



# **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 organization.

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

With rising cybersecurity budgets, large corporations pose greater challenges for cybercriminals to breach.

Consequently, attackers target small and medium businesses which often have limited resources allocated to combat cybercrime, making them more susceptible to attack. Protecting against advanced email attacks is now an imperative, not a luxury.

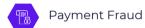
## **Defend Against**











#### 60%

of businesses close permanently within 6 months of a cyber-attack

#### \$55 Billion

Total losses globally from Business Email Compromise Scams.

#### 83%

Of attacks on small businesses are financially motivated.

# \$64,000

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 utilizes 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 organizations, employees, and data safe from compromise.

# **Delivered by Managed Service Providers**

The Mesh MSP Hub serves as a centralized platform designed specifically for managed service providers, enabling comprehensive management of all Mesh services.

This distinctive approach empowers MSPs with unmatched visibility and control over their client base, leading to an elevated level of protection for each organization they serve.

## **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

## Intelligent. Automated. Cost-effective.

# A Feature-rich Solution To Protect Against Targeted Email Attacks

Mesh Gateway is an incredibly powerful and automated email security solution, seamlessly combining user-friendliness with rapid deployment, making it an exceptionally cost-effective means to protect your organization's email defenses.

#### **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.



#### 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.



## **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 neverbefore-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, ultramodern quarantine digests.



## **DMARC, DKIM, SPF Verification**

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



# **Outbound Email Scanning**

Outgoing emails are scanned for malicious content, spam, and signs of mailbox compromise.



#### **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.

