

DATA SHEET

Trustwave MailMarshal

▶ MAKING EMAIL SAFER FOR YOUR BUSINESS

Benefits

Filters Email at the Gateway

- Analyzes email content and attachments entering your network to deliver a greater than 99.97% spam detection rate while blocking 99.99% of malicious spam

Superior Compliance and Data Protection

- Integrated with Microsoft Azure Rights Management Service
- Prevent loss of sensitive data
- Meet stringent compliance requirements

Protects Against Existing and Emerging Threats

- Integrates a wide variety of anti-spam and anti-threat, phishing and business email compromise technology to protect against known and emerging threats

Email attacks continue to proliferate because attackers have the time and businesses have the data they want. Monitoring email is essential because it provides the ability to identify potential risks in employee communications. Unmonitored email, on the other hand, presents a danger. The damage email can cause has become more costly each year in employee time, repair time, lost data and legal liability.

Finding alternative methodologies to protect people, data and brand reputation against security challenges -- that current infrastructures may not be adequately designed to meet -- could be exactly what is required to stop attackers and employees, who fail to recognize phishing and social engineering attacks, from putting a business at risk.

Prevent targeted email-borne attacks from occurring

Trustwave MailMarshal, a multi-layered intelligence and detection engine, filters inbound traffic in real-time to protect your users from cyber threats and spam while scrutinizing outbound email traffic to stop electronic distribution of your data and intellectual property.

Trustwave MailMarshal can help improve your security results through:

- Email management and configuration via a brand-new web-based user interface
- Full audit and review capabilities of configuration changes
- Configuration editing by multiple users at the same time
- Complete email protection against phishing, business email compromise
- Powerful data loss protection to help safeguard intellectual property, thwart inadvertent or intentional leakage of sensitive information and achieve regulatory compliance
- Syslog support for Security Intelligence and Event Management (SIEM) integration
- Domain protection from unauthorized use with Domain-based Message Authentication, Reporting and Conformance (DMARC)
- Detection of forged sender addresses in emails with Domain Keys Identified Mail (DKIM)
- Granular and flexible policy engine
- Enforcement of your email Acceptable Use Policy
- Delegation of email monitoring and control to other personnel
- Built-in intelligence from elite Trustwave Spider Labs email security researchers
- Around-the-clock support via online, email and phone, plus maintenance updates
- Easy integration with Trustwave Managed Security Services for more in-depth endpoint, database and network protection

Fortify your email management solution with the following supplementary services:

SECURITY MODULE	WHAT IT DOES FOR YOU
Email Archiving	Provides a systematic approach to save and protect the data contained in email messages to enable fast retrieval. Email Archiving plays an essential role at companies in which data permanence is a priority.
Email Encryption	Allows you to securely send emails containing sensitive or confidential information and documents to any recipient around the globe without requiring the recipient to download or install any software.
Malware Analysis Sandbox	Proactively prevents advanced malware and provides a safe environment in which to execute and observe malicious code or to encourage threats into exposing themselves. It also reduces the amount of time between infection and remediation, mitigates the risk of breaches, and detects zero day or unknown attacks.
Blended Threats	Helps identify, catch, neutralize and block, in real-time, websites that serves up suspicious or malicious code to business users.
Image Analyzer	Automatically scans and sorts images entering and leaving your business via email into two categories – offensive and pornographic and normal and acceptable. And stops the offensive and pornographic. Protects employees, customers, and suppliers from exposure to inappropriate and illegal content reducing and removing legal liability.
Supported Antivirus	Keep your existing anti-virus scanners from Sophos, McAfee, Kaspersky and Bitdefender.

Integrate with Microsoft Azure Information Protection (AIP) and Rights Management Services (RMS)

Microsoft AIP and RMS enables restricted access to documents and emails that are specific to identified individuals within your company and prevents others from viewing or editing these documents - even if they are sent outside the company.

Trustwave is the only secure email gateway solution with the ability to open, analyze and apply policies for data loss protection and acceptable use, then re-encrypt any RMS protected files and emails to ensure sensitive data does not leak from your company.