Software

How Dell SonicWALL Email Compliance and Encryption service enables compliance

Ensure the secure exchange of email containing sensitive customer data or confidential information.

The Dell SonicWALL Email Compliance and Encryption subscription service, an optional service available with Dell SonicWALL Email Security appliances and software, helps organizations achieve regulatory and industry compliance when moving PII (Personally Identifiable Information), PHI (Protected Health Information), proprietary data or any other types of sensitive information. HIPAA/HITECH, GLBA, PCI and other regulations require sensitive data be encrypted when transferred over a public network like the Internet. Since most organizations use email and simple file attachments as the preferred method for business communications, it's imperative that these be secured when transmitting sensitive data.

The Dell SonicWALL Email Compliance and Encryption service focuses on requirements surrounding the protection of data in motion, for example when sending messages and files to another person or system. Our services are just one part of your overall compliance strategy. Other services will be needed for local encryption such as disk, file or folder encryption.

Dell SonicWALL Email Compliance and Encryption service and HIPAA/ HITECH Compliance

According to HIPAA regulations section § 164.312 Technical Safeguards, protected information must have the following safeguards (note: only safeguards relevant to data in motion are listed):

HIPAA Safeguard	Dell SonicWALL Email Compliance and Encryption service control:
Access Control Persons should only be allowed to access information to which they have been granted access	The Email Compliance and Encryption service creates accounts which are used to uniquely identify and authenticate each user. Users are not allowed to gain access to another person's information.
Encryption Electronic Protected Health Information (PHI) must be encrypted	All Email Compliance and Encryption service access methods and delivery methods require encryption such as SSL, TLS, SSH and AES.
Audit Controls It must be possible to record and examine activity in systems that contain Protected Information (PI)	All Email Compliance and Encryption service system activity is audited. All messages are tracked regardless of how they are sent or received.
Transmission Security Protected health information must be protected while being transmitted over a communications network	All methods of accessing information in any direction are encrypted. Additionally any information on the Email Compliance and Encryption service cloud portal awaiting delivery is stored encrypted on the disk.
Additional HITECH requirements	
Extension of HIPAA requirements to Business Associates	The Email Compliance and Encryption service enables covered Business Associates to be compliant when communicating with your organization without any extra work for you or them.
Encryption as a recognized method for protecting PHI	The Email Compliance and Encryption service encrypts data in motion to ensure its confidentiality during transmission.

> "All methods of accessing information in any direction are encrypted. Additionally any information stored on the Email Compliance and Encryption service portal awaiting delivery is stored encrypted on the disk."

Dell SonicWALL Email Compliance and Encryption service and PCI-DSS Compliance

For any organization that deals with billing or other financial information, regardless of industry, compliance with PCI-DSS is very important. While not a government-issued regulation, this industry standard has such broad backing that not following it can severely impact a business.

PCI-DSS Compliance	Dell SonicWALL Email Compliance and Encryption service meets by:
PCI-DSS, Requirement 4.1 Strong cryptography and security protocols must be used to safeguard sensitive cardholder data during transmission over public networks	The Email Compliance and Encryption service uses SSL, TLS, SSH and AES encryption standards to provide secure transmission of data between the sender and recipient of any data.
PCI-DSS, Requirement 4.2 Account numbers must be encrypted when using "end-user messaging technologies" such as email	The Email Compliance and Encryption service allows an organization to securely send information using email in compliance with requirement 4.2.

The Email Compliance and Encryption service and Gramm-Leach-Bliley Act Compliance

The Gramm-Leach-Bliley Act (GLBA) has three primary requirements. Only two of these apply to service provided by the Dell SonicWALL Compliance and Encryption service: the Financial Privacy Rule and the Safeguards Rule.

Using the Email Compliance and Encryption service, an organization can ensure the privacy of their consumer's data while enabling it to be sent not only within their organization but also when exchanging data with the consumer directly. Additionally, for portions of communications running through the Email Compliance and Encryption service, the safeguard rules are handled by the Compliance and Encryption service as part of the service offering. Using the Email Compliance and Encryption service provides a monitored, governed, high availability solution that automatically encrypts all data that is transferred and stored within the service.

> "Using the Dell SonicWALL Email Compliance and Encryption service, an organization can ensure the privacy of their consumer's data while enabling it to be sent not only within their organization but also when exchanging data with the consumer directly."

For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our website for regional and international office information.