

# Email Compliance and Encryption subscription services

A powerful framework for managing compliance requirements and providing mobile-ready, secure email exchange

Today, email is the most widely used vehicle for distributing business data. Yet this communication poses a considerable risk for organizations of all sizes, as both small- to medium-sized businesses (SMBs) and enterprises must protect their intellectual property and sensitive information from inappropriate distribution while also ensuring compliance with new laws governing the protection of confidential information.

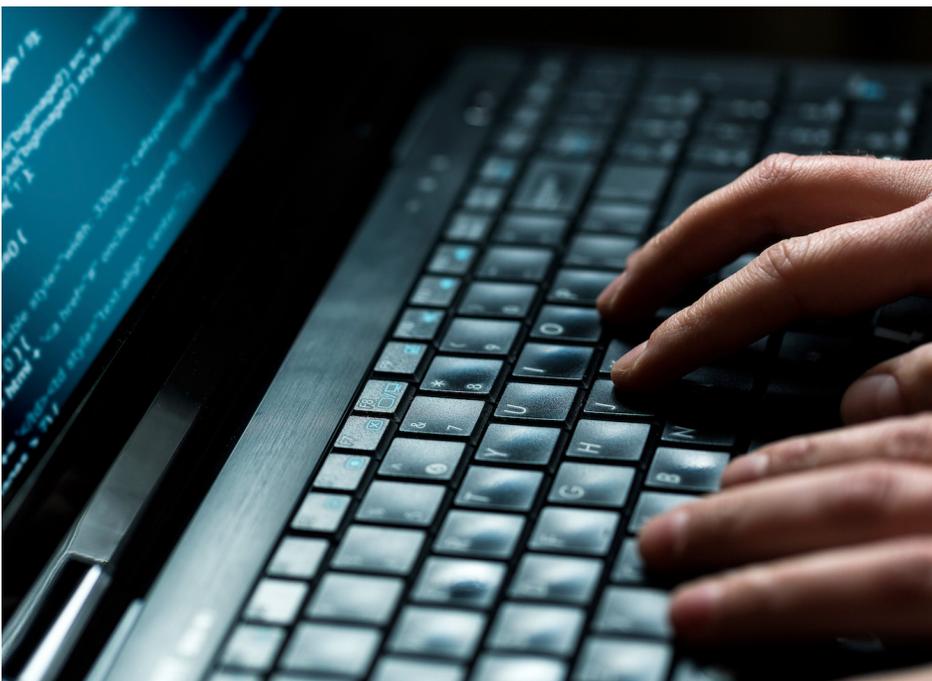
SonicWall Email Compliance and Encryption subscription services work with the SonicWall Email Security solution to provide organizations of all sizes with a powerful framework for stopping email threats, managing compliance requirements, and providing mobile-ready secure email exchange.

SonicWall Email Security is available as an appliance, a virtual appliance, Windows Server® software, or a hosted service. The solution combines an award-winning, anti-spam engine with anti-phishing, anti-virus, content filtering and policy management.

Adding Email Compliance and Encryption subscription services to the Email Security solution enables organizations to meet both regulatory and corporate requirements. The joint solution enables organizations to identify email for compliance policy enforcement; apply multiple email governance policies; monitor and report on email traffic; and ensure the secure exchange of sensitive and confidential information.

## Benefits:

- Record ID matching to easily search for predefined information
- Attachment scanning to stop the release of unauthorized information
- Predefined policies to achieve easy compliance
- Predefined dictionaries to ensure the protection of confidential information
- Approval boxes for scanning and approving emails before release
- Email encryption service to ensure secure exchange of confidential information
- Email archiving for simplified record keeping
- Compliance reporting and monitoring



## Features

**Record ID matching** — Searches for predefined social security numbers, bank routing numbers or credit card numbers. An easy-to-use, web-based UI enables custom record searches.

**Attachment scanning** — Looks for content within document attachments, including Word, PowerPoint, PDF and more than 300 other file types to ensure that sensitive data is not distributed.

**Predefined policies** — Set and enforce policies for common compliance setups.

**Predefined dictionaries** — Enable organizations handling health or financial records to monitor for HIPAA, SOX or GLBA violations. When these dictionaries are used in conjunction with Record ID matching, they ensure the protection of confidential information.

**Approval boxes** — Enable the viewing of email that potentially violates compliance policies before allowing it to be distributed outside the organization.

**Email Encryption** — Securely routes email that matches a specific policy to an integrated, seamless cloud encryption server to ensure the secure exchange of email containing sensitive customer data or confidential information.

**Email archiving** — Allows for inbound and outbound email archiving on the same server or appliances, for onpremise deployments. Additionally, organizations can route email that matches a specific policy to an external archive or hosted service.

**Compliance reporting** — Enables organizations to monitor and report on compliance-related email traffic.

## SonicWall Email Security administrative interface

The Email Security administrative interface enables centralized management. This makes it easy to create inbound and outbound policies for regulatory and corporate compliance on just one screen.

From a single screen, SonicWall Email Security allows the administrator to:

1. Select the component of the email to be searched and the attribute that indicates a policy violation.
2. Determine the enforcement action that should be taken if the attribute is found.
3. Choose the groups to which the policy should be applied.

The screenshot shows the 'Policy Filter' configuration window. It is divided into three main sections:

- Enable this Filter:** A checkbox that is checked.
- Conditions:** A section titled 'If All of the conditions are met:'. It contains a 'Message Part' dropdown set to 'Subject, Body or Attachments' and a 'Matching' dropdown set to 'with specific word'. To the right, there are options for 'Search Value', 'Use Dictionary' (selected), and 'Use Record Match'. Under 'Use Dictionary', 'Medical Terms' and 'Social Security' are selected. There are also checkboxes for 'Match Case', 'Intelligent Attachment Matching', and 'Disguised text ID'.
- Perform the following actions:** This section includes an 'Action' dropdown set to 'Issue Email Notification', a checked checkbox for 'And stop processing policy filters.', a 'From' field with 'corp\_security@corp.com', a 'Subject' field with 'HIPAA Violation', and a 'Message Text' field with 'Possible HIPAA Violation found in e-mail'.
- Compliance Name and Group:** This section has a 'Compliance Name' field with 'HIPAA' and an 'Apply this compliance to:' dropdown set to 'All Groups'. At the bottom are 'Save This Compliance Filter' and 'Cancel' buttons.

### Message components and attributes

To begin, select the part of the message to which you want to apply the compliance policy, such as from, to, body or attachment. Then determine the compliance policy attribute that indicates a violation. Pick from options including record matching, compliance dictionaries and disguised text identification.

### Enforcement actions

Once the policy is set, select the enforcement action for non-compliant email, for example: encrypt, archive, block, review, copy or quarantine.

### Groups

Choose the groups to which the policy applies. The policy can be applied to the entire organization or just a department, group or individual.

## Email Encryption service

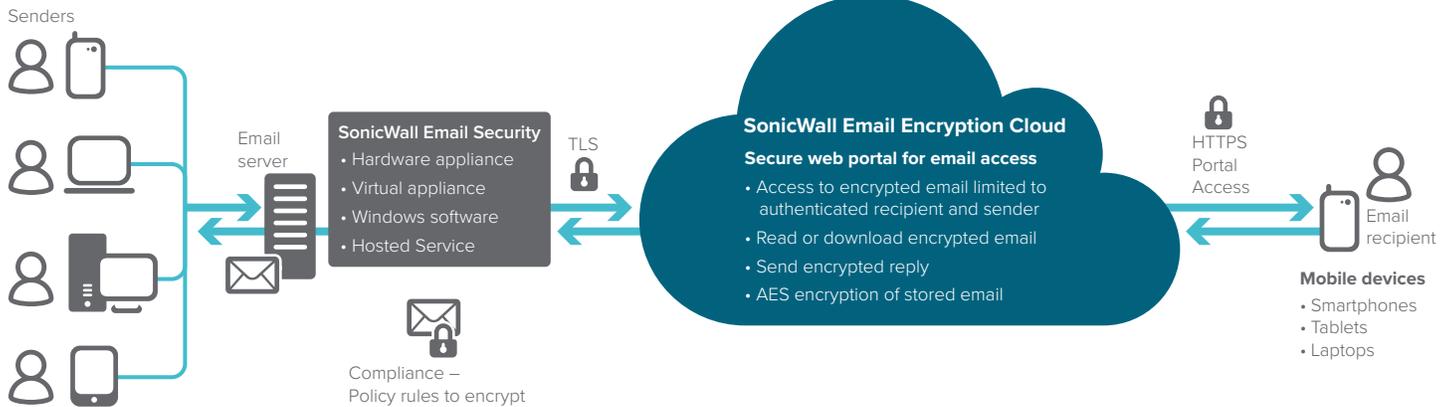
The SonicWall Email Encryption services provide integrated, policy-enforced and on-demand email encryption. With this service, policies may be configured to scan outbound email content and attachments for sensitive data and, if found, securely route sensitive email for

encryption and secure exchange with customers and partners.

Encrypted email can be tracked to confirm the time of receipt and time opened. A notification email is then delivered to the recipient's inbox with easy-to-follow instructions to log on

to a secure portal to read or securely download the email. The service is cloud-based; no additional client software is required. Unlike competitive solutions, SonicWall subscription services allow encrypted email to be accessed and read from mobile devices and laptops.

## SonicWall Email Compliance and Encryption Service



SonicWALL | Edit Filter

Enable this filter:

If **Any** of these conditions are met:

Select: **Subject** Matching: **starts with** Search value: **[SECURE]**

Use dictionary: **content-classes**

Use record ID: **Social Security Number**

Match case

Intelligent attachment matching

Disguised text identification

Perform the following actions:

Action: **Route to Encryption Service**

Stop processing policy filters

Filter name:

Filter name: **Send Secure Mail: Deliver Message via Enc**

Apply this filter to: **Apply to everyone**

Save This Filter Cancel

## Platform support

### SonicWall platforms supported:

All SonicWall Email Security appliances, Email Security software and Hosted Email Security service.

SonicWall Email Compliance 1-year subscription service	
Number of users	SKU number
25	01-SSC-6639
50	01-SSC-6640
250	01-SSC-6641
750	01-SSC-6642
2,000	01-SSC-6643
5,000	01-SSC-6644
10,000+	01-SSC-6645

SonicWall Email Encryption 1-year subscription service	
Number of users	SKU number
25	01-SSC-7427
50	01-SSC-7440
100	01-SSC-7443
250	01-SSC-7446
500	01-SSC-7468
750	01-SSC-7593
1,000	01-SSC-7471
2,000	01-SSC-7474
5,000	01-SSC-7549
10,000	01-SSC-7568

SonicWall Email Encryption Service for Hosted Email Security 1-year subscription	
Number of users	SKU number
10	01-SSC-5078
25	01-SSC-5081
50	01-SSC-5084
100	01-SSC-5087
250	01-SSC-5091
500	01-SSC-5094
750	01-SSC-5097
1,000	01-SSC-5104

Multi-year SKUs are available. Please visit [www.sonicwall.com](http://www.sonicwall.com).

## About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.