Solution Brief

Mesh Unified

A 2-in-1 Solution Protecting Both The Perimeter & The Mailbox

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

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

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.

A Uniquely Multi-layered Solution

Mesh Unified 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 both the email perimeter and the mailbox, external attacks can be detected and blocked before they reach the mailbox, while attacks launched from within the organization can also be prevented.

Delivered by Managed Service Providers

All Mesh services are managed centrally from the Mesh MSP Hub - a platform purpose-built for managed service providers, delivering unparalleled visibility and control across their client base.

As a result of this unique approach, every client organization benefits from an enhanced level of protection.

Key Benefits

- Protects against the full spectrum of email based threats and spam
- Natively integrates with your Microsoft 365 tenant for maximum security
- Quick and easy deployment - No hardware or software to install or maintain
- Helps with compliance requirements
- Simple admin and intuitive end-user experience

Protecting Organisations Against Their Biggest Vulnerability - Email.

Every organisation now requires advanced email protection. Mesh Unified is an extremely powerful and robust email security platform, while remaining user-friendly and easy to deploy - and can be rolled out to businesses within minutes.

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, east-west or insider email attacks.

Unique

Threat Remediation

One-click threat remediation instantly removes already delivered emails from the inbox.

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.

RedQor

redqor.com

38 Thistle Street, Edinburgh, Scotland, EH2 1EN, United Kingdom