What started as a cost-effective way for people to send and receive messages, email is now the de facto communications tool with billions of users worldwide. Email now extends far beyond sending and receiving simple messages and has transformed into a collaboration, transactional, delivery tool and file repository, and is the primary channel for attackers to gain access to your company.

Stop Business Email Compromise
Fact. Cybercrime is increasing. You know cybercriminals want your sensitive and valuable data and access to unsuspecting employees. And to stay several steps ahead of your security team, they continually develop increasingly sophisticated methods to gain access. As a result of these intensifying threats, your security team is tasked with identifying, isolating, and stopping an ever-increasing number of sophisticated phishing or social engineering attacks, malicious attachments, ransomware attacks and account takeover.

Make Email Safer
Protecting your email environment while managing complex compliance policies is one of your top priorities yet it can be a daunting challenge. Trustwave MailMarshal Cloud multi-layered intelligence and detection engine filters your inbound email traffic, in real-time, to protect your users from cyber threats and spam while scrutinizing outbound email traffic to prevent the loss of your data and intellectual property.
By investing in a modern-day single source secure email gateway solution, you are giving your security staff the added tools they need to get ahead of cybercriminals and their sophisticated threats.

**Trustwave MailMarshal Cloud delivers you:**

- Advanced email protection against phishing, business email compromise, spam and malspam
- Reduced false positives
- Identifies, catches, neutralizes, and blocks, in real-time, websites that serves up suspicious or malicious code to company users
- Protects employees, customers, and suppliers from exposure to inappropriate and illegal content
- Powerful data loss protection to help safeguard your intellectual property 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)
- Built-in intelligence from Trustwave SpiderLabs 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

**Optional Security Modules**

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Archiving</td>
<td>Provides a systematic approach to preserve and protect the data contained in email messages to enable fast retrieval. This tool plays an essential role at companies in which data permanence is a priority.</td>
</tr>
<tr>
<td>Email Encryption</td>
<td>Company email users can 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.</td>
</tr>
<tr>
<td>Malware Analysis Sandbox</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.