking why the account was different.

The Solution

Considering competing solutions, the client selected Trustwave MailMarshal Cloud to protect the business from email attack. At a per user, per year cost, it was considerably less than upgrading their Mircosoft 365 license subscription tier or using a competitive solution. Also, MailMarshal was available in the cloud, simplifying the transition and ensuring an added layer of protection across all devices and browsers.

The use of Trustwave Mailmarshal Cloud with their Microsoft 365 environment automatically removes the large volume of inbound spam executives were dealing with daily. It also checks for suspicious emails using heuristic, human and machine learning based intelligence. The proprietary defence filters are constantly fine-tuned to ensure a high degree of accuracy and new rules and threat intelligence are automatically added to the detection and protection engines by the elite Trustwave SpiderLabs Email Security Research and Malware Analysis Team..

Product features to look for to help avoid BEC fraud

Not all fraud detection engines are created equally. Trustwave has talked with many organisations that have suffered losses even while using an email security platform that markets its ability to detect BEC fraud. When evaluating vendors' products be sure to look for engines that are specifically designed to address BEC fraud. It should complement your email security capabilities with a set of focused BEC policies and rulesets, as this evolving threat requires more than just scanners and anti-virus protections. It is imperative that these rulesets and engines are regularly updated with the latest intelligence to keep up with the landscape of this attack method.

> *"I can confidently assert to executive leadership that the risk of email attacks has been greatly eradicated"*
>
> – IT Manager

Trustwave®