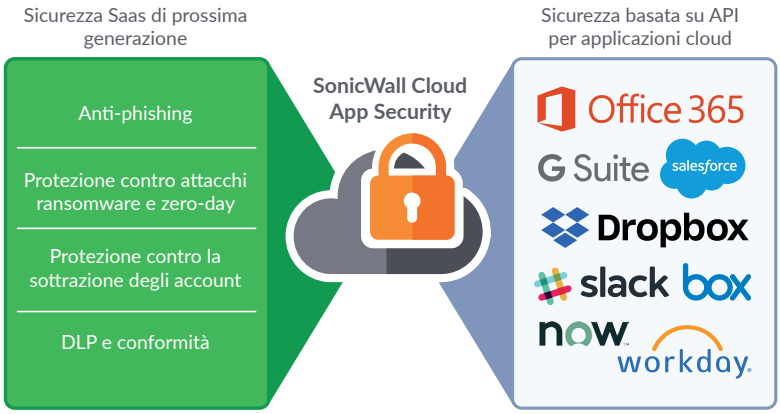
SONICWALL

SonicWall Cloud App Security

SonicWall Cloud App Security offre la sicurezza di prossima generazione delle applicazioni SaaS come Office 365 e G Suite, proteggendo email, dati e credenziali utente dalle minacce avanzate e garantendo al tempo stesso la conformità nel cloud. Se si sta passando al cloud, SonicWall offre la migliore sicurezza in assoluto basata su API con un basso TCO, minimi costi d'installazione e un'esperienza utente senza soluzioni di continuità.



Visibilità: Identificazione di tutti i servizi cloud (sanzionati e non) utilizzati dai dipendenti dell'organizzazione, compresa la visibilità del traffico est-ovest (da cloud a cloud), dal momento che gli utenti possono autenticarsi su applicazioni non sanzionate utilizzando software sanzionati, come Office 365.

Sicurezza della posta elettronica di prossima generazione: Dal momento che la posta elettronica sta diventando l'applicazione SaaS più diffusa, proteggere questo importante vettore è fondamentale per la sicurezza SaaS. La soluzione prevede il trasferimento degli allegati nella sandbox, la protezione avanzata degli URL e la protezione BEC (Business Email Compromise).

Protezione avanzata contro le minacce: Prevenzione della propagazione dei malware tramite app come OneDrive, Box e Dropbox con scansione in tempo reale delle minacce conosciute e sandboxing Capture ATP per le minacce zero-day e sconosciute.

Sicurezza dei dati: Attuazione di politiche di sicurezza data-centriche, che consentono controlli d'accesso granulari, impedendo il caricamento di file sensibili o riservati. La soluzione comprende strumenti politici basati sui ruoli, classificazione dei dati e tecnologie per la prevenzione delle perdite di dati per il monitoraggio dell'attività degli utenti e il blocco o la limitazione degli accessi.

Conformità: La soluzione raccoglie un audit trail completo per ogni azione, compresi gli eventi in tempo reale e quelli storici e mette a disposizione semplici modelli DLP per l'effettuazione dei controlli delle politiche e la conformità normativa in tempo reale.

Vantaggi:

Sicurezza della posta elettronica di prossima generazione

- Blocco dei ransomware, degli attacchi zero-day e delle email di phishing mirato prima che raggiungano la casella di posta in arrivo dell'utente
- Il trasferimento degli allegati nella sandbox e la protezione avanzata degli URL assicurano una protezione avanzata contro le minacce
- Scansione del traffico email in ingresso, in uscita e interno in Office 365 e G Suite
- Blocco degli attacchi di impersonazione tramite apprendimento automatico e intelligenza artificiale (AI)
- Richiamo di email nocive dalle caselle della posta in arrivo degli utenti dopo l'invio

Sicurezza SaaS di prossima generazione (CASB)

- Visibilità e controllo a livello granulare sulle applicazioni informatiche sanzionate e nascoste
- Copertura completa sul traffico user-to-cloud e cloud-to-cloud
- Prevenzione dell'upload di dati sensibili e della condivisione non autorizzati dei file
- Definizione di politiche coerenti in materia di sicurezza dei dati sulle applicazioni sanzionate
- Protezione contro la sottrazione degli account (ATO), minacce interne, credenziali compromesse
- Blocco della propagazione di ransomware e malware zero-day nel cloud
- Attuazione di politiche normative sulla conformità tramite semplici modelli DLP
- Identificazione delle violazioni e delle lacune di sicurezza tramite l'analisi degli eventi storici e in tempo reale

La sicurezza diventa semplice e accessibile

- Esperienza utente completa con accesso da qualsiasi dispositivo e da qualunque postazione
- Eliminazione di punti deboli, problematiche di latenza e necessità di riorientare il traffico tramite proxy
- Automazione dell'individuazione delle applicazioni nel cloud in abbinamento a SonicWall NGFW
- Riduzione del costo totale di proprietà (TCO) grazie alla rapidità d'installazione e alla facilità d'uso

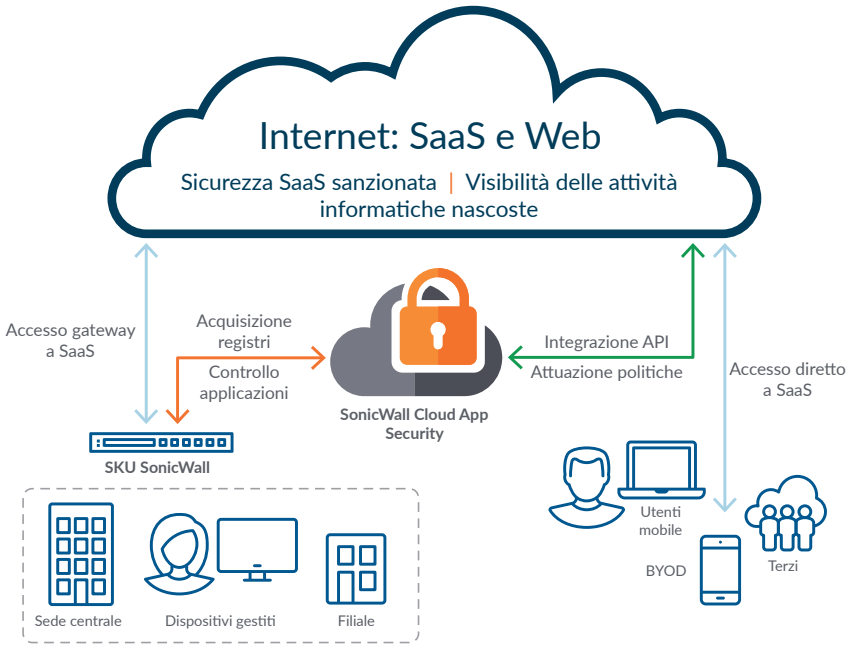
Panoramica della soluzione

Descrizione della soluzione SonicWall

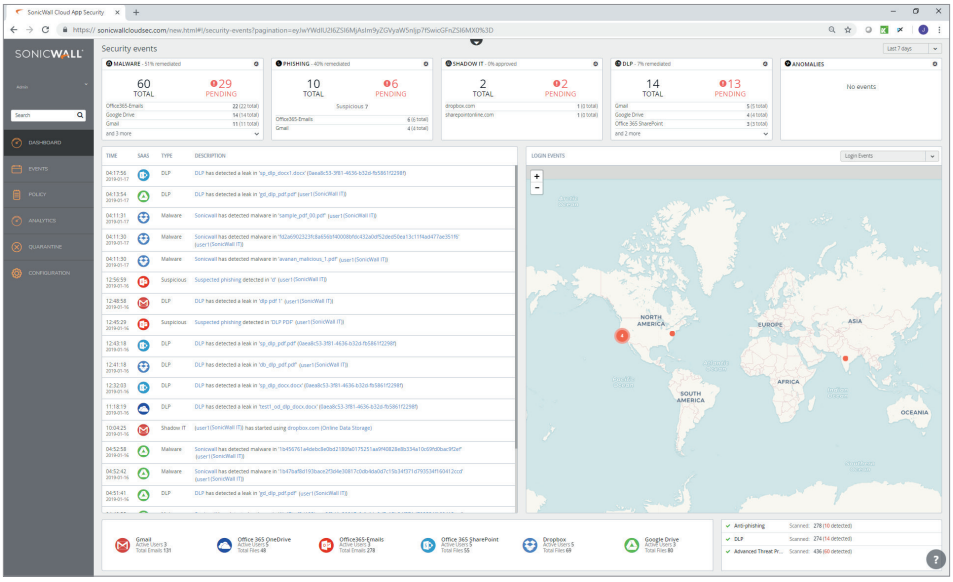
La soluzione SonicWall Cloud App Security consente la scansione fuori banda del traffico alle applicazioni SaaS sanzionate e non tramite API e analisi dei registri del traffico.

La soluzione si integra perfettamente con le applicazioni SaaS sanzionate utilizzando API native, mettendo a disposizione funzionalità CASB: visibilità, protezione avanzata delle minacce, prevenzione di perdite di dati (DLP) e conformità. Utilizzata in abbinamento a un firewall di prossima generazione (NGFW) SonicWall, Cloud App Security consente la visibilità e il controllo della visibilità delle attività informatiche nascoste per l'uso del cloud in rete.

La soluzione consente ai responsabili informatici di installare le applicazioni SaaS senza compromettere la sicurezza e la conformità. Gli amministratori possono definire da un'unica console le politiche coerenti per tutte le applicazioni SaaS installate a livello dell'organizzazione. È possibile utilizzare i modelli di report DLP e di conformità predefiniti per chiudere rapidamente le falle di sicurezza e definire politiche personalizzate per soddisfare le esigenze aziendali e normative. Sia che si debbano gestire pochi utenti o centinaia di migliaia di dipendenti in ogni parte del mondo, la soluzione può essere modulata in funzione delle proprie esigenze, senza bisogno d'installare e gestire alcun hardware.



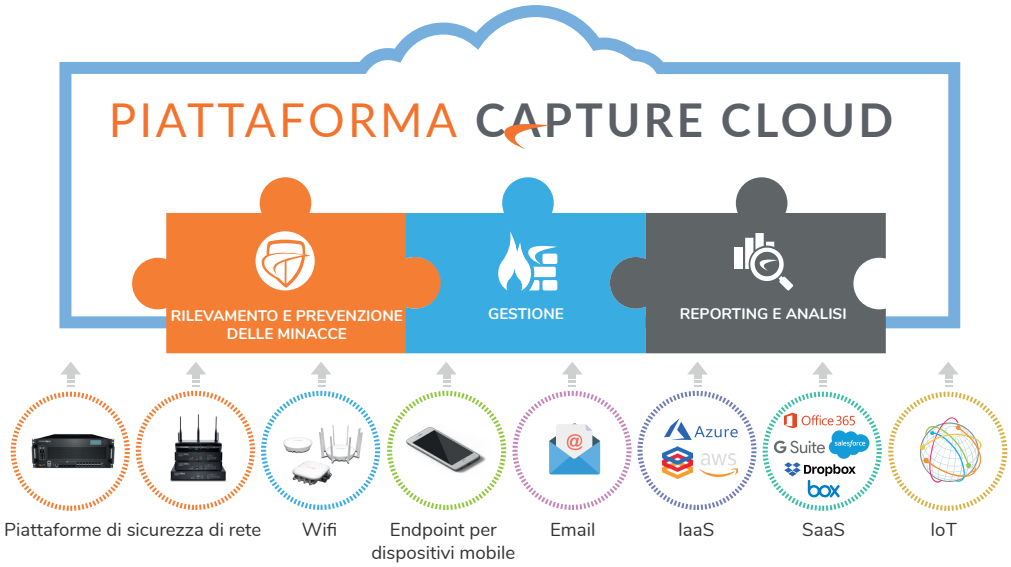
Sicurezza SaaS basata su API con funzioni CASB



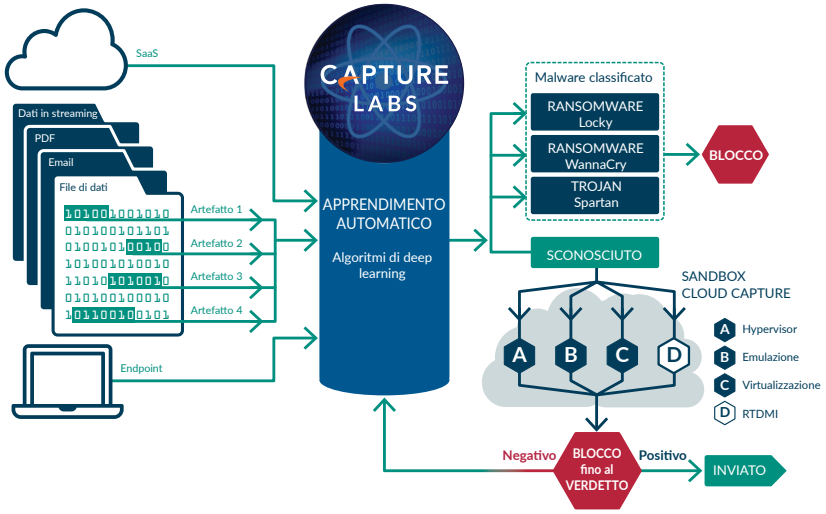
Il pannello di controllo in tempo reale consente agli amministratori di monitorare l'uso delle applicazioni a rischio, tracciare l'attività degli utenti, il volume delle transazioni e la sede in cui le applicazioni vengono utilizzate. La soluzione garantisce l'adozione sicura delle applicazioni SaaS senza ricadute sulla produttività del personale.

Integrazione con la piattaforma Capture Cloud di SonicWall

SonicWall Cloud App Security è un servizio cloud nativo strutturato mediante la piattaforma di cattura cloud e reso disponibile mediante Capture Security Center. La piattaforma Capture Cloud di SonicWall offre la prevenzione delle minacce basata sul cloud e la gestione della rete oltre a funzionalità di reportistica e analisi per organizzazioni di qualsiasi dimensione. La piattaforma consolida le informazioni sulle minacce raccolte da molteplici fonti, tra cui il nostro premiato servizio sandbox di rete multi-engine Capture Advanced Threat Protection, e oltre 1 milione di sensori SonicWall situati in tutto il mondo. Capture Security Center consente la gestione da un'unica finestra e gli amministratori hanno la possibilità di creare con facilità report in tempo reale e storici sull'attività di rete e cloud.



Per proteggere le applicazioni SaaS, SonicWall Cloud App Security utilizza la piattaforma Capture Cloud, che abbina l'intelligence globale della sicurezza della Capture Threat Network con la prevenzione avanzata delle minacce della sandbox multi-engine Capture ATP. Questo approccio permette a SonicWall di ampliare le funzioni di prevenzione delle violazioni automatizzate in tempo reale negli ambienti SaaS, consentendo alle organizzazioni di passare al cloud. Le API native si integrano direttamente con i servizi cloud, consentendo alla soluzione di effettuare la scansione dei file in applicazioni come OneDrive o Dropbox tramite il servizio Capture ATP con Real-Time Deep Memory Inspection™ (RTDMI™), impedendo l'accesso in rete a ransomware e zero-day.



Sicurezza completa per Office 365 e G Suite

Sicurezza di prossima generazione per la posta elettronica nel cloud

SonicWall Cloud App Security comprende la funzione di sicurezza della posta elettronica di prossima generazione progettata per le piattaforme di posta elettronica in cloud. Normalmente, quando le organizzazioni spostano la posta elettronica nel cloud, fanno esclusivamente affidamento sulla sicurezza offerta dal fornitore del servizio o la integrano con un proxy MTA tradizionale. I gateway di posta elettronica esterni, tuttavia, potrebbero non essere sufficienti per rilevare e bloccare le minacce di oggi.

Oltre ai tradizionali livelli di sicurezza della posta elettronica dei controlli SPF, DKIM e DMARC, ed al filtraggio degli URL tramite le principali fonti di dati per le blacklist degli URL, l'esclusiva architettura di Cloud App Security offre una protezione che le soluzioni con gateway esterni non sono in grado di dare, ovvero:

- Aggiunge un livello di protezione contro le minacce avanzate: Cloud App Security blocca i messaggi di phishing che Office 365 e G Suite non sono riusciti ad intercettare. La soluzione utilizza l'apprendimento automatico, l'intelligenza artificiale e l'analisi dei big data per offrire potenti funzioni anti-phishing, sandboxing degli allegati, protezione avanzata degli URL e protezione contro l'impersonazione.
- Monitora le email in arrivo, in uscita e interne: l'integrazione del SaaS in Cloud App Security consente di scansionare e mettere in quarantena tutte le email prima che arrivino nella casella di posta in arrivo dell'utente, sia che provengano dall'esterno dell'organizzazione, sia da un account interno compromesso.
- Scansiona i messaggi storici per individuare eventuali minacce: alla prima connessione Cloud App Security scansiona i messaggi storici (anche quelli degli account chiusi) per individuare potenziali violazioni o account compromessi.
- Richiamo messaggi a livello globale: i messaggi dannosi possono essere modificati o richiamati in qualsiasi momento indipendentemente dal fatto che siano dannosi, contengano informazioni riservate o siano stati trasmessi perché accidentalmente un dipendente ha selezionato "rispondi a tutti".

Poiché la protezione della posta elettronica di Cloud App Security viene applicata a monte della casella di posta in arrivo ma a valle dei filtri inattivi Microsoft o Google (come pure degli eventuali gateway MTA installati), i suoi algoritmi di apprendimento automatico sono tarati espressamente per individuare le minacce che non sono state ancora intercettate. Inoltre, Cloud App Security è in grado di integrare i risultati delle scansioni native nei suoi algoritmi di rilevamento.

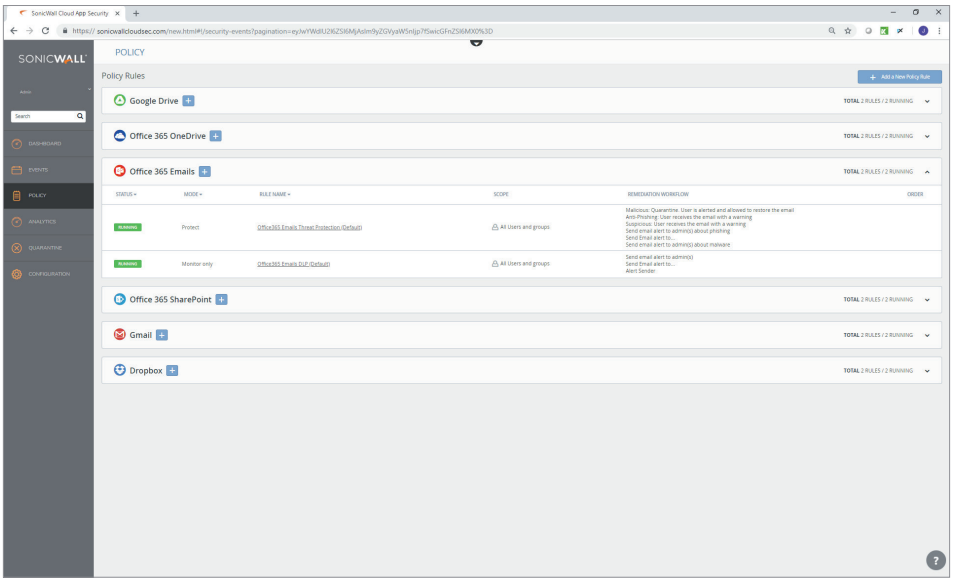
La protezione virtuale in linea blocca i messaggi dannosi prima che raggiungano la casella di posta in arrivo degli utenti

Sicurezza di prossima generazione per la suite di produttività completa

Cloud App Security offre una sicurezza completa per Office 365 o G Suite basata sulla sicurezza approfondita. Sia che si utilizzino la posta elettronica, unità condivise, la messaggistica istantanea o l'intero ambiente collaborativo, la soluzione aiuta a:

- Prevenire che phishing e malware si propaghino nell'organizzazione o si diffondano a clienti e partner.
- Verificare i singoli file per individuare contenuto dannoso tramite sandboxing Capture ATP e analisi dei contenuti attivi per mettere in quarantena le minacce prima che vengano scaricate dagli utenti.
- Identificare informazioni riservate ed applicare le politiche cloud-aware per non farle uscire dall'organizzazione o dai gruppi di lavoro. Gli utenti possono sfruttare l'intera potenza della suite di produttività basata sul cloud, mentre flussi di lavoro automatici si fanno carico della conformità normativa, garantendo che i dati PCI, HIPAA, PII o altri dati riservati non vengano condivisi all'esterno.

Protezione completa per l'intera suite di Office nel cloud



Tutte le applicazioni SaaS hanno engine di politica completamente diversi, ognuno con i suoi ruoli esclusivi e le sue funzioni di attivazione specifiche. Le soluzioni SonicWall le mappano sulle applicazioni SaaS sanzionate e consentono controlli più granulari. In questo modo Cloud App Security consente di definire un'unica politica che viene applicata in modo coerente in tutte le applicazioni.

Inoltre le politiche contestuali consentono di creare flussi di lavoro esecutivi che informano gli utenti sulle problematiche, propongono opzioni di sicurezza basate sulle politiche e risposte di verifica che vanno oltre i controlli dei permessi normalmente previsti dalle singole SaaS.

Sicurezza SaaS

Per rendere sicuro l'uso di SaaS nelle organizzazioni, SonicWall Cloud App Security offre:

Sicurezza delle attività informatiche sanzionate: integrazione diretta con i servizi cloud tramite API per la protezione avanzata dalle minacce e la prevenzione della perdita dei dati in ambienti SaaS.

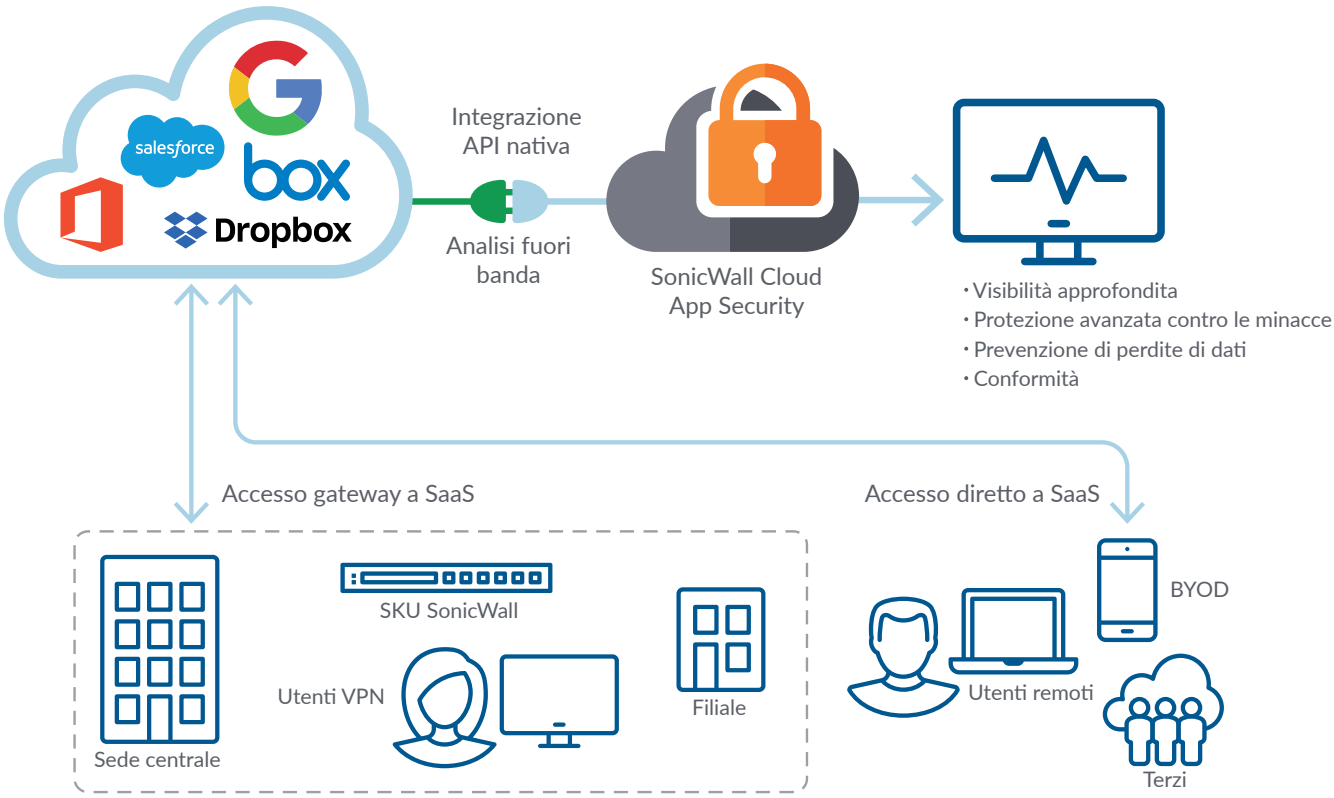
Visibilità e controllo delle attività informatiche nascoste: integrazione completa con SonicWall NGFW per l'individuazione delle applicazioni cloud e la valutazione dei rischi in modo automatico tramite l'analisi dei registri del traffico.

Sicurezza delle attività informatiche sanzionate

Adottando applicazioni SaaS come Box e Dropbox la responsabilità di garantire la sicurezza dei dati dell'organizzazione resta di competenza dell'organizzazione e non del fornitore dei servizi cloud (CSP). Questa riserva viene spesso specificata a caratteri microscopici ed i CSP non sono responsabili in caso di perdita di dati o di propagazione di malware e di infezioni. Se le organizzazioni decidono di utilizzare queste applicazioni, devono prendere in considerazione l'installazione di una soluzione in grado di verificare i dati nelle applicazioni cloud.

Soltanto le soluzioni basate su API possono ispezionare i dati residenti nelle applicazioni SaaS mentre le soluzioni in linea basate su proxy ispezionano solo i dati caricati sul cloud da dietro un firewall. Poiché molte organizzazioni hanno già molti volumi di dati memorizzati nel cloud, le API vengono utilizzate per attuare le politiche su di essi. Tra le altre funzionalità - possibili solo quando ci si collega direttamente ad un'applicazione tramite API - figurano la possibilità di scansionare le impostazioni di configurazione della sicurezza nell'applicazione e di suggerire cambiamenti atti a migliorare la sicurezza, come pure la possibilità di effettuare la scansione dei permessi di condivisione di file e cartelle per valutare il rischio di accesso esterno e da parte di terzi ai dati aziendali. La soluzione consente una visibilità approfondita, una protezione avanzata contro le minacce tramite la sandbox Capture ATP e la prevenzione delle perdite di dati per le applicazioni SaaS, come le email basate su cloud, oltre ad applicazioni per la condivisione dei file e la memorizzazione nel cloud, come Google G Suite e Microsoft Office 365.

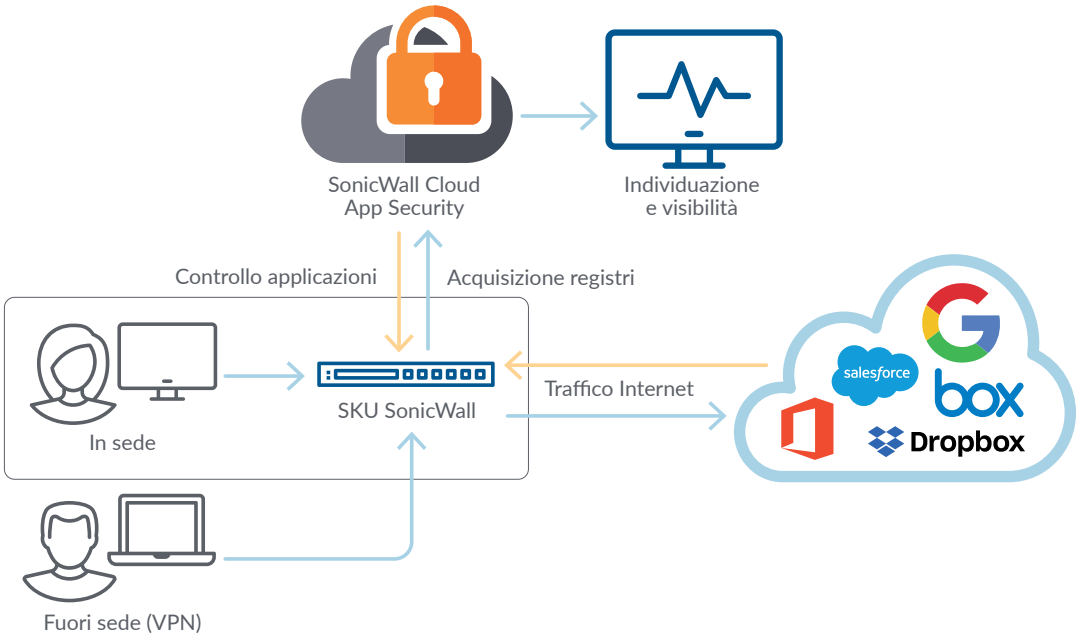
SonicWall Cloud App Security analizza tutto il traffico (eventi registrati, attività degli utenti, file di dati e oggetti, stato di configurazione etc.) ed attiva le necessarie politiche di sicurezza integrandosi direttamente con le API native del servizio cloud. Dal momento che sfrutta le API native, la soluzione non utilizza alcun proxy né deve stare in-line tra utente e cloud. Ciò consente alla soluzione di garantire la copertura per l'applicazione interessata, indipendentemente dal dispositivo dell'utente o dalla rete. Inoltre l'approccio basato sulle API facilita l'installazione, consente il controllo granulare ed è a impatto zero sull'esperienza dell'utente.



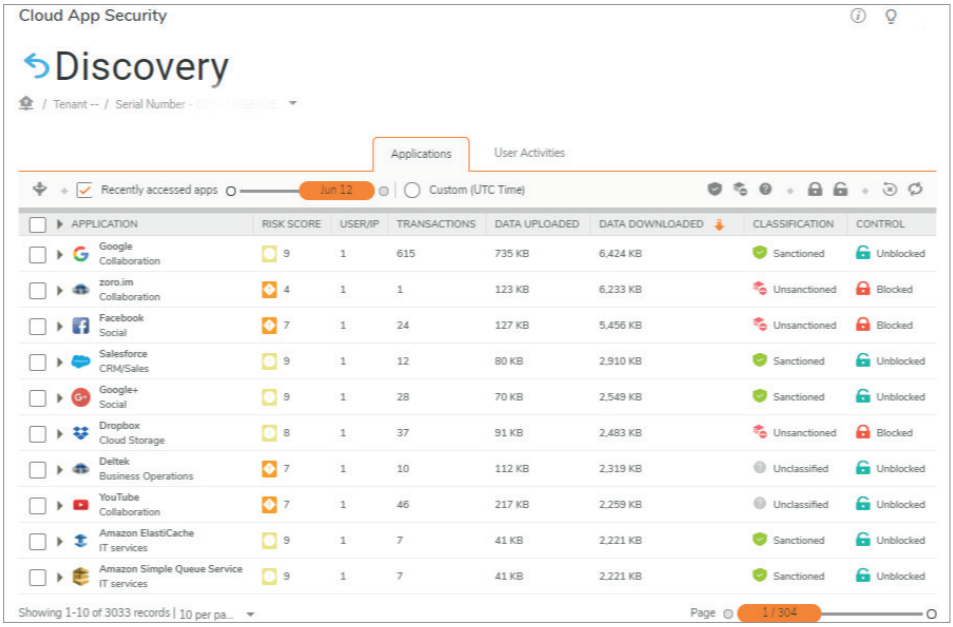
Applicazioni SaaS sicure sanzionate

Rilevamento e controllo delle attività informatiche nascoste

I firewall di prossima generazione (NGFW) di SonicWall analizzano e registrano tutto il traffico in entrata e in uscita dalla rete. I log generati per i dati del traffico in uscita non distinguono chiaramente le applicazioni cloud utilizzate e non forniscono un punteggio di rischio per ogni applicazione utilizzata dai dipendenti. Per i dipendenti remoti che vengono reindirizzati attraverso il firewall NGFW utilizzando la VPN, la soluzione raccoglie ulteriori dettagli da questi log relativi alle azioni eseguite dagli utenti nell'ambito dei servizi cloud. Cloud App Security elabora i file di log dei firewall NGFW di SonicWall e mostra i servizi cloud utilizzati dagli utenti, i volumi di dati caricati e scaricati dal cloud e il rischio e la categoria di ogni servizio cloud. Di fatto, Cloud App Security consente all'infrastruttura esistente di interagire perfettamente con i servizi cloud. Con i dipendenti che utilizzano in misura sempre crescente le applicazioni cloud per lavoro, Cloud App Security consente agli amministratori di rilevare eventuali lacune nell'approccio alla sicurezza, di classificare le applicazioni cloud in applicazioni informatiche sanzionate e non e di adottare politiche di accesso per bloccare le applicazioni a rischio. Cloud App Security è una componente essenziale della visione di SonicWall per offrire funzioni di rilevamento automatizzato e di prevenzione in tempo reale delle violazioni ai clienti che adottano tecnologie cloud.



Individuare le attività informatiche nascoste in rete



SonicWall Cloud App Security individua e segnala i servizi informatici nascosti a rischio tramite un database IT di reputazione esclusivo dei servizi basati sul cloud gestito da SonicWall.

Alle applicazioni individuate vengono assegnati dei punteggi di rischio calcolati tramite un algoritmo basato sulla reputazione e sulle certificazioni di sicurezza e conformità. I responsabili informatici possono classificare le applicazioni per l'uso sulla base del punteggio di rischio come Sanzionate o Non sanzionate. Tramite Capture Security Center la soluzione consente ai responsabili di definire politiche di blocco/sblocco e di controllare le attività informatiche nascoste in rete.

Caratteristiche

FUNZIONALITÀ		VANTAGGIO
Visibilità	Cloud Application Discovery	Individua automaticamente le applicazioni nel cloud utilizzando i file di registro dei firewall SonicWall per individuare le attività nascoste in rete
	Visibilità dell'uso del cloud	Visualizzazione grafica in tempo reale delle applicazioni in uso, del volume di traffico, dell'attività degli utenti e delle sedi
	Valutazione dei rischi delle applicazioni	Assunzione di decisioni informate di blocco/sblocco delle applicazioni sulla base della valutazione del rischio
	Monitoraggio eventi	Monitoraggio delle singole azioni, compresi gli eventi in tempo reale e quelli storici, effettuato nell'ambiente SaaS aziendale
Sicurezza della posta elettronica di prossima generazione	Anti-phishing	Blocco degli attacchi di phishing progettati per aggirare la sicurezza predefinita di Office 365 o G Suite
	Anti-spoofing	Protezione del marchio aziendale e degli utenti dalle frodi mediante posta elettronica e dagli attacchi di impersonazione
	Sandboxing degli allegati	Blocca gli allegati nocivi ai messaggi di posta elettronica per impedire che arrivino nella casella di posta in arrivo degli utenti
	Protezione avanzata degli URL	Garantisce la protezione degli utenti dagli URL nocivi integrati
Protezione avanzata contro le minacce	Protezione contro i malware zero-day	Impedisce la memorizzazione e la propagazione dei malware tramite applicazioni come Box, Dropbox, OneDrive e G Drive
	Protezione contro la sottrazione degli account	Protegge le credenziali SaaS individuando il comportamento anomalo degli utenti, le violazioni dei permessi e la variazione delle configurazioni
Sicurezza dei dati	Classificazione dei dati	Identifica i dati sensibili o riservati ed applica le politiche a livello di SaaS per controllare come possono essere condivise le informazioni
	Controllo accessi incentrato sui dati	Gestisce i permessi dei file sulla base del tipo di dati che contengono
	Individuazione delle anomalie tramite flussi di lavoro	Garantisce che la messa in sicurezza dei dati non abbia ricadute sull'attività mediante esecuzione in tempo reale
Conformità	Modelli di conformità	Riduce il carico di lavoro amministrativo utilizzando semplici modelli di conformità per soddisfare i requisiti per SOX, PCI, HIPAA e GDPR
	Audit trail	Accede ai dati degli eventi storici per le verifiche di conformità retrospettiva e reportistica in tempo reale
	Attuazione delle politiche	Attua la conformità in tempo reale con ogni SaaS per controllare i permessi di accesso, spostare file, bloccare e modificare messaggi di posta elettronica e comunicare con utenti ed amministratori

SonicWall Cloud App Security	CLOUD APP SECURITY – VERSIONE BASE	CLOUD APP SECURITY – VERSIONE AVANZATA
Gestione cloud unificata (Capture Security Center)	●	●
Applicazioni cloud supportate	Selezionare 1 app SaaS (Office 365 o G Suite)	Scegliere fino a 10 app SaaS
Anti-phishing per O365 Mail o Gmail	●	●
Capture ATP* per allegati di posta elettronica	●	●
Protezione avanzata degli URL	●	●
Capture ATP* per file memorizzati in SaaS	●	●
Protezione contro la sottrazione degli account	●	●
Protezione contro le perdite di dati	—	●
Visibilità delle attività informatiche nascoste**	—	●

SonicWall Capture ATP comprende Real-Time Deep Memory Inspection™ (RTDMI™)
***Richiede SonicWall NGFW*

Informazioni per l'ordinazione di Cloud App Security:

Per informazioni sulle modalità di ordinazione di Cloud App Security e sui prezzi rivolgersi al proprio partner o all'ufficio vendite SonicWall qui.

Fare clic qui per richiedere una prova gratuita di 30 giorni di SonicWall Cloud App Security - Versione avanzata

Per ulteriori informazioni su Cloud App Security visitare www.sonicwall.com/casb.

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 sul sito www.sonicwall.com/PES.

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 e territori, 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 maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-US-VG-MKTG5359