Solution Brief

Mesh 365

Detect Advanced Threats Designed to Evade Microsoft

The Challenge

With over 250 Million users on Microsoft 365 sharing the same entry point - email - it is the #1 target for cybercriminals. While the inbuilt filters from Microsoft are effective at protecting against most known threats, they are often incapable of detecting new, targeted attacks.

Why Small & Mid-sized Enterprises are Most Vulnerable

Attackers are constantly testing and developing new ways of avoiding being detected by Microsoft's native filters. While larger organizations have more resources and significant budgets to bolster their overall defenses with additional layers of protection, small and medium sized enterprises and non-profits tend to rely solely on Microsoft to keep their email safe. This leaves them particularly vulnerable to new, innovative attacks that have been specifically designed to evade Microsoft's detection. Microsoft on its own is not sufficient to protect organizations against advanced, targeted threats.

Most Damaging Email Attacks

- Business Email Compromise
- Spear-Phishing
- Social Engineering
- Ransomware
- Insider Attacks

18,000,000

Covid-related phishing and malware attacks each day.

£18 Billion

Total losses globally from Business Email Compromise Scams.

83%

Of attacks on orgnisations financially motivated.

£46,000

The average cost of downtime following a ransomware attack.

Securing the Inbox: A Native API-based Solution

Mesh 365 protects businesses against targeted email attacks, reducing the risk of financial and data loss. It utilizes powerful detection features driven by machine learning with an intuitive end-user experience.

By securing the inbox, even attacks that have been weaponized post-delivery can be detected and removed - keeping organizations, employees, and data safe from compromise.

Simple Deployment and Onboarding

Unlike email security gateways, Mesh 365 does not disrupt mail flow. There is no need to update mx records, create allow rules, or any other updates to your existing setup. Instead, Mesh integrates seamlessly into users' mailboxes and deployment takes only a couple of minutes.

As the filtering takes place within the mailbox, there is no separate login or quarantine area for users to manage and user training is not required.

Key Benefits

- Protects against the full spectrum of email based threats and spam
- Advanced add-on to Microsoft 365 or Additional Layer of Security behind a Gateway
- Quick and easy deployment - No need to change mx records
- Helps with compliance requirements
- Simple admin and intuitive end-user experience

Protect Organisations Against from Their Biggest Vulnerability - Email.

Every organisation now requires advanced email protection. Mesh 365 is an intelligent, specialist layer of protection for Microsoft 365 that integrates seamlessly with their existing email setup - meaning it can be deployed within seconds. Mesh 365 can also be deployed behind existing Email Gateways for an advanced layer of protection.

Features

Unique

Financial Fraud Prevention

Analyzes email containing payment requests, banking information and other financial content for signs of fraud and deception.

No MX Change

Deploy in seconds as Mesh 365 integrates fully with Microsoft 365 via Microsoft's Graph API without disrupting current email traffic flow.

URL Protect

All URLs are subjected to scanning against real-time threat feeds for known and unknown malicious sites and fake login pages.

Unique

4x Antivirus & Antimalware Engines

Multiple award-winning signature-based and heuristic-based scanning engines, detecting known and unknown types of malware, such as ransomware, botnets, and trojans.

Unique

Impersonation Detection

Inspects email content, language, tone, and cadence, combined with checks on the sender for matches and/or similarities with the recipient organization visually and phonetically.

Attachment Sandboxing

Unknown and potentially malicious attachments are detonated virtually, protecting against never-before-seen, zero-hour threats like polymorphic malware and new variants of ransomware.

Unique

Insider Threat Protect

Internally sent emails are subject to rigorous scanning and inspection, protecting against lateral attacks from already compromised mailboxes within the organization.

Warning Banners

Informed employees are safer employees. Banners can be applied to emails warning of danger, empowering staff to safely navigate their inbox.

Threat Remediation

Already delivered email that is now known to be malicious can be removed manually or automatically, defending against post-delivery weaponization and zero-days.

Unique

Predictive Threat Intelligence

Mesh utilizes a combination of Passive DNS Sensors, Deep-Relationship Analysis, Neural Networks and other information sources to detect abnormalities and predict where future attacks are likely to originate.

Dynamic Content Scanning

Next-gen spam filtering - Text and images in the message body are dynamically scanned for indicators of spam, nefarious intent, and evasive techniques

Microsoft Azure

Built in Microsoft Azure

For maximum reliability and scalability, all Mesh services are built in Microsoft Azure Datacenters, helping you to meet some of the highest data center requirements for compliance and redundancy.

Learn more at
www.meshsecurity.io