SonicWall® CAPTURE ADVANCED THREAT PROTECTION SERVICE

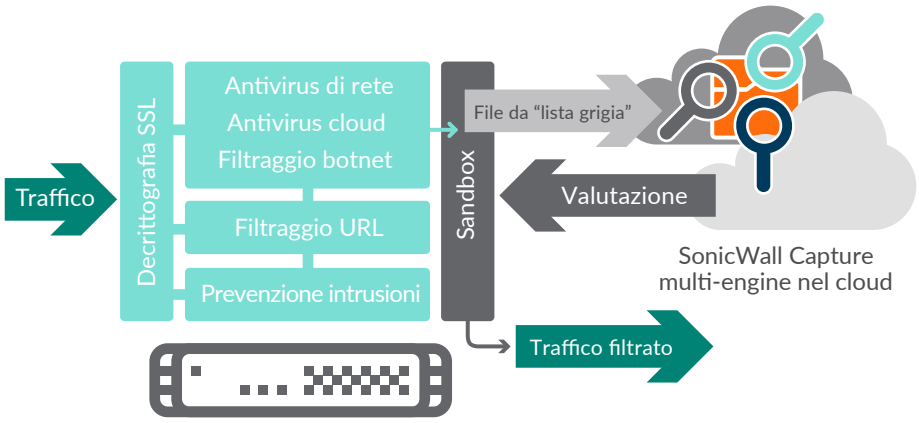
Moltiplicate l'efficacia del vostro sandbox avanzato di protezione dalle minacce

Per ottenere una protezione efficace contro le minacce zero-day le aziende necessitano di soluzioni che includano tecnologie di analisi del malware e che siano in grado di rilevare minacce e malware avanzati di tipo evasivo, oggi e domani.

Per proteggere i clienti contro i sempre maggiori pericoli delle minacce zero-day, SonicWall Capture Advance Threat Protection Service, un servizio basato sul cloud disponibile con i firewall SonicWall, è in grado di rilevare e bloccare al gateway le minacce avanzate fino al verdetto. Questo servizio è l'unico tipo di rilevamento di minacce avanzate abbinato a sandbox multi-livello, comprese tecniche complete di emulazione e virtualizzazione dei sistemi, per analizzare il comportamento di codice sospetto.

Questa potente combinazione rileva più minacce rispetto alle soluzioni sandbox single-engine, le quali sono specifiche per un dato ambiente di calcolo e suscettibili di evasione.

La soluzione esegue la scansione del traffico ed estrae il codice sospetto per l'analisi, ma, a differenza di altre soluzioni gateway, analizza un'ampia gamma di dimensioni e tipi di file. L'infrastruttura di intelligence contro le minacce globali implementa rapidamente firme di remediation per le nuove minacce identificate mettendole a disposizione di tutte le appliance di sicurezza di rete SonicWall, prevenendo quindi ulteriori infiltrazioni. I clienti traggono beneficio dall'efficacia ad alta sicurezza, da rapidi tempi di risposta e da un ridotto costo totale di proprietà.



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

Vantaggi:

- Elevata efficacia di sicurezza contro le minacce sconosciute
- Implementazione delle firme quasi in tempo reale per proteggere dagli attacchi successivi
- Ridotto costo totale di proprietà

Per una migliore protezione contro le minacce zero-day, l'architettura della soluzione consente di aggiungere dinamicamente nuove tecnologie di analisi del malware seguendo l'evoluzione del panorama delle minacce.

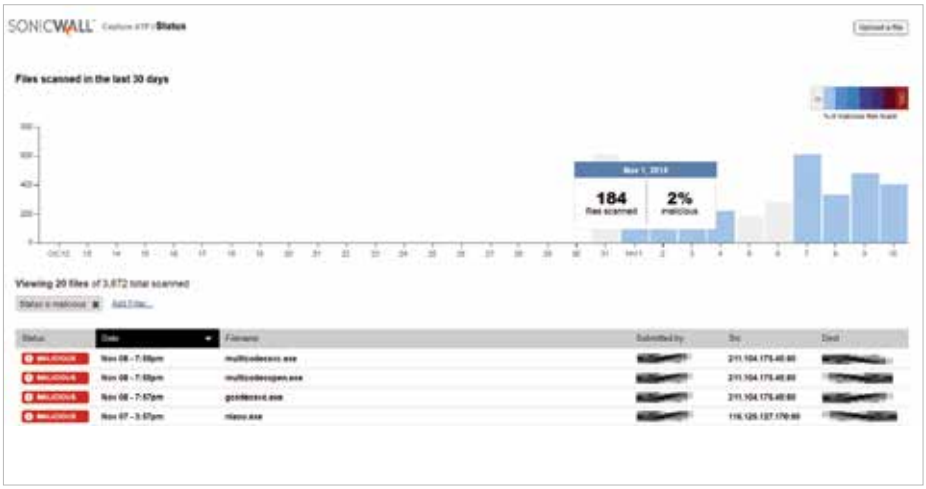
Caratteristiche

Analisi delle minacce avanzate multi-engine — SonicWall Capture Service estende la protezione dalle minacce del firewall per rilevare e prevenire gli attacchi zero-day. Il firewall ispeziona il traffico e, quindi, rileva e blocca le intrusioni e il malware noto. I file sospetti vengono inviati al servizio cloud SonicWall Capture per l'analisi. La piattaforma sandbox multi-engine, che include sandboxing virtualizzato, tecnologia completa di emulazione del sistema e analisi a livello hypervisor, esegue il codice sospetto e ne analizza il comportamento, consente una visibilità completa dell'attività pericolosa, resistendo al tempo stesso alle tattiche di evasione e massimizzando il rilevamento delle minacce zero-day.

Analisi per un'ampia gamma di tipi di file — Il servizio supporta l'analisi di una grande varietà di dimensioni e tipi di file, inclusi i programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a numerosi sistemi operativi, inclusi Windows e Android. Gli amministratori possono personalizzare la protezione selezionando o escludendo i file da inviare al cloud per l'analisi per tipo di file, dimensione del file, mittente, destinatario o protocollo. Inoltre, gli amministratori possono inviare manualmente i file al servizio cloud per l'analisi.

Blocco fino al verdetto — Per evitare che i file potenzialmente dannosi entrino nella rete, i file inviati al servizio cloud per l'analisi possono essere trattenuti al gateway fino all'emissione di un verdetto.

Rapida implementazione di firme di remediation — Quando un file viene identificato come dannoso, una firma viene immediatamente resa disponibile ai firewall con abbonamenti SonicWall Capture per prevenire attacchi successivi. Inoltre, il malware viene inviato al SonicWall Threat Intelligence Team per un'ulteriore analisi e per l'inclusione nei database di firme Gateway Anti-Virus e IPS insieme alle informazioni sulla minaccia. Inoltre, esso viene inviato a database URL, IP e di reputazione dei domini entro 48 ore.

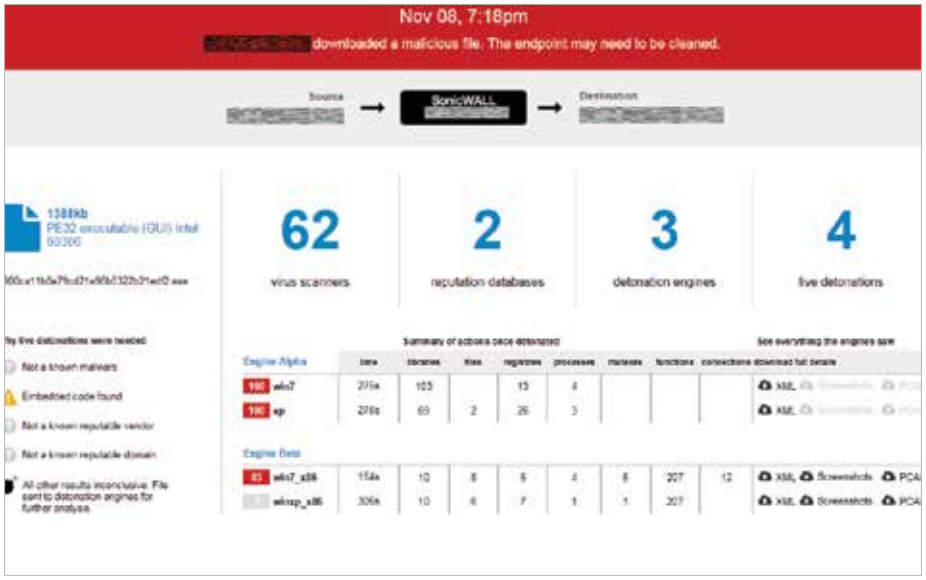


La pagina dei rapporti di SonicWall Capture offre una vista immediata dei risultati giorno per giorno. Le barre colorate sui rapporti indicano i giorni il cui è stato rilevato del malware. Gli amministratori possono cliccare su singoli risultati di un giorno specifico e applicare filtri per visualizzare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

Report e avvisi — Il SonicWall Capture Service fornisce cruscotti e report riassuntivi di analisi delle minacce, che contengono risultati dettagliati dell'analisi per i file inviati al servizio, con origine, destinazione e un riepilogo dettagliato dell'azione del malware una volta attivato. Gli avvisi di log del firewall forniscono la notifica dei file sospetti inviati al SonicWall Capture Service e il verdetto dell'analisi dei file.

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla sicurezza della rete alla protezione degli accessi fino alla sicurezza dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti consentendo alle organizzazioni di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall permette ai suoi clienti di guardare al futuro con fiducia.



Inoltre è disponibile un report di analisi dettagliato per il file analizzati per agevolare la remediation.

PIATTAFORME SUPPORTATE

SonicWall Capture Service è supportato sulle seguenti appliance di sicurezza di rete SonicWall con sistema operativo SonicOS 6.2.5 e superiore:

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NSA 5600
NSA 4600
NSA 3600
NSA 2600

TZ600
TZ500 e TZ500 Wireless
TZ400 e TZ400 Wireless
TZ300 e TZ300 Wireless

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Per gli utenti al di fuori del Nord America i contatti delle sedi più vicine sono riportati sul nostro sito Web.
www.sonicwall.com

DataSheet-AdvancedThreatProtection-EU-IMAG-26742