5 REASONS WHY ADVANCE EMAIL SECURITY IS IMPORTANT

If your email security solution isn't adequately protecting your organization, you may be part of the growing number of companies who have had costly security breaches.

1 EMAIL IS THE MOST COMMON IT SECURITY THREAT FOR ORGANIZATIONS

Whether it be malware, phishing, URL-based threats, impostor-driven schemes like business email compromise (BEC), email is the primary method hackers use to deliver harmful programs to an organization or individual.

An estimated **75 percent** of identified, impactful threats were initially entered via email attachments and 46 percent of attacks were executed by users clicking web links in email, according to the SANS
Cyber Security survey.

2 EMAIL-BASED ATTACKS AFFECT THE ENTIRE ORGANIZATION

Due to the continued prevalence of email, a harmful email that slips through your defence can wreak havoc throughout your organization.

All employees are affected by phishing email, using carriers, banks or sharing solutions brands name to lure them. It can seriously harm your company, especially if a ransomware effectively holds your company information and/or systems hostage.

3 BASIC ANTI-SPAM EMAIL FILTERS ARE NOT ENOUGH

Hackers are developing increasingly sophisticated ways to bypass email security systems, including redirecting good URL addresses to phishing URLs.

The growing challenge then is for organizations to ensure they have the right email defences in place to detect and stop advanced threats. Often, additional layers of email security are needed on top of base email security.

4 EMAIL-BASED THREATS ARE EVOLVING AND INCREASING, EVERY YEAR.

With email as the main entry point for cyber attackers, it's important that companies ensure their email protection is actually protecting them from new and evolving threats. New predictive email security defences are helping organizations significantly improve their email security.

About 91 percent of all hacking attacks start with a phishing or spear-phishing attempt. Yet a successful email security system can quickly recognize and block spear phishing attempts, which will significantly decrease your risk of a serious breach..

5 YOUR EMAIL SECURITY FILTER ONLY CATCHES KNOWN THREATS

Most email defence systems aren't predictive, but rather reactive. The most sophisticated cloud email security today is predictive in that they augment standard signature-based and anti-spam capabilities with contextual inspection as well as spoof and anomaly detection.

This is achieved by amassing comprehensive threat intelligence databases worldwide and using Artificial intelligence (AI), heuristics and machine learning for real time analysis of suspicious emails, attachments, and URLs that can easily evade a traditional protection.

Using a global analysis of fingerprint and reputational elements, new email security technologies complement existing email security by combining global and local analysis.

Global analysis of email and email-borne threats enables learning from the past to predict the future. – Gartner Newsletter: Securing Cloud-Based Email. The Need for Complementary Solutions Backed by Artificial Intelligence