Trustwave Secure Email Gateway Cloud Prospecting Guide

Solution Description

Trustwave Secure Email Gateway (SEG) Cloud is a comprehensive email security platform and email business workflow toolbox that provides advanced email security, robust data protection and extensive policy control and reporting. SEG Cloud will help protect a company's email environment against unwanted email, phishing, business email compromise, advanced malware, malspam and ransomware, while preventing loss of intellectual property and managing complex compliance policies.

Trustwave SEG Cloud:

1. Is the only email gateway on the market that integrates with Azure Information Protection and Rights Management Services (AIP/RMS). SEG Cloud:
   - Unpacks and decrypts attachments
   - Scans content and strips out sensitive data and violations of acceptable use policies
   - Re-encrypts the attachment

   ** Without visibility into Rights Management Services protected attachments, a business runs the risk of sensitive data leaking from the organization.
2. Is a cost-effective companion package to Office 365, Google G-Suite or other email gateway environments. SEG pricing structure is per user/per year, versus per user/per month pricing for Office 365
3. Has a flexible email management toolbox with advanced routing, autoresponders, header rewriting and external commands.
4. Has extensive policy controls that support customizable rules based on trigger points, full visibility into email activity, actionable insights into types and volumes of threats, where emails are coming from and which policies are being triggered.

Key Buyers and Discovery Questions

Security Leader (CISO, VP/Dir. Security)	IT/Security Operations (IT Ops/Security Ops Dir./Mgr., Email Admin)	Compliance Buyer
Responsible for security strategy, risk management and brand, intellectual property (IP) and data protection	Responsible for the operations and security of the organizations email / messaging infrastructure	Responsible for regulatory compliance, data governance and privacy
Discovery Questions		
• Have you experienced any issues with Business Email Compromise (BEC) fraud emails getting to your end-users? • What impact does email blocked as spam have on your help desk? • Does your current email security platform integrate into your SIEM solution? • How well does your policy engine handle non-standard configurations? • How is that platform performing in terms detection rates? • If you have not yet migrated to the cloud but are planning to, have you considered how you will continue to secure your email via the cloud? Most people are finding the email security from their email cloud provider is not sufficient.	• How much time do you spend tuning your email security solution to increase detection/decrease false positives? • Can your email security solution analyze your Azure RMS encrypted content? • Tell me about other 3rd party email security platforms you are using today? • Talk to me about your satisfaction level with (name of third-party provider) • What is the biggest gap in your current email security system? • How well does your email security solution understand the web to enable it to combat blended web/email threats? • How well does your policy engine handle non-standard configurations? • How much effort goes into enforcing your acceptable-use policy?	• What standards do you need to adhere to in terms of email security (HIPAA, PCI-DSS, SEC, Sarbanes-Oxley, GDPR, CCPA, etc.?) • How can you tell if sensitive / confidential data is leaving your organization via email? • Can your email security solution analyze your Azure RMS encrypted content? • What are you doing to maintain an archive of your email content? Is it meeting your needs? • How do you handle the encryption of sensitive content?
Keywords to Listen For		
• We were phished • We were hit with malicious spam • We were hit with a business email compromise • A data breech almost occurred • Intellectual property was stolen • Need to get increased visibility into our overall security risk position	• Substantial increase in ransomware, business email compromise, phishing attacks • Not seeing enough of a decrease in ransomware, business email compromise, phishing attacks with existing technology	• Leakage of sensitive and proprietary information and data • inbound and outbound emails containing sensitive/proprietary data not being encrypted or stored properly • My archiving costs are overwhelming

Trustwave SEG Cloud Value Proposition

Trustwave SEG Cloud is a cost-effective way for you to identify and thwart sophisticated inbound attacks on your business while scrutinizing your outbound traffic to prevent the loss of your sensitive data and intellectual property. SEG Cloud delivers unprecedented detection and extended protection in real time by proactively detecting suspicious email, removing them from end user access and shielding well-intentioned end users from falling prey to known and targeted attacks.

Trustwave Secure Email Gateway Cloud Prospecting Guide

Competitive Positioning by Key Competitor

Competitor	Strengths	Weaknesses	Positioning

ProofPoint	• Invests heavily in R&D
	• Strong product
	• Strong competitor
	• Dedicated focus on email security
		• Only focused on email security.
		• Can't offer integrated email, web and other security solutions
		• Their Threat Lab only deals with email-based threats; limited insight into blended threats.
		• Products are challenging to configure
			• Trustwave SEG is the only email gateway on the market that is integrated with Microsoft Azure Information Protection and Rights Management Services (AIP/RMS)
			• Secure Email Gateway:
			  ○ Blocks 99.97% of spam with almost zero false positives
			  ○ Blocks 99.99% of malicious spam
			  ○ Provides complete email protection against phishing, business email compromise, ransomware
			  ○ Has powerful data loss protection to help safeguard your intellectual property and achieve regulatory compliance
			  ○ Integrates with any SIEM to provide real-time analysis of security alerts through syslog support
			  ○ Detects forged sender addresses in emails and email spam through DKIM
			  ○ Provides domain protection from unauthorized use through DMARC
			  ○ Supports a lower cost per user, per year model
			  ○ Has a granular and flexible policy engine and comprehensive management controls
			  ○ Includes built-in intelligence from our elite Trustwave Spider Labs email security team
			  ○ Easily integrates with Trustwave Managed Security Services for more in-depth endpoint, database and network protection

Cisco IronPort	• Deployed as physical or virtual appliances, cloud based or hybrid • Tightly integrated with Cisco's Endpoint console and threat response engines • Deep discounts given to "buy" business	• Acquired IronPort's extensive customer base but Cisco hasn't kept up development • Customers prone to phishing and BEC attacks • Product requires expensive add-ons to be on par with SEG	
Symantec	• Integrates with Symantec's Cyber Defense Platform to protect against both email and web-based threats • Integrates with their overall DLP portfolio • Deep discounts given to "buy" business	• Customer base from MessageLabs acquisition is vulnerable; especially after the Broadcom acquisition • Current clients are concerned about the future of Symantec email security product – will they be a focus? • Limited policy options • Limited development of cloud solution	
Mimecast	• Fully cloud-based, providing scalability and removing the customer's need to manage software and hardware • Has a proprietary DLP engine to score attachments based on content and apply rules to outbound emails	• Underlying security engines are questionable, with limited configuration • Not effective at blocking attachments that contain malware • Requires add-ons or upgrades to block embedded URLs • Questionable data sovereignty support for GDPR purposes	

Objection Handling

We don't have the time or resources to switch out our email security solutions, and it's not a priority.
Talk to me about your current configuration. Who is doing the heavy lifting and evaluating your current solution? How much time is spent on that? What else is your organization doing to enhance the current solution? Yes, a switch does require time and planning. However, switching to SEG Cloud will actually result in time savings because the time you're investing today enhancing your current solution will be saved with SEG's increased productivity, protection from advanced threats, and better compliance and acceptable use controls.

How do I know your solution is better than what I have now?
Do you ever see legitimate business email caught as spam (false positive) or are your users constantly dealing with spam in their inboxes? Has your organization been affected by BEC fraud? Can your current solution do everything you need from an email solution, or are you having to supplement it with other products or put up with its restrictions? Would a more advanced and flexible policy engine for example better fit what you need not only today but also in the future? How does your current solution collect threat intel? What is the level/maturity of the threat intel it does collect? How much visibility do you have into this?

It is my understanding that Trustwave is not an email security specialist.
Trustwave SEG has been a leading email security solution for over 20 years. To stop modern, blended and targeted attacks requires extensive knowledge across many threat vectors, not just email. Our Global Threat Database, based on SpiderLabs research, is the only threat database that combines threat intelligence from multiple technologies and information from breach and forensics research. And, Trustwave has the only Secure Email Gateway on the market that can unpack, analyze and repack Azure RMS attachments and emails. I invite you to trial our SEG for 30 days. Once you install it you can, following the User Guide and Eval Guide, start using it immediately and experience its performance first-hand.

I've never heard of Secure Email Gateway (SEG).
SEG is formerly known as MailMarshal. MailMarshal has been around for over 20 years and was the 2nd email security solution in the market long before spam existed.

Customer Success Story

One of the largest publicly funded public health organizations in the United Kingdom with 78,000 employees and numerous health boards delivering healthcare services to 3+ million people

One of the healthcare organizations within the network **was not** effected in 2017 by WannaCry ransomware, a ransomware that hit most public health organizations in the UK, because this particular trust was protected from WannaCry emails by Trustwave SEG within minutes of this new attack emerging.