Trustwave MailMarshal FAQ: Covering our Layered Approach, Complementing Microsoft 365, and More

Q: Why is it important to have a multi-layered approach to email security?

For the same reason a multi-layered approach is important for all other aspects of cyber security: because no one tool can do the job on its own. By the same token, most secure email gateways (SEGs) are good at detecting known threats, but not both known and unknown. With the rising instance of zero-day threats in the wild, the ability to catch unknown threats is a must.

Q: Why is Trustwave MailMarshal any better than other SEGs at detecting email threats?

MailMarshal's multi-layered security is more sophisticated and mature than other solutions. MailMarshal has a long track-record of success: 20+ years without a major threat reported. MailMarshal takes advantage of the deep security research capabilities of the Trustwave SpiderLabs team. More than 150 certified SpiderLabs research engineers constantly monitor for new security incidents and feed what they find to MailMarshal detection engines, thus providing the latest updates and solutions to email threats. Over the last 15 years, SpiderLabs has discovered more than 30,000 vulnerabilities, including 9,000 with ratings of high or critical. The only way to keep up with the latest threats is to have an experienced research organization like SpiderLabs – and most companies simply do not.

Q: What's the impact of MailMarshal's layered approach on users? Is this going to be a hassle for them?

Clients get higher resilience to ransomware, phishing attacks, and other malicious attacks targeting email systems. For example, they'll be prevented from opening a malicious attachment or clicking on a nefarious URL, and will get a warning explaining why. We think that's much less of a hassle than cleaning up after a breach. Not to mention, features like encryption require no additional software downloads – so no hassle.

Q: I've got Microsoft 365 and Exchange Online Protection. I should be covered for email security, right?

Not really. This gets back to the layered approach question above. You'll be covered only for basic, known email threats. For more protection, you'll want an additional solution such as Trustwave MailMarshal, which is compatible with E1, E3, and E5 Microsoft packages, as well as other email systems. **(See "Why Microsoft 365 Needs Additional Email Security" for additional information.)**

Q: I've got operations in multiple countries, including in Europe. Does Trustwave MailMarshal preserve data sovereignty?

Yes. With Trustwave MailMarshal On-Prem & Hybrid Cloud, you control where to install and have the data reside. Trustwave MailMarshal Cloud supports in-region data sovereignty. It is hosted on separate Azure instances in the United States, United Kingdom, Europe, and Australia. We can ensure data is not shared across regions to comply with GDPR and other, similar data privacy regulations.

Q: I'm concerned about data loss prevention (DLP). Does MailMarshal help with that?

Yes. Trustwave MailMarshal scans outbound emails and attachments to provide full DLP-level inspection to manage confidential data and meet stringent industry and regulatory requirements. Companies can also define rules for what sort of content is and is not allowed to be sent via email, to prevent a rogue employee from emailing a customer list, for example.

Q: Can MailMarshal deal with blended threats?

Yes, through the Trustwave MailMarshal blended threat module. A blended threat is an attempt to compromise information security using multiple vectors such as phishing emails and links to a website hosting malicious code. The blended threat module uses several validation methods – including real- time behavioral analysis and content inspection as well as information from several industry standard sources – to identify and block sites that serve suspicious or malicious code. Since validation is performed in real time by a cloud service when a link is clicked, it provides superior effectiveness in catching and neutralizing new exploits for all users on any device from any location. See our **MailMarshal Blended Threats FAQ** document for more information.

Q: Is MailMarshal a cloud or on-premises solution?

Trustwave MailMarshal comes in two editions: one is cloud-based and the other may be installed on your premises. As a result, it works in either environment as well as in hybrid configurations where clients use both cloud and on-premises email systems.

Q: I've had trouble deploying and configuring security packages in the past. How difficult is MailMarshal to deploy?

MailMarshal is quite simple to deploy. The on-prem version comes with a click-through wizard; most users have it up and running within minutes. The cloud version requires no installation at all. Just update your Mail Exchange (MX) record to reflect the mail server address we'll give you. Both have a single point of control and you can leverage more than 130 built-in rule sets to cover common custom mail-handling scenarios.

Q: What if I still need deployment help. Does Trustwave have professional services available?

Yes. Trustwave offers Consulting & Professional Services (CPS) to assist with any level of deployment and architecture design required. CPS can also help in implementing specific policy rules for security and business process concerns.

Q: Is the on-premises version delivered as a dedicated hardware appliance or software?

Trustwave MailMarshal on-premises is software installed on Windows Servers.

Q. How do you control email policy and secure your email when using cloud email?

Customers using cloud email like Microsoft 365 often realize they have a lot of complexity to overcome managing internal SMTP traffic. Business critical processes that rely on automatically generated emails – helpdesk, invoicing, payments, shipping logistics, credit card transactions and more – may not work well, if at all, with a cloud-based email solution. MailMarshal remedies the issue, with a single portal to manage policy and compliance.

Q: Some of my users need to encrypt their emails. Is that supported?

With an optional add-on, email users can securely send emails containing sensitive or confidential information and documents to any recipient around the globe. Even better, they can do it without requiring the recipient to download or install any software.

To learn more, visit the **Trustwave MailMarshal Suite** webpage. If you like what you see, **schedule a demo** or **try it for free**.

Trustwave®

www.trustwave.com