SONICWALL

Email Security appliances and software

Protect your infrastructure from advanced email threats and compliance violations with powerful, easy-to-use solutions

Email is crucial for your business communication, but it is also the number one vector for threats such as ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses. What's more, government regulations now hold your business accountable for protecting confidential data and ensuring it is not leaked and that email containing sensitive customer data or confidential information is securely exchanged. Whether your organization is a growing small-to medium-sized business (SMB), a large, distributed enterprise or a managed service provider (MSP), you need a cost-effective way to deploy email security and encryption, and the scalability to easily grow capacity for — and delegate management across — organizational units and domains.

SonicWall Email Security appliances and software provide multi-layered protection from inbound and outbound email threats and compliance violations by scanning all inbound and outbound email content, URLs and attachments for sensitive data, delivering real-time protection ransomware, targeted phishing attacks, spoofing, viruses, malicious URLs, zombies, directory harvest (DHA), Denial of Service (DoS) and other attacks. The solution leverages multiple, patented SonicWall threat detection techniques and a unique, worldwide attack identification and monitoring network.

SonicWall Capture Advanced Threat Protection service delivers industry-leading, multi-engine sandboxing, with patent-pending Real-time Deep memory inspection (RTDMI™) technology, to isolate unknown threats found in suspicious file attachments and URLs, so you can stop advanced threats before they reach your users' inboxes. Email Security with Capture ATP gives you a highly effective and responsive defense against ransomware and zero-day attacks.

The solution also includes Domain-based Message Authentication, DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework), Reporting and Conformance (DMARC), a powerful email authentication method that helps identify spoofed mail, reducing spam and targeted phishing attacks such as spear-phishing, whaling, CEO fraud and business email compromise, It also reports on sources and senders of email, so you can identify and shut down unauthorized senders falsifying email with your address and protect your brand. In addition, it prevents confidential data leaks and regulatory violations with advanced compliance scanning and management, including integrated email encryption cloud service to ensure secure exchange of sensitive data.

Administration of the Email Security solution is intuitive, quick and simple. You can safely delegate spam management to end users, while still retaining ultimate control over security enforcement. You can also easily manage user and group accounts with seamless multi-LDAP synchronization. For large, distributed environments, multi-tenancy support lets you delegate sub-administrators to manage settings at multiple organizational units (such as enterprise divisions or MSP customers) within a single Email Security deployment.

Benefits

- Stop ransomware and zero-day malware from reaching you inbox with Capture Advanced Threat Protection
- Protect users from clicking on malicious links across any device and from any location with time-of-click URL protection
- Advanced analysis techniques to stop targeted phishing attacks, email fraud and business email compromise (BEC)
- Stop new threats with real-time threat intelligence updates from SonicWall Capture Labs
- Maintain email hygiene with powerful anti-spam and anti-virus
- Protect your data by enforcing granular data loss preventions (DLP) and compliance policies
- Simplify management with intelligent automation, task delegation, at-a-glance customizable dashboard and robust reporting
- Leverage flexible, scalable deployment options, including hardened physical appliances, robust virtual appliances and powerful Windows Server® software

[1] *U.S. Patents 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

Features

Advance Threat Protection

Detect and block advanced threats until verdict. This service is the only advanced-threat-detection offering that combines multi-layer sandboxing, including Real-Time Deep Memory Inspection, full system emulation and virtualization techniques, to analyze suspicious code behavior within emails, to protect customers against the increasing dangers of zero-day threats. The service includes advanced URL protection that dynamically analyzes embedded URLs, to block and quarantine messages with malicious URLs before they reach the inbox, so users never click on them and become compromised. Capture ATP service delivers finer granularity with file attachments and URLs analysis, additional in-depth reporting capabilities, and a streamlined user-experience.

In addition, SonicWall Email Security rewrites all embedded URLs to block emails with malicious or phishing URLs, so users are protected at the time of click across any device and from any location.

Some organizations and government agencies cannot leverage cloud-based techniques for file inspection, such as Capture ATP, for compliance or latency reasons. Integrate your Email Security appliance with SonicWall Capture Security appliance (CSa) to examine suspicious files coming through email within your own datacenter. CSa can be referenced by IP address or FQDN which makes it an excellent resource for threat prevention.

Targeted attack protection

SonicWall's anti-phishing technology uses a combination of methodologies, including machine learning, heuristics, reputation and content analysis, to stop sophisticated phishing attacks. The solution also includes powerful email authentication standards, such as SPF, DKIM and DMARC, to stop spoofing attacks, business email compromise and email fraud.

Real-time threat intelligence

Receive the most accurate and up-to-date protection against new spam attacks while ensuring delivery of benign email with real-time threat information from the SonicWall Capture Threat Network, which collects information from millions of data sources. The SonicWall Capture Labs analyzes that information and performs rigorous testing to establish reputation scores for senders and content, identifying new threats in real-time.

Anti-virus and anti-spyware protection

Get up-to-date anti-virus and anti-spyware protection. The solution utilizes signatures from industry leading anti-virus databases and malicious URL detections for multi-layer protection that is superior to that provided by solutions that rely on a single anti-virus technology.

In addition, predictive analysis enables you to safeguard your network from the time a new virus outbreak occurs until the time an anti-virus signature update is available.

Intelligent automation, task delegation and robust reporting

Simplify management with intelligent automation, task delegation and robust reporting. Automatically manage email addresses, accounts and user groups. Seamlessly integrate with multiple-LDAP servers. Confidently delegate spam management to end users with the downloadable Junk Button for Outlook® plug-in, while still retaining full control. Locate any email in seconds with the Rapid Message Search Engine. Centralized reporting (even in split mode) gives you easily customizable, system-wide and granular information on attack types, solution effectiveness and built-in performance monitoring and reports are available in PDF and JPEG formats.

Compliance Policy Management

This add-on service enables compliance with regulatory mandates by helping you to identify, monitor and report on email that violates compliance regulations and guidelines (e.g., HIPAA, SOX, GLBA, and PCI-DSS) or corporate data loss guidelines. The subscription service also enables policy-based routing of mail for approval, archiving and encryption.

Email Encryption

Add a powerful framework for stopping data leaks, managing and enforcing compliance requirements and providing mobile-ready secure email exchange for organizations of all sizes.

Encrypted email can be tracked to confirm the time of receipt and time opened. Intuitive for the recipient, a notification email is delivered to the recipient's inbox with instructions to simply log into a secure portal to read or securely download the email. The service is cloud-based with no additional client software necessary and unlike competitive solutions; the encrypted email may be accessed and read from mobile devices or laptops.

Flexible deployment options

Gain scalable, long-term value by configuring your solution for growth and redundancy with minimal upfront costs. You can deploy Email Security as a hardened, high-performance appliance, as software leveraging existing infrastructure or as a virtual appliance leveraging shared computing resources to optimize utilization, ease migration and reduce capital costs. Start with a single system and then as your business grows, add capacity and move to a fail-over enabled, split-mode architecture. Multi-tenancy support allows large enterprise or managed service provider deployments with multiple departments or customers to

establish organizational units with one or multiple domains. The deployment may be centrally managed, but still allows a given organizational unit to have its own users, sub-administrators, policy rules, junk boxes and more.

SonicWall Email Security deployment options

The highly flexible architecture of SonicWall Email Security enables deployments in organizations that require a highly scalable, redundant and distributed email protection solution that can be centrally managed. SonicWall Email Security can be deployed in either all-in-one or split mode.

In split mode, systems may be configured as a remote analyzer or a control center. In a typical split-mode setup, one or more remote analyzers is 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 benign 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 the solution to cost-effectively scale and protect both inbound and outbound email for growing organizations. Using SonicWall Email Security Virtual Appliances, split mode can be fully deployed on one or multiple servers for optimal efficiencies of scale.

Features

	APPLIANCE, VIRTUAL APPLIANCE	WINDOWS SERVER®
Advanced Total Secure subscription - Advanced protection bundle		
Includes SonicWall Capture ATP advanced attachment and URL protection, in addition to the Total Secure subscription	Yes	Yes
Time-of-click URL protection	Yes	Yes
Total Secure subscription – Basic protection bundle		
Includes email protection dynamic 24x7 subscription plus multi-layer anti-virus, malicious URL detection and compliance management subscription features	Yes	Yes
Ransomware & Zero-day protection - optional		
SonicWall Capture ATP advanced attachment and URL protection add-on for Total Secure subscription	Yes	Yes
Complete inbound and outbound email protection		
Anti-spam	Yes	Yes
Connection management with advanced IP reputation	Yes	Yes
Phishing detection, classification, blocking	Yes	Yes
Directory harvest, denial of service, NDR protection	Yes	Yes
Anti-spoofing with support for SPF, DKIM and DMARC	Yes	Yes
Policy rules for user, group, all	Yes	Yes
In memory message transfer agent (MTA) for enhanced throughput	Yes	Yes
Easy administration		
Installation	< 1 hour	< 1 hour
Management per week	< 10 min	< 10 min
Automatic multi-LDAP sync for users, groups	Yes	Yes
Compatible with all SMTP email servers	Yes	Yes
SMTP Authentication support (SMPT AUTH)	Yes	Yes
Allow/deny end user controls	Yes	Yes
Customize, schedule and email 30+ reports	Yes	Yes
Judgment details	Yes	Yes
At-a-glance, customizable management dashboard	Yes	Yes
Rapid message search engine	Yes	Yes
Scalable split-mode architecture	Yes	Yes
Clustering and remote clustering	Yes	Yes
Easy for end users		
Single sign-on	Yes	Yes
Per user junk boxes, junk box summary actionable email	Yes	Yes
Per user anti-spam aggressiveness, block/allow lists	Yes	Yes
Email protection subscription with dynamic support–required		
SonicWall cloud anti-virus, anti-spam, anti-phishing auto-updates every minute	Yes	Yes
24x7 support	Yes	Yes
RMA (appliance replacement)	Yes	Yes
Software/firmware updates	Yes	Yes
Anti-virus subscription–optional		
Signature feeds from industry leading anti-virus databases	Yes	Yes
SonicWall TimeZero anti-virus	Yes	Yes
Zombie detection	Yes	Yes
Compliance subscription–optional		
Robust policy management,	Yes	Yes
Attachment scanning	Yes	Yes
Record ID matching	Yes	Yes
Dictionaries	Yes	Yes
Approval boxes/workflow	Yes	Yes
Email archiving	Yes	Yes
Compliance reporting	Yes	Yes
Encryption subscription–optional		
Compliance subscription capabilities plus policy-enforced email encryption and secure email exchange	Yes	Yes

System Specifications

EMAIL SECURITY APPLIANCES	5000	7000	9000
Domains		Unrestricted	
Operating system		Hardened SonicWall Linux OS appliance	
Rackmount chassis	1RU	1RU	1RU
CPU(s)	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 GB	16 GB	32 GB
Hard drive	500 GB	1 TB	1 TB
Redundant disk array (RAID)	—	RAID 1	RAID 5
Hot swappable drives	No	Yes	Yes
Redundant power supply	No	No	Yes
SAFE Mode Flash	Yes	Yes	Yes
Dimensions	17.0 x 16.4 x 1.7 in 43.18 x 41.59 x 4.44 cm	17.0 x 16.4 x 1.7 in 43.18 x 41.59 x 4.44 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	16 lbs / 7.26 kg	50.0 lbs/ 22.7 kg
WEEE weight	16 lbs / 7.37 kg	16 lbs / 22.2 kg	48.9 lbs/ 22.2 kg
Power consumption (watts)	46	48	158
BTUs	155	162	537
MTBF @25C in hours	130,919	150,278	90,592
MTBF @25C in years	14.9	17.2	10.3
EMAIL SECURITY SOFTWARE			
Domains		Unrestricted	
Operating system		Microsoft Hyper-V Server 2012 (64-bit) or higher Windows Server 2008 R2 or higher x64 bit only	
CPU		Intel or AMD 64-bit processor	
RAM		8 GB minimum configuration	
Hard drive		160 GB minimum configuration	
EMAIL SECURITY VIRTUAL APPLIANCE			
Hypervisor		ESXi™ and ESX™ (version 5.0 and newer)	
Operating system installed		8 GB (expandable)	
Allocated memory		4 GB	
Appliance disk size		160 GB (expandable)	
VMware hardware compatibility guide		http://www.vmware.com/resources/compatibility/search.php	

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

SONICWALL®

SonicWall Email Security ordering information

SonicWall Email Security Appliances

Product	SKU
Sonicwall Email Security Appliance 9000	01-SSC-7605
Sonicwall Email Security Appliance 7000	01-SSC-7604
Sonicwall Email Security Appliance 5000	01-SSC-7603
SonicWall Email Security Software	01-SSC-6636
SonicWall Email Security Virtual Appliance	01-SSC-7636

SonicWall Email Security Subscriptions

Subscription	SKU
SonicWall Email Protection Subscription	
SonicWall Email Protection Subscription and 24X7 Support 25 Users - 1 Server (1yr)	01-SSC-6669
SonicWall Email Protection Subscription and 24X7 Support 1,000 Users - 1 Server (1yr)	01-SSC-6678
SonicWall Email Protection Subscription and 24X7 Support 10,000 Users - 1 Server (1yr)	01-SSC-6730
SonicWall Email Anti-Virus Subscription	
SonicWall Email Anti-Virus 25 Users - 1 Server (1yr)	01-SSC-6759
SonicWall Email Anti-Virus 1,000 Users - 1 Server (1yr)	01-SSC-6768
SonicWall Email Anti-Virus 10,000 Users - 1 Server (1yr)	01-SSC-7562
SonicWall Email Encryption Subscription	
SonicWall Email Encryption Service 25 Users (1yr)	01-SSC-7427
SonicWall Email Encryption Service 1,000 Users (1yr)	01-SSC-7471
SonicWall Email Encryption Service 10,000 Users (1yr)	01-SSC-7568
SonicWall Email Compliance Subscription	
SonicWall Email Complaince Service 25 Users - 1 Server (1yr)	01-SSC-6639
SonicWall Email Complaince Service 1,000 Users - 1 Server (1yr)	01-SSC-6648
SonicWall Email Complaince Service 10,000 Users - 1 Server (1yr)	01-SSC-6735
SonicWall TotalSecure Email Subscription	
SonicWall TotalSecure Email Subscription 25 Users (1yr)	01-SSC-7399
SonicWall TotalSecure Email Subscription 1,000 Users (1yr)	01-SSC-7398
SonicWall TotalSecure Email Subscription 10,000 Users (1yr)	01-SSC-7405
Capture ATP Add-on for TotalSecure Email Subscription	
Capture ATP for SonicWall TotalSecure Email Subscription 25 Users (1yr)	01-SSC-1526
Capture ATP for SonicWall TotalSecure Email Subscription 1,000 Users (1yr)	01-SSC-1874
Capture ATP for SonicWall TotalSecure Email Subscription 10,000 Users (1yr)	01-SSC-1883
SonicWall Advanced TotalSecure Email Subscription (Capture ATP included)	
SonicWall Advanced TotalSecure Email Subscription 25 Users (1yr)	01-SSC-1886
SonicWall Advanced TotalSecure Email Subscription 1,000 Users (1yr)	01-SSC-1904
SonicWall Advanced TotalSecure Email Subscription 10,000 Users (1yr)	01-SSC-1913

SonicWall Email Security Appliance Bundles and subscriptions are available in 25, 50, 100, 250, 500, 1,000, 2,000, 5,000, and 10,000 user packs and as 1yr, 2yr and 3yr options. Support is available as 8X5 option as well. Please consult with your local SonicWall reseller for a complete list of SKUs.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150