

Mesh Gateway

Advanced Threat Protection Powered By Machine Learning

The Challenge

91% of cyber-attacks begin with email, making it the easiest way for hackers to gain access to an organisation.






Highly-sophisticated and targeted campaigns are widespread, with Ransomware, Phishing, and Social Engineering Scams among the most lucrative threat types utilized by cybercriminals.

Small & Medium Sized Businesses are Most Targeted

Due to ever increasing cybersecurity budgets, it is becoming more difficult and expensive for cybercriminals to successfully penetrate large corporations' defenses.

Instead, they focus on easy wins with small and medium businesses that have far fewer resources dedicated to preventing cybercrime. Protection against advanced email attacks is no longer a luxury, it is a necessity.

Most Damaging Email Attacks

-  Business Email Compromise
-  Spear-Phishing
-  Social Engineering
-  Ransomware
-  Payment Fraud

18,000,000

Covid-related phishing and malware attacks each day.

Over £15 Billion

Total losses globally from Business Email Compromise Scams.

83%

Of attacks on small businesses are financially motivated.

£46,000

The average cost of downtime following a ransomware attack.

The Intelligent Solution

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






By securing the email perimeter, attacks are detected and blocked before they reach the network - keeping organisations, employees, and data safe from compromise.

The Opportunity for Managed Service Providers

All Mesh services are managed centrally from the Mesh MSP Hub - a platform purpose-built for Managed Service providers, delivering genuine centralized management with unique visibility and control.

From Global Threat Hunting and Remediation to Custom Templates and Global Analytics, Mesh helps MSPs to achieve better results with fewer resources - boosting efficiency and profitability while enhancing protection.

Key Benefits

-  Protects against the full spectrum of email based threats and spam
-  Compatible with Cloud | On-Prem | Hybrid email platforms
-  Quick and easy deployment - No hardware or software to install or maintain
-  Helps with compliance requirements
-  Simple admin and intuitive end-user experience

Protect Your Clients from Their Biggest Vulnerability - Email.

Every organisation now requires advanced email protection. Mesh Gateway is an extremely powerful and robust email security platform, while remaining user-friendly and easy to deploy - perfect for MSPs to rollout to their clients within minutes.

Features



Financial Fraud Prevention

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



URL Protect

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



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.



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.



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.



End-User Quarantine Digests

Quarantined emails can be released by end users (if permitted) with intuitive, easy-to-use, ultra-modern quarantine digests.



DMARC, DKIM, SPF Verification

Inbound emails are subject to DMARC, DKIM, and SPF verification checks, which assist in authenticating the sender.



Email Spooling

If you experience downtime and your mail server is offline, we will queue your email until you are back online.



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.



Graymail Filtering

Blocks unsolicited marketing emails and no longer wanted newsletters, improving employee productivity.



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.

ABOUT MESH

Mesh is the first email security platform purpose-built for Managed Service Providers, combining a revolutionary multi-tenant management console (Mesh MSP Hub) with machine learning powered email protection against the full spectrum of email attacks.

Free Trial



Learn more at
www.meshsecurity.io



© 2021 Mesh Security Ltd | All rights reserved