

Hosted Email Security

A cloud-based multi-tenant security service that protects against today's advanced email threats.

Email is the primary tool for business communications worldwide for organizations of all sizes. Email is also the number one threat vector for cyber-attacks. Email threats have evolved from mass spam and phishing email campaigns to highly-targeted phishing attacks that can deliver ransomware and zero-day malware. These attacks can also take the form of business email compromise (BEC) attacks that seek wire transfers or confidential information. This new wave of sophisticated phishing attacks cannot be stopped by the traditional anti-spam and anti-malware solutions. What's more, government regulations now hold your business accountable for protecting confidential data, ensuring it is not leaked and ensuring the secure exchange of email containing sensitive customer data or confidential information.

To protect against these constantly evolving email threats, organizations must deploy a layered security solution that goes beyond anti-spam and anti-malware. This solution should include dedicated, advanced-threat protection capabilities, and protect against malicious attachments and URLs, as well as impostor-based attacks. In addition, managing and maintaining an on-premises email security solution can become costly and time-consuming. As such, organizations can benefit from replacing legacy solutions with an easy-to-use, affordable hosted email security solution that easily integrates with existing email infrastructure, that can be quickly provisioned without upfront expense and that dynamically responds to new threats

while reducing ongoing administration cost and complexity.

SonicWall Hosted Email Security offers superior, cloud-based protection from inbound and outbound threats, including ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses, at an affordable, predictable and flexible monthly or annual subscription price. At the same time, it minimizes upfront deployment time and costs, as well as ongoing administration expenses.

SonicWall Hosted Email Security with Capture Advance Threat Protection service dynamically scans all suspicious email attachments and URLs, analyzes them in a multi-engine sandbox, and blocks dangerous files or URLs before they reach your network. Capture ATP includes our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine proactively detects and blocks massmarket, zero-day threats and unknown malware by inspecting directly in memory. SonicWall Hosted Email Security with Capture ATP delivers advanced attachment and URL protection to protect against ransomware and targeted phishing attacks.

The service also includes advanced compliance scanning, management and optionally, email encryption, to prevent confidential data leaks, regulatory violations and to ensure the secure exchange of sensitive data. Policies may be configured at the organizational level, to scan outbound email content and attachments for sensitive data and



Benefits:

- Protect against targeted phishing attacks and email fraud
- Stop ransomware and zero-day malware before they reach your inbox
- Secure your Office 365, G Suite and on-premises email server
- Block emerging threats with real-time threat intelligence
- Secure your data by enforcing granular data loss prevention (DLP) and compliance policies
- Experience true multi-tenancy with granular control over management, provisioning, reporting and branding for each tenant
- Get the scalability you need with predictable subscription rates and zero up-front costs
- Reduce overhead for administrators and service providers with easy management and reporting
- Harness the power of the cloud and preserve your network bandwidth
- Ensure emails are always delivered, and productivity is not impacted during planned or unplanned outages

route email for approval or encryption. 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. Unlike competitive solutions, the encrypted email may be accessed and read from mobile devices or laptops.

In addition, the service includes Domain-based Message Authentication, Reporting and Conformance (DMARC), a powerful email authentication method that helps identify spoofed mail, reducing advanced phishing attacks such as spear-phishing, whaling, CEO fraud and business email compromise. DMARC 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.

SonicWall Hosted Email Security integrates multiple anti-virus technologies to deliver best-in-class email security. The SonicWall Capture Labs performs rigorous testing and evaluation of millions of emails every day, and then reapplies this constantly updated analysis to provide exceptional spam-blocking results and anti-virus and anti-spyware protection.

In addition, with SonicWall Hosted Email security, there is no equipment to install on premises, eliminating upfront hardware and software expenses, and minimizing the time and resources needed to deploy and manage email security. Also, with a hosted service, there are no additional ongoing hardware or software updates, maintenance tasks or expenses. SonicWall takes care of keeping the service up to date so you always have access to the latest features and most secure service offering, allowing you to free up IT resources to focus on other tasks. With SonicWall Hosted Email Security, organizations get superior email security while reducing the administrative burden.

For MSPs and VARs

SonicWall Hosted Email Security is also available to MSPs and VARs interested in establishing a differentiated, highly profitable, email security software-as-a-service (SaaS) offering for customers that delivers superior, cloud-based protection from inbound and outbound spam, phishing, BEC, ransomware and malware without incurring upfront expense or financial risk. With the addition of a hosted solution to its already extensive email security lineup, SonicWall offers VARs and MSPs a greater opportunity to compete and grow revenue while minimizing risk, overhead and ongoing costs.

MSPs can experience true multi-tenancy with granular control over management, provisioning, reporting and branding for each tenant. A centralized administration page provides a single-pane-of-glass view to manage all tenants. The solution enables granular management to automate license provisioning and policy enforcement. In addition, a rich and powerful set of RESTful APIs enables MSPs to customize the solution as their business requires.

Finally, SonicWall offers Email Continuity to minimize business impact of planned or unplanned outages to on-prem email servers or cloud-based services, such as Office 365 and G Suite. With Email Continuity, MSPs can ensure 24x7 service availability and adhere to stringent Service Level Agreements (SLAs).

Features

Advanced Threat Protection — SonicWall Email Security Capture Advance Threat Protection Service detects and can 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 and protect customers against the increasing dangers of zero-day threats. Capture ATP service delivers finer granularity with dynamic attachment

and URL analysis, additional in-depth reporting capabilities, and a streamlined user-experience.

Improved Office 365 support — The SonicWall Hosted Email Security service integrates with Office 365 and G Suite, to deliver a method for ensuring a correct/mapped message matching in a hosted, multi-tenant environment. In addition, Hosted Email Security supports the Automatic Office 365 and G Suite IP address Allow List.

Stop sophisticated phishing using advanced techniques including SonicWall's anti-phishing technology uses a combination of methodologies such as 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.

Keep email hygiene — The technology also provides directory harvest attack (DHA) protection, Denial of Service (DoS) protection and sender validation. Advanced techniques are also used to analyze email content, such as a Support Vector Machine (SVM) algorithm, adversarial Bayesian filtering, image analysis and gibberish detection to uncover hidden known threats, and new threats. Outbound email scanning safeguards your reputation by scanning for — and blocking — traffic from zombies, unauthorized senders and email containing malicious viruses.

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

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

Get multi-AV protection, including malware signatures from SonicWall Capture Labs and 3rd party anti-virus technologies, resulting in protection superior to that provided by solutions that rely on a single anti-virus technology. In addition, to prevent infection by new viruses before anti-virus signature updates are available by utilizing predictive technologies to identify email containing suspect new viruses and immediately quarantine it, thereby safeguarding the network from the time a new virus outbreak occurs until the time an anti-virus signature update is available.

Email Compliance Policy Management and Encryption – Comply with regulatory mandates by identifying, monitoring and reporting on email that violates compliance regulations and guidelines (e.g., HIPAA, SOX, GLBA, and PCI-DSS) or corporate data loss guidelines. With compliance policy management, you can configure record ID matching to easily search for predefined information and

attachment scanning to stop the release of unauthorized information, You can also select from predefined policies to achieve easy compliance, including predefined dictionaries to ensure the protection of confidential information. Also, you can establish approval boxes for scanning and approving emails before release and enable policy-based routing of mail for encryption to ensure the secure exchange of sensitive data.

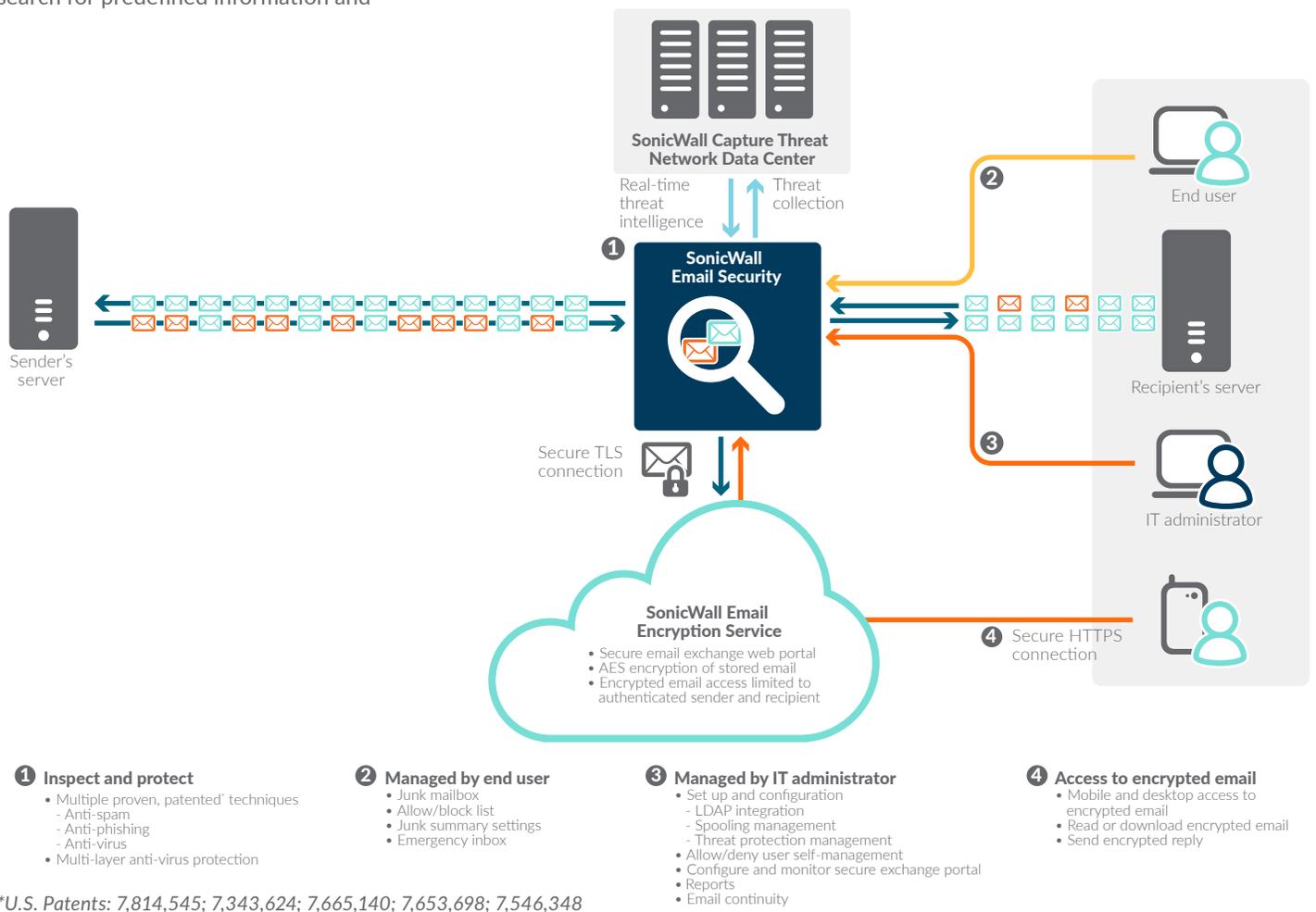
Achieve 24x7 service availability with email continuity – Ensure emails are always delivered and productivity is not impacted during planned or unplanned outages of on-prem email servers or a cloud provider, such as Office 365 and G Suite. During outages, users can access a secure, web-browser-based, Emergency Inbox to compose, read and respond to messages. Email spooling ensures no messages are lost when email servers are unavailable and delivers them when the servers are up.

Preserve network bandwidth by blocking spam and viruses in the cloud before delivering good email to the recipient mail infrastructure.

Simplify end-user spam management by safely delegating spam management to end users. Users get the freedom to personalize the aggressiveness of their spam detection settings, while IT retains ultimate control over the overall level of security enforced.

Increase efficiency and cost-effectiveness by reducing your up-front deployment expenses, as well as ongoing administrative costs. With SonicWall Hosted Email Security, no on-premises hardware or software installation is required.

Simplify operations for managed service providers with multi-tenant management, flexible purchase options and automated provisioning for multiple subscribers.



Reports and monitoring

Email Security is easy to set up, easy to manage, and easy to own. Customizable, drag and drop dashboard, real-time and PDF formatted reports.



Junk Box summaries

Junk Box Summaries optimize end-user email productivity, reduce complaints and improve overall effectiveness.

Junk Box Management / Junk Box

Inbound | Outbound

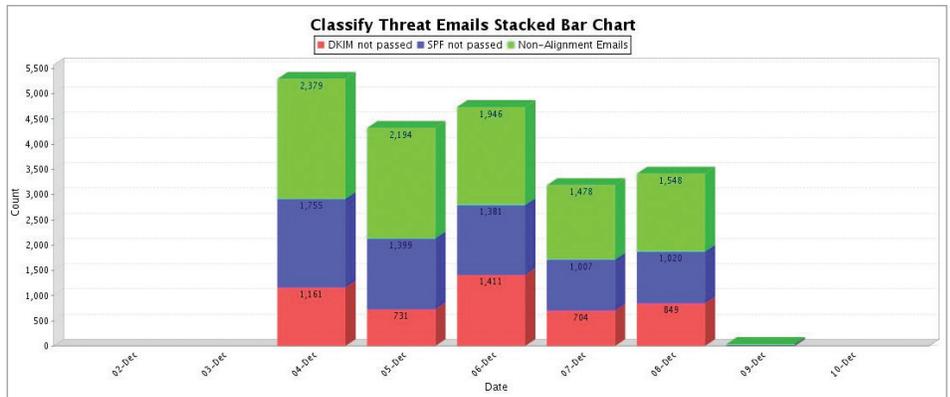
Simple search: _____ in **Subject** Search

Items in the Junk Box will be deleted after 30 days.
For Advanced search filters, click on **Open** in respective column.
Displaying 15/175 records (0.855 sec)

| To | Threat | TLS | Subject | From | Received |
|------------------|--------------|-----|-------------------------------|-----------------|---------------------|
| bracham@sonic... | Likely Virus | | advic.test.for.zara.dex.virus | patlav@mail.com | 03/22/2016 03:05 PM |
| profic1@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic2@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic3@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic4@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| bracham@sonic... | Likely Virus | | advic.test.for.zara.dex.virus | patlav@mail.com | 03/22/2016 03:05 PM |
| profic1@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic2@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic3@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic4@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| bracham@sonic... | Likely Virus | | advic.test.for.zara.dex.virus | patlav@mail.com | 03/22/2016 03:05 PM |
| profic1@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic2@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic3@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| profic4@sonic... | Likely Virus | | unsubscribe | patlav@mail.com | 03/22/2016 03:05 PM |
| bracham@sonic... | Likely Virus | | advic.test.for.zara.dex.virus | patlav@mail.com | 03/22/2016 03:05 PM |

Anti-spoofing DMARC report

Identify sources and senders of unauthorized email.



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

Features

| COMPLETE INBOUND AND OUTBOUND EMAIL PROTECTION | |
|---|----------|
| Capture ATP (Advanced attachment and URL protection) | Optional |
| Anti-spam effectiveness | Yes |
| Sender IP reputation | Yes |
| Directory harvest, denial of service, protection | Yes |
| Capture Labs reputation services | Yes |
| SonicWall Cloud Anti-Virus | Yes |
| Multi Anti-Virus | Yes |
| Malicious URL detection | Yes |
| Phishing detection, classification, blocking | Yes |
| Zombie detection, flood protection | Yes |
| Policy rules | Yes |
| EASY ADMINISTRATION | |
| Multi-tenant management | Yes |
| Office 365 and G Suite support | Yes |
| Automated provisioning and setup | Yes |
| Reputation auto-updates | Yes |
| Anti-spam auto-updates | Yes |
| Automatic upgrades and maintenance | Yes |
| Anti-virus signature auto-updates | Yes |
| Customize, schedule and email reports | Yes |
| Automatic LDAP Sync | Yes |
| Rapid message search engine | Yes |
| EASY FOR END-USERS | |
| SMTP Auth for inbound/outbound | Yes |
| Allow/deny all end user controls | Yes |
| Emergency inbox | Optional |
| Per user junk boxes | Yes |
| Per user anti-spam aggressiveness | Yes |
| Per user allowed/blocked lists | Yes |
| Junk box summaries in 15 languages | Yes |
| Judgement details | Yes |
| SYSTEM FEATURES | |
| Compatible with all SMTP email servers | Yes |
| SMTP Authentication support (SMTP AUTH) | Yes |
| Unrestricted domains supported | Yes |
| Email continuity | Optional |
| 15 days of junk email retention | Yes |
| Email spooling up to 7 days | Yes |
| COMPLIANCE POLICY AND MANAGEMENT | |
| Attachment scanning | Yes |
| Record ID matching | Yes |
| Dictionaries | Yes |
| Approval boxes/workflow | Yes |
| Compliance reporting | Yes |

Features con't

| EMAIL ENCRYPTION SERVICE FOR HOSTED EMAIL SECURITY - OPTIONAL | |
|--|-----|
| Policy-enforced secure email exchange | Yes |
| Works natively on mobile devices (no app required) | Yes |
| Outlook Send Secure add-on button | Yes |
| Quickly encrypts file attachments up to 100MB | Yes |
| Send messages directly to recipient with nothing for them to install | Yes |
| Message notification includes link to auto-provisioned recipient accounts | Yes |
| Replies are automatically decrypted into sender's inbox | Yes |
| Built in tracking of all messages and files sent, received, and opened | Yes |
| Rebrand encrypted email | Yes |
| Reporting and monitoring | Yes |
| 500 MB per company | Yes |
| Industry-standard, compliance-grade encryption: AES 256, TLS | Yes |
| No keys to manage or lose | Yes |
| Portal localized in ten languages including English, French, Italian, German, Spanish, Japanese, Brazilian Portuguese, Simplified & Mandarin Chinese, and Korean | Yes |
| Outlook 2010/2013/2016 support | Yes |
| SSAE 16, SAS 70 Type II & Fedramp Certified Data Center | Yes |
| SUPPORT AND SERVICES | |
| 24x7 email and phone support | Yes |
| Multiple data centers | Yes |

| Hosted Email Security Subscription Service (1 Year) | |
|---|-------------|
| Number of users | SKU number |
| 10 | 01-SSC-5030 |
| 25 | 01-SSC-5033 |
| 50 | 01-SSC-5036 |
| 100 | 01-SSC-5039 |
| 250 | 01-SSC-5042 |
| 500 | 01-SSC-5045 |
| 750 | 01-SSC-5057 |
| 1,000 | 01-SSC-5048 |
| 2,000 | 01-SSC-5051 |

| Email Encryption Service for Hosted Email Security (1 Year) | |
|---|-------------|
| Number of users | SKU number |
| 10 | 01-SSC-5078 |
| 25 | 01-SSC-5081 |
| 50 | 01-SSC-5084 |
| 100 | 01-SSC-5087 |
| 250 | 01-SSC-5091 |
| 500 | 01-SSC-5094 |
| 750 | 01-SSC-5097 |
| 1,000 | 01-SSC-5104 |
| 2,000 | 01-SSC-5107 |

| Capture ATP Service for Hosted Email Security (1 Year) | |
|--|-------------|
| Number of users | SKU number |
| 10 user pack | 01-SSC-1650 |
| 25 user pack | 01-SSC-1653 |
| 50 user pack | 01-SSC-1656 |
| 100 user pack | 01-SSC-1659 |
| 250 user pack | 01-SSC-1838 |
| 500 user pack | 01-SSC-1511 |
| 750 user pack | 01-SSC-1514 |
| 1,000 user pack | 01-SSC-1517 |
| 2,000 user pack | 01-SSC-1520 |
| 5,000 user pack | 01-SSC-1523 |

| Continuity for Hosted Email Security (1 Year) | |
|---|-------------|
| Number of users | SKU number |
| 10 | 01-SSC-3068 |
| 25 | 01-SSC-3071 |
| 50 | 01-SSC-3074 |
| 100 | 01-SSC-3077 |
| 250 | 01-SSC-3080 |
| 500 | 01-SSC-3083 |
| 750 | 01-SSC-3086 |
| 1,000 | 01-SSC-3089 |
| 2,000 | 01-SSC-3092 |
| 5,000 | 01-SSC-3095 |

Multi-year SKUs are available. Please visit www.sonicwall.com.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.