



# 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.

Dell™ SonicWALL™ Email Compliance and Encryption subscription services work with the Dell 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.

Dell SonicWALL Email Security is available as an appliance, a virtual appliance or Windows Server® software. 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 archiving**—Allows for inbound and outbound email archiving on the same server or appliance. Additionally,

organizations can route email that matches a specific policy to an external archive.

**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.

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

## Dell SonicWALL Email Security administrative interface

The Email Security administrative interface is web-based to enable 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, Dell 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 displays the 'Policy Filter' configuration interface. It includes the following sections:

- Enable this Filter:** A checkbox that is checked.
- Conditions:** A section titled 'If All of the conditions are met:' containing:
  - Message Part:** A dropdown menu set to 'Subject, Body or Attachments'.
  - Matching:** A dropdown menu set to 'with specific word'.
  - Search Value:** An empty text input field.
  - Use Dictionary:** A radio button that is selected, with a dropdown menu showing 'Medical Terms' and 'Social Security'.
  - Use Record Match:** An unselected radio button.
  - Match Case:** An unchecked checkbox.
  - Intelligent Attachment Matching:** An unchecked checkbox.
  - Disguised text ID:** An unchecked checkbox.
- Perform the following actions:** A section containing:
  - Action:** A dropdown menu set to 'Issue Email Notifier'.
  - And stop processing policy filters:** A checked checkbox.
  - From:** A text input field containing 'corp\_security@corp.com'.
  - Subject:** A text input field containing 'HIPAA Violation'.
  - Message Text:** A text area containing 'Possible HIPAA Violation found in e-mail'.
- Compliance Name and Group:** A section containing:
  - Compliance Name:** A text input field containing 'HIPAA'.
  - Apply this compliance to:** A dropdown menu set to 'All Groups'.

Buttons for 'Save This Compliance Filter' and 'Cancel' are located at the bottom of the form.

### 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 Compliance and Encryption subscription service

The Dell SonicWALL Email Compliance and Encryption subscription service provides integrated, policy-enforced and on-demand email encryption. With this service, policies may be configured to scan outbound email content and

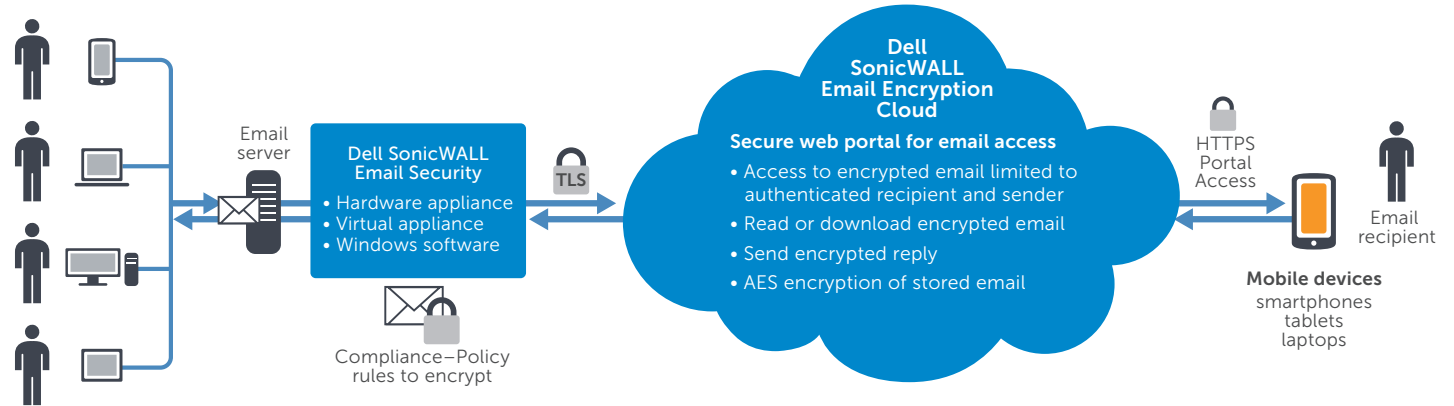
attachments for sensitive data and, if found, securely route sensitive email for encryption and secure exchange with customers and partners.

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, Dell SonicWALL subscription services allow encrypted email to be accessed and read from mobile devices and laptops.

### Dell SonicWALL Email Compliance and Encryption Service

Senders



The screenshot shows the 'Edit Filter' configuration window in the Dell SonicWALL management console. The window title is 'Dell SonicWALL | Edit Filter'. It includes the following sections:

- 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
  - Buttons: Save This Filter, Cancel



## Platform support

### Dell SonicWALL platforms supported:

All Dell SonicWALL Email Security appliances and Email Security software.



#### Dell SonicWALL Email Compliance 1-year subscription service

Email Compliance Subscription—25 users  
01-SSC-6639

Email Compliance Subscription—50 users  
01-SSC-6640

Email Compliance Subscription—250 users  
01-SSC-6641

Email Compliance Subscription—750 users  
01-SSC-6642

Email Compliance Subscription—  
2,000 users  
01-SSC-6643

Email Compliance Subscription—  
5,000 users  
01-SSC-6644

Email Compliance Subscription—  
10,000+ users  
01-SSC-6645

#### Dell SonicWALL Email Encryption and Compliance 1-year subscription service

Email Encryption with Compliance  
Subscription—25 Users (1-year)  
01-SSC-7427

Email Encryption with Compliance  
Subscription—50 Users (1-year)  
01-SSC-7440

Email Encryption with Compliance  
Subscription—100 Users (1-year)  
01-SSC-7443

Email Encryption with Compliance  
Subscription—250 Users (1-year)  
01-SSC-7446

Email Encryption with Compliance  
Subscription—500 Users (1-year)  
01-SSC-7468

Email Encryption with Compliance  
Subscription—750 Users (1-year)  
01-SSC-7593

Email Encryption with Compliance  
Subscription—1,000 Users (1-year)  
01-SSC-7471

Email Encryption with Compliance  
Subscription—2,000 Users (1-year)  
01-SSC-7474

Email Encryption with Compliance  
Subscription—5,000 Users (1-year)  
01-SSC-7549

Email Encryption with Compliance  
Subscription—10,000 Users (1-year)  
01-SSC-7568

### For more information

Dell SonicWALL  
2001 Logic Drive  
San Jose, CA 95124

[www.sonicwall.com](http://www.sonicwall.com)  
T +1 408.745.9600  
F +1 408.745.9300

### Dell Software

5 Polaris Way, Aliso Viejo, CA 92656 | [www.dell.com](http://www.dell.com)  
If you are located outside North America, you can find local  
office information on our Web site.

© 2014 Dell, Inc. ALL RIGHTS RESERVED. Dell, Dell Software, the Dell Software logo and products—as  
identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries.  
All other trademarks and registered trademarks are property of their respective owners.  
DataSheet-EmailComplianceAndEncryptionSubscriptionServices-US-TD585-20140108

