HOSTED EMAIL SECURITY CON SERVIZIO DI CRITTOGRAFIA

Il servizio per la sicurezza dell'e-mail migliore della categoria, con protezione opzionale per lo scambio sicuro dei messaggi

L'e-mail continua ad avere un ruolo fondamentale per le comunicazioni e l'operatività in azienda. Purtroppo, però, insieme al volume di messaggi aumenta anche il numero di ransomware e di attacchi di phishing, business email compromise (BEC), spoofing, spam e virus. Secondo le normative vigenti, è responsabilità dell'azienda impedire la divulgazione accidentale di dati riservati e garantire lo scambio sicuro dei messaggi e-mail contenenti informazioni riservate o dati sensibili dei clienti. Come se non bastasse, anche lo spoofing è in crescita: gli autori degli attacchi di spam falsificano l'indirizzo dei mittenti delle e-mail per aggirare i destinatari, danneggiando in questo modo anche la reputazione delle aziende all'oscuro di tutto.

Proteggersi dal proliferare di minacce sempre diverse e, al tempo stesso, gestire e mantenere una soluzione locale per la sicurezza dell'e-mail costa tempo e denaro. Per questo motivo le aziende dovrebbero sostituire le applicazioni legacy con una soluzione di sicurezza e-mail in hosting che sia intuitiva, conveniente e facile da integrare nell'infrastruttura e-mail esistente. Una soluzione dal provisioning rapido, senza grossi investimenti iniziali e capace di reagire in modo dinamico alle nuove minacce, riducendo al contempo la complessità e i costi amministrativi.

SonicWall™ Hosted Email Security offre un'eccellente protezione basata sul cloud contro le minacce in entrata e in uscita come ransomware, phishing, business email compromise (BEC), spoofing, spam e virus, a fronte di un abbonamento mensile o annuale flessibile, a costi accessibili e prevedibili. Questa soluzione permette di ridurre al minimo non solo i costi e i tempi di installazione iniziali, ma anche le spese di amministrazione continuative.

SonicWall Hosted Email Security è ora integrabile con il servizio Capture Advanced Threat Protection per fornire un'ispezione del traffico SMTP granulare e trasparente per l'utente. Il servizio Capture ATP basato su cloud è in grado di scansionare un'ampia gamma di allegati e-mail, analizzarli in una sandbox multi-engine e bloccare le e-mail o i file pericolosi prima che raggiungano la rete. SonicWall Hosted Email Security in combinazione con Capture ATP offre una difesa altamente efficace e reattiva contro il ransomware e gli attacchi zero-day.

Inoltre le avanzate opzioni di analisi e gestione della conformità, combinate alla crittografia opzionale dei messaggi e-mail, proteggono lo scambio delle informazioni sensibili, prevenendo la divulgazione accidentale dei dati riservati e la violazione delle normative. È possibile configurare policy a livello aziendale per analizzare la presenza di dati sensibili nei contenuti e negli allegati delle e-mail in uscita, reindirizzando i messaggi per sottoporli ad approvazione o crittografia. Le e-mail crittografate possono essere monitorate per sapere quando vengono recapitate e aperte. Il destinatario riceverà un'e-mail di notifica intuitiva con semplici istruzioni per accedere a un portale sicuro in cui leggere o scaricare l'e-mail in tutta tranquillità. Il servizio è basato su cloud e non richiede alcun software client aggiuntivo. A differenza di quanto accade con le soluzioni della concorrenza, le e-mail crittografate sono accessibili e consultabili da dispositivi mobili o notebook.

La soluzione include anche il meccanismo DMARC (Domain-based Message Authentication, Reporting and Conformance), un potente metodo di autenticazione delle e-mail che consente di identificare i messaggi di spoofing e contrastare gli attacchi phishing avanzati come spear-phishing, whaling, truffa del CEO e business email compromise (BCE), oltre a segnalare le fonti e i mittenti dei messaggi e-mail. Le aziende possono così tutelarsi, identificando e bloccando i mittenti non autorizzati che falsificano le e-mail con l'indirizzo aziendale.

Vantaggi:

- Protezione da ransomware e malware zero-day con il servizio Capture ATP
- Blocco degli attacchi di spam, phishing, zombie e malware
- Protezione mirata e aggiornata contro i nuovi attacchi di spam
- Protezione antivirus su più livelli
- Ottimizzazione della larghezza di banda della rete
- Semplice gestione dello spam a livello di utente
- Maggiore efficienza e convenienza
- Protezione dell'e-mail in caso di mancata disponibilità dei server
- Operazioni semplificate per i fornitori di servizi gestiti
- Analisi e gestione avanzate per la prevenzione delle violazioni di conformità e servizio opzionale di crittografia dell'e-mail
- Dashboard personalizzabile, rapporti in tempo reale e in formato PDF

SonicWall Hosted Email Security è l'unica soluzione in hosting che integra diverse tecnologie antivirus, tra cui SonicWall Cloud Anti-Virus, SonicWall Time Zero e tecnologie antivirus di terze parti per offrire la migliore sicurezza e-mail della categoria. SonicWall Capture Labs sottopone milioni di e-mail a rigorosi test e valutazioni ogni giorno, ripetendo questa analisi costantemente aggiornata per garantire risultati eccezionali di protezione contro spam, virus e spyware.

Un altro vantaggio di SonicWall Hosted Email Security è che non richiede l'installazione di apparecchiature in locale, eliminando così le spese iniziali di hardware e software e riducendo al minimo il tempo e le risorse necessari per installare e gestire la soluzione di sicurezza dell'e-mail. La formula del servizio in hosting non richiede aggiornamenti ricorrenti dell'hardware o del software, né attività o spese di manutenzione. SonicWall mantiene il servizio sempre aggiornato per consentire all'azienda di disporre sempre delle ultime funzionalità e del servizio più sicuro, lasciando il personale di IT libero di concentrarsi su altre attività. SonicWall Hosted Email Security offre alle organizzazioni una protezione superiore dell'e-mail, a fronte di un carico amministrativo ridotto.

Per MSP e VAR

SonicWall Hosted Email Security è disponibile anche per gli MSP e i VAR interessati a proporre ai clienti una soluzione di sicurezza e-mail software-as-a-service (SaaS) differenziata e altamente redditizia, che offra una protezione superiore e basata sul cloud contro gli attacchi di spam, phishing, zombie e malware in entrata e in uscita, senza spese iniziali o incognite finanziarie. Aggiungendo una soluzione in hosting a una gamma già esaustiva di tecnologie per la sicurezza, SonicWall offre a questi fornitori e rivenditori maggiori opportunità competitive e di guadagno, riducendo al tempo stesso i rischi, le spese generali e i costi correnti. SonicWall Hosted Email Security include caratteristiche adatte agli MSP, come la gestione centralizzata di più sottoscrittori, opzioni di acquisto flessibili e provisioning automatizzato. Grazie a SonicWall Hosted Email Security, MSP e VAR possono finalmente contare su una soluzione di sicurezza e-mail in hosting garantita da un'azienda leader del settore.

Caratteristiche

Protezione contro le minacce avanzate – Il servizio SonicWall Email Security con Capture Advanced Threat Protection rileva e blocca le minacce avanzate fino alla loro identificazione. Questo è l'unico servizio di rilevamento delle minacce avanzate che abbina il sandboxing multilivello all'emulazione completa del sistema e a tecniche di virtualizzazione per analizzare il comportamento del codice sospetto nei messaggi e-mail, proteggendo i clienti dal crescente pericolo delle minacce zero-day. Email Security Capture offre ora una migliore granularità con la possibilità di ispezionare un numero maggiore di tipi di file, ulteriori capacità per la creazione di report dettagliati e un'esperienza più semplice e discreta per gli utenti.

Supporto ottimizzato per Office 365 – Il servizio SonicWall Hosted Email Security si integra con Office 365, fornendo un metodo per garantire la corrispondenza tra messaggi corretti/mappati in un ambiente multi-tenant in hosting. Inoltre, Hosted Email Security supporta l'elenco automatico degli indirizzi IP consentiti di Office 365.

Blocco degli attacchi di spam, phishing, zombie e malware mediante comprovate tecniche brevettate*, tra cui i controlli della reputazione che non solo verificano l'attendibilità del mittente in base all'indirizzo IP, ma anche quella dei contenuti, della struttura, dei collegamenti, delle immagini e degli allegati. Oltre a eseguire la convalida del mittente, questa tecnologia protegge dagli attacchi di tipo Directory Harvest (DHA) e Denial of Service (DoS). Per individuare le nuove minacce e quelle già note in agguato, i contenuti delle e-mail vengono analizzati con tecnologie avanzate come l'algoritmo SVM (Support Vector Machine), il filtraggio bayesiano, l'analisi delle immagini e il rilevamento di contenuti sospetti. L'analisi delle e-mail in uscita permette di salvaguardare la reputazione aziendale intercettando e bloccando il traffico associato a zombie, mittenti non autorizzati ed e-mail infette con virus dannosi.

Protezione mirata e aggiornata contro i nuovi attacchi di spam, con in più la garanzia di recapitare solo e-mail legittime e la certezza di ricevere informazioni sulle minacce in tempo reale tramite SonicWall Capture Threat Network, che raccoglie i dati da milioni di fonti. Il team di ricerca delle minacce di SonicWall analizza queste informazioni ed esegue rigorosi test, assegnando poi un punteggio alla reputazione di mittenti e contenuti per identificare le nuove minacce in tempo reale.

Protezione multilivello, con SonicWall Cloud Anti-Virus e tecnologie antivirus di terze parti, per fornire una protezione superiore a quella offerta dalle soluzioni basate su una sola tecnologia antivirus. Per prevenire le infezioni di virus prima che siano disponibili le firme antivirus aggiornate, SonicWall Time Zero Virus Protection sfrutta tecnologie predittive per identificare e mettere subito in quarantena le e-mail contenenti potenziali nuovi virus, proteggendo la rete dal momento stesso in cui compare un virus nuovo e finché non viene reso disponibile un aggiornamento delle firme antivirus.

Crittografia e gestione delle policy di conformità dell'e-mail: il rispetto degli obblighi normativi è garantito con l'identificazione, il monitoraggio e la segnalazione delle e-mail che violano le normative e le linee guida in materia di conformità (ad esempio HIPAA, SOX, GLBA e PCI-DSS) o le indicazioni aziendali sulla perdita di dati. Mediante la gestione delle policy di conformità è possibile configurare la corrispondenza tra ID dei record in modo da ricercare informazioni predefinite e analizzare gli allegati per impedire la divulgazione non autorizzata delle informazioni. È inoltre possibile selezionare policy predefinite per assicurare facilmente la conformità e impostare dizionari predefiniti con cui garantire la protezione delle informazioni di natura riservata. Infine, è possibile definire criteri per l'analisi e l'approvazione delle e-mail e per il routing della posta da sottoporre a crittografia, in modo da assicurare uno scambio sicuro dei dati sensibili.

**Brevetti statunitensi: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

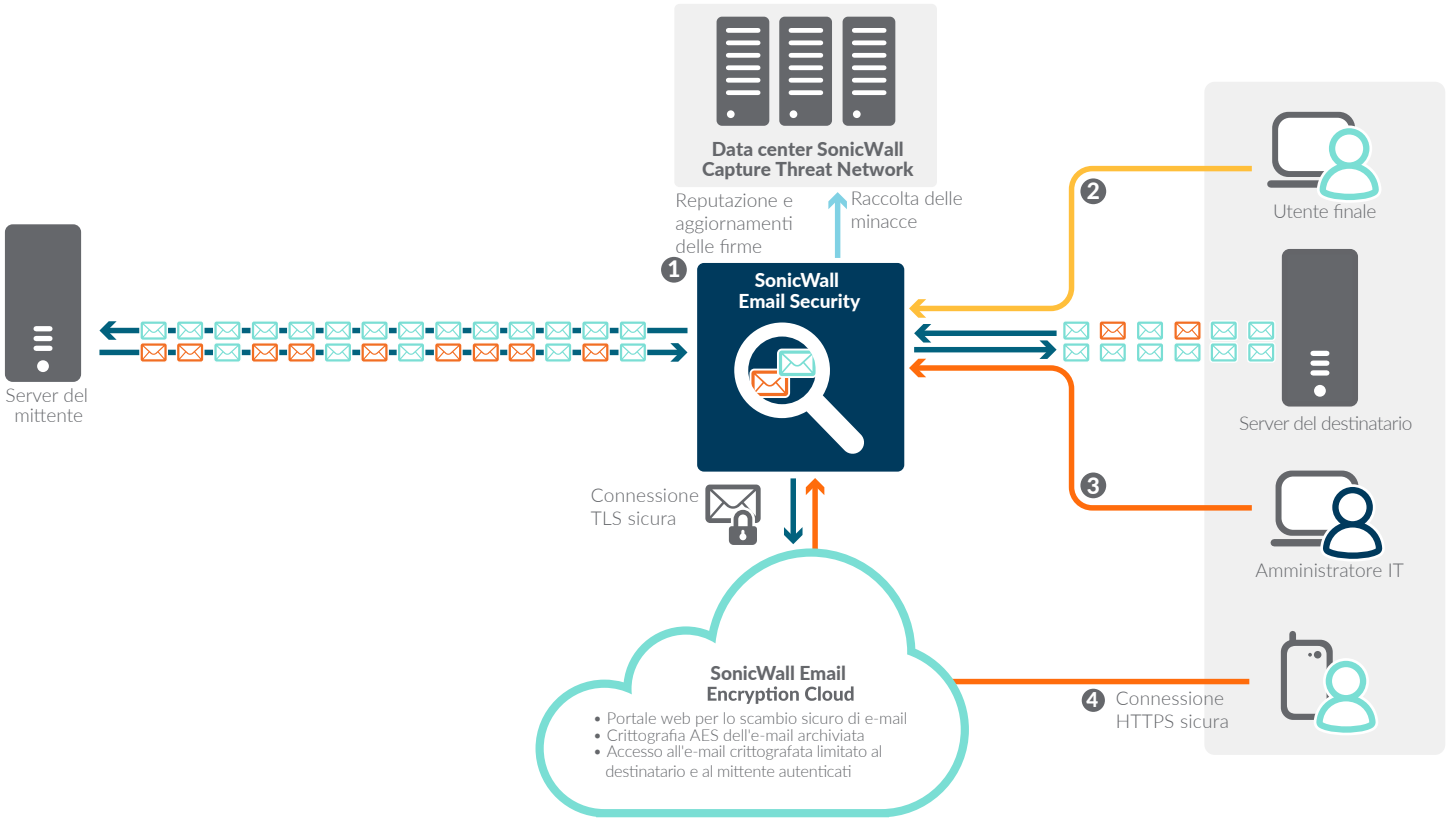
Ottimizzazione della larghezza di banda della rete grazie al blocco di spam e virus nel cloud, per recapitare solo e-mail legittime all'infrastruttura e-mail del destinatario.

Gestione semplificata dello spam a livello di utente finale, delegando la gestione dello spam ai singoli utenti. Ogni utente è libero di personalizzare il livello delle impostazioni di rilevamento dello spam, mentre il reparto di IT mantiene il controllo definitivo sul livello di sicurezza complessivo.

Maggior efficienza e convenienza con la riduzione delle spese di installazione iniziali e dei costi di amministrazione correnti. SonicWall Hosted Email Security non richiede l'installazione di hardware o software a livello locale.

Protezione dell'e-mail in caso di mancata disponibilità dei server grazie allo spooling dei messaggi e-mail filtrati e al successivo recapito degli stessi una volta che i server tornano operativi.

Operazioni semplificate per i fornitori di servizi gestiti grazie alla gestione centralizzata degli account, a opzioni di acquisto flessibili e al provisioning automatizzato di più sottoscrittori.



1 Ispezione e protezione
- Tecniche comprovate e brevettate*
  - Antispam
  - Antiphishing
  - Antivirus
- Protezione antivirus multilivello

2 Gestione da parte dell'utente finale
- Casella della posta indesiderata
- Elenco di blocchi/autorizzazioni
- Impostazioni di riepilogo della casella della posta indesiderata

3 Gestione da parte dell'amministratore IT
- Installazione e configurazione
  - Integrazione LDAP
  - Gestione dello spooling
  - Gestione della protezione dalle minacce
- Gestione autonoma di autorizzazioni/rifiuti da parte degli utenti
- Configurazione e monitoraggio del portale per lo scambio sicuro di e-mail
- Rapporti

4 Accesso all'e-mail crittografata
- Accesso all'e-mail crittografata da desktop e dispositivi mobili
- Lettura o download dell'e-mail crittografata
- Invio della risposta crittografata

**Brevetti statunitensi: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

Monitoraggio e creazione di report

Email Security è facile da configurare, gestire e amministrare. Dashboard personalizzabile con funzionalità drag-and-drop e creazione di rapporti in tempo reale e in formato PDF.

Riepiloghi della posta indesiderata

I riepiloghi delle caselle di posta indesiderata (Junk Box) consentono di ottimizzare la produttività degli utenti finali, riducendo i reclami e migliorando l'efficacia complessiva.

Rapporto anti-spoofing DMARC

Consente di identificare le fonti e i mittenti delle e-mail non autorizzate.

**Brevetti statunitensi: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

SONICWALL®

Caratteristiche

PROTEZIONE COMPLETA DELLE E-MAIL IN ENTRATA E IN USCITA	
SonicWall Capture Advanced Threat Protection	Sì
Efficacia antispam	Sì
Reputazione IP del mittente	Sì
Protezione contro Directory Harvest e Denial of Service	Sì
Servizi Capture Labs per il controllo della reputazione	Sì
SonicWall Cloud Anti-Virus	Sì
SonicWall Time-Zero	Sì
Protezione antivirus multilivello	Sì
Rilevamento di URL dannosi	Sì
Rilevamento, classificazione e blocco del phishing	Sì
Rilevamento di zombie, protezione da flooding	Sì
Regole delle policy	Sì
SEMPLICITÀ DI AMMINISTRAZIONE	
Provisioning e configurazione automatizzati	Sì
Aggiornamenti automatici per il controllo della reputazione	Sì
Aggiornamenti automatici per il controllo antispam	Sì
Upgrade e manutenzione automatici	Sì
Aggiornamenti automatici per Cloud Anti-Virus	Sì
Personalizzazione, pianificazione e invio per e-mail dei rapporti	Sì
Sincronizzazione LDAP automatica	Sì
Motore di ricerca rapida dei messaggi	Sì
FACILITÀ PER GLI UTENTI FINALI	
Autenticazione SMTP per la posta in entrata/in uscita	Sì
Autorizzazione/blocco di tutti i controlli per utenti finali	Sì
Caselle di posta indesiderata per singolo utente	Sì
Definizione delle impostazioni antispam per singolo utente	Sì
Elenchi di blocco/autorizzazione per singolo utente	Sì
Riepiloghi della casella di posta indesiderata in 15 lingue	Sì
Dettagli di valutazione	Sì
CARATTERISTICHE DI SISTEMA	
Compatibilità con tutti i server di e-mail SMTP	Sì
Supporto dell'autenticazione SMTP (SMTP AUTH)	Sì
Supporto per domini illimitati	Sì
Conservazione posta indesiderata per 15 giorni	Sì
Spooling e-mail per un massimo di 4 giorni	Sì
POLICY E GESTIONE DELLA CONFORMITÀ	
Scansione degli allegati	Sì
Corrispondenza degli ID dei record	Sì
Dizionari	Sì
Caselle/flussi di lavoro di approvazione	Sì
Rapporti sulla conformità	Sì

Caratteristiche (continua)

SERVIZIO OPZIONALE DI CRITTOGRAFIA DELL'E-MAIL PER HOSTED EMAIL SECURITY	
Scambio sicuro dei messaggi e-mail basato su policy	Sì
Funzionamento nativo su dispositivi mobili (nessuna app richiesta)	Sì
Pulsante aggiuntivo di invio sicuro tramite Outlook	Sì
Crittografia rapida dei file allegati (fino a 100 MB)	Sì
Invio diretto di messaggi al destinatario senza necessità di installazione	Sì
Notifica di messaggio con link agli account di destinatari con provisioning automatico	Sì
Decrittografia automatica delle risposte nella casella del mittente	Sì
Tracciamento integrato di tutti i messaggi e i file inviati, ricevuti e aperti	Sì
Rebranding dell'e-mail crittografata	Sì
Monitoraggio e creazione di rapporti	Sì
500 MB per azienda	Sì
Crittografia a scopo di conformità standard di settore: AES 256, TLS	Sì
Nessun codice da gestire, con il rischio di smarrirlo	Sì
Portale localizzato in 10 lingue: inglese, francese, italiano, tedesco, spagnolo, giapponese, portoghese brasiliano, cinese mandarino e semplificato, coreano	Sì
Supporto per Outlook 2010/2013/2016	Sì
SSAE 16, SAS 70 Type II e Fedramp Certified Data Center	Sì
SUPPORTO E SERVIZI	
Supporto telefonico e via e-mail 24x7	Sì
Data center multipli	Sì

SERVIZIO IN ABBONAMENTO HOSTED EMAIL SECURITY (1 ANNO)

Numero di utenti	Codice SKU
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

SERVIZIO EMAIL ENCRYPTION PER HOSTED EMAIL SECURITY (1 ANNO)

Numero di utenti	Codice SKU
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
2000	01-SSC-5107

SERVIZIO CAPTURE ATP PER HOSTED EMAIL SECURITY (1 ANNO)

Numero di utenti	Codice SKU
Pacchetto per 10 utenti	01-SSC-1650
Pacchetto per 25 utenti	01-SSC-1653
Pacchetto per 50 utenti	01-SSC-1656
Pacchetto per 100 utenti	01-SSC-1659
Pacchetto per 250 utenti	01-SSC-1838
Pacchetto per 500 utenti	01-SSC-1511
Pacchetto per 750 utenti	01-SSC-1514
Pacchetto per 1.000 utenti	01-SSC-1517
Pacchetto per 2.000 utenti	01-SSC-1520
Pacchetto per 5000 utenti	01-SSC-1523

Sono disponibili anche SKU per più anni. Visitare il sito www.sonicwall.com

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.