Trustwave®

Why a Layered Approach is Crucial for Effective Email Security

CISOs know proper cybersecurity requires a layered approach, with various defensive tools and techniques protecting against threats from the cloud to the network perimeter and the core. It should come as no surprise, then, that proper email protection is much the same, given companies must protect against ransomware, business email compromise (BEC), phishing, malware and more.

In this guide, we'll lay out the features and functions to look for in a secure email gateway (SEG) to help you vet vendors and make the best SEG decision for your organization.

Known vs. unknown threats

Most any SEG solution will do a reasonable job at protecting against known threats. This involves using signatures that detect well-understood instances of malware as well as exploits targeting known vulnerabilities. But that's just table stakes.

Threat actors today are far more advanced than that, with many launching attacks that exploit zero-day threats – new threats for which no signatures yet exist. That kind of protection requires more advanced mechanisms that can flag emails based on criteria such as abnormal behavior and similarities to previously known threats.

Data loss protection

In addition to incoming threats, organizations also need to protect against employees sending sensitive data via email, whether inadvertently or with ill intent. To that end, you need an SEG solution that supports data loss protection (DLP) by scanning outbound emails and attachments.

The idea is to detect any content that violates policies around what sorts of data can be sent via email, as opposed to more secure channels. DLP is often required in industries subject to stringent industry and regulatory requirements.

Granular content inspection of email body and attachments is critical to protect from data loss. If you employ the Microsoft Azure Rights Management (Azure RMS) encryption and protection solution, you'll want to ensure your SEG solution integrates with it. Otherwise, your SEG won't be able to inspect emails and attachments covered by Azure RMS.

Some SEGs offer their own email encryption capability, enabling users to securely send emails containing sensitive or confidential information and documents. Ideally, you want a solution that makes the process simple by not requiring the recipient to download or install any software.

Advanced image analysis, anti-virus, sandboxing, link protection, and more

Advanced image analysis may be another consideration. If your organization routinely sends or receives images via email (as most do), you should consider whether your SEG can examine image files for inappropriate images and threats.

And while you likely already have an anti-virus solution, the ability for your SEG to scan emails for viruses adds another layer of protection. MailMarshal allows you to choose the antivirus provider you prefer: Sophos, McAfee, or Bitdefender.

Malware sandboxing is a way of dynamically running an untrusted file or application within a safe, isolated environment to check what it does. Sandboxing can detect many behaviors, including Operating System calls, file activity, Registry edits, in- memory activity, and network traffic. The Sandbox destroys fast-moving threats like EMOTET early in the attack chain and minimizes the risk of exposure to costly malware attacks.

URL validation is another good feature to look for in an SEG. Many cyberattacks, including phishing, attempt to lure targets to click on a link to a malicious webpage. Look for a tool that ensures links are legitimate at the time users click on them – not just when the link is received – to provide protection at any time from any device.

Support for blended threats

The ability to support all of the above features represents a good start in finding a quality SEG. But a step above is a solution that can deal with blended threats, which combine multiple threat vectors.

A blended threat may involve an email message crafted to appear like it comes from a trusted sender, along with links to a malicious website, and/or an attempt to entice the user to divulge personal information. Defending against such threats requires an SEG that supports 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.

To be effective, such a solution should have the backing of a threat lab that keeps track of not just email-based threats, but all sorts of cyber threats.

SpiderLabs: A secret weapon

Trustwave SpiderLabs, for example, includes a team of more than 50 cyber security experts who constantly scour the cyber universe for threats. They maintain the Trustwave Global Threat Database, which holds billions of records about cyber threats, malware and vulnerabilities from around the world, including malicious URLs, IP addresses, file hashes and more.

Trustwave MailMarshal, like other Trustwave security products, takes advantage of this advanced threat intelligence to secure not just email, but blended threats that may involve other vectors.

That advanced intelligence also enables MailMarshal to block thousands more malicious spam messages than other SEGs – reducing spam by over 99.9% – and inspect 5x more email attachment file types.

It all adds up to a layered approach and results that speak volumes: a 20+-year record without a major reported client incident.

To learn what layered email security should look like, check out the **Trustwave MailMarshal Suite**. If you like what you see, **schedule a demo** or **try it for free**.

Trustwave®

www.trustwave.com

MMLA_1222