SIX SIGNS YOUR EMAIL GATEWAY MIGHT NEED REPLACING

SIMPLIFY BUSINESS EMAIL SECURITY

MISSING SMARTS

What threat intelligence data sources does yours use to reduce malicious spam and thwart attacks? Detection filters built on multiple threat information sources combined with human insight and machine optimisation is essential.

GETTING TOO MUCH SPAM

Has it been a while since your gateway was tuned or updated? New types of SPAM driven by advanced techniques are getting through.

TOTAL COST OF OWNERSHIP

For some, it can be a high-cost monthly priced option to upgrade every user to a Microsoft Defender for Office 365 E5 license, just to maximise email protection. Unless you're ready to leverage your O365 deployment and use every advanced application and feature, perhaps you're just paying for stuff you're not going to use. Look to minimise your total cost of ownership.

TARGETED ATTACKS

Business Email Compromise (BEC) is a targeted form of phishing ultimately designed to steal money from your organisation. Check that your gateway has an engine specifically designed to address BEC fraud.

SUCCESSFUL PHISHING

How smart are your end users? Can they detect a phishing attack that is well disguised? Is your gateway up to the task of blocking attacks on their behalf? Attack methods are changing every day - **read more here**.

PRICEY FEATURES

The advanced functionality needed to prevent data loss and ensure intellectual property protection can often come with a high price (think image image analysers, keyword scanning, Azure RMS support and compliance tools). Look for cost effective packages that offer the security features you need today.

These issues indicate that your current email gateway might not be the right fit for your business.

Trustwave®

www.trustwave.com