Servizio SonicWall Capture Advanced Threat Protection

Rilevamento e blocco di attacchi zero-day e di altre minacce sconosciute

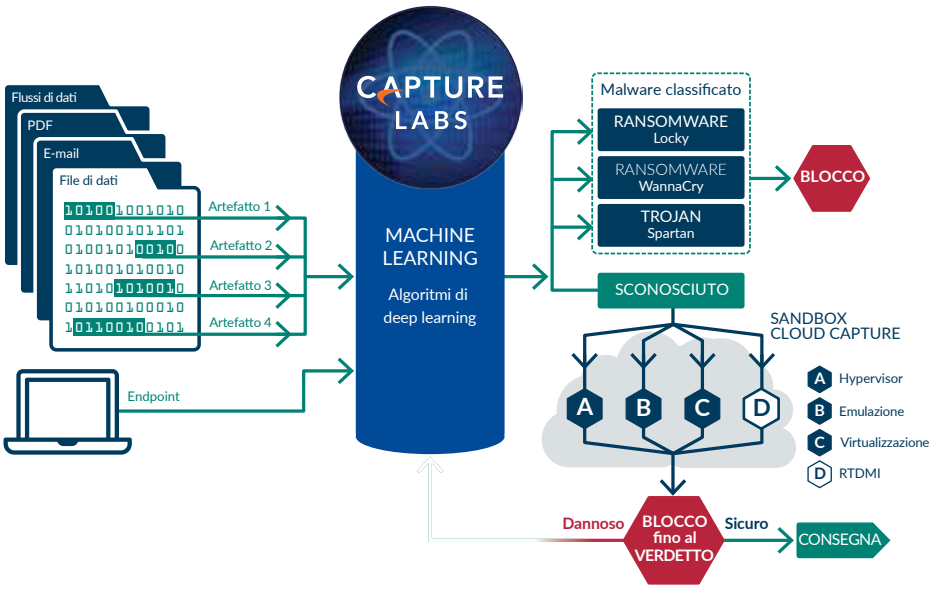
Per proteggersi in maniera efficace dalle minacce zero-day, le aziende hanno bisogno di soluzioni basate su tecnologie di analisi del malware che siano in grado di rilevare il malware e le minacce evasive avanzate odierne e quelle future.

SonicWall Capture Advanced Threat Protection, un servizio basato su cloud per i firewall SonicWall, protegge i clienti dal crescente pericolo delle minacce zero-day rilevando e bloccando le minacce avanzate al gateway finché non viene identificata la loro natura. Questo è l'unico servizio di rilevamento delle minacce avanzate che utilizza il sandboxing multilivello in combinazione con la tecnologia Real-Time Deep Memory Inspection (RTDMI™) di SonicWall, l'emulazione completa del sistema e tecniche di virtualizzazione per analizzare il comportamento del codice sospetto. Questa potente combinazione consente di rilevare più minacce rispetto alle soluzioni sandbox basate su un unico motore, che sono specifiche per l'ambiente di calcolo e suscettibili a tecniche di evasione.

La soluzione scansiona il traffico ed estrae il codice sospetto per sottoporlo all'analisi, ma a differenza di altre soluzioni gateway, analizza un'ampia varietà di tipologie e dimensioni di file. Un'infrastruttura di intelligence globale delle minacce distribuisce rapidamente le firme di riparazione delle minacce appena rilevate a tutte le appliance di sicurezza di rete SonicWall, prevenendo un'ulteriore infiltrazione. Per i clienti, questo si traduce in un'elevata efficacia in termini di

Vantaggi:

- Protezione altamente efficace contro le minacce sconosciute
- La distribuzione delle firme quasi in tempo reale protegge da attacchi successivi
- Costo totale di proprietà ridotto
- Blocco dei file al gateway fino al verdetto
- Motori multipli elaborano i file in parallelo per fornire rapidamente un verdetto
- Il motore RTDMI di SonicWall blocca il malware sconosciuto utilizzando tecniche di ispezione in tempo reale basate sulla memoria



Una soluzione multi-engine basata su cloud per bloccare gli attacchi sconosciuti e zero-day al gateway

Per garantire la migliore protezione contro le minacce zero-day, la soluzione viene aggiornata dinamicamente con nuove tecnologie di analisi del malware per stare al passo con l'evolversi delle minacce informatiche.

sicurezza, in tempi di risposta rapidi e in una riduzione del costo totale di proprietà.

Caratteristiche

Analisi multi-engine delle minacce avanzate – Il servizio SonicWall Capture ATP estende la protezione dalle minacce del firewall per rilevare e prevenire gli attacchi zero-day. Il firewall ispeziona il traffico, identifica e blocca le intrusioni e il malware conosciuto. I file sospetti vengono inviati al servizio SonicWall Capture ATP nel cloud per essere analizzati. La piattaforma sandbox multi-engine, che include il motore RTDMI, la piena emulazione di sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità sulle attività dannose, potenziando la resistenza alle tattiche di elusione e aumentando il rilevamento di minacce zero-day.

Real-Time Deep Memory Inspection (RTDMI) – Il servizio Capture ATP multi-engine di SonicWall è ulteriormente potenziato dalla nostra tecnologia d'ispezione 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. Grazie all'architettura in tempo reale, la tecnologia RTDMI di SonicWall è precisa, riduce il numero di falsi positivi e consente di identificare e mitigare gli attacchi sofisticati.

Analisi di vari tipi di file – Il servizio supporta l'analisi di file di svariate tipologie e dimensioni, tra cui programmi eseguibili (PE), DLL, documenti PDF e MS Office, archivi, JAR e APK, su diversi sistemi operativi come Windows e Android. Gli amministratori possono personalizzare la protezione selezionando o escludendo i file da sottoporre all'analisi nel cloud in base a tipo o dimensione di file, mittente, destinatario o protocollo. Inoltre è possibile inviare manualmente singoli file al servizio di analisi nel cloud.

Blocco fino all'identificazione – Per impedire l'ingresso di file potenzialmente dannosi nella rete, i file inviati al servizio di analisi cloud possono essere trattenuti al

La pagina dei rapporti di SonicWall Capture ATP offre una vista immediata dei risultati giorno per giorno. Le barre colorate sui rapporti indicano i giorni il cui è stato rilevato del malware. Gli amministratori possono cliccare su singoli risultati di un giorno specifico e applicare filtri per visualizzare rapidamente i file dannosi con i relativi risultati.

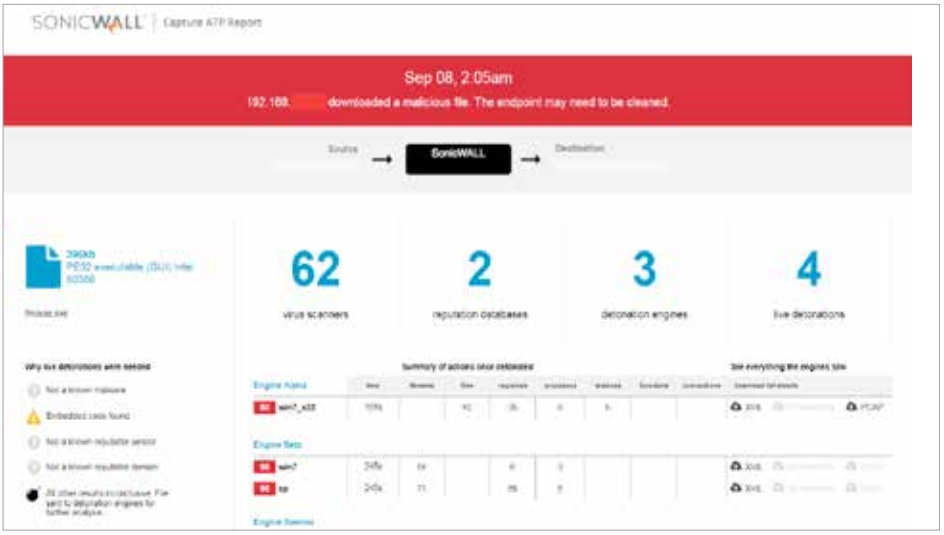
gateway finché non viene determinata la loro natura.

Rapida distribuzione delle firme di riparazione – Quando un file viene identificato come dannoso, una firma corrispondente è immediatamente disponibile per i firewall abbonati al servizio SonicWall Capture ATP, in modo da prevenire attacchi successivi. Inoltre, il malware viene ulteriormente analizzato dal team di ricerca delle minacce del SonicWall Capture Labs e incluso nei database delle firme di Gateway Anti-Virus e IPS con informazioni dettagliate sulla minaccia. Entro 48 ore, queste informazioni vengono inviate anche ai database di reputazione degli URL, degli IP e dei domini.

Report e avvisi – Il servizio SonicWall Capture ATP offre un dashboard intuitivo per l'analisi delle minacce e rapporti con risultati dettagliati dell'analisi per i file che sono stati inviati al servizio, con informazioni come sorgente e destinazione, e un riepilogo accurato della reazione del malware dopo la detonazione. Gli avvisi relativi ai log dei firewall forniscono notifiche su file sospetti inviati al servizio SonicWall Capture ATP e sull'esito dell'analisi dei file.

Informazioni su SonicWall

Da oltre 27 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 rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza.



Per i file analizzati è anche disponibile un report dettagliato dell'analisi per facilitare l'eventuale correzione.

PIATTAFORME SUPPORTATE

Il servizio SonicWall Capture ATP è supportato sui seguenti firewall SonicWall con sistema SonicOS 6.2.6 e superiore:

NS*sp* 12800
NS*sp* 12400

NS*a* 9650
NS*a* 9450
NS*a* 9250
NS*a* 6650
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

TZ600 Series
TZ500 Series
TZ400 Series
TZ300 Series

NSv 1600
NSv 800
NSv 400
NSv 300
NSv 200
NSv 100
NSv 50
NSv 25
NSv 10

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

DataSheet-CaptureAdvancedThreatProtection-US-VG-MKTG4093