

SALES PLAYBOOK

Secure Email Gateway

Version 2.1

November 2019

Table of Contents

- Product at-a-Glance 3**
 - Product Description 3
 - Value Proposition 6
 - Differentiators and Proof 7
 - 30-Second Commercial (Elevator Pitch) 9
 - Business Metrics 10

- Customer Overview 10**
 - Customer Objective(s) 10
 - Business Challenges/Pain Points 10
 - Business Outcomes 11

- Market Overview and Opportunity 12**
 - Market Research 12
 - Target Markets 14
 - Target Audience 15
 - Use Cases 16
 - Competitive Positioning by Key Competitor 18
 - Buying Factors with Competitive Ranking 20
 - What Can Slow Down or Kill a Deal 21

- Having Conversations 22**
 - Discovery Questions 23
 - Objection Handling 23

- Key Resources, Processes and Contacts 26**
 - Top Marketing Resources 26
 - Sales Process Steps 26
 - Key Contacts 26

- Appendix A – Rounding Out Email Security Needs 27**
 - Email Archiving 27
 - Email Encryption 28
 - Blended Threats Module 33
 - Image Analyzer 33
 - Anti-Virus Scanning 34

Product at-a-Glance

Product Description

Trustwave Secure Email Gateway (SEG) protects against unwanted email, advanced malware, Business Email Compromise (BEC), Account Takeover and other security threats, and prevents the loss of sensitive data and intellectual property while managing complex compliance policies. And with the expansion of mobile, IOT and “Bring Your Own” devices into the workplace, the number of user endpoints, the largest attack surface in any company has grown exponentially.

SEG’s multi-layered intelligence and detection engine filters inbound email traffic, in real-time, to protect users from cyber threats and spam while scrutinizing outbound email traffic to prevent company data and intellectual property from electronically leaving the building. And SEG provides email administrators and security personnel the flexibility to define custom rules to enable specific management of email workflow and process such as email routing, header rewriting, auto-responder rules, external commands, message stamping and more. SEG provides:

- Unparalleled Email Security
 - Dynamic Malware Analysis
 - Blocks 99.9% of spam with virtually zero false positives
 - Stops unknown, obfuscated malware in real-time
 - Blocks malicious links embedded in emails
 - Protection Against Fraud and Spoofing
 - Detects and blocks spoofing
 - Authenticates the sender
 - Effectively identifies spam and phishing messages, keeping them out of users’ inboxes
 - Advanced Threat Protection:
 - Automates response to malicious email activities
 - Detection and response findings can be forwarded into security infrastructure
- Powerful Business Workflow Management Controls
 - Advanced Policy Engine
 - Customize rules based on client defined trigger points
 - Enable specific management of email workflow and process such as content filtering, email routing, header rewriting, auto-responder rules, external commands, message stamping and more
 - Allows for non-standard configurations

- Management and Reporting
 - Full visibility into email activity
 - Customizable reports
 - Actionable insights into types and volumes of threats, where emails are coming from and which policies are being triggered
 - Ensure compliance with acceptable use policies
- Superior Compliance and Data Protection
 - Prevent Data Loss
 - Controls outbound content to provide full Data Loss Prevention (DLP) inspection of emails and attachments
 - Seamless cloud-based encryption
 - Meet Stringent Compliance Requirements
 - Manages complex policy configurations
 - Provides auditable proof of deletion of personally identifiable information (PII) with email archiving option
 - Integrate with Microsoft (MS) Azure Rights Management Services (RMS)
 - **Trustwave is the first and only secure email gateway provider to support MS Azure Information Protection and Rights Management Service** to allow review and protection of RMS encrypted messages. Other secure email gateway solutions cannot unpack RMS encrypted emails --- meaning MS Azure RMS will not work with competitor's solutions
 - Restricts access to emails
 - Cloud-based encryption, identity and authorization policies to secure email

SEG is offered in three different deployment models (Cloud, On-Premise, Service Provider Edition) to best suit the customer's need:

- **SEG Cloud (SaaS offering)** – A 100% cloud-hosted email security solution that providing time-to-value with simplified deployment and cloud-based management. SEG Cloud is provided in three service levels:
 - **Standard Protection** - This version of SEG Cloud is hosted by Trustwave and provides essential email security:
 - Anti-Malware/Virus
 - Anti-Spam
 - Specialized detection engine targeting malicious activity to include Phishing, Spoofing, BEC

- Control of environmental email parameters to include size, bandwidth, attachments, and files
- Standard implementation of best practice email policies which are continually refined to solve over 97% of client email issues. These rules are continually augmented by the renowned SpiderLabs' Research Team, for advanced protection of client inbound and outbound email (See SEG Cloud Policy Listing for all rule packages)
- **Office 365 / G Suite Protection** - (SEG supports other cloud-based email services as well)
 - In addition to the features listed above in the "Standard Protection" service level, Microsoft Office 365 / G Suite Protection package adds:
 - Advanced Protection Package: Uses Blended Threat Module (BTM) for safe link checking; URL analyzer and validator
 - Data Protection Package: DLP to protect PII and other sensitive information
 - Acceptable Use package: To protect against objectionable material like hate speech, pornographic material and more
 - Extends security beyond the basic Exchange Online Protection (EOP) included in Office 365
 - Provides enhanced security and savings over the high cost of moving up to E5 service level or buying Microsoft Advanced Threat Protection (ATP) - SEG provides superior email security at a fraction of the E5 cost

NOTE: G-Suite Gmail (or any cloud-based email service customers) can be supported within this service level.

- **SEG Cloud Advanced** - In addition to the features listed in the Office 365 / G Suite Protection service level above, the SEG Cloud Advanced package also:
 - Enables Advanced Policies feature with policy wizard to create rules specific to your company's email security and process needs
 - Gives customers the ability to create up to 20 custom rules

Alternatively, SEG Cloud customers can purchase add-on packages, a la carte, for packages that are not included in the core bundle they purchase:

- Advanced Protection Package: Uses BTM for safe link checking; URL analysis and validation
- Data Protection Package: DLP capability to protect PII and other sensitive information
- Acceptable Use Package: Uses SEG Image Analyzer to protect against objectionable material
- Secure Encryption Packages: Available in an Essential or Advanced option as an add-on to all bundles
- Secure Archiving: Available as an add-on to all bundles

	Standard Protection	Office 365 / G Suite Protection	SEG Cloud Advanced
Anti-Virus	X	X	X
Anti-Spam	X	X	X
Specialized Detection Engine	X	X	X
Control of Key Email Parameters (including size, bandwidth, attachments, files)	X	X	X
Implementation of Best Practice Policies	X	X	X
Advanced Protection Package (for safe link checking; URL analysis and validation)	Optional	X	X
Data Protection Package (to protect PII and other sensitive information)	Optional	X	X
Acceptable Use Package (to protect against objectionable material)	Optional	X	X
Advanced Policies feature with Policy Wizard	NA	NA	X
Custom Rules (Up to 5)	Optional	Optional	NA
Custom Rules (Up to 20)	NA	NA	X
Email Encryption	Optional	Optional	Optional
Email Archiving	Optional	Optional	Optional

- SEG On-Premise** – SEG On-Premise is deployed and managed within a customer’s environment and provides customers with robust email security for inbound and outbound content and a complete set of security business workflow controls, policy capabilities and management tools. It is the strongest “email toolbox” in the market to meet both customer email content security and email process capabilities. SEG On-Premise has been designed to scale from tens of users to over 250,000 users.
- SEG Service Provider Edition** – Provides a multi-tenant version of SEG to enable ISP’s, MSP’s and other like companies to launch their own hosted email security solution or embed email protection into their core solutions. SEG for Service Providers is typically hosted within the customer’s on-premise or cloud environment; however, it can be hosted within a Trustwave managed cloud environment (at an additional cost).

Value Proposition

SEG is the magnifying glass that helps security teams bring into focus, identify and thwart uber-sophisticated inbound attacks that exploit companies through their ever-expanding user endpoints. SEG stops inbound phishing or social engineering attacks, malicious attachments and ransomware attacks while scrutinizing outbound traffic to prevent your sensitive data and intellectual from electronically leaving the building.

A company that invests in a modern-day single source secure email gateway solution like SEG, is giving their security staff the added tools they need to get a leg up on cybercriminals and their sophisticated threats. And SEG goes beyond this core security function to also provide clients with the industry’s leading email process business workflow capabilities. SEG allows clients to customize the rules and policies of our solution to enable complex routing, email management and client specific external commands to meet their email process needs. This differentiating capability expands the value of SEG beyond the email security function to position SEG as the leading “email content and process security” solution in the market.

SEG delivers:

- Complete email protection against phishing, and BEC
- Sophisticated, multi-layered approach that reduces false positives
- Powerful data loss protection to help safeguard your intellectual property and achieve regulatory compliance
- Granular and flexible policy engine, customizable by the client
- Comprehensive email management controls
- Built-in intelligence from elite Trustwave Spider Labs email security researchers
- Around-the-clock support via online, email and phone, plus maintenance updates

Another benefit of using a cloud service to deploy a secure email gateway is scalability. If there are spikes in your email traffic or an increase in the number of users, a cloud service can quickly scale to maintain security and performance.

Differentiators and Proof

Customer Success Story – Protected from WannaCry Malware:

Among the many customer stories around the impact of WannaCry in 2017 was how the UK National Health Service (NHS) was affected. Operations cancelled and patient care affected with possible deaths as clinicians were unable to access IT systems due to WannaCry infections. One bright spot was an NHS provider in southwest Great Britain, an SEG customer for many years.

When WannaCry began to emerge in eastern Europe, the Trustwave SpiderLabs team was able to quickly analyze the attack, identify the domains and attack techniques being used. SpiderLabs then pushed urgent updates to SEG and SEG Cloud, blocking these domains and other Indicator of Compromise (IOC's). The result was SEG customers, running all the default email security rules including the unknown attack rules from SpiderLabs, they were able to prevent the malicious activity of WannaCry.

Broad-Based Global Players	<h2 style="margin: 0;">The Trustwave Difference</h2>	Low Cost or Point Solution Players
Feature-rich, but hard to fully adopt	Robust features; easy to manage and administer	Low cost players: not security companies; don't protect as well
Product development allowed to wane in favor of "hotter" technologies	Consistent development since early 2000s along with other portfolio investments	Low cost players: development may lag the industry
Limited ability to detect dynamic malware in real-time	Industry-leading, real-time malware protection (Trustwave proprietary multi-layered engines)	Point solution providers: do email security well, but managing multiple techs can be a headache
Threat feeds may miss threats or deliver false positives	SpiderLabs threat feeds analyzed by specialized email security experts	Low cost player: No threat feeds Pt solution: may not have adequate threat intelligence
Data loss prevention (DLP) can be expensive; may require professional svcs	Versions with customizable on-prem DLP or cloud-based, with built-in rules covering 99.9% of use cases	Low cost player: Limited or no DLP
Doesn't address the user problem	Industry-leading Security Awareness Education & SpiderLabs Phishing Services to educate and test users	Pt Sols: only focused on technology, not ppl/processes
High TCO	Favorable TCO	Low costs: need to augment w/other techs Pt Sols: might pay for more than you need

A quick view at SEG differentiation:

Top reasons to choose Trustwave for Email Security:

- **Advanced Protection**
 - The only email gateway on the market that integrates with Azure RMS
 - Better identifies spam and phishing messages
 - Industry-leading malware protection that stops unknown, obfuscated malware in real-time
 - Blocks malicious links embedded in emails
 - Delivers zero-day protection against the latest email threats
- **Extensive Policy Controls**
 - Customize 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
- **Data security and compliance** -Controls outbound content to provide full DLP inspection on emails and attachment
- **MS Azure RMS Support** -

- Trustwave is the ONLY SEG vendor to integrate with MS Azure RMS to unpack, scan and re-pack encrypted files. This enables clients to take advantage of the Microsoft Azure RMS capabilities and know that their SEG solution can validate the defined policies and protection.
 - SEG provides the ability to decrypt email and enforce all RMS outbound policy controls before re-encrypting the email and sending it
 - SEG can even enforce MS Azure RMS controls if they are forgotten by the user; based on policy triggers, SEG will detect defined data (e.g. credit card data) and either reject back to user, forward to compliance officer or combination of these actions
 - SEG is the only secure email gateway that can detect the following MS Azure RMS controls – view, open, read, copy, view rights, allow macros, print, forward, reply, reply all, save, edit content
- Leading-edge Threat Intelligence - SEG is powered by a combination of real-time and near real-time threat intelligence derived from Trustwave SpiderLabs Email Security Team, an elite team of email threat detection and email security professionals. As new intel on threats are identified and collected, it is pushed to SEG customers.
 - Specialized BEC Engine - SEG incorporates a dedicated BEC fraud detection engine for identifying low volume highly targeted spear-phishing attacks. This engine is regularly updated with the latest threat intelligence and maintained by Trustwave SpiderLabs renowned for their pioneering research in the BEC field.
 - Integrated Managed Security Solution (MSS) - We offer a comprehensive portfolio of managed security services to combat the next-gen threats in the current security landscape. By ensuring email security plays a role in the overall Trustwave MSS solution story, we can nurture and develop a customer's cyber security posture and maturity across all key vectors – including email malware and phishing
 - Business Workflow Tool - SEG is a flexible email management toolbox with advanced routing, autoresponders, header rewriting and external commands. This helps us stand out from the rest of the competition and allows the ability to take the discussion beyond email security. While undertaking all email malware/compromise activities, SEG is also utilized by many customers to effectively integrate their business processes, activities and cadence between two or more systems or organizations to improve business workflow.

30-Second Commercial (Elevator Pitch)

We partner with organizations like yours to combat spoofing, email fraud and reduce spam by over 99.9%. Our multi-layered intelligence and detection engine filter's your inbound email traffic, in real-time, to protect your users from cyber threats and spam. In addition, SEG scrutinizes outbound email traffic to prevent your data and intellectual property from electronically leaving the building – even Microsoft Azure RMS protected content. Our security research team continually updates threat detection algorithms to detect new forms of spam, mass mailing worms, and phishing scams and publishes zero-day updates to meet specific threats. And the SEG business workflow tools simplify the management of email and content processes.

By investing in a modern-day single source secure email gateway solution like SEG, you can stop inflow of email attacks while stopping the unintentional outflow of sensitive data. Trustwave is committed to

helping you improve your defenses against targeted email and multi-vector attacks, enhance data protection, add value back to your business and reduce IT administration overhead.

Business Metrics

Link to standard service/product business metrics.

[SEG Business Metrics](#)

Customer Overview

Customer Objective(s)

To protect an organization's email environment against malicious activity while minimizing the management burden:

- Protect organizational assets from spam, malware, phishing attacks, BEC, account takeover, ransomware
- Ensure sensitive data does not leave an organization unexpectedly
- Enable email administrators and security personnel to define custom rules and policies to meet their security and email processing needs – SEG goes beyond the email security to provide email content and process security
- Increase email security effectiveness while reducing email management burden and Total Cost of Ownership (TCO)
- Manage complex compliance policies

Business Challenges/Pain Points

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. Email has transformed into a collaboration, transactional, delivery tool and file repository that makes it a prized target for cybercriminals looking to gain access to a company's data.

- The risk, sophistication, and cost of email attacks
 - 39% of inbound email is spam
 - 26% of spam is malicious
 - BEC is overtaking ransomware and data breaches in cyber-insurance claims with BEC-related cyber-insurance claims accounting for nearly a quarter of all claims in the EMEA region as reported by American multinational finance and insurance corporation
 - \$12.5B in financial losses in the US in 2018 as a result of BEC
- There are several internal challenges related to email security
 - Employees unintentionally email sensitive and proprietary data, intellectual property, confidential documents and financial records to external recipients

- Employees fall victim to fraudsters posing as an executive to trick individuals into sending money or sensitive data
- Regulatory compliance
- Too many security issues to address, not enough staff/skills, dwindling budgets
- Unidentified (new forms of) cybercrime
- Globally, email provides the largest attack surface with the greatest opportunity for malicious activity
- Securing email is critical to organizational viability:
 - The most common form of organizational communication
 - A transaction tool for orders, payment processing, delivery logistics, and workflows
 - A filing tool as employees often use email as a second file repository

Business Outcomes

- Complete protection against fraud and spoofing - Trustwave's proprietary, multi-layered approach builds on industry-standard technologies to detect and block spoofing, authenticate the email's sender and make it easier to identify spam and phishing emails
- Protection from targeted attacks - Detection of malicious URLs backed by the global web and threat intelligence of Trustwave SpiderLabs
- Regulatory Compliance - Integrated DLP with custom regulatory compliance classifications that exceeds the DLP-lite found in many email security solutions, including support for Azure Rights Management Services (RMS) encrypted attachments
- Business Workflow Integration - Unique business workflow capabilities that integrate capabilities directly within customer workflow. Workflow requirements can be as unique as the customer itself; however, the following examples illustrate how the SEG solution can facilitate desired business outcomes:
 - **Global Telecommunications Company:** To protect the global brand, executive management leverages an internal Security Operations Center to provide intelligence to decision makers based on three key processes:
 - Data collection and management
 - Data analysis and operations
 - Reporting and information sharing

After a migration to G Suite from on-premise MS Exchange, the customer lost the ability to transparently (without user exposure) archive copies of corporate emails with the existing Proofpoint security solution and had limited ability to direct alerts/notifications into the local Splunk-based SIEM. After SEG was implemented, the customer had the ability to create custom rules and header rewrite rules that forwarded every outbound mail into the GSOC transparently and easily. Additionally, they could create endless combinations of DLP policies to enhance their existing applications and systems. And, lastly, leveraged SEG SYSLOG

support to feed email logs into Splunk and integrated critical email-related activities within the overall monitoring infrastructure. **BOTTOM LINE:** In addition to email security, SEG provided unique business workflow and security infrastructure integration that demonstrated greater ROI.

- **Major Airline:** A large American airline was challenged to effectively support the workflow between varied suppliers (to include catering, fuel, ground handling, in-flight entertainment, pre-flight special orders, delivery, crew control, insurance, IT, fleet management, leasing, and aviation logistics). Not surprisingly, it was determined that email was the only consistent method to comprehensively communicate, transact, track, deliver, and file between all of the suppliers. Leveraging Trustwave's unique Business Workflow capabilities, the airline was able to create header rewrite rules and custom scripts to route all those emails to help manage business data in order to properly employ and control resources as well as serve clients efficiently. They also created custom rules to flag any email delivery failures to any of its vendors, catering services, etc. via auto-email alerts to ensure there is no delay or breakdown in their logistical chain. (Business workflow tool capabilities are unique to Trustwave's SEG and not commonly found in competitive Secure Email Gateway solutions.) **BOTTOM LINE:** In addition to email security, SEG was able to uniquely provide customer value by unifying key partner workflows in support of business operations.
- **Retail:** Similar to the Major Airline example (above), a large American office supply company (77,000 employees, over 1200 stores across North America, online sales, and 40 warehouses/fulfillment centers) had the need to span workflow over tens of thousands of suppliers worldwide. As the customer was unable to find a single workflow solution to span multiple market segments (consumer, SMB, B2B, public sector), this retailer turned to Trustwave's SEG Business Workflow tools to manage the workload across multiple applications and systems globally that process POs, track transactions, send/receive invoices and payments, shipping logistics, inventory database management across warehouses, business-to-business (B2B) delivery services, credit card transactions, and recordkeeping. **BOTTOM LINE:** In addition to email security, SEG was able to address the customer's workflow challenges to support business operations through the only common means of communication (email).

Market Overview and Opportunity

Market Research

- Email security market predicted to grow to USD\$18 billion by 2023 at 22% CAGR¹
- USD\$26 billion lost to BEC between June 2016 and July 2019²

¹ "Email Security Market Worth US \$18 Billion by 2023 at 22% CAGR | Global Leaders Analysis: Microsoft, McAfee, Cisco Systems, SAP SE, Fortinet, Dell, Symantec, Apptix, Mimecast", MarketWatch, Published 9 July 2018, Analyst Firm: Market Research Future.

² "FBI Says \$26B Lost to Business Email Compromise Over Last 3 Years", TechTarget: SearchSecurity, Published 11 Sep 2019, Rob Wright.

- 84% of BEC messages do not spoof the address found in the “From” field³
- 45% of all email is spam⁴

According to Gartner⁵

- By 2023, 65% of organizations will inspect their intradomain email traffic for advanced threats, which is a major increase from 7% in 2019
- Impersonation and account takeover attacks are increasing and causing direct financial loss, because users place too much trust in the identities associated with incoming email and are inherently vulnerable to deception and social engineering. This growing problem can only be reduced through education, social graph impersonation filtering, improved indicators of identity in email and suspicious email workflow.
- The adoption rate and gravitational pull of Google and Microsoft toward their respective cloud office systems is forcing security and risk management leaders to evaluate every product in their email security architectures against the native capabilities these vendors claim to provide
- As more organizations accept and become familiar with cloud platforms, the demand for on-premises products has diminished. ...some organizations with unique requirements will continue to keep SEG implementations on-premises, due to residual privacy, data sovereignty, legal, integration support and network design concerns.
- The email security market is starting to adopt a continuous adaptive risk and trust assessment (CARTA) mindset and acknowledge that perfect protection is not possible. As a result, vendors are evolving or emerging to support new detect and response capabilities by integrating directly with the email system via API.
- By 2022, at least one major secure email gateway (SEG) vendor will “end of life” its on-premises components.

According to Statista⁶:

- Email usage is predicted to grow by 2 to 3% each year from 2018 to 2023
- 82% of workers check email outside of normal business hours

According to IDC⁷:

- Proofpoint was leading the market with US\$365m in revenues and 15.9% market share.
- Proofpoint, Symantec and Cisco are the most common competitors seen with Mimecast becoming more common.
- All vendors trying to show how they add capability to Office 365.

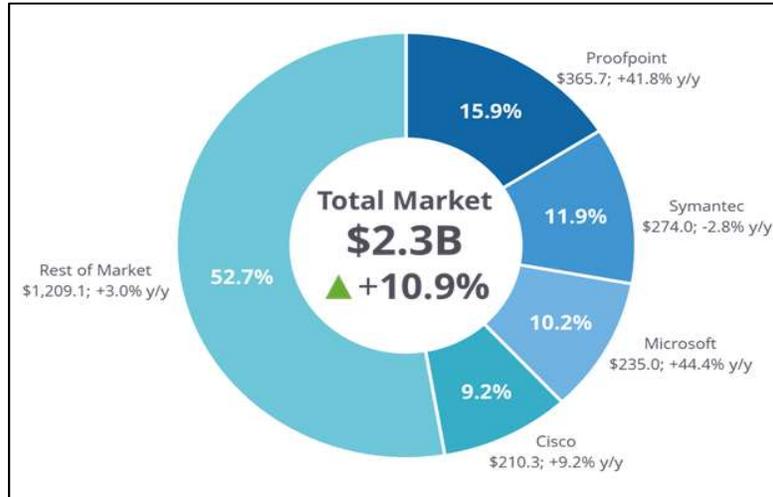
³ “2019 Trustwave Global Security Report”, Trustwave, Published January 2019, Analyst: Trustwave SpiderLabs Research Team.

⁴ “2019 Trustwave Global Security Report”, Trustwave, January 2019, Analyst: Trustwave SpiderLabs Research Team.

⁵ “Market Guide for Email Security”, Gartner, 06 June 2019, ID: G00400856, Analyst(s): Neil Wynne , Peter Firstbrook.

⁶ “[Number of e-mail worldwide from 2017 to 2023 \(in millions\)](#)”, Statista, 09 August 2019, J. Clement.

⁷ “Worldwide Messaging Security Market Shares, 2017: As Email Moves to the Cloud, Protection Follows”, IDC, August 2018, Doc: US44182418, Analysts: Robert Ayoub, Sean Pike, Pete Finalle, Frank Dickson.



2017 Market Share, IDC

Target Markets

Email is a standard communication tool and business necessity across all segments and verticals. However, the variation of SEG offering may vary depending on the customer segment:

- SMB to Lower Midmarket
 - SEG recommendations: Standard Protection or Office 365/G Suite Protection.
 - Rational: Tends to focus on the cost and resource efficiencies of cloud-based solutions. More so than other segments, this group may need assistance in understanding why the native security provided with cloud-based email is not sufficient.
- Mid-Market
 - SEG recommendations: Office 365/G Suite Protection or SEG Cloud Advanced. In addition, this segment may include a customer base that is most interested in SEG Service Providers Edition (providing a multi-tenant version of SEG to enable ISP's, MSP's and others to launch their own hosted email security solution or embed email protection into their core solutions).
 - Rational: Trending toward resource efficiencies of cloud-based email (whether migration from on-premise or direct to cloud) especially from larger providers (Microsoft O365 and Google G-Suite). Clients in this segment value greater manageability and control (especially in disparate environment locations common in hospitality and retail) as well as expanded support for complementary services (i.e., encryption, archiving) for greater ROI (particularly in Financial and Healthcare verticals).
- Enterprise
 - SEG Recommendations: SEG Cloud Advanced with enhanced management capabilities, custom rules, and optional modules (most notably Encryption) may appeal customers with mature email environments. For those who are tied to on-premise solutions, SEG On-

Premise provides all of the advantages of Trustwave SEG within the customer's existing environment.

- Rational: Customers in this segment tend to have the most mature email solutions in place. The market trend toward cloud-based email solutions applies; however, the transition will tend to be more measured and executed at a slower pace. (This transition will typically occur most quickly with Financial Services and Healthcare vertical markets.)

NOTE: Each customer segment can take advantage of SEG's Business Workflow capabilities that provide additional value outside of competitive Secure Email Gateway solutions.

Target Audience

SEG target audience will typically be focused on IT-related mid to senior level management responsible for security and compliance.

Role	Description	Buyer Profile
Security Leader (CISO, VP/Dir. Security)	Responsible for security strategy, risk management and brand, intellectual property (IP) and data protection.	Reports up into company leadership and is responsible for the information security policies, security budget, talent development, risk mitigation, threat response, resilience and more. Must remain up to speed on: <ul style="list-style-type: none"> • Company's strategic direction and how information security enables business growth • Latest security threats and trends • Regulatory compliance, such as <u>PCI</u>, <u>HIPAA</u>, <u>GDPR</u> • Security vendor landscape • Latest security approaches and technology developments • Cybersecurity awareness of organization's employees, contractors and partners
IT/Security Operations (Director/Manager: IT Operations/Security Operations, Email/Messaging Administrator)	Responsible for the operations and security of the organization's messaging infrastructure.	The role may report into either the security stack or the IT stack. Must remain up to speed on the latest email and web-based security threats and trends. Specific responsibilities include: <ul style="list-style-type: none"> • Analysis of quarantined and dead-lettered email • Analysis and release of end-user emails via request or ticketing system • Deal with consequences of unfiltered or unscanned email being delivered to end users • Prevent delivery of malware via email, embedded URLs and attachments • Review use of company email against organizational acceptable use policies and prevent sensitive data from leaving the company via email

<p>Compliance/Legal (Compliance Officer)</p>	<p>Responsible for full business compliance with all national and international laws and regulations that pertain to its specific industry, as well as professional standards, accepted business practices, and internal standards.</p>	<p>The role may report into either the security stack or corporate Legal department. Specific responsibilities include:</p> <ul style="list-style-type: none"> Regulatory compliance, such as <u>PCI</u>, <u>HIPAA</u>, <u>GDPR</u>
-----------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Use Cases

The following are a number of Use Case examples for Trustwave SEG in different customer verticals:

CASE STUDY

Healthcare

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

The Challenges:

- There were 22 local health boards and seven trusts that needed restructuring and consolidation.
- IT operations managed five separate data centers that hosted multiple Exchange servers.
- Users received over 3 million emails and sent over 1.5 million emails per month.
- They needed a comprehensive data loss prevention solution to scan for specific information and respond accordingly.
- They also required flexibility to allow senders the ability to bypass data loss prevention policies in life-threatening situations.

The Solution:

- A move to Trustwave Secure Email Gateway On Premise to benefit from its robust, flexible policy engine that allows for:
 - The construction of extensive policies and custom routing scripts.
 - Management of their messaging infrastructure.
 - Advanced email security protection.

The Results:

- Successfully integrated Trustwave Secure Email Gateway On Premise into their Exchange environments.
- Created custom lexicon to scan for specific information and content relationships.
- Fine-tuned Data Loss Prevention scoring to minimize false positives, and meet government regulations.
- This healthcare organization was not effected in 2017 by WannaCry Ransomware, a ransomware that hit the majority of public health organizations in the UK.

CASE STUDY

Telecommunication / Mass Media

An American multinational telecommunications conglomerate and one of the largest communication technology companies in the world with 150,000 employees, operating in 150 countries with over 2300 retail stores to serve over 160 million customers.

The Challenges:

- Migrate from Microsoft On Premise Exchange to Google G Suite Enterprise.
- They purchased Proofpoint to supplement their email security for Gmail.
 - Proofpoint could not integrate into their Global Security Operations Center's extensive monitoring systems and native applications.
- Their Global Security Operations Center needed to monitor all outbound traffic for data loss prevention, conduct content inspections, and deliver cyber intelligence to decision makers.
- Their Global Security Operations Center required exposure to traditional emails via the Exchange environment through Cloud and Gmail, encrypted and unencrypted network traffic, off-network content and removable storage, confidential data, source code, and more.

The Solution:

- Use Secure Email Gateway On Premise to create header rewrite rules to blind copy every outbound email passing through Proofpoint for content inspection and machine / human analysis.

The Results:

- Successfully integrated Secure Email Gateway On Premise into their Global Secure Operations Center monitoring platform.
- Paired with Trustwave Data Loss Prevention products.
- Constructed comprehensive custom scripts to filter all outbound traffic for content inspection.
- Created extensive rules with different criteria to trigger alerts with varying degrees of risk.

...malformed messages holding

employ and control resources while efficiently serving customers.

email Gateway APIs, to send email campaigns via SendGrid.

CASE STUDY

Electronics Manufacturer

One of the world's largest distributors of electronic components and embedded solutions with over 15,000 employees in 125 locations. They work with more than 1,400 technology suppliers and serve 2.1 million customers in over 140 countries.

The Challenges:

- Growth through acquisition left disparate Information Technology systems operating globally, each with their own policies, standards, regulations and controls.
- US operations team was using Cisco IronPort®, and their users were suffering from overwhelming phishing email scams and ransomware attacks.
 - EMEA operations team was using Trustwave Secure Email Gateway On Premise for 15+ years.

The Solution:

- EMEA and US operations conducted a bakeoff with both solutions.
 - Trustwave Secure Email Gateway captured phishing and malicious spam emails that Cisco IronPort® missed.
- US operations replaced all Cisco IronPort® appliances and deployed Trustwave Secure Email Gateway globally.

The Results:

Elimination of the phishing, email scam and ransomware threats.

A significant decrease in helpdesk calls, support tickets from user complaints and high spam volumes.

Consolidation of their security program and products, operation alignment and installation of corporate-wide best practices across multiple subsidiaries.



CASE STUDY

Office Supply Retail Chain

One of the largest office supply retailers in the world with over 1,200 stores, 40 warehouses/fulfillment centers and 77,000 employees across North America.

The Challenges:

- They work with tens of thousands of vendors.
- They did not have a robust supply chain management solution that could manage multiple applications and systems across their global business operations.
- They lacked protection for business processes such as:
 - Purchase Order processing, invoicing and payments
 - Shipping logistics, inventory database management
 - Delivery services, credit card transactions, and recordkeeping.
- They could not find a single solution that could work across all of their supply chain activities to serve multiple market segments.

The Solution:

- A move to Trustwave Secure Email Gateway On Premise for its robust, flexible policy engine to create header rewrite rules and custom scripts to:
 - Route all email to the corresponding systems, applications, and business units.
 - Process and manage their massive global supply chain.

The Results:

Successfully integrated Trustwave Secure Email Gateway On Premise into their supply chain.

Expanded Secure Email Gateway On Premise within their business operations over the last 19 years taking advantage of its multipurpose functionality.

Migrated to the cloud and relied on Trustwave to provide Platform-as-a-Service and Infrastructure-as-a-Service to consolidate their supply chain infrastructure.



CASE STUDY

Banking Services

A multinational bank and global leader in food and agriculture financing. Sustainability-oriented banking with over 1,000 branches and offices operating in more than 40 countries.

The Challenges:

- Targeted phishing attacks and business email compromise scams constantly plagued branches and global locations.
 - Corporate users were unaffected.
- Its bank branches and global locations, supporting 35,000 employees, used Cisco IronPort®.
 - Corporate headquarters used Trustwave Secure Email Gateway On Premise to protect its 11,000 employees.

The Solution:

- Replace all Cisco IronPort® appliances and install Trustwave Secure Email Gateway in four of its data centers to serve all branch and global locations.
- Migrate all users' email traffic through the new messaging infrastructure with comprehensive protection from Trustwave Secure Email Gateway.

The Results:

An immediate relief from rampant phishing, spoofing, and Business Email Compromise.

They were given time to focus on the next big project. A move to the cloud, and migration from an On-Premise Exchange, to Microsoft® Office 365®.



Competitive Positioning by Key Competitor

Enterprise Competitors

Competitor	Strengths	Weaknesses	Positioning
Proofpoint	<ul style="list-style-type: none"> Invests heavily in R&D Strong competitor with a strong product Dedicated focus on email security 	<ul style="list-style-type: none"> Only focused on email security. Can't offer integrated email, web and other security solutions. Their Threat Lab organization only deals with email-based threats; limited insight into blended threats. Products are challenging to configure, not as easy to stand up as our SEG. 	<p>This is what we hear from former Proofpoint customers:</p> <ul style="list-style-type: none"> Trustwave's policy engine is more flexible Trustwave's BEC engine is more advanced Trustwave's SEG Cloud POPs are 100% local data sovereignty compliant.
Cisco (IronPort)	<ul style="list-style-type: none"> Cisco's solution can be deployed as physical or virtual appliances, cloud based or hybrid. Tightly integrated with Cisco's Endpoint console and threat response engines Cisco will deeply discount the product to buy business 	<ul style="list-style-type: none"> Acquired IronPort's extensive customer base but Cisco hasn't kept up development Customers prone to BEC attacks and we have won significant business away from Cisco Product requires expensive add-ons to be on par with SEG 	<p>We talk to a significant number of Cisco customers who are looking to switch because IronPort does not sufficiently protect against BEC attacks.</p>
Symantec	<ul style="list-style-type: none"> Integrates with Symantec's Cyber Defense Platform to protect against both email and web-based threats. Integrates with their overall DLP portfolio 	<ul style="list-style-type: none"> Customer base from MessageLabs acquisition is vulnerable. Limited policy options. SEG products have a wide range of policy options. 	<p>Probe for pain points around Symantec's cloud solution and its ability to prevent BEC attacks.</p> <p>The cloud platform is also not 100% local data sovereignty compliant, an</p>

Competitor	Strengths	Weaknesses	Positioning
	<ul style="list-style-type: none"> Symantec will deeply discount to “buy” business 	<ul style="list-style-type: none"> Limited development of cloud solution leaving customers vulnerable. 	increasing area of concern for customers.

SMB/Mid-Market Competitors

Competitor	Strengths	Weaknesses	Positioning
Mimecast	<ul style="list-style-type: none"> Fully cloud-based, providing scalability while 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. 	<ul style="list-style-type: none"> 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. 	Former Mimecast customers tell us that detection rates are limited with high levels of false positives. Limited BEC fraud engine. The cloud platform is also not 100% local data sovereignty compliant.
Barracuda	<ul style="list-style-type: none"> Customers like their per server, vs. per user licensing model Easy to stand up and administer the product 	<ul style="list-style-type: none"> Limited development activity, product is a collection of open source projects and perceived as a minimum tick box type of product. Primarily known as a sales and marketing company, not a technology company. Ineffective against BEC. Limited DLP capability 	<p>Best known for their airport ads and not the capability of their products.</p> <p>Trustwave has been in the security business for more than 20 years. Security is in our DNA, unlike Barracuda, whose products provide bare bones security.</p>

Buying Factors with Competitive Ranking

Buying Factors integrates customer objectives with key vendor required capabilities and a competitive ranking against other vendors. (“0” = low, “4” = high)

Customer Need	What are the Key Buying Factors when choosing a security email gateway vendor?	Trustwave	Proofpoint	Mimecast	Microsoft	Cisco
Platform Support	On-Premise Gateway	4	4	4	4	4
	Cloud-based Gateway	4	4	4	4	3
	Cloud-hosted Email Services (Office 365, Google GSuite, etc.)	4	4	4	4	4
Core Features	Anti-malware (viruses, worms, trojans, ransomware, spyware, etc.)	4	3	4	3	3
	Anti-spam	4	4	3	3	3
	Anti-phishing	3	4	4	3	2
	Business Email Compromise (BEC)	4	4	4	3	2
Advanced Threat Protection <small>*coming soon</small>	Impersonation/spoof detection	4	4	4	4	2
	URL rewriting, inspection, and time-of-click analysis	3	4	3	3	2
	Attachments	3	3	3	2	3
	Account Takeover	4	4	4	3	3
	Network sandbox	0*	4	4	3	3
	Content disarm and reconstruction (CDR)	0*	0	2	0	0

Customer Need	What are the Key Buying Factors when choosing a security email gateway vendor?	Trustwave	Proofpoint	Mimecast	Microsoft	Cisco
	Anomaly detection	0*	0	2	0	0
Data Protection	Data loss prevention (DLP)	4	4	4	2	4
	Email encryption	4	4	3	3	3
Data Retention	Email archiving	4	4	4	3	3
	Advanced eDiscovery/legal hold	4	4	4	3	2
	Email continuity	4	4	4	2	2
Compliance Support	HIPAA, GLBA, SEC, SOX, GDPR, CCPA	4	4	4	4	4
Ease of Use	Pre-defined policies	4	4	4	3	3
	Flexible policy management	4	3	3	1	3
	Custom policies	4	3	3	1	3
	Effective monitoring and notification	4	4	4	3	3
	Integration within Threat Detection and Response Ecosystem	3	1	1	2	3

What Can Slow Down or Kill a Deal

This section provides the opportunity to share proof points and anecdotal information about potential hurdles that Sales/SE's might discover in the field.

- Trustwave SEG's biggest challenge in the field is brand recognition:
 - SEG meets, and often beats, competitive offering comparisons by feature and platform support.
 - Though SEG has a strong legacy which began years ago as "MailMarshal", other brands (such as Proofpoint) have developed greater market presence and brand recognition. And,

since Gartner stopped tracking the Secure Email Gateway Magic Quadrant in 2015, it has been more challenging to demonstrate an evolving market position.

- Differentiate Trustwave's SEG through our strong partnerships, namely Microsoft and Trustwave's unique support of Office 365.
 - Microsoft is a recognized leader in managing business-related email.
 - Microsoft is leading the charge into cloud-enabled business email from its dominant position with on-premise MS Exchange.
 - Microsoft is working closely with Trustwave as evidenced by Trustwave SEG being the first and only secure email gateway provider to support MS Azure Information Protection and Rights Management Service.

Having Conversations

Consider the following before having a conversation with potential SEG customers:

- Email security is not always considered a strategic priority. **Disrupt this thinking.**
 - Email is the #1 method used by cybercriminals to infiltrate and steal data and money
 - Business email compromise and phishing drive 48% of all internet crime-driven financial loss
- Sell the Trustwave value
 - Avoid a “feature fight”
 - Learn our ownable differences and how Trustwave is a more strategic choice for email security
 - We are committed to email security – strategically investing in the technology since the early 2000s
 - Many of the global players have allowed SEG investment to wane in favor of hotter technologies
 - Newer cloud competitors do not have the security DNA like Trustwave
 - SEG offers superior protection, easy adoption and a more favorable TCO model
 - We also solve the email user problem with a full catalog of educational courses to train and test email users
 - **Only secure email gateway that integrates with Azure RMS**
- Key selling opportunity is at renewal time
 - Learn what technologies they are currently using
 - Outlook on Exchange, Office 365-cloud, IBM, Gmail/GSuite, etc.
 - Email content filtering product (appliance or software) or service (SaaS, subscription model)

- Understand where their pain points are with the incumbent email security solution
- Understand how Trustwave augments security gaps in Microsoft Office 365 and other cloud solutions
- Overcome their concerns about switching providers
 - The market is moving from appliance-based to cloud-based
 - SEG Cloud makes it easy with pre-configured filtering rules that get customers up and running in no time

Discovery Questions

- Uncovering SECURITY challenges
 - What is the biggest gap in your current email security system?
 - Have you experienced any issues with BEC fraud emails getting to your end-users?
 - How well does your email security solution understand the web to enable it to combat blended web/email threats?
- Uncovering MANAGEMENT challenges
 - How much time do you spend tuning your solution to increase detection/decrease false positives?
 - 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?
- Uncovering DATA PROTECTION challenges
 - How can you tell if sensitive/confidential data is leaving your organization via email?
 - How much effort goes into enforcing your acceptable-use policy?
 - What standards you need to adhere to in terms of email security (HIPAA, PCI-DSS, SEC, Sarbanes-Oxley, GDPR, etc.)?
- Understanding ON PREMISE or CLOUD challenges
 - Have you recently moved to Office 365 or Google G-Suite?
 - How is that platform performing in terms detection rates?
 - If you have not migrated yet but are planning to, have you considered if all the base capability will really meet your requirements and expectations?

Objection Handling

- **“I have never heard of Trustwave SEG”**

Trustwave SEG was previously known as MailMarshal. MailMarshal was the 2nd email security solution in the market even before spam existed. There are thousands of companies globally that rely on SEG for their email security and management tasks

- **“I do not see you on the magic quadrant”**

Gartner last did their email magic quadrant in 2015. Trustwave was listed. Since then we have been concentrating on our Managed Security Services where we are now in the leader's quadrant. Trustwave is again engaging with email analysts and you will see us being included in the future.

- **“Microsoft tells me they can do everything I need”**

Microsoft does have a good solution in Office 365[®] but we find that most organizations end up relying on a 3rd party email security and management platform to supplement the base Office 365[®] features. Please refer to our Office 365[®] whitepaper where we discuss the main areas where we see our services supplementing Office 365[®].

- **“I am told you are not a specialist in email security”**

We are dedicated to helping our customers across all their cyber-security needs, including email security, with all the technology we own, the leading technology vendors we partner with and as well as all the direct customer work we do around incident response, application and penetration testing and so on. We have a massive amount of data and knowledge around cyber-security which we then work back into all our products to ensure they are protecting and adding value for our loyal customers.

- **“I'm happy with our current solution.” OR “How do I know your solution is better than what I have now?”**

How well is your current solution performing in your environment? 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? 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. One example of this was WannaCry, SEG customers were protected from WannaCry emails within minutes of this new attack emerging.

And, Trustwave has the only Secure Email Gateway on the market that can unpack, analyze and repack Azure RMS attachments and emails.

- **“We're moving/have moved to Office 365 and email security is built in.”**

If moving to O365: What are you switching from? What are your expectations for O365 in terms of email security?

If already switched: How does O365 differ from the previous solution?

Microsoft Office 365 is a great solution for email hosting - not so much for email security and data loss prevention. In many situations, you can achieve better email security, and save money, by complementing Office 365 with SEG Cloud.

If asked, what do we provide that O365 doesn't: Office 365 is a fantastic tool for productivity and collaboration, but it's unrealistic to expect that one cloud-based tool would be able to match the effectiveness of a legacy solution which likely included multiple layers of security software and add-ons.

Here are a few key areas where SEG helps companies maximize their O365 investment:

- BEC attacks: O365 relies on basic spam filtering which is ineffective here. SEG has a specialized fraud detection engine.
- Policy engine: O365's policy is not enterprise-ready. Our policy engine is the most flexible solution on the market – allowing for granular control that can evolve with business needs.
- DLP capabilities: The highest licensing tier of O365 is needed to get baseline content inspection. SEG offers full DLP inspection on emails and attachments.
- Enterprise class email archiving platform as an optional extra: Full eDiscovery and enterprise class feature set in a simple, affordable licensing model. We don't expose internet services that use our backend database and have firewalls in place.

- **“Your cloud product seems simplistic.”**

SEG Cloud's standard package is designed with a default rule set that 80% of organizations would use. It can be simply refined further by enabling or disabling various settings, or custom rules can be added. For those who need more than this in a cloud offering, we just released the new SEG Cloud Advanced and SEG Cloud Enterprise offerings.

- **“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? A switch does require time and planning. However, a switch to Trustwave will actually result in time savings because the time you're investing in enhancing your current solution will be saved with SEG's increased productivity, protection from advanced threats, and better compliance and acceptable use controls.

- **“I have been using the solution I have now for many years, it has never let me down, why should I look at what you have?”**

That's great that its been working well for you, but is it holding you back? Are there for example certain policies that you wish you could implement? Has your organization had any impact from BEC fraud? Are you aware of any new regulatory compliance requirements that you might need to support in your email system in the future, are you sure your current solution will be able to support those? Are you sure you are getting good value for investment?

Key Resources, Processes and Contacts

Top Marketing Resources

- [New Methods for Solving Phishing, Business Email Compromise, Account Takeover and Other Security Threats](#) whitepaper
- [In, Out and Around: 360° Security for Office 365](#) white paper
- [Don't Be a Phish Out of Water](#) infographic
- [3 Reliable Methods to Safeguard Microsoft Office 365 Users and Data](#) blog post
- Look to Sales Hub for [SEG on-premise](#) and [SEG Cloud](#) resources, as well as our [external website](#).

Sales Process Steps

1. Generate enough interest to secure a 15-minute discovery call
2. Goal of discovery call is to understand:
 - a. Business drivers, use case, what they do today
 - b. When is their current solution up for renewal?
 - c. Who handles email security? Does it roll up into IT operations, Security or another stack?
 - d. Decision makers, influencers and process
3. Schedule follow-up call with the customer and your SE on <date/time>:
 - a. Tell our email security story. Use the [customer presentation](#) deck on Sales Hub.
 - b. Enable your SE to explore the “technical fit” and discuss solution capabilities. A Demo may be scheduled after that.
 - c. Continue to gather information from the customer.
 - d. Promote the 30-day free [SEG Trial](#) or the free SEG Cloud Trial (ask your SE to set up).
4. Execute sales qualification process

Look to [Sales Hub](#) and the [external website](#) for more materials.

Key Contacts

Solutions Architect – AMS	Craig Sargent and Dimitris Vassilopoulos
Solutions Architect – EMEA	Dimitris Vassilopoulos
Solutions Architect – APJ	Craig Sargent

VP - Solutions Architect	Andrew Herlands
Product Manager	Jenny Chen
Product Marketing Manager	Donna Niemann

Appendix A – Rounding Out Email Security Needs

This section provides greater detail into the SEG optional security modules and software.

Optional Security Modules	Benefits
Email Archiving	Provides a systematic approach to save 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.
Email Encryption	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.
Blended Threat	Identifies, catches, neutralizes and blocks, in real-time, websites that serves up suspicious or malicious code to company users.
Image Analyzer	<ul style="list-style-type: none"> Automatically scans and sorts images entering the company via email into two categories – offensive and pornographic and normal and acceptable. Protects employees, customers, and suppliers from exposure to inappropriate and illegal content reducing and removing legal liability.
Anti-Virus Scanning	Keep your existing anti-virus scanners from Sophos, McAfee, Kaspersky and Bitdefender to provide an extra layer of malicious code detection.

Email Archiving

Email Archiving is a 100% cloud-based secure, compliant, and cost-effective archiving solution that stores company emails in a reliable and secure format that is easy to search and retrieve email data. This

solution allows customers to retain and maintain email data securely for extended periods of time with security exposure while email storage & management related costs.

Secure email archiving is not just about sending and receiving. It's about saving and finding.

- Simplify email searching - Intuitive simple to use interfaces enable a wide variety of customers to benefit from the solution
- Speed of Search - Lightning fast search no matter how many mailboxes or amount of mail
- Forensic Email Archiving - Our history is in forensic email archiving for the most highly regulated industries
- Cost Effective Deployment - Save money on your core email service offering

SPECIAL NOTE REGARDING THE SEARCH FUNCTIONALITY IN OFFICE 365: Due to the mailbox-based indexing model, Office 365 **does not** execute searches in real-time. Instead, a search job needs to be created and the search requestor will get notified when the search is complete. The requestor can either copy the results to another “discovery mailbox” (in which case your search results are limited to the 50 GB maximum mailbox size) or create an Export job directly to PST files. While this model may work if the requestor is extracting a whole mailbox, it does not allow for investigation, or search refinement. The result is that downstream discovery costs may be higher, as more data needs to be processed.

Office 365 executes searches on a mailbox by mailbox basis. As a result, the more mailboxes that are searched within, the longer it will take for the batch search to be completed. A search requestor can't preview results or initiate an export task until the search is complete, so there can be significant wasted time during key discovery tasks if you don't initiate follow on steps immediately after the search completes.

To quote the Microsoft Services Agreement (part 6b):

“We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. **We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.**”

Email Encryption

Email Encryption is a 100% cloud-based solution to compose, send and reply to sensitive emails or confidential documents from any recipient in the world without requiring the recipient to establish a relationship, via download or software install, prior to exchanging encrypted messages. It protects personal information while in transit and while being stored, providing advanced protection seamlessly and without disruption to current email practices. Our cloud-based Email Encryption provides:

- Policy-based message routing and encryption management
- Completely hosted in the cloud so there is no software to install and maintain
- Supports industry standards-based encryption
- Content-aware encryption filters that scan SMTP headers, body and attachments

- Single sign-on support for seamless integration between the secure website of the customer and web pick-up portal
- Intelligent one-click encryption auto selects best method encryption based on a per recipient basis
- Multiple signing modes when using digital signatures for compliance purposes

We have two Email Encryption offerings:

- **Email Encryption Essential:** A policy-based email encryption solution that consists of a fixed set of features leveraging static design Portal encryption. Email Encryption Essential includes:
 - Web Portal Encryption: Enables secure delivery of encrypted messages via a secure website. The email is not delivered to the recipient, but instead users are notified in their regular inbox that an encrypted message is waiting for them.
 - Recall, read receipts
 - All or a subset of languages available in the Portal
 - 25 MB maximum email size
 - Social Login Connectors
 - 30 Day Portal Message Retention
 - Secure Reply

Email Encryption Essential customers users may send on average, up to 240 secure email messages per month having an average pre-encryption file size of 500 KB. For the purpose of calculating the number of secure email messages sent, the number of recipients on a message are counted separately.

- **Email Encryption Advanced:** Offers extensive encryption delivery flexibility and features to meet a wide range of company and branding requirements:
 - Transport Layer Security (TLS) Encryption: Encryption of messages and attachments in transport directly to the recipient. No setup or password requirements to provide the most seamless method.
 - TLS connection is verified for validity on-the-fly
 - Configure a White List (only send to) or Blacklist (do not send) of TLS domains through a web-based administration console

PROS:

- Senders simply send messages and our Secure Email Encryption platform takes care of the rest
- No need for recipients to change behavior – customer-centric at every step
- If TLS is not available, Secure Email Encryption automatically offers alternative secure encryption delivery options, like Web Portal or Secure PDF – ensuring the messages are not sent unprotected
- Can be branded (footer or header)
- Ideal for B2B when whitelist employed to ensure recipient is using TLS for replies

CONS:

- If the customer wants secure messages to stay encrypted at rest post-transit, TLS should not be used.
- Message not secured at rest
- Secure replies are not provided unless customer uses TLS
- Encrypted PDF: Encrypt both body and attachments contained in outgoing email using standard PDF, Office and ZIP technologies.
 - Self-Registration: Recipient gets one-time registration message to set their own password
 - Registration process can also include an out-of-band confirmation
 - Authentication can be through existing bank portals without the need for additional URLs. The customer logs into an existing portal and is auto logged into a PDF password management portal via webservice calls
 - Sender-Set Password: Recipient provides the password set by the sender at time of sending through a plugin or subject line trigger

PROS:

- Excellent mobile experience
- Complete branded experience for recipient including all customer-facing webpages, encrypted messages and email notifications
- Deliver encrypted PDFs direct to an inbox
- Secure messages are encrypted at rest post-delivery
- Messages are available locally for offline viewing. offline
- Ability for secure passwords to be set by either sender or recipient
- Secure reply functionality with the option to have a secure copy for recipient
- Any standard PDF viewer on any device may be used to open an encrypted PDF

CONS:

- Limited message tracking.
- No read receipt option for sender.
- Encrypted PDF: Encrypt both body and attachments contained in outgoing email using standard PDF, Office and ZIP technologies.
 - Self-Registration: Recipient gets one-time registration message to set their own password
 - Registration process can also include an out-of-band confirmation
 - Authentication can be through existing bank portals without the need for additional URLs. The customer logs into an existing portal and is auto logged into a PDF password management portal via webservice calls
 - Sender-Set Password: Recipient provides the password set by the sender at time of sending through a plugin or subject line trigger

PROS:

- Excellent mobile experience
- Complete branded experience for recipient including all customer-facing webpages, encrypted messages and email notifications

- Deliver encrypted PDFs direct to an inbox
- Secure messages are encrypted at rest post-delivery
- Messages are available locally for offline viewing. offline
- Ability for secure passwords to be set by either sender or recipient
- Secure reply functionality with the option to have a secure copy for recipient
- Any standard PDF viewer on any device may be used to open an encrypted PDF

CONS:

- Limited message tracking.
- No read receipt option for sender.
- Encrypted Attachment: Deliver sensitive documents in messages as encrypted any attachments – without appearing in body of email. This option is useful for generating and processing bulk electronic statements.
 - Encrypted PDF attachments remain unchanged from their original formats
 - Support for Office Document encryption
 - Support for ZIP file encryption
 - Support to wrap files into encrypted PDF or ZIP
 - Self-Registration (same as Encrypted PDF)
 - Sender Set Passwords (same as Encrypted PDF)
 - Branded header and/or footers added to the message body with an account management link or Shared Secret Hint.

PROS:

- Message body remains clear-text – only the attachments are encrypted
- Excellent mobile experience
- Messages can be sent with multiple encrypted attachments in their original native format
- Complete branded experience for recipient including all customer facing webpages, encrypted messages and email notifications
- Deliver encrypted PDFs and Office documents direct to an inbox
- Message remains encrypted at rest post-delivery
- Ability to save messages locally or offline
- Ability for secure passwords to be set by either sender or recipient
- Offline reading of attachments

CONS:

- For Secure ZIP, recipient must have ZIP software installed capable of opening AES 256-bit files (such as WinZIP, SecureZIP, WinRAR, 7-ZIP)
- Limited message tracking
- No read receipt option for sender
- Certificate Encryption: Beneficial when recipients already have a third-party S/MIME or PGP key.

- Certificate Encryption is based on a user uploaded public certificate
- External lookup in LDAP for public recipient certificate
- Full PGP key creation / management for senders to external PGP users
- External users will get a PGP encrypted email that is a digitally signed with a public key attached for the sender. Eliminates need for PGP desktop software under PGP communication

PROS:

- Upload existing keys to our Secure Email Encryption platform
- Auto generate new keys as needed, maintaining current and future identities
- No need for recipients to change behavior
- Secure delivery can be made to any email address in the world (assuming key exists)

CONS:

- Configuration of inbound email flow is required to detect encrypted reply messages
- Web Portal Encryption: Enables secure delivery of encrypted messages via a secure website. The email is not delivered to the recipient, but instead users are notified in their regular Inbox that an encrypted message is waiting for them.
 - Self-Registration: Recipient gets one-time registration message and registers and set their own password
 - Registration optionally support out-of-band confirmation (on registration).
 - Authentication can also be through OAuth connectors.
 - Authentication can be through existing portals (no URLs in notifications).
 - No-Authentication: Recipient gets a URL that directly opens the message (no registration).
 - Sender Set Password: Recipient enters a password the sender set at time of sending through the plugin or through subject line trigger.
 - Out of Band Password: System generates a per message password and emails it back to a sender. The recipient must obtain this system password out-of-band from the sender to gain access to the message.

PROS:

- Excellent mobile experience.
- Complete branded experience for recipient including all customer facing webpages, encrypted messages and email notifications.
- Message remains encrypted at rest post-delivery.
- Ability to save messages locally in several formats from Outlook to encrypted pdf.
- Ability for secure passwords to be set by the sender or by the recipient.
- Secure reply functionality.
- Read receipts.
- Full message audit for both sender and Administrator. Message recall for both sender and Administrator.

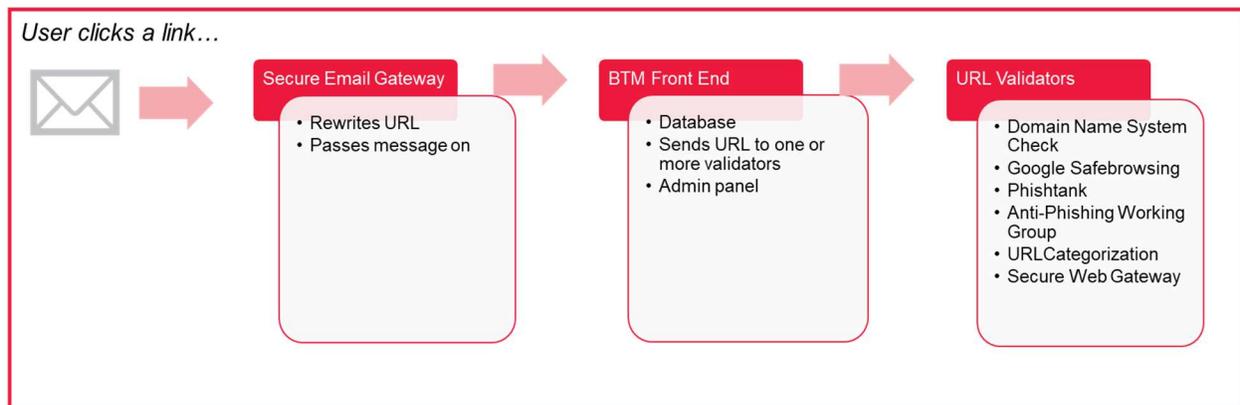
CONS:

- Retention period (30, 60, 90 days) then deleted.
- Recipient must leave their local mailbox to retrieve messages online
- **Outlook Encryption Add-In:** An optional Microsoft Outlook Add-In. Both a desktop version and O365 Outlook Web version are available. Email Encryption Advanced add-in installs an encrypt button into the Outlook Compose page so that senders can initiate encryption of their messages (if desired). The Outlook Add-In adds MIME x-headers into the outbound message that will be detected by the DLP service and mapped to a policy. The email is consequently routed to Email Encryption Advanced for encryption. The Add-In is popular due to its ease of use, categorization of messages, and feature that offers a Shared Secret Passphrase.
- **Web-based Administration:** Email Encryption Advanced can be administered via the web-Based Admin Console. Customers who subscribe to the Email Encryption Advanced will have a unique profile on the platform can also be granted Administrative access. The customer can query recipient accounts and perform actions such as password reset and delete account. They can run reports to view details of encrypted messages.

Any or all Email Encryption Advanced delivery methods listed above can be used at the same time with customizable encryption policy options.

Blended Threats Module

BTM identifies, catches, neutralizes and blocks, in real-time, websites that serves up suspicious or malicious code to company users within emails and attachments.



Blended Threat Module Process

Through the process, the BTM:

- Validates and rewrites the URL, keeping the validated URL with the original email (remains with email when forwarded as well).
- BTM only requires online access (no requirement for MS Exchange connection).
- Provides seven layers of URL validators (competitive differentiator as not all BTM are equal).
- Supports all devices.

Image Analyzer

Image Analyzer modules provides protection against sexually explicit email attachments that can:

- Damage brand and company reputation
- Degrade company culture
- Increase company legal liability
 - Duty of care to protect employees
 - Proliferation of pornography contributes to hostile working environment
 - Sexual harassment lawsuits (Company Vicariously Liable)
 - Illegal images

Our Image Analyzer module can:

- Detect 9 out of 10 commercial pornographic images
- Produce near zero false positives
- Identify suspect image attachments in emails
- Educate users about company policy when questionable content is detected
- Monitor emails to provide visibility of misuse
- Enforce company policy and protects reputation by taking appropriate action on emails containing explicit content

Anti-Virus Scanning

Anti-Virus (AV) Scanning modules provide an extra layer of malicious code detection.

- SEG Cloud: Sophos AV protection is integrated within SEG Cloud and provided to customers at no additional cost.
- SEG On-Premise: Customers have the option to purchase AV Scanning support for the following AV solutions:
 - Bitdefender
 - Kaspersky
 - Sophos

NOTE: Subscription cost must match the corresponding SEG user count. Subscription cost varied depending on preferred AV solution.

Cautions



Note: This symbol indicates information that applies to the task at hand.



Tip: This symbol denotes a suggestion for a better or more productive way to use the product.



Caution: This symbol highlights a warning against using the software in an unintended manner.



Question: This symbol indicates a question that the reader should consider.

This template comes with a built-in 3 column table in Trustwave colors. You can insert the table with the following menu selections: **Home | Insert | Table | Quick Tables | TW Table 3 Column**

Or you can copy and paste this one, provided here so you can do exactly that.

Note the formatting:

- Table heading row: *tbl.header*
- Table cells: *tbl.body*
- Table cells with bullets (col 3): *tbl.bullet*

Table 1: Table Caption (TW Table 3 Column – Red)

Version	Date	Changes
1.0		• Initial release
2.0		•
3.0		•

Table 2: Table Caption (TW Table 3 Column – Black)

Version	Date	Changes
1.0		• Initial release
		•
		•

Table 3: Table Caption (TW Table 3 Column – Blue)

VERSION	DATE	CHANGES
1.0		• Initial release
		•
		•