TRUSTWAVE SEG

The Importance of Keeping Your Trustwave Secure Email Gateway Up-to-Date

Contents

Introduction

Email-borne security threats are constantly evolving.

- Spam volume is down, but the proportion of malicious spam and targeted threats continues to rise.
- Data breaches, many of which originate with phishing, are a continuing threat.
- Targeted Business Email Compromise or “whaling” for fraudulent transfer of funds is an emerging problem.
- New vectors, strategies, and threats are constantly emerging.

To have the best defenses in place against these threats, it is critical to have an advanced, stable, and up-to-date email security solution in place. Yet for many organizations that have a highly functional solution like Trustwave SEG in place, it is all too easy to “set and forget” email security – “if it ain’t broke, why fix it?” This is particularly true with today’s tight resourcing and other unexpected business challenges.

With data breaches, fraud, ransomware and other issues costing hundreds of thousands, and even millions of dollars at a time, and harming company reputations, complacency is a serious risk. Email protection must be kept up to date and relevant.

Below are just some of the benefits of upgrading Trustwave SEG.

Benefits of Upgrading

Enhanced Security and Protection

Among the many benefits of a maintenance subscription for Trustwave SEG are a number of automatically updating technologies to block spam, malware, and other unwanted or dangerous email.

Software upgrades are also included with valid maintenance, but the SEG software does not self-upgrade. Upgrade must be manually initiated, and in most cases is a quick in-place process replacing the existing software.

Security and protection features recently introduced include:

- Targeted detection of BEC/CEO fraud
- Advanced Malware Exploit detection (AMAX) engine, a scripted anti-malware engine based on YARA that is regularly updated by Trustwave SpiderLabs based on their threat intelligence
- DMARC support, in conjunction with existing SPF and DKIM support
- Blended Threats Module for point of click malware detection
- Updated TLS support

Planned for the near future is a sandboxing feature to further enhance malware detection.

Reduction in Spam, Malicious Email, and False Positives/Negatives

Trustwave anti-spam and anti-malware engines are constantly evolving. Updates to the engines often depend on technology that is only present in current product releases. Customers using older releases miss out on these improvements.

Minimizing Support Calls

Many calls to Trustwave Support relate to older product versions. Sometimes a customer describes frustration with a long standing detection problem or worse, when that issue was already addressed a year or more earlier in the regular product release cycle. Trustwave's self-service resources like the Knowledge Base and Forum give good information about the latest releases, improvements, and fixes in SEG.

Improved Performance

SEG version 8.0 and above is designed to best utilize the current Windows 64 bit OS versions running on modern hardware or virtual machines. Even with the addition of security layers, SEG throughput continues to improve. SEG can be installed in cloud environments now (supporting Azure SQL), and is moving toward increased cloud install support.

Upgrade time is also the best time to review existing policy with the help of the Default Rules published for each major release. Old, redundant, and bloated policies can seriously affect performance and in the worst case can compromise security.

SEG includes a policy profile tool that can be used to evaluate policy usage. For more information, see the links at the end of this document.

Improved Visibility and Integration

Trustwave SEG provides a full email management console and dashboard with levels of access, as well as end user administration of suspected spam. In the enterprise, where email is only one aspect of security, an integrated view of threats is also necessary. SEG 8.X and above provides the ability to export the full email stream logging to a Syslog feed for consumption by enterprise SIEM solutions. This ability gives the opportunity for correlation of threat indicators and early detection of problems.

For another level of management visibility, SEG 10.0 introduces full auditability of SEG policy changes.

Managed Change

Upgrades to SEG do not change the existing policy (with a few exceptions related to clear security threats). This design allows for safe upgrade. At the same time, it is important for customers to review the new abilities and enable policy to leverage the improvements. To help customer manage change, Release Notes, Default Rule listings, and other technical papers are part of every release.

Noteworthy New Features in SEG 10.0

The features mentioned below have been introduced in SEG 10.0. For full details and additional items, see the Release Notes.

- **New User Interface:** Configuration and Console functions are combined in a new web based interface. The legacy Configurator, Console, and Web Console are no longer used.
- **Auditability:** Configuration changes are fully auditable. Changes can be reviewed before commit.
- **Rule Condition AND/OR selection:** Rule conditions that include multiple TextCensor scripts or Category scripts can be set to trigger if **any** of the selected items match. The default behavior still requires **all** selected items to match.

- **Updated TLS support:** TLS protocol version 1.3 is now available. Additional Elliptic Curves are available for Perfect Forward Secrecy.

Noteworthy New Features in SEG 8.x

The features mentioned below have been introduced in various 8.x releases. For full details and additional items, see the Release Notes for each version.

- **Native 64-bit executables:** Trustwave SEG is now compiled as a 64-bit application. Malware scanner plug-ins are also provided in 64-bit versions. (8.0)
- **Support for DMARC:** Trustwave SEG now supports checking and reporting of DMARC information. (8.0)
- **Azure Information Protection Rights Management (AIP RMS)** support: Trustwave SEG supports content scanning of items protected by AIP RMS. (8.2)
- **Azure SQL Server support:** Trustwave SEG supports use of Azure SQL for databases (where SEG is deployed on Azure). (8.2)
- **Remote server archiving support:** Trustwave SEG supports delivery of messages to an archive server for long-term retention and searching. (8.2)
- **Syslog support:** Trustwave SEG can send detailed message handling information to a Syslog server. (8.1)
- **Improved TextCensor scripts and new PCI DSS Rules:** New scripts for Credit Card and Social Security detection are included. On upgrade, existing rules are updated if possible. New rules for Credit Card detection are included in Policy Management (inbound and outbound), disabled by default. The rules may be helpful to customers complying with the Payment Card Industry Data Security Standard. (8.1)
- **Enhanced BEC Fraud detection:** SEG provides Executive Names and Domain Similarity matching to combat BEC fraud. (8.0)

Upgrading Tips & Tricks

Upgrading Versions

Take a moment to read the upgrade advice for your current version of SEG or MailMarshal SMTP. Always read the Release notes for the specific version you are planning to install.

To 10.0 from Trustwave SEG 8.2 (8.2.3 or later)

- SEG attempts to upgrade the configuration as required. Certain rare issues require you to make changes in the SEG 8.2 configuration before you can complete the upgrade. For more details, please see Trustwave Knowledge Base article Q21122.
- To validate the changes and list any items that require manual update, use the SEG 10.X Upgrade Preview tool.
- You can upgrade/migrate in place, subject to Operating System and database server version prerequisites. Your product key remains the same.
- The SEG database remains the same. A new Configuration Service database is created to support the web Management Console and auditing functions.

To 8.2 from MailMarshal SMTP 7.3.0 through 7.5.X

- This upgrade requires migration from the 32 bit version to the 64 bit version of the software.
- Be sure to review the Release Notes for details.
- You can upgrade/migrate in place, subject to Operating System prerequisites. Your product key remains the same. Install folder and Registry location are changed.
- TextCensor and Category scripts are updated automatically when upgrading to version 8.X from 7.X. To validate the changes and list any scripts that require manual update, use the SEG 8.X Upgrade Preview tool.
- Your database remains the same. Note that supported versions of SQL Server have changed.

System Requirements

The following system requirements are the minimum levels required for a typical "standalone" installation of a single server hosting the Trustwave SEG 10 Array Manager, email processing, and selected database.

A full discussion of requirements for all supported configurations is available in the *Trustwave SEG User Guide.* See also Trustwave Knowledge Base article Q11358.

Category	Requirements
Processor	Core i5 or similar performance
Disk Space	20GB (NTFS), and additional space to support email quarantine/archiving
Memory	6GB (3GB available to SEG; 2GB for SQL Express; 1GB for operating system)
Supported Operating System	• Windows Server 2012, Server 2012 R2, Server 2016, Server 2019 (Standard or Enterprise versions) • Windows 7 (SP1), Windows 8, Windows 8.1, Windows 10 *(Installation of server components on these workstation operating systems is not recommended)*
Network Access	• External DNS name resolution - DNS MX record to allow Trustwave SEG Server to receive inbound email
Software	• Microsoft .NET Framework 3.5 SP1 and Microsoft .NET Framework 4.6.1 • Database server (managed cloud service): Azure SQL Database • Database server: SQL Server 2017, SQL Server 2016, SQL Server 2014, SQL Server 2012 • Database server (free versions): SQL 2017 Express, SQL 2016 Express, SQL 2014 Express, SQL 2012 Express • IIS

Category	Requirements
Port Access	• Port 25 - for email traffic • Port 53 - for DNS external email server name resolution • Port 80 (HTTP) and Port 443 (HTTPS) - for SpamCensor and other automatic updates • Port 1433 - for connection to SQL Server database and Reports console computers • Port 19001 - between Array Manager and Processing Nodes

Upgrading a Single Server

To upgrade a single SEG server from any version supporting direct upgrade, install the new version on the existing server. You do not need to uninstall your existing version. The database will be upgraded in place, if necessary.

Upgrading an Array of Servers

- After upgrading the Array Manager, upgrade the processing servers. In some cases you may be able to upgrade the processing servers through the Configurator, with no need to log on to the processing servers. For full information, see the Upgrading section in the *User Guide.*

Additional Resources

- Trustwave Support Portal for SEG – documentation and downloads
  https://www3.trustwave.com/support/mailmarshal-smtp/

- Trustwave Forum – Subscribe for SEG update news and important product announcements. Note: requires login
  https://www3.trustwave.com/support/forum/Forum9-1.aspx

- Is my version of SEG currently supported? This Knowledge Base article is kept up to date with current and end of life versions
  https://www3.trustwave.com/support/kb/KnowledgebaseArticle20961.aspx

- Spiderlabs Blog – research and findings from Trustwave's elite team of ethical hackers, forensic investigators and researchers
  https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/

- Policy Profile tool - more information on the tool to help refine policy
  https://www3.trustwave.com/support/kb/article.aspx?id=11981