SONICWALL

Software e apparecchiature per la sicurezza della posta elettronica

Proteggete le vostre infrastrutture dalle minacce avanzate per posta elettronica e dalle violazioni di conformità con potenti soluzioni, di facile uso

La posta elettronica è fondamentale per la comunicazione aziendale, ma è anche il principale vettore delle minacce come ransomware, phishing, business email compromise (BEC), spoofing, spam e virus. Inoltre, in base alle normative vigenti, è responsabilità dell'azienda proteggere i dati riservati impedendo eventuali perdite di dati e assicurare lo scambio sicuro di email contenenti informazioni riservate o dati sensibili dei clienti. Le organizzazioni di ogni dimensione, dalle PMI in crescita alle grandi aziende con ambienti distribuiti fino ai fornitori di servizi gestiti (MSP), necessitano di una soluzione a costi contenuti che garantisca la sicurezza e la crittografia dei messaggi di posta elettronica e la modularità necessaria per aumentare agevolmente la capacità delle unità organizzative e dei domini delegando la gestione.

Il software e le apparecchiature SonicWall Email Security offrono una protezione multilivello dalle minacce e dalle violazioni di conformità provenienti dall'interno e dall'esterno attraverso la posta elettronica, effettuando la scansione dei dati sensibili in tutti i contenuti, gli URL e gli allegati dei messaggi di posta elettronica in entrata e in uscita, offrendo una protezione in tempo reale contro ransomware, attacchi di phishing mirati, spoofing, virus, URL dannosi, zombi, attacchi Directory Harvest (DHA), Denial of Service (DoS) e altri. La soluzione sfrutta tecniche multiple di rilevamento delle minacce brevettate di SonicWall e un'esclusiva rete internazionale di identificazione e monitoraggio degli attacchi.

Il servizio SonicWall Capture Advanced Threat Protection prevede il sandboxing multi-engine leader del settore, con tecnologia RTDMI™ (Real-Time Deep Memory Inspection) in attesa di brevetto, per isolare le minacce sconosciute riscontrate in URL e file allegati sospetti, consentendo di bloccare le minacce avanzate prima che arrivino nelle caselle di posta degli utenti. La soluzione Email Security abbinata a Capture ATP offre una difesa decisamente efficace e tempestiva nei confronti del ransomware e degli attacchi zero-day.

La soluzione comprende anche DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework) e Domain-based Message Authentication, Reporting and Conformance (DMARC), un potente metodo di autenticazione dei messaggi di posta elettronica che contribuisce a individuare i messaggi di posta falsificati, riducendo lo spam e gli attacchi di phishing mirati come spear-phishing, whaling, truffa del CEO e compromissione delle email aziendali. Inoltre questo metodo segnala la provenienza e i mittenti dei messaggi di posta elettronica, consentendo di individuare e bloccare mittenti non autorizzati che falsificano i messaggi con l'indirizzo dell'azienda e di proteggere il vostro marchio. Inoltre, impedisce la perdita di dati riservati e le violazioni normative con una scansione e una gestione che garantiscano la conformità avanzata, compreso il servizio integrato di crittografia dei messaggi nel cloud per garantire lo scambio sicuro di dati sensibili.

La soluzione Email Security è intuitiva, rapida e semplice da gestire. La gestione dello spam può essere delegata agli utenti finali, mantenendo comunque il massimo controllo sull'applicazione della sicurezza. Inoltre la sincronizzazione con più server LDAP senza soluzione di continuità consente di gestire facilmente gli account degli utenti e dei gruppi. In ambienti distribuiti di grande estensione, il supporto multi-tenancy consente di delegare ad amministratori subordinati la gestione delle impostazioni su più unità organizzative (come divisioni aziendali o clienti MSP) all'interno di un'unica installazione di Email Security.

Vantaggi

- Impediscono al ransomware e al malware zero-day di raggiungere la casella di posta grazie a Capture Advanced Threat Protection
- Impediscono agli utenti di fare clic su link nocivi da qualsiasi dispositivo e da qualsiasi sede grazie alla protezione time-of-click degli URL
- Utilizzano tecniche di analisi avanzate per bloccare gli attacchi di phishing mirati, le frodi via email e la compromissione delle email aziendali (BEC)
- Bloccano le nuove minacce grazie agli aggiornamenti dell'intelligenza delle minacce in tempo reale forniti da SonicWall Capture Labs
- Mantengono l'igiene della posta elettronica grazie a potenti anti-spam e anti-virus
- Proteggono i dati attuando la prevenzione granulare della perdita dei dati (DLP) e politiche di conformità
- Semplificano la gestione grazie all'automazione intelligente, alla delega dei processi, al pannello di controllo facilmente personalizzabile e ad una reportistica avanzata
- Utilizzano opzioni di installazione flessibili e modulari, tra cui apparecchiature fisiche hardened, apparecchiature virtuali robuste e un potente software Windows Server®

[1] Brevetti USA 7.814.545; 7.343.624; 7.665.140; 7.653.698; 7.546.348

Funzioni

Protezione contro le minacce avanzate

Individuare e bloccare le minacce avanzate fino al verdetto. Questo è l'unico servizio di individuazione 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 di posta elettronica e proteggere i clienti dai crescenti pericoli delle minacce zero-day. Il servizio prevede la protezione avanzata degli URL, che analizza dinamicamente gli URL integrati in modo da bloccare e mettere in quarantena messaggi con URL dannosi prima che raggiungano le caselle di posta evitando che gli utenti possano fare clic su di essi, con conseguente compromissione. Il servizio Capture ATP offre una migliore granularità, con l'analisi dei file allegati e degli URL, ulteriori capacità per la creazione di report dettagliati e un'esperienza utente razionalizzata.

SonicWall Email Security riscrive altresì tutti gli URL incorporati per bloccare i messaggi di posta elettronica contenenti URL di phishing o dannosi; in questo modo, gli utenti sono protetti al momento del clic su qualsiasi dispositivo e da qualunque sede.

Alcune organizzazioni ed enti pubblici non possono utilizzare tecniche basate su cloud per il controllo dei file, come Capture ATP, per ragioni di conformità o di latenza. Integrate le vostre apparecchiature Email Security con le apparecchiature SonicWall Capture Security (CSa) per esaminare direttamente nel vostro datacenter i file sospetti che arrivano attraverso la posta elettronica. CSa può essere referenziato mediante indirizzo IP o FQDN, il che ne fa un'ottima risorsa per la prevenzione delle minacce.

Protezione dagli attacchi mirati

La tecnologia anti-phishing di SonicWall usa una combinazione di metodologie quali apprendimento automatico, euristica e analisi della reputazione e del contenuto per bloccare attacchi di phishing sofisticati. La soluzione prevede anche potenti standard di autenticazione della posta elettronica come SPF, DKIM e DMARC per bloccare attacchi di spoofing, compromissione delle email aziendali e frodi via email.

Intelligenza delle minacce in tempo reale

Beneficiate della protezione più approfondita e aggiornata contro i nuovi attacchi di spam, che garantisce al tempo stesso la consegna dei messaggi di posta elettronica legittimi con informazioni sulle minacce in tempo reale provenienti da SonicWall Capture Threat Network, che raccoglie i dati da milioni di fonti. SonicWall Capture Labs analizza queste informazioni ed esegue rigorosi test, assegnando poi un punteggio alla reputazione di mittenti e contenuti per individuare le nuove minacce in tempo reale.

Protezione anti-virus e anti-spyware

Beneficiate di una protezione aggiornata anti-virus e anti-spyware. La soluzione utilizza segnature provenienti dai principali database anti-virus del settore e il rilevamento degli URL dannosi per offrire una protezione multilivello superiore a quella offerta dalle soluzioni che si basano su singole tecnologie anti-virus.

Inoltre, l'analisi predittiva consente di proteggere la rete quando si diffonde un nuovo virus fino a quando non viene reso disponibile l'aggiornamento della segnatura anti-virus.

Automazione intelligente, delega dei processi e reportistica avanzata

Semplificate la gestione grazie all'automazione intelligente, alla delega dei processi e ad una reportistica avanzata. Gestite automaticamente i gruppi di utenti, gli account e gli indirizzi di posta elettronica. Beneficiate di un'integrazione avanzata con più server LDAP. Delegate con fiducia la gestione dello spam agli utenti finali grazie al plug-in scaricabile del pulsante di posta indesiderata di Outlook®, mantenendo nel contempo il pieno controllo locale. Individuate qualsiasi messaggio di posta nel giro di pochi secondi con il Rapid Message Search Engine. La reportistica centralizzata (anche in modalità split) fornisce informazioni granulari a livello dell'intero sistema, facilmente personalizzabili sui tipi di attacchi, sull'efficacia delle soluzioni e sul monitoraggio integrato delle prestazioni, con reportistica disponibile in formato PDF e JPEG.

Gestione delle politiche di conformità

Questo servizio aggiuntivo consente la conformità con gli obblighi normativi aiutandovi a individuare, monitorare e segnalare i messaggi di posta elettronica che violano le normative e le linee guida in materia di conformità (es., HIPAA, SOX, GLBA e PCI-DSS) e le linee guida aziendali sulla perdita di dati. Inoltre, il servizio in abbonamento consente l'instradamento basato sulle politiche della posta per approvazione, archiviazione e crittografia.

Crittografia dei messaggi di posta elettronica

Utilizzate una potente struttura per impedire la perdita di dati, gestire e attuare i requisiti di conformità e consentire uno scambio sicuro dei messaggi compatibili con i dispositivi mobili.

I messaggi crittografati possono essere monitorati per sapere quando vengono recapitati e aperti. Il destinatario riceverà un intuitivo messaggio di notifica con semplici istruzioni per accedere a un portale sicuro in cui leggere o scaricare il messaggio in tutta tranquillità. Il servizio è basato su cloud e non necessita di software client aggiuntivo, e diversamente dalle soluzioni della concorrenza i messaggi crittografati sono accessibili e possono essere letti dai dispositivi mobili e dai portatili.

Opzioni di installazione flessibili

Ottenete valore modulare a lungo termine configurando la vostra soluzione in funzione della crescita e della ridondanza con minimi costi iniziali. È possibile installare Email Security come apparecchiatura hardened dalle prestazioni elevate, come software che sfrutta l'infrastruttura esistente o come apparecchiatura virtuale che sfrutta le risorse di calcolo condivise per ottimizzare l'utilizzo, facilitare la migrazione e ridurre i costi di investimento. Iniziate con un sistema singolo e man mano che la vostra

azienda cresce aggiungete capacità e passate a un'architettura in modalità split e abilitata per il fail-over. La compatibilità multi-tenancy consente alle grandi aziende o ai fornitori di servizi gestiti di effettuare installazioni in più dipartimenti o clienti per istituire unità organizzative con uno o più domini. L'installazione può essere gestita centralmente, pur consentendo alle singole unità organizzative di avere in proprio utenti, sub-amministratori, regole di politica, caselle di posta indesiderata e altro ancora.

Opzioni di installazione di SonicWall Email Security

L'architettura decisamente flessibile di SonicWall Email Security consente l'installazione in organizzazioni che richiedono una soluzione altamente modulare, ridondante e distribuita per la protezione della posta elettronica gestibile centralmente. SonicWall Email Security può essere installata in modalità all-in-one o in modalità split.

In modalità split, i sistemi possono essere configurati come analizzatore remoto o centro di controllo. In una tipica configurazione in modalità split, uno o più analizzatori remoti sono collegati a un centro di controllo. L'analizzatore remoto riceve i messaggi di posta elettronica da uno o più domini e applica tecniche di gestione delle connessioni, filtraggio dei messaggi (anti-spam, anti-phishing e anti-virus) e politiche avanzate per consegnare i messaggi legittimi ai server di posta elettronica a valle. Il centro di controllo gestisce centralmente tutti gli analizzatori remoti e acquisisce e memorizza i messaggi indesiderati provenienti dagli stessi. La gestione centralizzata comprende funzioni di reportistica e monitoraggio di tutti i sistemi correlati. Questo paradigma consente la modularità della soluzione con un valido rapporto costi-benefìci e protegge i messaggi di posta elettronica in entrata e in uscita per le organizzazioni in crescita. Utilizzando le apparecchiature virtuali SonicWall Email Security, la modalità split può essere completamente installata su uno o più server per un'ottimale efficienza di scala.

Funzioni

	APPARECCHIATURA, APPARECCHIATURA VIRTUALE	WINDOWS SERVER®
Abbonamento Advanced Total Secure – Pacchetto di protezione avanzata		
Comprende la protezione avanzata degli allegati e degli URL SonicWall Capture ATP, oltre all'abbonamento Total Secure	Sì	Sì
Protezione time-of-click degli URL	Sì	Sì
Abbonamento Total Secure – Pacchetto di protezione di base		
Comprende un abbonamento 24x7 alla protezione dinamica della posta elettronica più anti-virus multilivello, rilevamento degli URL dannosi e gestione della conformità in abbonamento	Sì	Sì
Ransomware e protezione zero-day – opzionale		
Componente aggiuntivo per la protezione avanzata degli allegati e degli URL SonicWall Capture ATP per l'abbonamento Total Secure	Sì	Sì
Protezione completa dei messaggi di posta elettronica in entrata e in uscita		
Anti-spam	Sì	Sì
Gestione delle connessioni con reputazione IP avanzata	Sì	Sì
Rilevamento, classificazione e blocco del phishing	Sì	Sì
Protezione contro Directory Harvest, Denial of Service e NDR	Sì	Sì
Anti-spoofing con supporto per SPF, DKIM e DMARC	Sì	Sì
Regole di politica per utenti, gruppi, tutti	Sì	Sì
MTA (Message Transfer Agent) in memoria per una maggiore velocità	Sì	Sì
Facilità di amministrazione		
Installazione	< 1 ora	< 1 ora
Interventi di gestione settimanali	< 10 min	< 10 min
Sincronizzazione automatica multi-LDAP per utenti, gruppi	Sì	Sì
Compatibilità con tutti i server di posta elettronica SMTP	Sì	Sì
Compatibilità autenticazione SMTP (SMPT AUTH)	Sì	Sì
Autorizzazione/rifiuto dei controlli per utenti finali	Sì	Sì
Personalizzazione, programmazione e invio per posta elettronica di oltre 30 rapporti	Sì	Sì
Particolari sulle valutazioni	Sì	Sì
Pannello di controllo facilmente personalizzabile	Sì	Sì
Rapid Message Search Engine	Sì	Sì
Architettura modulare in modalità split	Sì	Sì
Clustering e clustering remoto	Sì	Sì
Facilità per gli utenti finali		
Single Sign-On	Sì	Sì
Caselle di posta indesiderata per i singoli utenti e riepilogo posta indesiderata	Sì	Sì
Definizione delle impostazioni di spam per singoli utenti, elenchi blocchi/autorizzazioni	Sì	Sì
Abbonamento alla protezione dei messaggi di posta elettronica con supporto dinamico necessario		
Aggiornamenti automatici anti-virus, anti-spam, anti-phishing SonicWall nel cloud ogni minuto	Sì	Sì
Supporto 24x7	Sì	Sì
RMA (sostituzione dell'apparecchiatura)	Sì	Sì
Aggiornamenti software/firmware	Sì	Sì
Abbonamento anti-virus – opzionale		
Feed segnature dai principali database anti-virus del settore	Sì	Sì
Anti-virus SonicWall TimeZero	Sì	Sì
Rilevamento zombi	Sì	Sì
Abbonamento Email Compliance – opzionale		
Gestione avanzata delle politiche	Sì	Sì
Scansione degli allegati	Sì	Sì
Corrispondenza degli ID dei record	Sì	Sì
Dizionari	Sì	Sì
Caselle/flussi di lavoro di approvazione	Sì	Sì
Archiviazione messaggi	Sì	Sì
Rapporti sulla conformità	Sì	Sì
Abbonamento Email Encryption – opzionale		
Possibilità di abbonamento Compliance più crittografia dei messaggi di posta elettronica basata sulle politiche e scambio sicuro dei messaggi	Sì	Sì

Specifiche del sistema

APPARECCHIATURE EMAIL SECURITY	5000	7000	9000
Domini		Illimitato	
Sistema operativo		Apparecchiatura SonicWall hardened per Linux OS	
Chassis per montaggio a rack	1RU	1RU	1RU
CPU	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 GB	16 GB	32 GB
Disco rigido	500 GB	1 TB	1 TB
Redundant disk array (RAID)	—	RAID 1	RAID 5
Unità sostituibili a caldo	No	Sì	Sì
Alimentazione ridondante	No	No	Sì
SAFE Mode Flash	Sì	Sì	Sì
Dimensioni	17,0 x 16,4 x 1,7 pollici (43,18 x 41,59 x 4,44 cm)	17,0 x 16,4 x 1,7 pollici (43,18 x 41,59 x 4,44 cm)	27,5 x 19,0 x 3,5 pollici (69,9 x 48,3 x 8,9 cm)
Peso	16 libbre / 7,26 kg	16 libbre / 7,26 kg	50 libbre / 22,7 kg
Peso RAEE	16 libbre / 7,37 kg	16 libbre / 22,2 kg	48,9 libbre / 22,2 kg
Potenza assorbita (Watt)	46	48	158
BTU	155	162	537
MTBF @25C in ore	130.919	150.278	90.592
MTBF @25C in anni	14,9	17,2	10,3
SOFTWARE EMAIL SECURITY			
Domini		Illimitato	
Sistema operativo		Microsoft Hyper-V Server 2012 (64-bit) o superiore Windows Server 2008 R2 o superiore solo x64 bit	
CPU		Processore Intel o AMD a 64 bit	
RAM		Configurazione minima 8 GB	
Disco rigido		Configurazione minima 160 GB	
APPARECCHIATURA VIRTUALE EMAIL SECURITY			
Hypervisor		ESXi™ ed ESX™ (versione 5.0 e successive)	
Sistema operativo installato		8 GB (espandibile)	
Memoria allocata		4 GB	
Dimensioni apparecchiatura su disco		160 GB (espandibile)	
Guida alla compatibilità hardware per VMware		http://www.vmware.com/resources/compatibility/search.php	

Servizi attivati dai partner

Serve aiuto per pianificare, installare od ottimizzare la soluzione SonicWall? I SonicWall Advanced Services Partner hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Ulteriori informazioni su www.sonicwall.com/PES.

Informazioni per l'ordinazione di SonicWall Email Security

Apparecchiatura SonicWall Email Security

Prodotto	SKU
Apparecchiatura Sonicwall Email Security 9000	01-SSC-7605
Apparecchiatura Sonicwall Email Security 7000	01-SSC-7604
Apparecchiatura Sonicwall Email Security 5000	01-SSC-7603
Software SonicWall Email Security	01-SSC-6636
Apparecchiatura virtuale SonicWall Email Security	01-SSC-7636

Abbonamenti SonicWall Email Security

Abbonamento	SKU
Abbonamento SonicWall Email Protection	
Abbonamento SonicWall Email Protection e supporto 24X7 25 utenti – 1 server (1 anno)	01-SSC-6669
Abbonamento SonicWall Email Protection e supporto 24X7 1.000 utenti – 1 server (1 anno)	01-SSC-6678
Abbonamento SonicWall Email Protection e supporto 24X7 10.000 utenti – 1 server (1 anno)	01-SSC-6730
Abbonamento SonicWall Email Anti-Virus	
SonicWall Email Anti-Virus 25 utenti – 1 server (1 anno)	01-SSC-6759
SonicWall Email Anti-Virus 1.000 utenti – 1 server (1 anno)	01-SSC-6768
SonicWall Email Anti-Virus 10.000 utenti – 1 server (1 anno)	01-SSC-7562
Abbonamento SonicWall Email Encryption	
SonicWall Email Encryption Service 25 utenti (1 anno)	01-SSC-7427
SonicWall Email Encryption Service 1.000 utenti (1 anno)	01-SSC-7471
SonicWall Email Encryption Service 10.000 utenti (1 anno)	01-SSC-7568
Abbonamento SonicWall Email Compliance	
SonicWall Email Compliance Service 25 utenti – 1 server (1 anno)	01-SSC-6639
SonicWall Email Compliance Service 1.000 utenti – 1 server (1 anno)	01-SSC-6648
SonicWall Email Compliance Service 10.000 utenti – 1 server (1 anno)	01-SSC-6735
Abbonamento SonicWall TotalSecure Email	
Abbonamento SonicWall TotalSecure Email 25 utenti (1 anno)	01-SSC-7399
Abbonamento SonicWall TotalSecure Email 1.000 utenti (1 anno)	01-SSC-7398
Abbonamento SonicWall TotalSecure Email 10.000 utenti (1 anno)	01-SSC-7405
Add-on Capture ATP per abbonamento TotalSecure Email	
Capture ATP per abbonamento SonicWall TotalSecure Email 25 Utenti (1 anno)	01-SSC-1526
Capture ATP per abbonamento SonicWall TotalSecure Email 1.000 Utenti (1 anno)	01-SSC-1874
Capture ATP per abbonamento SonicWall TotalSecure Email 10.000 Utenti (1 anno)	01-SSC-1883
Abbonamento SonicWall Advanced TotalSecure Email (compreso Capture ATP)	
Abbonamento SonicWall Advanced TotalSecure Email 25 utenti (1 anno)	01-SSC-1886
Abbonamento SonicWall Advanced TotalSecure Email 1.000 utenti (1 anno)	01-SSC-1904
Abbonamento SonicWall Advanced TotalSecure Email 10.000 utenti (1 anno)	01-SSC-1913

I pacchetti e gli abbonamenti per le apparecchiature SonicWall Email Security sono disponibili in confezioni da 25, 50, 100, 250, 500, 1.000, 2.000, 5.000 e 10.000 utenti e nelle opzioni da 1, 2 e 3 anni. Il supporto è disponibile anche come opzione 8X5. Per l'elenco completo degli SKU rivolgersi al rivenditore locale SonicWall di fiducia.

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 email, alle applicazioni e ai dati relativi, in oltre 215 paesi, consentendo alle organizzazioni di funzionare in modo più efficace e con meno timori per la sicurezza. Per ulteriori informazioni visitare www.sonicwall.com o seguirci su Twitter, LinkedIn, Facebook e Instagram.

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

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150