E-Class Email Security Series

Email security for the enterprise

High-performance, highly scalable email security

Many email security vendors cannot keep up with today's increasing volumes of sophisticated email attacks, stricter new compliance regulations and dynamic business environments. Enterprises demand powerful solutions that reduce costs and complexity.

Offering outstanding performance value and the most flexible delivery of Email Security solutions available in the marketplace today, Dell® SonicWALL® E-Class Email Security delivers highly effective, responsive protection that streamlines administrative overhead. Available as a Dell SonicWALL E-Class Email Security Appliance (ESA) ES6000 and ES8300, as a Dell SonicWALL E-Class Email Security Software on a third party Windows® server, or as a Dell SonicWALL Email Security Virtual Appliance in a VMWare® environment, Dell SonicWALL E-Class Email Security solutions provide self-running, self-updating, future-proofed security. Scanning both inbound and outbound traffic, E-Class Email Security boosts productivity by stopping spam, viruses and phishing; and supports regulatory compliance by blocking leaks of confidential data.

Dell SonicWALL E-Class is a line of premium, enterprise-class solutions offering outstanding protection and high-performance protection while also delivering scalability, elegant simplicity and unparalleled value. The E-Class portfolio of products and services offers a comprehensive line of email protection, network security and secure remote access solutions.

- **Inbound and outbound email threat management**
- **Hardware, software, and virtual appliance options**
- **Highly available and scalable split mode architecture**
- **Regulatory compliance framework**
- **Email policy management**
- **Advanced Reputation Management**
- **Seamless multi-LDAP integration**
- **Robust reporting**
- **Dell SonicWALL GRID Anti-Virus**
- **DHA, Dos, and zombie attack protection**
- **Advanced end-user controls**
- **Rapid installation and ease-of-management**

Features and benefits

Inbound and outbound email threat management scans inbound email to block spam, phishing, and malware before they enter the network, and scans outbound email and email attachments to prevent data leakage and malware proliferation.

Flexible deployment options include **hardware appliance** (leveraging a hardened high-performance appliance, server **software** (leveraging existing infrastructure), or **virtual appliance** (leveraging shared computing resources to optimize utilization, ease migration and reduce capital costs).

Highly available and scalable split mode architecture lets businesses flexibly mix and centrally manage Dell SonicWALL E-Class hardware appliances, software, and virtual appliances to effectively meet their needs, unlike the mandated limitations of competing vendors. Dell SonicWALL offers a truly scalable, highly available, email protection solution for archiving, outsourcing, managed services, mergers, acquisitions and expansion into globally distributed environments.

Regulatory compliance framework enables organizations to intelligently identify, monitor and report on email that violates compliance regulations and guidelines (HIPAA, SOX, GLBA, PCI) and uses policy-based routing to send mail to archiving and encryption technologies.*

Email policy management enables IT to enforce organizational policies such as preventing the dissemination of inappropriate content, protecting confidential information, adding email disclaimers or blocking distribution of executables.

Advanced Reputation Management rejects up to 90% of known junk email upon connection, with any remaining junk email being removed by Dell SonicWALL Advanced Content Management, resulting in improved performance and scalability, with complete visibility (unlike competing products).

Seamless multi-LDAP integration ensures that Dell SonicWALL E-Class Email Security solutions automatically synchronize with multiple LDAP servers to automatically manage email addresses, accounts and user groups.

Robust reporting provides easily customizable, system-wide and granular reporting, including information on attack types, solution effectiveness and built-in performance monitoring. For systems deployed in Split Mode, reporting and monitoring is completely centralized for all systems, saving valuable time and simplifying overall system management.

Dell SonicWALL GRID Anti-Virus™ leverages Dell SonicWALL's anti-virus and anti-spyware technology to deliver anti-virus and anti-spyware protection. Dell SonicWALL also offers additional layers of protection with signature update subscriptions from McAfee® and Kaspersky Lab®.*

DHA, Dos, and zombie attack* protection starts with powerful connection management capabilities to defer, throttle or block invalid connections before they reach your system. When combined with Dell SonicWALL's anti-spam, anti-phishing and anti-virus capabilities these capabilities establish a complete solution for stopping all types of email threats.

Advanced end-user controls enable administrators to give end-users greater control over their own spam management, allowed and blocked lists, spam aggressiveness, and account delegation. Using the downloadable Junk Button for Outlook® plug-in, end-users may actively respond to junk email that inadvertently arrives in their inbox. The administrator defines all end-user controls, and may assign them by user, group or function.

Rapid installation and ease-of-management drastically reduces the burden on IT departments to implement and manage a comprehensive email security solution. Judgment Details provides insight into message judgment to ease troubleshooting and prevent legitimate email from being junked.

*Additional subscription service required.

Dell SonicWALL Email Security deployments

The highly flexible architecture of Dell SonicWALL Email Security (SES) enables deployments in organizations that require a highly scalable, redundant and distributed email protection solution that can be centrally managed. SES can be deployed in either all-in-one or split mode. In split mode a system can be a remote analyzer or a control center.

A typical split-mode setup is one or more **remote analyzers** connected to a **control center**: The **remote analyzer** receives email from one or more domains and applies connection management, email filtering (anti-spam, anti-phishing and anti-virus) and advanced policy techniques to deliver good email to the downstream email server. The **control center** centrally manages all remote analyzers and collects and stores junk email from the remote analyzers. Centralized management includes reporting, and monitoring of all related systems. This paradigm allows Dell SonicWALL Email Security to adapt its solution to protect both inbound and outbound email for any organization in a cost-effective, comprehensive manner. Using Dell SonicWALL Email Security Virtual Appliances, split mode can be fully deployed on one or multiple servers, for optimal efficiencies of scale.

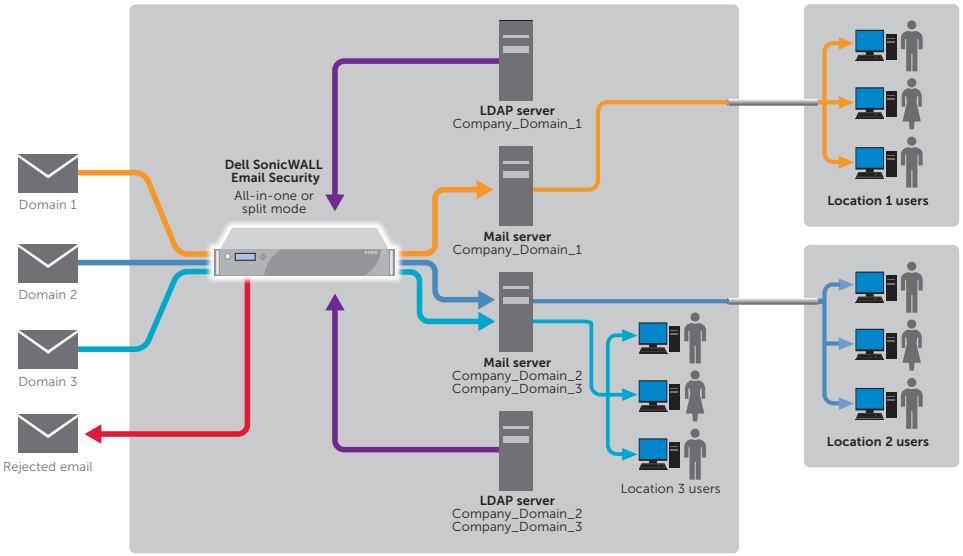
Multi-domain, central control

Dell SonicWALL Email Security centralizes management of multiple email domains.

Typically used in medical consortiums, insurance companies, franchises, multi-brand/multi-division companies.

Benefits

- Easy-to-use centralized management of multiple domains
- Apply corporate (centralized) email policies to everyone and/or apply policies per domain/group/user
- Centralized per-domain reporting
- Centralized control over outbound email to apply policy/routing rules per domain or on a corporate-wide basis



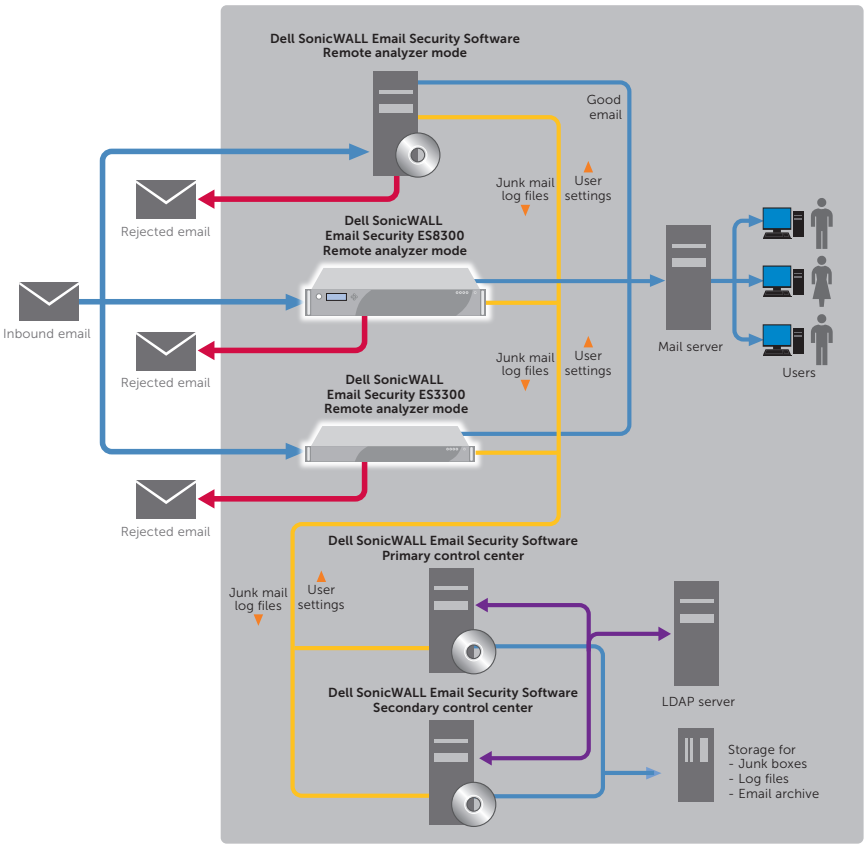
Scalable and redundant

A centrally managed email security system that is highly scalable, can utilize multiple types of platforms (software, hardware appliance or virtual appliance) and has failover built into the architecture as well as the hardware.

Typically used in medium and large enterprises, organizations with high uptime requirements for email security, mixed platform environments or organizations with a requirement to store email on SAN (Storage Area Network).

Benefits

- Any remote analyzer can failover to any other remote analyzer–ensuring mail-flow continues
- Having primary and secondary control centers provides complete redundancy
- Storing email, etc., on corporate SAN centralizes data storage and simplifies backup procedures
- Allowing mixed platforms to be centrally controlled reduces management overhead
- Adding a remote analyzer easily scales the system or extends deployment to other locations as desired



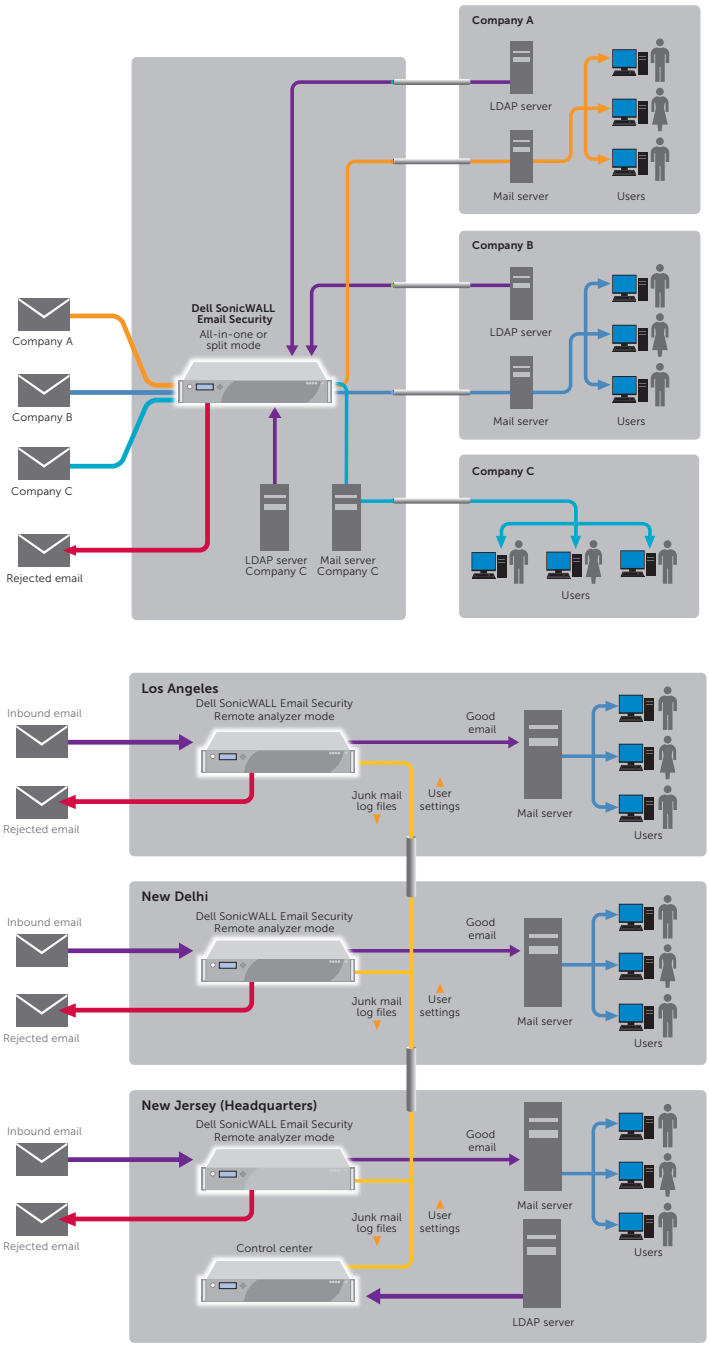
SonicWALL

Managed service provider

A managed service provider (MSP) can provide email filtering services for their clients and possibly email server services as well. The Dell SonicWALL Email Security solution is flexible enough to allow for multiple domains that can be centrally managed by the MSP, but still allows a given client to have their own users, policy rules, Junk Boxes and more, all under the control of the MSP.

Benefits

- Centralized management of multiple domains to remove junk email for everyone
- Centralized email policies for everyone and/or client policies per domain/group/user
- Centralized reporting, with per-domain reporting
- Centralized control over outbound email can be used for some or all of the clients, and policy/routing can be applied on per-domain basis
- Allows email servers and LDAP servers to reside with the customer or with the MSP or any in combination
- Flexible expansion allows the MSP to start with a single system and scale as needed to the highly scalable, failover-enabled, split-mode architecture
- Virtual appliance deployment speeds solution roll-out to new or existing customers, with minimal incremental investment or deployment overhead



Multi-location, central control

For distributed organizations, the optimal location for processing email—centralized versus local—is critical: too centralized, and valuable IT time is wasted; too local, and corporate security can be compromised. The flexible Dell SonicWALL Email Security architecture enables a solution that fits the unique needs of any distributed organization.

Typically used in companies with multiple locations, companies with recently added locations, such as through an acquisition or franchises that centralize the email management of their corporate-owned or franchised operations.

Benefits

- Localized processing of email to remove junk and deliver good email, reducing network traffic
- Centralized management of multiple locations, including policy enforcement, reporting and monitoring
- Centralized control over outbound email to apply policy/routing rules per domain, per location or on a corporate-wide basis
- Clustering of remote analyzers allows for failover from location to location

Specifications

	SMB (Available for smaller deployments)		E-Class (Enterprise)	
Email Security Appliances	**3300**	**4300**	**ES6000**	**ES8300**
Domains	Unlimited			
Operating system	Hardened Dell SonicWALL Linux OS appliance			
Rackmount chassis	1RU		1U Mini	2RU
CPU(s)	Intel 2.0GHz	Intel Dual Core 2.0GHz	3.2GHz	Quad Core Xeon 2.0GHz
RAM	2 GB	4 GB	2 GB	4 GB
Hard drive	250 GB	2 x 250 GB	2 x 160 GB	4 x 750 GB
Redundant disk array (RAID)	–	RAID 1	X	RAID 5
Hot swappable drives	–	–	–	X
Redundant power supply	–	–	–	X
Dimensions	17.0 x 16.4 x 1.7 in 43.18 x 41.59 x 4.44 cm		16.8 x 14.0 x 1.7 in 42.67 x 35.56 x 4.32 cm	27.5 x 19.0 x 3.5 in 69.9 x 48.3 x 8.9 cm
Weight	16 lbs 7.26 kg		19 lbs 8.62 kg	50.0 lbs 22.7 kg
WEEE weight	16 lbs 7.37 kg		14 lbs 6.35 kg	48.9 lbs 22.2 kg
Power consumption (watts)	86	101	201	280
BTUs	293	344	685.41	1098.0
MTBF @25C in hours	125,004			
MTBF @25C in years	14.27			
Email Security Software				
Domains	Unlimited			
Operating system	Runs on Microsoft Windows 2003 Server or Microsoft Windows 2008 Server			
CPU	2.66 GHz minimum configuration			
RAM	2 GB recommended, 1 GB minimum configuration			
Hard drive	40 GB additional minimum configuration			
Email Security Virtual Appliance				
Hypervisor	ESXi™ and ESX™ (version 4.0 and newer)			
Operating system installed	Hardened SonicLinux			
Allocated memory	2 GB			
Appliance disk size	80 GB			
VMware hardware compatibility guide	http://www.vmware.com/resources/compatibility/search.php			
Appliance and software features –subscriptions available for enterprise deployments in 1,000, 2,000, 5,000, and 10,000 user packs				
Threat protection				
Inbound and outbound email protection	Yes			
Anti-spam effectiveness	98%+			
Anti-phishing identified separately	Yes			
Dell SonicWALL GRID anti-virus	Yes			
Anti-Virus: dual-layer commercial	Yes			
Time Zero Virus Protection	Yes			
DHA, DoS, other attack protection	Yes			
LDAP/Exchange accelerator	Yes			
Multi-LDAP support	Yes			
Connection management with IP reputation	Yes			
Compliance subscription				
Robust policy management	Yes			
Attachment scanning	Yes			
Dictionaries	Yes			
Approval boxes/workflow	Yes			
Installation and management				
Installation	< 1 hour			
Management per week	< 10 min			
Compatible with all email servers	Yes			
Single sign-on	Yes			
Group and user management	Yes			
End user quarantine and settings	Yes			
Junk box summary actionable email	Yes			
Monitoring, reporting and log management	Yes			
Judgment details	Yes			
Rapid message search engine	Yes			
Clustering and remote clustering	Yes			

Dell SonicWALL E-Class Email Security Appliances

Dell SonicWALL Email Security ES6000
01-SSC-6604

Dell SonicWALL Email Security ES8300
01-SSC-6609

Dell SonicWALL E-Class Email Security Software
01-SSC-6636

Dell SonicWALL E-Class Email Security Virtual Appliance
01-SSC-7636

Subscriptions–E-Class
5,000 User Pack Subscriptions

Dell SonicWALL Email Protection with 24 x 7 support (1-year)
01-SSC-6674

Dell SonicWALL Email Compliance (1-year)
01-SSC-6644

McAfee Anti-Virus with Dell SonicWALL Time-Zero (1- year)
01-SSC-6764

Kaspersky Anti-Virus with Dell SonicWALL Time-Zero (1-year)
01-SSC-6774

Visit **www.sonicwall.com** for additional user packs.

Licensing Overview
Dell SonicWALL E-Class Email Security (appliance, software or virtual appliance)
- Message Transfer Agent (MTA)
- Directory Harvest Attach/Denial of Service protection
- Web-based management
- Policy management/Email content filtering
- Reporting and monitoring
- LDAP synchronization

Email Protection Subscription with Dynamic Support (8x5 or 24x7) – Required
- Anti-spam (1-year)
- 8x5 or 24x7 support (1-year)
- Anti-phishing (1-year)
- RMA (Appliance replacement)
- Software/Firmware updates (1-year)

Compliance Subscription
- Dictionaries (functionality)
- Approval boxes
- Attachment scanning
- Record ID matching
- Encryption reporting
- Email archiving
- Predefined policies
- Compliance reports

Anti-Virus Subscription (Kaspersky Lab and/or McAfee with Dell SonicWALL Time Zero Anti-Virus)
- Kaspersky Anti-virus
- Dell SonicWALL Time Zero Anti-Virus
- McAfee Anti-virus
- Zombie detection

Security Monitoring Services from Dell SecureWorks are available for this appliance Series. For more information, visit **www.dell.com/secureworks**

DELL SonicWALL