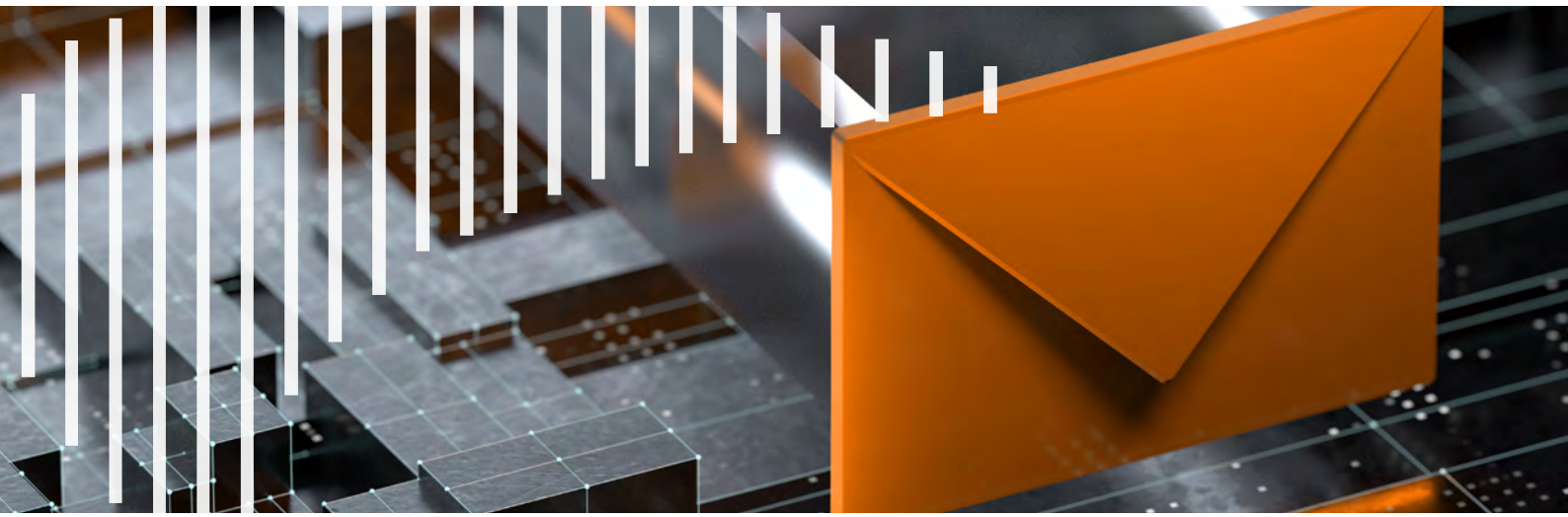


Protezione e-mail adattiva per l'era del cloud

Funzionalità essenziali per impedire alle minacce basate su e-mail di raggiungere la casella di posta elettronica

ABSTRACT

Il cloud è un agente di cambiamento inarrestabile. La sua efficienza, elasticità e scalabilità stanno spingendo le aziende a sostituire i loro strumenti di produttività on-premise e back-office, tra cui e-mail, collaborazione e condivisione dei file, con le nuove versioni cloud. L'adozione di queste applicazioni comporta tuttavia due problemi essenziali: sicurezza e disponibilità del servizio.

Questo documento descrive come la soluzione SonicWall Email Security combina le più recenti tecnologie di sicurezza e-mail per combattere minacce in continua evoluzione come phishing mirato, compromissione della posta elettronica aziendale (BEC), frodi degli account, perdite di dati e ransomware.

Introduzione

Quando si tratta di minacce trasmesse attraverso la posta elettronica, i criminali sono pronti a seguire le ultime tendenze. Il passaggio al telelavoro e la pandemia di COVID-19 sono due degli esempi più recenti di tendenze che hanno reso la comunicazione e-mail un vettore di attacco più redditizio per gli attacchi phishing e ransomware mirati. Come abbiamo imparato dalle violazioni di dati negli ultimi tempi, questi attacchi comportano spesso diverse tattiche, tecniche e procedure (TTP) per compromettere l'utente.

Questi eventi ripetuti hanno dimostrato che l'e-mail è spesso il primo strumento a fornire:

- L'URL incorporato iniziale che rimanda a un sito web di phishing offuscato o a un download dannoso.
- L'allegato che contiene un payload dannoso.
- L'inizio di un attacco di social engineering, ad esempio con frodi e-mail o attacchi per la raccolta delle credenziali.

Per bloccare queste minacce sofisticate, le aziende devono implementare un sistema di filtraggio dei contenuti e-mail costantemente aggiornato e in grado di apprendere e adattarsi a nuove tattiche, tecniche e procedure di phishing. Allo stesso tempo, l'analisi delle minacce avanzate del sistema può bloccare efficacemente attacchi di phishing personalizzato a basso volume e di alta qualità, compromissione della posta elettronica aziendale (BEC), impersonificazione e attacchi zero-day con maggiore accuratezza e meno falsi positivi.

La soluzione deve essere in grado di:

- Analizzare tutto il traffico e-mail – e non solo i messaggi in entrata e in uscita – poiché le minacce basate su e-mail e i furti di dati possono sfruttare account compromessi o la diffusione da un dipendente all'altro.
- Applicare tecniche di machine learning e intelligenza artificiale per rilevare attacchi di phishing difficili da riconoscere, progettati per ingannare gli utenti e aggirare i filtri di sicurezza. Queste tecniche includono il rilevamento di anomalie, frodi e attacchi BEC, l'elaborazione di linguaggi naturali, l'identificazione di indicatori chiave di compromissione e attacchi misti che sfruttano vulnerabilità in livelli di sicurezza noti.
- Eseguire la scansione delle e-mail nel cloud prima che arrivino alla casella di posta. Questo approccio permette alle aziende di ottenere il meglio di entrambe le opzioni e garantire la sicurezza per la casella di posta di ogni utente.

SOLUTION BRIEF

Architetture di SonicWall Email Security

La soluzione SonicWall Email Security offre un sistema di sicurezza ampio e completo, che fornisce una protezione ottimale sia per ambienti on-premise basati su Exchange sia per sistemi per ufficio nel cloud (ad es. Microsoft 365 o Google Workspace).

È possibile scegliere tra un approccio basato su gateway o su API a seconda delle proprie esigenze specifiche di implementazione. Entrambi utilizzano le tecnologie più recenti per rilevare forme complesse di phishing, compromissione della posta elettronica aziendale (BEC), frodi e-mail e attacchi di impersonificazione prima che raggiungano le caselle di posta elettronica degli utenti. Oltre a impedire che gli utenti vengano ingannati da questi schemi dannosi, la soluzione contribuisce anche a ridurre i rischi umani, eliminando potenziali decisioni o azioni sbagliate da parte degli utenti che potrebbero causare infezioni da ransomware, perdite di dati o violazioni della conformità.

Protezione delle e-mail basata su API

SonicWall Cloud App Security (CAS) è una soluzione di protezione della posta elettronica nativa del cloud, basata su API e progettata per bloccare attacchi di phishing e zero-day complessi di alta qualità. Questi attacchi mirati a basso volume vengono appositamente sperimentati sul campo per aggirare i filtri di sicurezza integrati di Microsoft e Google.

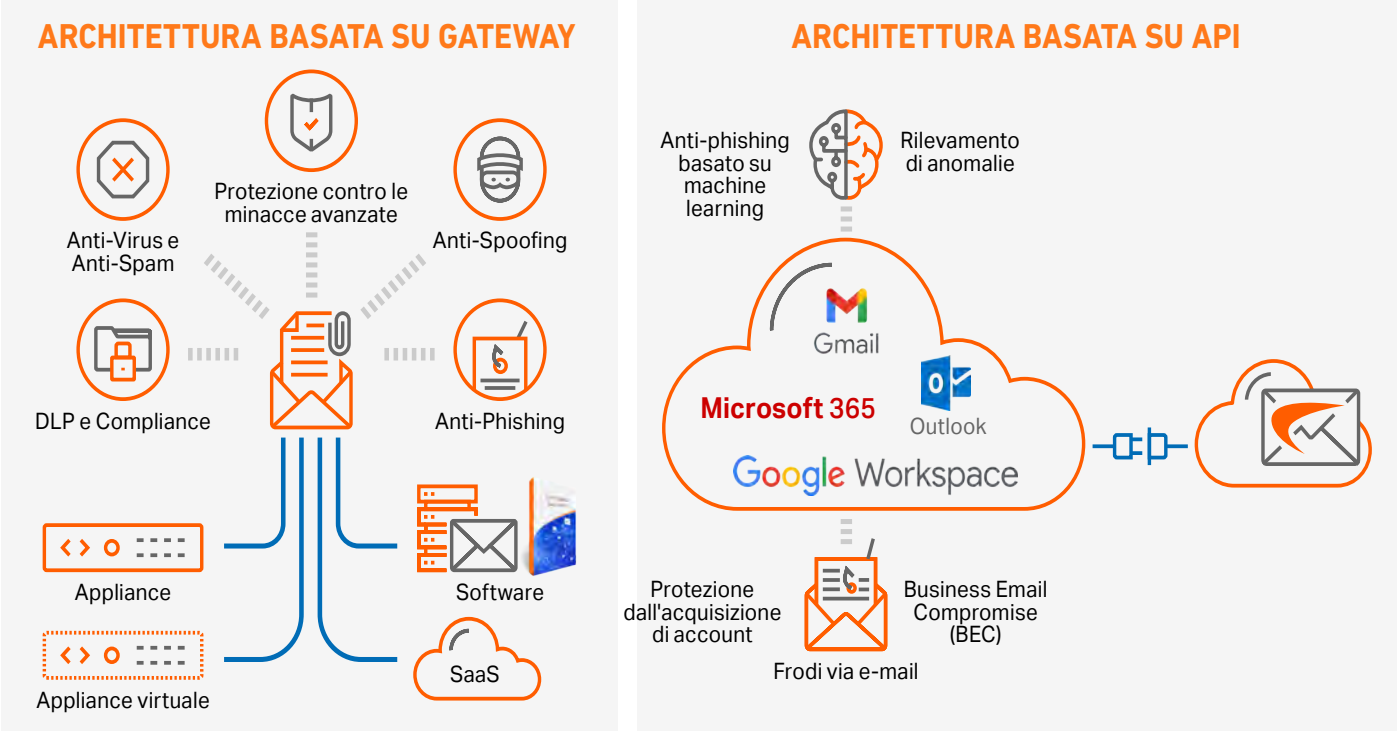
Attraverso le API, la soluzione si integra perfettamente nei workflow di sicurezza dei sistemi cloud per ufficio, dove viene ottimizzata per identificare gli attacchi che aggirano i filtri di sicurezza delle suite per ufficio nel cloud. Inoltre, il suo sistema di prevenzione delle minacce multilivello in linea è invisibile agli hacker e offre protezione completa per le applicazioni SaaS ed e-mail nel cloud.

NESSUN MESSAGGIO E-MAIL, LINK O ALLEGATO PUÒ RAGGIUNGERE LA CASELLA DI POSTA FINCHÉ CAS NON L'HA ESAMINATO E STABILITO CHE È INNOCUO AL 100%.

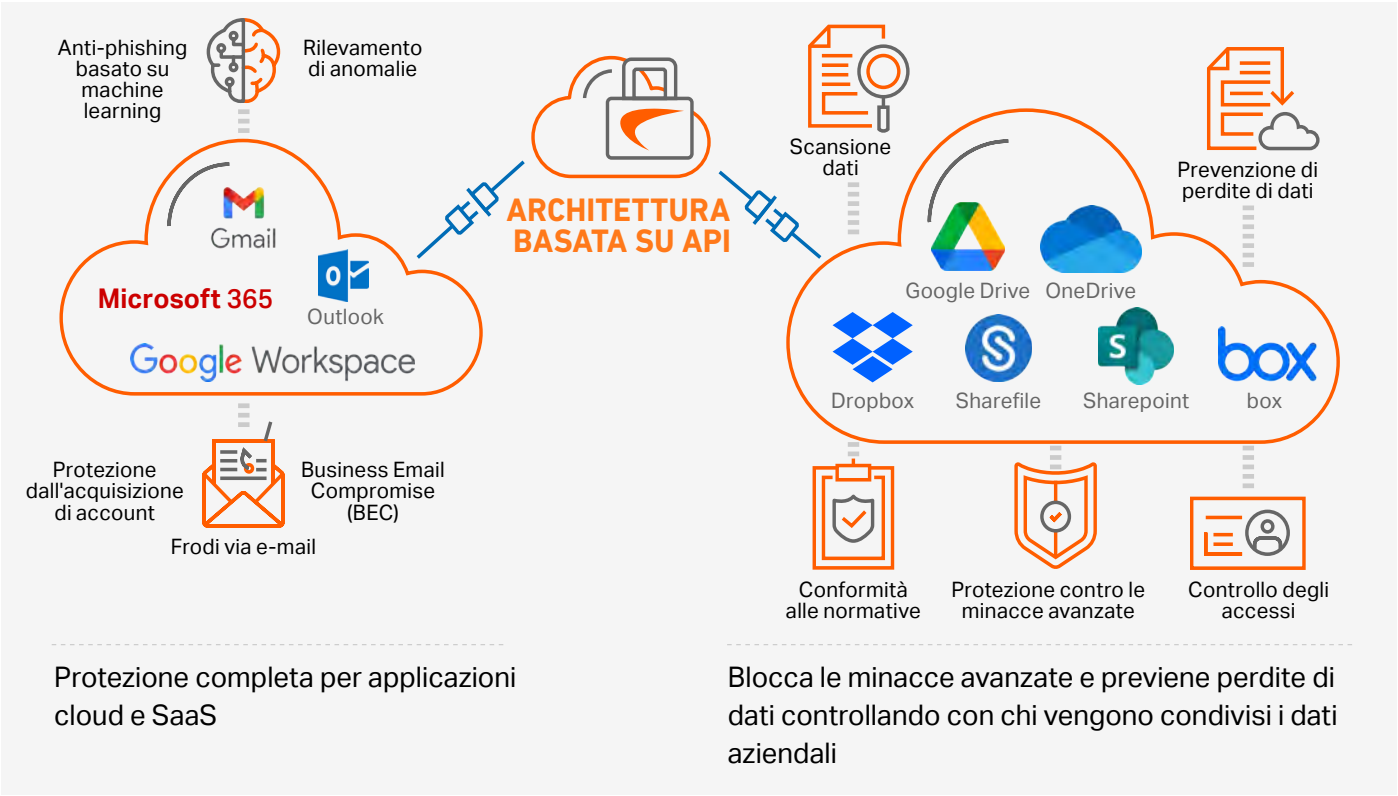
CAS è installabile nel giro di pochi minuti e utilizza le tecnologie di machine learning e intelligenza artificiale più recenti combinate all'analisi dei big data. L'intelligenza artificiale addestra dinamicamente e in modo continuo diversi motori di apprendimento automatico e di emulazione delle minacce per riconoscere e rilevare nuovi comportamenti di phishing e le loro tattiche, tecniche e procedure.

Questi motori analizzano centinaia di indicatori di minacce uniche, fornendo protezione efficace contro phishing, BEC

Tecnologie di SonicWall Email Security



SonicWall Cloud App Security



Protezione completa per applicazioni cloud e SaaS

Blocca le minacce avanzate e previene perdite di dati controllando con chi vengono condivisi i dati aziendali

(Business Email Compromise), sandboxing degli allegati, analisi time-of-click degli URL e frodi.

Un motore di machine learning è personalizzato specificamente per l'organizzazione, ossia addestrato in base all'ambiente specifico del cliente per identificare le minacce mirate in particolare contro l'organizzazione, consentendo una risposta personalizzata.

Un altro motore di machine learning è appositamente configurato per il rilevamento di anomalie e l'analisi del comportamento degli utenti. Questo motore esclusivo rileva le azioni o i comportamenti che risultano anomali nel contesto delle attività storiche di un'organizzazione e degli utenti. Il motore analizza analizza il comportamento tramite algoritmi di machine-learning che creano un profilo basato sulle informazioni storiche degli eventi, comprese le posizioni di accesso e gli orari, il comportamento di trasferimento dei dati e i modelli dei messaggi e-mail. Al rilevamento di anomalie viene generato un evento di sicurezza che fornisce il contesto e altre informazioni necessarie per le indagini.

CAS esegue l'analisi preliminare di tutti i messaggi, incluse le e-mail in entrata, in uscita e interne. Nessun messaggio e-mail, link o allegato può raggiungere la casella di posta finché CAS non l'ha esaminato e stabilito che è innocuo al 100%. Le notifiche impostabili segnalano potenziali violazioni al personale competente, ad esempio un amministratore o un analista di sicurezza, in modo che possa adottare misure di risoluzione o ripristino anche dopo l'invio di un messaggio.

Protezione delle e-mail basata su gateway

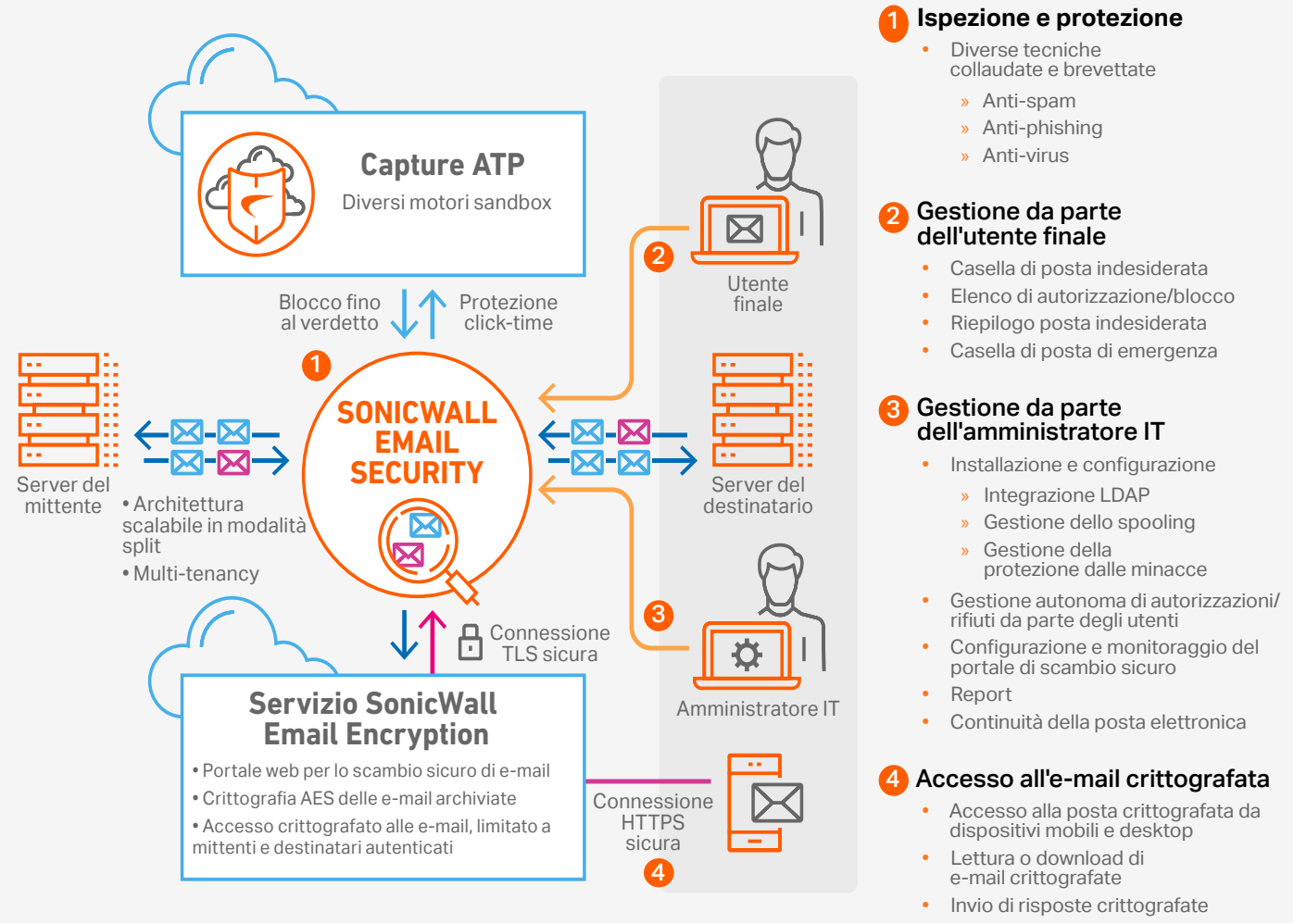
La soluzione gateway SonicWall Email Security combina intelligenza artificiale e tecniche di machine learning con funzionalità di euristica e analisi della reputazione e del contenuto per garantire una protezione completa contro attacchi mirati di phishing, spoofing e ransomware.

La linea di difesa iniziale elimina fino al 99% dello spam facile da rilevare a livello di connessione, prima che abbia la possibilità di accedere alla rete. Advanced Management Content (ACM) di SonicWall analizza e filtra le eventuali e-mail dannose restanti. Il sistema di scansione di ACM blocca in modo efficace le campagne di phishing e di impersonificazione più avanzate utilizzando le analisi Adversarial Bayesian™. Le tecniche utilizzano motori avanzati di analisi di testi e immagini, distanza lessicografica, analisi dell'immagine (bianco su bianco, caratteri minuscoli ecc.) e rilevamento di frasi senza senso per scoprire le tattiche, tecniche e procedure usate dalle campagne di phishing per nascondere il loro intento dannoso.

ACM analizza ogni parte del componente e-mail (ad es. metadati, corpo, oggetto, allegati, URL, ecc.) per garantire la conformità alle policy aziendali. Le e-mail non conformi vengono poi bloccate o reinstradate a gruppi o persone LDAP pertinenti per richiedere l'approvazione.

Email Security si integra anche con il sistema LDAP aziendale per prevenire gli attacchi DHA (Directory Harvest Attacks). Inoltre utilizza feed di firme anti-virus leader del settore

Email Security – Protezione basata su gateway



costantemente aggiornati per fornire una protezione avanzata contro il malware. Allo stesso tempo applica diversi standard di autenticazione delle e-mail come SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting and Conformance) per bloccare attacchi di spoofing, compromissione della posta elettronica aziendale e frodi via e-mail.

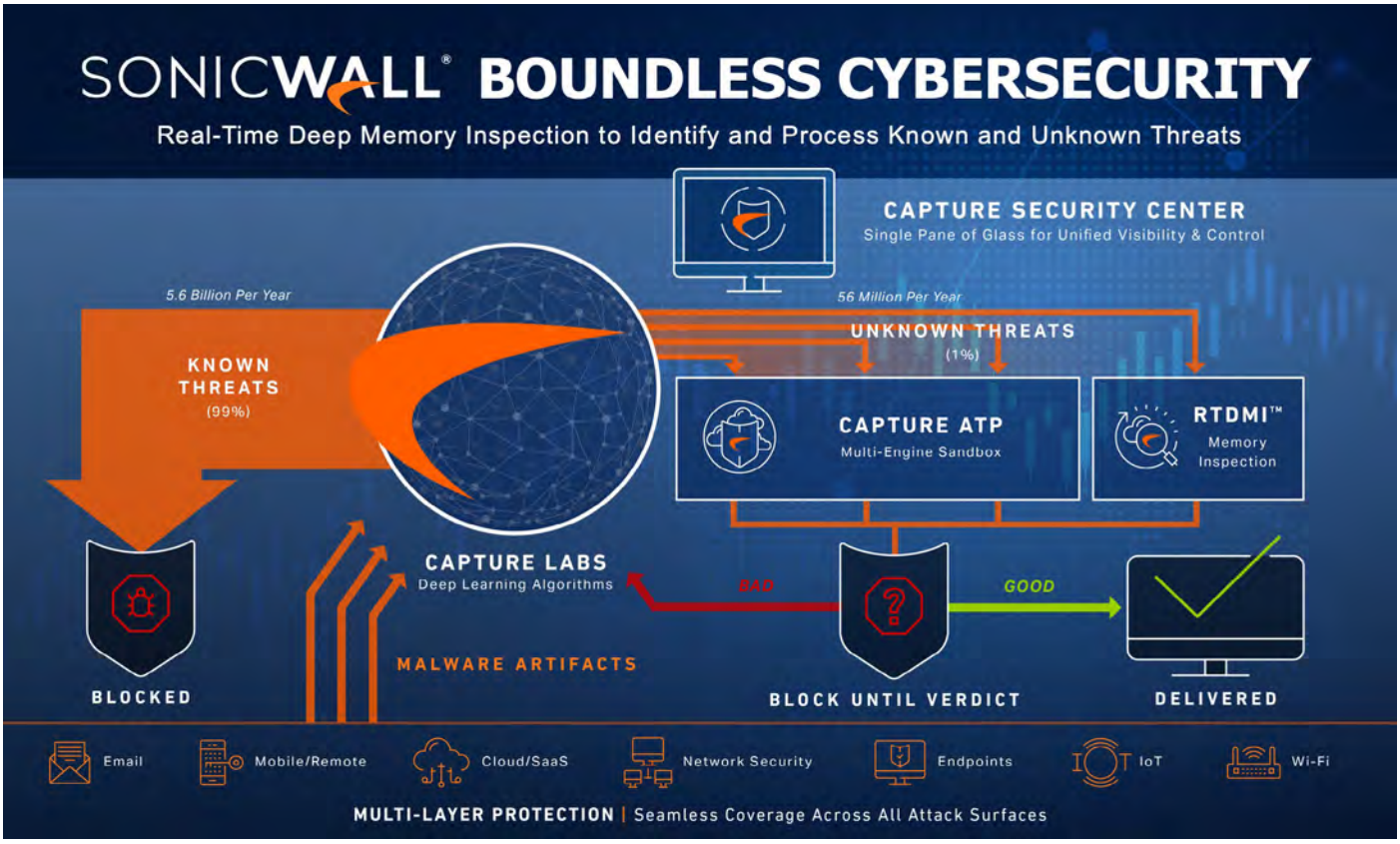
Rilevamento di attacchi BEC e frodi via e-mail

La scienza alla base del riconoscimento e blocco degli attacchi di compromissione della posta elettronica aziendale (BEC), di impersonificazione e delle frodi è il contesto interno. Uno dei principali vantaggi dell'approccio basato su API di CAS nel servizio e-mail nel cloud è l'accesso immediato allo storico delle conversazioni. L'intelligenza artificiale di CAS analizza fino a cinque giorni di dialoghi e-mail, nel giro di poche ore dopo l'installazione, per stabilire l'attendibilità e l'autenticità dei mittenti.

Allo stesso tempo crea una rete di reputazione con apprendimento continuo delle relazioni e dei comportamenti dei mittenti, garantendo un rilevamento accurato di eventuali attacchi BEC e riducendo il numero di falsi positivi che affliggono la maggior parte delle altre soluzioni e-mail. Il processo di ottimizzazione, che in genere richiede mesi con altre soluzioni di sicurezza, avviene in modo immediato e automatico utilizzando milioni di conversazioni e-mail passate. La soluzione è anche in grado di riconoscere comunicazioni anomale degli utenti, mentre altre soluzioni avrebbero difficoltà a rilevare questo tipo di e-mail.

Rilevamento di anomalie e acquisizioni di account

Le anomalie sono spesso un indicatore di possibili account compromessi. CAS utilizza un motore proprietario di rilevamento delle anomalie per monitorare le azioni o i comportamenti che risultano anomali nel contesto delle attività storiche di un utente. Mediante algoritmi di machine-learning, il motore analizza queste irregolarità e crea dei profili in base alle informazioni sugli eventi passati di ogni utente, comprese le posizioni di accesso e gli orari, il comportamento di trasferimento dei dati e i modelli dei messaggi e-mail. Se vengono rilevate anomalie, la soluzione genera eventi di sicurezza e avvisi con relativo contesto e altre informazioni necessarie e li invia agli analisti e ai



responsabili degli incidenti per consentire eventuali indagini e misure correttive.

Protezione contro le minacce avanzate

I prodotti SonicWall per la protezione della posta elettronica sono parte integrante della piattaforma SonicWall Capture Cloud. In questo modo interagiscono perfettamente con l'intera gamma di prodotti di sicurezza SonicWall – inclusi i firewall e le soluzione di protezione degli endpoint e sicurezza dell'accesso – e garantiscono una gestione sincronizzata delle minacce.

Inoltre utilizzano il servizio SonicWall Capture ATP con tecnologia Real-Time Deep Memory Inspection™ (RTDMI), l'unico sistema di rilevamento delle minacce avanzate pluripremiato che utilizza motori di sandboxing multipli per analizzare gli allegati sospetti e gli URL all'interno delle e-mail.

Il brevettato motore di analisi dei file RTDMI di SonicWall analizza i file sospetti monitorando il comportamento dannoso di un'applicazione in memoria. RTDMI rileva qualsiasi tecnica di offuscamento o crittografia che un malware può implementare per eludere l'analisi sandbox, fornendo un rilevamento estremamente accurato degli attacchi incorporati in documenti, file eseguibili, file di archivio e altri tipi di file.

RTDMI funziona anche in combinazione con l'analisi statica della reputazione e i controlli degli hash globali di altre soluzioni di intelligence sulle minacce per fornire risultati rapidi. Una volta rilevate varianti di malware e ransomware mai viste prima, queste vengono utilizzate per creare delle signature per una parte della catena di difesa, che immediatamente vengono messe a disposizione dell'intero ecosistema di difesa multilivello di SonicWall in tempo reale. **L'intero processo viene eseguito in pochi secondi, riducendo in modo significativo la finestra di esposizione**.

Protezione anche dopo la consegna

La pandemia di COVID-19 del 2020 ha creato la forza lavoro maggiormente distribuita nella storia dell'umanità, con miliardi di persone che usano ogni giorno la posta elettronica nel comfort delle proprie case. Purtroppo, molte di loro non sono state addestrate per distinguere le e-mail legittime da quelle false o riconoscere link sospetti. L'aspetto più preoccupante è che oggi le e-mail di phishing possono apparire autentiche anche agli utenti più esperti di sicurezza.

Come sappiamo, nessun dipendente è perfetto: basta un semplice clic, un download sbagliato o un attimo di disattenzione per mettere in moto il processo di infezione. Per ridurre efficacemente il rischio umano, SonicWall ha aggiunto la **protezione CTP (Click-Time Protection)**. Conosciuta anche come protezione Time-of-Click, questa funzione di sicurezza post-consegna è stata appositamente progettata come misura di sicurezza aggiuntiva per proteggere gli

utenti dai propri errori inconsapevoli e, di conseguenza, per risparmiare potenziali disastri alle aziende.

La funzione principale di CTP consiste nell'esaminare ogni URL e allegato quando l'utente clicca su un link o scarica un file incorporato in un'e-mail, anche se è inoltrato a un'altra persona. Un motore di scansione in tempo reale rileva e mette in quarantena gli URL errati, quindi informa gli utenti tramite una schermata di notifica. Inoltre, se l'URL sospetto è associato a una campagna di phishing, CTP può richiamare ed eliminare i messaggi e-mail dannosi utilizzati dalla stessa campagna.

Prevenzione di perdite di dati

Email Security basato su gateway e le soluzioni CAS dispongono di un proprio modulo di conformità alla sicurezza, che consente di controllare come e con chi vengono condivisi i dati dell'azienda. Entrambe le soluzioni consentono di stabilire e sincronizzare criteri unificati di crittografia e prevenzione della perdita di dati (DLP) per gli utenti e le applicazioni per ufficio basate sul cloud. Inoltre attingono a più di un centinaio di tipi di informazioni e supportano classificatori di dati da oltre 40 paesi.

La soluzione analizza tutte le parti dell'e-mail e delle comuni applicazioni di condivisione in cloud, inclusi gli allegati, per garantire che i dati di proprietà intellettuale, le informazioni personali identificabili (PII) e altri dati di conformità non escano dalla rete dell'organizzazione per errore o deliberatamente. La soluzione fornisce inoltre modelli di policy conformi a HIPAA, SOX, PCI, GDPR e altre normative per facilitare la preparazione agli audit e ai criteri di conformità.

Conclusioni

Le soluzioni SonicWall Email Security applicano le più recenti tecnologie di intelligenza artificiale e apprendimento automatico per rilevare attacchi mirati di phishing, BEC e impersonificazione delle e-mail prima che raggiungano la casella di posta elettronica.

Scoprite come le soluzioni SonicWall Email Security possono proteggere la vostra azienda dalle minacce avanzate basate su e-mail.

www.sonicwall.com/email-security

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla nuova "normalità iperdistribuita", in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibile economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni potete 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

SolutionBrief-AdaptiveEmailSecurity-COG-5189