SONICWALL

Hosted Email Security

Un servizio di sicurezza multi-tenant basato su cloud che protegge dalle minacce e-mail avanzate di oggi.

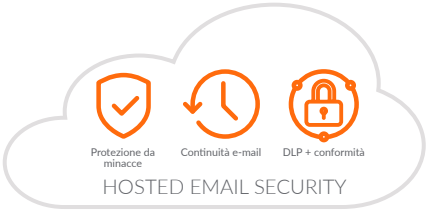
L'e-mail è il principale strumento di comunicazione aziendale per organizzazioni di ogni dimensione in tutto il mondo. Allo stesso tempo, è anche il vettore più utilizzato per gli attacchi informatici. Le minacce diffuse tramite e-mail si sono evolute da semplici campagne di spam e phishing di massa ad attacchi di phishing altamente mirati che possono distribuire ransomware e malware zero-day. Questi attacchi possono anche assumere la forma di truffe BEC (business email compromise, compromissione della posta elettronica aziendale) per indurre le vittime a effettuare un bonifico bancario o a fornire informazioni riservate. Questa nuova ondata di attacchi phishing sofisticati non può essere fermata con le tradizionali soluzioni antispam e antimalware. Tra l'altro, i regolamenti governativi impongono all'azienda di impedire la divulgazione accidentale di dati riservati e garantire lo scambio sicuro dei messaggi e-mail contenenti informazioni riservate o dati sensibili dei clienti.

Per proteggersi da queste minacce e-mail in costante evoluzione, le aziende devono adottare una soluzione di sicurezza multilivello che vada oltre la semplice protezione antispam e antimalware. Questa soluzione dovrebbe includere funzionalità dedicate di protezione contro minacce avanzate, allegati e URL dannosi nonché attacchi basati su truffatori. Inoltre, la gestione e la manutenzione di una soluzione di sicurezza e-mail in sede possono richiedere parecchio tempo e denaro. Per questo motivo, le aziende dovrebbero sostituire le applicazioni tradizionali 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 su 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 soltanto i costi e i tempi di installazione iniziali, ma anche le spese di amministrazione continuative.

SonicWall Hosted Email Security con il servizio Capture Advance Threat Protection scansiona dinamicamente tutti gli allegati e-mail e gli URL sospetti, li analizza in una sandbox multi-engine e blocca i file o gli URL pericolosi prima che raggiungano la rete. Capture ATP include la nostra tecnologia Real-Time Deep Memory Inspection (RTDMI™) in attesa di brevetto. Il motore RTDMI rileva e blocca proattivamente minacce zero-day comuni e malware sconosciuto mediante l'analisi diretta in memoria. SonicWall Hosted Email Security con Capture ATP fornisce una protezione avanzata time-of-click degli URL e degli allegati per proteggere dal ransomware e da attacchi di phishing mirati.

Inoltre, le avanzate opzioni di analisi e gestione della conformità, unite 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



Vantaggi:

- Protezione da attacchi di phishing mirati e frodi via e-mail
- Blocco di ransomware e malware zero-day prima che raggiungano le caselle di posta
- Protezione degli utenti da clic o link nocivi su qualsiasi dispositivo e da qualunque sede grazie alla protezione time-of-click degli URL
- Protezione dei server di Office 365, G Suite e di posta locale
- Blocco di minacce emergenti con l'intelligence delle minacce in tempo reale
- Protezione dei dati tramite prevenzione granulare della perdita dei dati (DLP) e policy di conformità
- Approccio realmente multi-tenant con controllo granulare di attività come gestione, provisioning, creazione di rapporti e branding per ogni tenant
- Tutta la scalabilità necessaria, con tariffe di abbonamento prevedibili e nessun costo iniziale
- Minore impegno per amministratori e fornitori di servizi grazie alla gestione semplificata e ai report
- Mantenimento della larghezza di banda della rete grazie alla potenza del cloud
- Consegna garantita dei messaggi e-mail, senza impatti sulla produttività in caso di interruzioni pianificate o impreviste

o crittografia. Le e-mail crittografate possono essere monitorate per sapere quando vengono recapitate e aperte. Il destinatario riceverà un'intuitiva e-mail di notifica 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 delle soluzioni della concorrenza, le e-mail crittografate sono accessibili e consultabili da dispositivi mobili o notebook.

La soluzione include anche il DMARC (Domain-based Message Authentication, Reporting and Conformance), un potente metodo di autenticazione delle e-mail che consente di identificare i messaggi di spoofing, riducendo così gli attacchi di phishing avanzati come spear-phishing, whaling, truffa del CEO e compromissione della posta elettronica aziendale (BCE). DMARC riporta anche le fonti e i mittenti delle e-mail, consentendo agli utenti di identificare e bloccare i mittenti non autorizzati che falsificano le e-mail usandone impropriamente l'indirizzo, e di proteggere così il proprio marchio.

SonicWall Hosted Email Security integra diverse tecnologie antivirus 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: ciò significa eliminare le spese iniziali di hardware e software, e ridurre 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 costantemente aggiornato per consentire all'azienda di disporre sempre delle ultime funzionalità e del servizio più sicuro, lasciando il personale IT libero di concentrarsi su altre attività. SonicWall Hosted Email Security offre alle aziende una protezione superiore dell'e-mail, a fronte di un onere 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 su cloud contro gli attacchi spam, phishing, BEC, ransomware e malware in entrata e in uscita, senza spese iniziali o rischi finanziari. 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.

I fornitori di servizi gestiti (MSP) possono contare su una multi-tenancy vera e propria, con controllo granulare della gestione, provisioning, creazione di rapporti e branding per ogni tenant. Una pagina di amministrazione centralizzata offre un'interfaccia unificata per gestire tutti i tenant. La soluzione consente una gestione granulare per automatizzare il provisioning delle licenze e l'applicazione delle policy. Un ampio set di API RESTful permette agli MSP di personalizzare la soluzione secondo le proprie esigenze aziendali.

Inoltre, SonicWall offre l'add-on Email Continuity per ridurre al minimo l'impatto commerciale di eventuali interruzioni pianificate o impreviste dei server e-mail installati in sede o di servizi basati su cloud, come Office 365 e G Suite. Con la continuità delle e-mail, gli MSP possono garantire la disponibilità dei servizi 24 ore su 24, 7 giorni su 7, e rispettare i più rigorosi contratti di servizio (SLA).

Caratteristiche

Protezione contro le minacce avanzate – SonicWall Email Security con il servizio Capture Advanced Threat Protection rileva le minacce avanzate e può bloccarle finché non vengono identificate. Questo è l'unico servizio di rilevamento delle minacce avanzate che combina il sandboxing multilivello, inclusi la tecnologia Real-Time Deep Memory Inspection, l'emulazione completa del sistema e tecniche di virtualizzazione, per analizzare il comportamento del codice sospetto nei messaggi e-mail e proteggere i clienti dai crescenti pericoli delle minacce zero-day. Il servizio Capture ATP offre una migliore granularità, con l'analisi dinamica degli allegati e degli URL, ulteriori capacità per la creazione di report dettagliati e facilità d'uso per gli utenti.

Supporto ottimizzato per Office 365 e G Suite – Il servizio SonicWall Hosted Email Security si integra con Office 365 e G Suite, 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 e G Suite.

SonicWall Email Security riscrive altresì tutti gli URL incorporati per bloccare le e-mail con URL di phishing o contenenti malware; in questo modo, gli utenti sono protetti al momento del clic su qualsiasi dispositivo e da qualunque sede.

Blocco del phishing sofisticato mediante tecniche avanzate come la tecnologia antiphishing di SonicWall, che usa una combinazione di metodologie quali apprendimento automatico, euristica e analisi della reputazione e del contenuto per fermare attacchi di phishing sofisticati. La soluzione include anche potenti standard di autenticazione della posta elettronica come SPF, DKIM e DMARC per fermare attacchi di spoofing, truffe BEC e frodi via e-mail.

Protezione costante delle e-mail – 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 grazie all'intelligence delle minacce in tempo reale di SonicWall Capture Threat Network, che raccoglie i dati da milioni di fonti. Il team di ricerca dei SonicWall Capture Labs 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 antivirus multipla, incluse firme malware provenienti dai SonicWall Capture Labs 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 nuovi virus prima che siano disponibili le firme antivirus aggiornate, vengono inoltre utilizzate tecnologie predittive per identificare e mettere subito in quarantena le e-mail contenenti potenziali nuovi virus, proteggendo la rete dal momento 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 direttive 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 base alla policy, in modo da assicurare uno scambio sicuro dei dati sensibili.

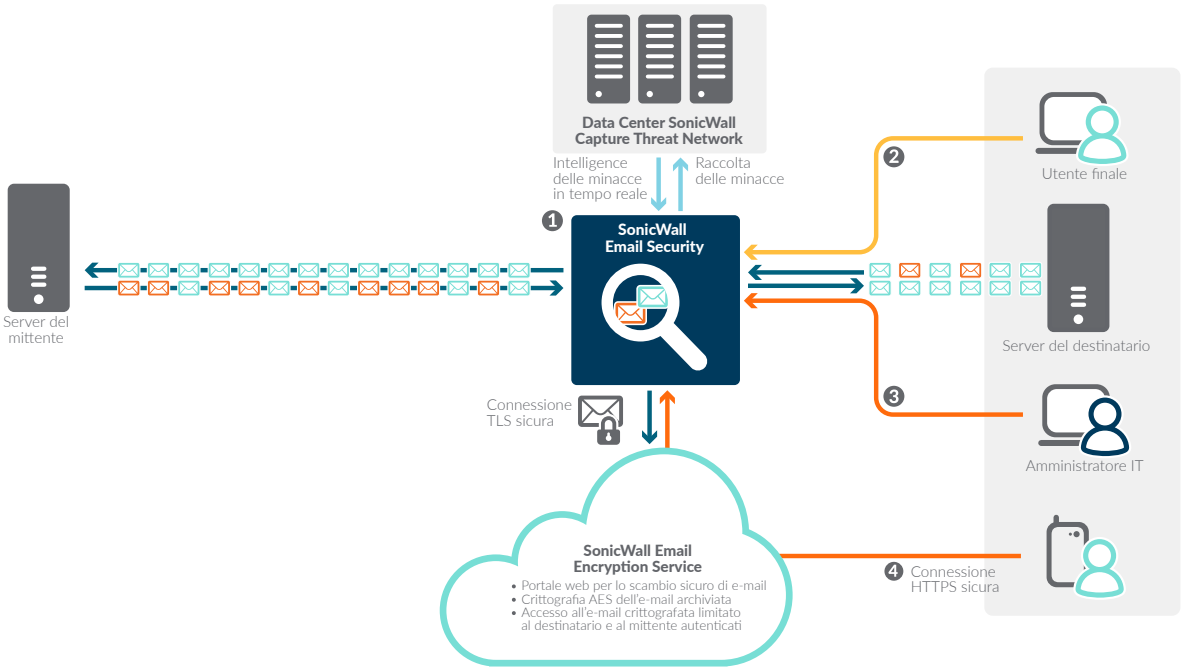
Disponibilità dei servizi 24x7 e continuità dell'e-mail – Consegna garantita dei messaggi e-mail, senza impatti sulla produttività in caso di interruzioni pianificate o impreviste dei server di posta elettronica in sede o di un provider di servizi cloud, come Office 365 e G Suite. Durante eventuali interruzioni del servizio, gli utenti possono accedere a una casella di posta di emergenza sicura, basata su browser web, per comporre, leggere e rispondere ai messaggi. Lo spooling dei messaggi e-mail garantisce che nessun messaggio vada perso in caso di mancata disponibilità dei server, recapitando i messaggi appena i server tornano operativi.

Mantenimento 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 sicura dello spam ai singoli utenti finali. Ogni utente è libero di personalizzare il livello delle impostazioni per il rilevamento dello spam, mentre il reparto di IT mantiene il controllo definitivo sul livello di sicurezza complessivo.

Maggior efficienza e convenienza mediante 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.

Operazioni semplificate per i fornitori di servizi gestiti grazie a un'unica finestra di login per l'amministrazione tramite Capture Security Center e alla gestione multi-tenant, 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 di posta indesiderata
- Casella di posta di emergenza

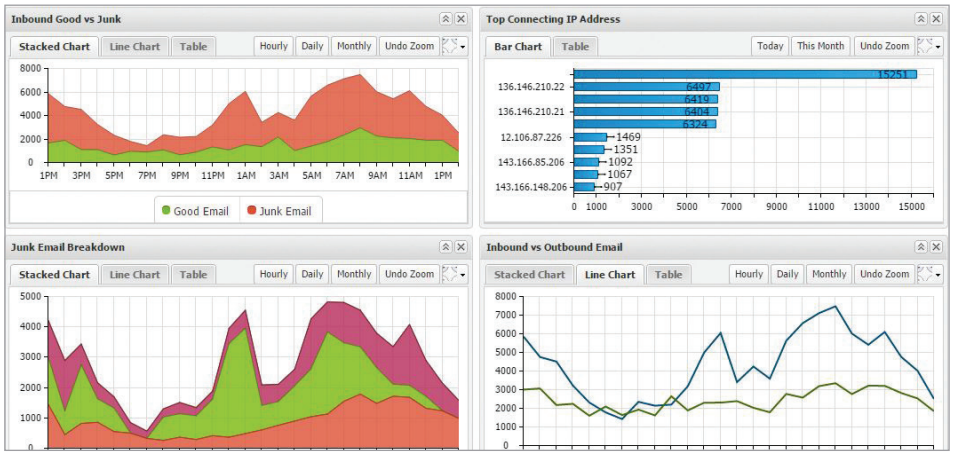
3 Gestione da parte dell'amministratore IT
- Installazione e configurazione
  - Integrazione LDAP
  - Gestione dello spooling
  - Gestione della protezione dalle minacce
- Gestione autonoma di autorizzazioni/rifiuti da parte degli utenti
- Configurazione e monitoraggio del portale per lo scambio sicuro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

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*

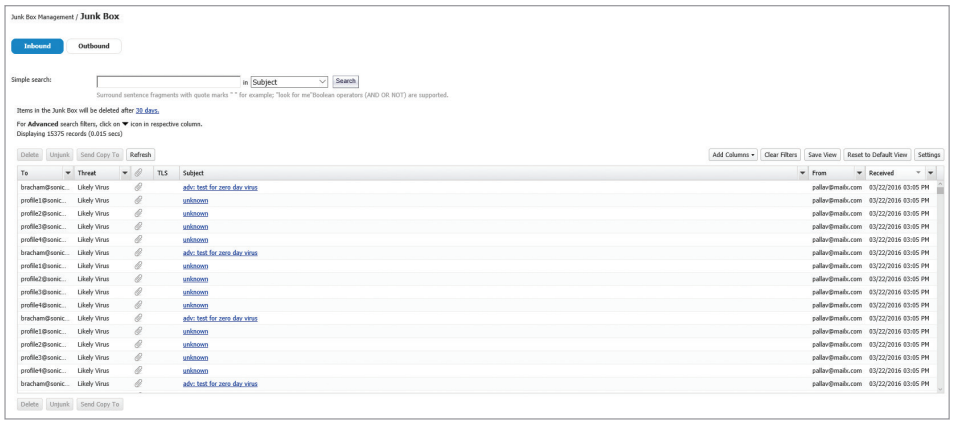
Monitoraggio e creazione di rapporti

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.



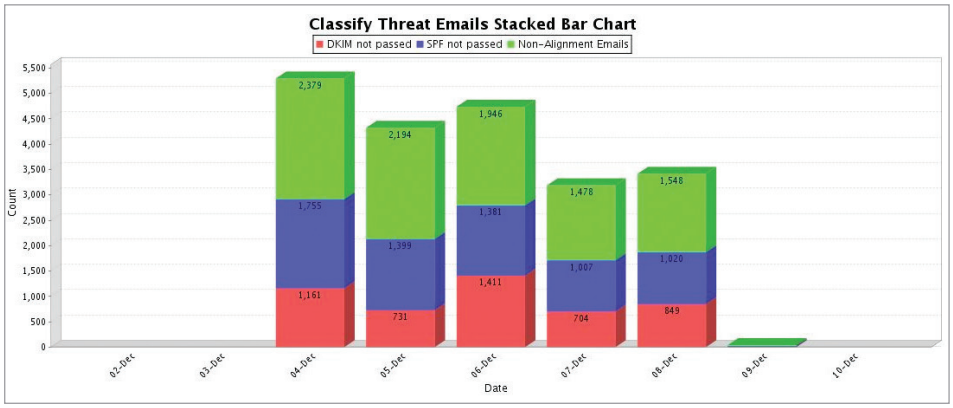
Riepiloghi della casella di posta indesiderata

I riepiloghi della casella di posta indesiderata permettono di ottimizzare la produttività degli utenti finali dell'e-mail, riducendo i reclami e migliorando l'efficacia complessiva.



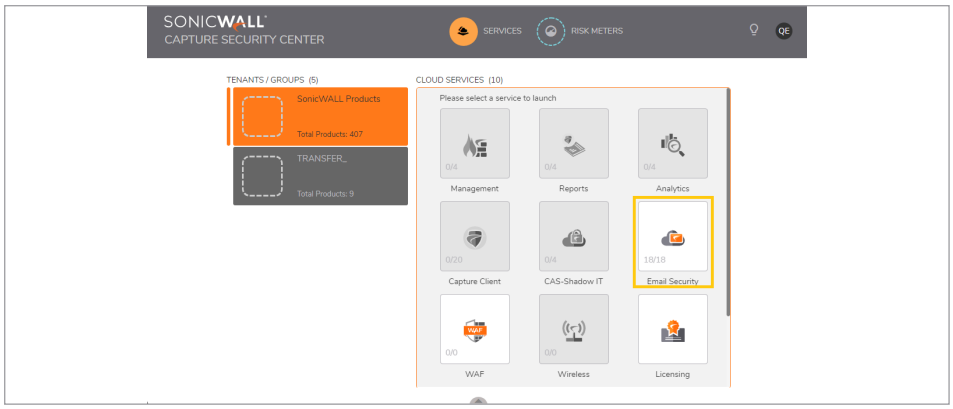
Rapporto antispoofing DMARC

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



Login con Capture Security Center

Consente di effettuare il login e gestire il servizio di sicurezza delle e-mail tramite Capture Security Center.



Caratteristiche

Protezione completa delle e-mail in entrata e in uscita	
Capture ATP (protezione avanzata contro allegati e URL)	Opzionale
Protezione time-of-click contro gli URL	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
Protezione antivirus multipla	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	
Gestione centralizzata con Capture Security Center	Sì
Gestione multi-tenant	Sì
Supporto di Office 365 e G Suite	Sì
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 delle firme antivirus	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
Casella di posta di emergenza	Opzionale
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
Continuità della posta elettronica	Opzionale
Conservazione posta indesiderata per 15 giorni	Sì
Spooling e-mail per un massimo di 7 giorni	Sì

Caratteristiche - continuazione

Policy e gestione della conformità	
Scansione degli allegati	Sì
Corrispondenza degli ID dei record	Sì
Dizionari	Sì
Caselle di e-mail/flusso di lavoro di approvazione	Sì
Rapporti sulla conformità	Sì
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 24 ore su 24, 7 giorni su 7	Sì
Data center multipli	Sì

Abbonamento	SKU
Servizio Hosted Email Security in abbonamento	
Servizio Hosted Email Security in abbonamento 10 utenti - (1 anno)	01-SSC-5030
Servizio Hosted Email Security in abbonamento 25 utenti - (1 anno)	01-SSC-5033
Servizio Hosted Email Security in abbonamento 50 utenti - (1 anno)	01-SSC-5036
Servizio Hosted Email Security in abbonamento 100 utenti - (1 anno)	01-SSC-5039
Servizio Hosted Email Security in abbonamento 250 utenti - (1 anno)	01-SSC-5042
Servizio Hosted Email Security in abbonamento 500 utenti - (1 anno)	01-SSC-5045
Servizio Hosted Email Security in abbonamento 750 utenti - (1 anno)	01-SSC-5057
Servizio Hosted Email Security in abbonamento 1.000 utenti - (1 anno)	01-SSC-5048
Servizio Hosted Email Security in abbonamento 2.000 utenti - (1 anno)	01-SSC-5051
Servizio Capture ATP per Hosted Email Security	
Servizio Capture ATP per Hosted Email Security Pacchetto per 10 utenti (1 anno)	01-SSC-1650
Servizio Capture ATP per Hosted Email Security Pacchetto per 25 utenti (1 anno)	01-SSC-1653
Servizio Capture ATP per Hosted Email Security Pacchetto per 50 utenti (1 anno)	01-SSC-1656
Servizio Capture ATP per Hosted Email Security Pacchetto per 100 utenti (1 anno)	01-SSC-1659
Servizio Capture ATP per Hosted Email Security Pacchetto per 250 utenti (1 anno)	01-SSC-1838
Servizio Capture ATP per Hosted Email Security Pacchetto per 500 utenti (1 anno)	01-SSC-1511
Servizio Capture ATP per Hosted Email Security Pacchetto per 750 utenti (1 anno)	01-SSC-1514
Servizio Capture ATP per Hosted Email Security Pacchetto per 1.000 utenti (1 anno)	01-SSC-1517
Servizio Capture ATP per Hosted Email Security Pacchetto per 2.000 utenti (1 anno)	01-SSC-1520
Servizio Capture ATP per Hosted Email Security Pacchetto per 5.000 utenti (1 anno)	01-SSC-1523
Continuity for Hosted Email Security	
Continuity for Hosted Email Security 10 utenti - (1 anno)	01-SSC-3068
Continuity for Hosted Email Security 25 utenti - (1 anno)	01-SSC-3071
Continuity for Hosted Email Security 50 utenti - (1 anno)	01-SSC-3074
Continuity for Hosted Email Security 100 utenti - (1 anno)	01-SSC-3077
Continuity for Hosted Email Security 250 utenti - (1 anno)	01-SSC-3080
Continuity for Hosted Email Security 500 utenti - (1 anno)	01-SSC-3083
Continuity for Hosted Email Security 750 utenti - (1 anno)	01-SSC-3086
Continuity for Hosted Email Security 1.000 utenti - (1 anno)	01-SSC-3089
Continuity for Hosted Email Security 2.000 utenti - (1 anno)	01-SSC-3092
Continuity for Hosted Email Security 5.000 utenti - (1 anno)	01-SSC-3095
Servizio Email Encryption per Hosted Email Security	
Servizio Email Encryption per Hosted Email Security 10 utenti - (1 anno)	01-SSC-5078
Servizio Email Encryption per Hosted Email Security 25 utenti - (1 anno)	01-SSC-5081
Servizio Email Encryption per Hosted Email Security 50 utenti - (1 anno)	01-SSC-5084
Servizio Email Encryption per Hosted Email Security 100 utenti - (1 anno)	01-SSC-5087
Servizio Email Encryption per Hosted Email Security 250 utenti - (1 anno)	01-SSC-5091
Servizio Email Encryption per Hosted Email Security 500 utenti - (1 anno)	01-SSC-5094
Servizio Email Encryption per Hosted Email Security 750 utenti - (1 anno)	01-SSC-5097
Servizio Email Encryption per Hosted Email Security 1.000 utenti - (1 anno)	01-SSC-5104
Servizio Email Encryption per Hosted Email Security 2.000 utenti - (1 anno)	01-SSC-5107

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

SonicWall

SonicWall è attiva nel settore della lotta al cibercrimine da più di 27 anni a difesa delle PMI, delle imprese e degli enti pubblici in ogni parte del mondo. Grazie alla ricerca dei SonicWall Capture Labs, le nostre premiate soluzioni di rilevamento e prevenzione delle violazioni in tempo reale garantiscono più di un milione di reti, unitamente alle e-mail, alle applicazioni e ai dati relativi, in oltre 215 paesi, consentendo alle aziende di funzionare in modo più efficace e con meno timori per la sicurezza. Per ulteriori informazioni visitare www.sonicwall.com o seguire la nostra azienda su Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

DataSheet-HostedEmailSecurity-US-VG-MKTG5162