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 by supporting multiple organizational units and domains and by delegating role-based management capabilities to various admins.

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 against ransomware, targeted phishing, 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 (ATP) 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 uses powerful email authentication mechanisms such as SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance) 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.

The administration of the Email Security solution is intuitive, quick and straightforward. 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 for 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 your 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 prevention (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

Advanced Threat Protection

SonicWall Capture ATP is the only advanced threat detection offering that subjects suspicious files and URLs embedded inside emails through multiple sandboxing engines to detect never-before-seen threats at high efficacy. Additionally, SonicWall's patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology unveils and blocks modern malware that does not exhibit malicious behavior and hides its weaponry via custom encryption. Thus, organizations are protected against complex threats, such as fileless malware that bypass traditional sandboxing technologies. The block until verdict feature ensures that malicious file never reaches user's inbox while sandboxing analysis is pending. The sandboxing service includes advanced URL protection that dynamically analyzes embedded URLs to prevent messages with malicious links from reaching the inbox. Capture ATP delivers finer granularity with file attachments and URLs analysis, in-depth reporting capabilities, and a seamless user experience.

In addition, SonicWall Email Security rewrites all embedded URLs and protects users at the time of click by blocking access to malicious and phishing URL across any device.

Some organizations and government agencies cannot leverage cloud-based techniques for file inspection, such as Capture ATP, for compliance or latency reasons. Instead, such organizations can deploy the SonicWall Email Security appliance along with the SonicWall Capture Security appliance (CSa) to examine suspicious files coming through email within their own datacenter using the same powerful sandboxing techniques as available in cloud-based Capture ATP. CSa can be referenced by IP address or FQDN, making it an excellent threat prevention resource.

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 phishing, malware and 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 when a new virus outbreak occurs until the time an anti-virus signature update is available.

Intelligent automation, task delegation and robust reporting

Daily tasks, such as managing email addresses, accounts and user groups, are carried out using intelligent automation and task delegation. Email Security solution seamlessly integrates with multiple LDAP servers. Admins can confidently delegate spam management to end-users with the downloadable Junk Button for Outlook® plug-in while retaining full control. Admins can also 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. Reports are available in PDF and JPEG formats.

Compliance Policy Management

The Data Leakage Prevention and Compliance feature 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. This feature 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 emails are tracked to confirm the time of receipt and the time of opening the email. Intuitive for the recipient, a notification email is delivered to the recipient's inbox with instructions to 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 assigned 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 remote analyzer or as 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 features such as anti-spam, anti-phishing, anti-spoofing, anti-virus, malicious URL detection and compliance management along with 24x7 support	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
Support and Updates		
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		
Signature feeds from industry leading anti-virus databases	Yes	Yes
SonicWall TimeZero anti-virus	Yes	Yes
Zombie detection	Yes	Yes
Compliance		
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	5050	7000	7050	9000
Domains			Unrestricted		
Operating System			Hardened SonicWall Linux OS		
CPU Model	Intel Celeron G1820	Intel Celeron G3930E	Intel Core i3-4330	Intel Core i3-7101E	Intel Xeon E3-1275 v3
Number of cores	2	2	2	2	4
Rackmount	1U	1U	1U	1U	1U
RAM	8 GB DDR3	16 GB DDR4	16 GB DDR3	32 GB DDR4	32 GB DDR3
Hard Drive	500 GB	1 TB	1 TB	1 TB	1 TB
Redundant disk array (RAID)	-	-	RAID 1	RAID 1	RAID 5
Hot swappable drives	No	No	Yes	Yes	Yes
Redundant power supply	No	No	No	No	Yes
SAFE Mode Flash	Yes	Yes	Yes	Yes	Yes
Dimensions	17.0 x 16.4 x 1.7 in or 43.18 x 41.59 x 4.44 cm	16.9 x 16.3 x 1.8 in or 43 x 41.5 x 4.5 cm	17.0 x 16.4 x 1.7 in or 43.18 x 41.59 x 4.44 cm	16.9 x 16.3 x 1.8 in or 43 x 41.5 x 4.5 cm	27.5 x 19.0 x 3.5 in or 69.9 x 48.3 x 8.9 cm
Weight	16 lbs / 7.26 kg	14.7 lbs / 6.7 kg	16 lbs / 7.26 kg	14.7 lbs / 6.7 kg	50.0 lbs/ 22.7 kg
WEEE weight	16 lbs / 7.37 kg	19 lbs / 8.6 kg	16 lbs / 7.37 kg	19 lbs / 8.6 kg	48.9 lbs/ 22.2 kg
Power consumption (watts)	46	43.3	48	61.8	158
BTUs	155	148	162	211	537
MTBF @25C in hours	130,919	74,364	150,278	69,204	90,592
MTBF @25C in years	14.9	8.4	17.2	7.9	10.3
EMAIL SECURITY WINDOWS SERVER/ HYPER-V					
Domains			Unrestricted		
Operating system			Microsoft Hyper-V Server 2019 (64-bit) Microsoft Hyper-V Server 2016 (64-bit) Windows Server 2016 (64-bit)		
CPU			Intel or AMD 64-bit processor, 4 cores		
RAM			16 GB of RAM minimum 32 GB of RAM recommended		
Hard drive			160 GB minimum		
EMAIL SECURITY VIRTUAL APPLIANCE					
Hypervisor			ESXi 5.5, 6.X		
CPU			Intel or AMD 64-bit processor, 4 cores		
Allocated memory			16 GB of RAM minimum 32 GB of RAM recommended		
Appliance disk size			160 GB (expandable)		
VMware hardware compatibility guide			http://www.vmware.com/resources/compatibility/search.php		

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

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

DataSheet-EmailSecurityAppsAndSoftware-US-JK-5100

SONICWALL®