Solution Brief

Mesh 365

Detect Threats That Evade Microsoft & Other Email Gateways

MESH 365

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

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

60%

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

$21 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.

Intelligent, Native API-based Integration

Fully integrated with Microsoft 365, Mesh 365 utilizes advanced algorithms and machine learning capabilities to analyze both internal and external email communication in real-time.

The API-based integration allows for detection of sophisticated threats, specifically designed to evade detection by Microsoft, bolstering businesses' email security posture and reducing the risk of financial and data loss.

Managed By MSPs

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

- ✓ Enhances existing email security posture
- ✓ Deploy instantly with native API integration. No changes to mailflow, no downtime, no risk
- ✓ One-click remediate threats found in the inbox
- ✓ Helps with compliance requirements
- ✓ Simple admin and intuitive end-user experience

Intuitive. Automated. Cost-effective.

A Feature-rich Solution To Seamlessly Bolster Email Security Posture

Mesh 365 is an incredibly powerful and automated email security solution, seamlessly combining user-friendliness with instant deployment, making it an exceptionally cost-effective means to fortify your existing email defenses.

Features

Unique

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.

Unique

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.

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.

End-User Quarantine Digests

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

Insider Threat Protection

Internal email communication is analyzed providing protection against lateral or insider email attacks.

Unique

Threat Remediation

One-click threat remediation instantly removes already delivered emails from the inbox, centrally across multiple sites.

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.

Graymail Filtering

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

Warning Banners

Customizable banners can be applied to emails warning of danger or advising caution, empowering staff to safely navigate their inbox.

Learn more at
www.meshsecurity.io