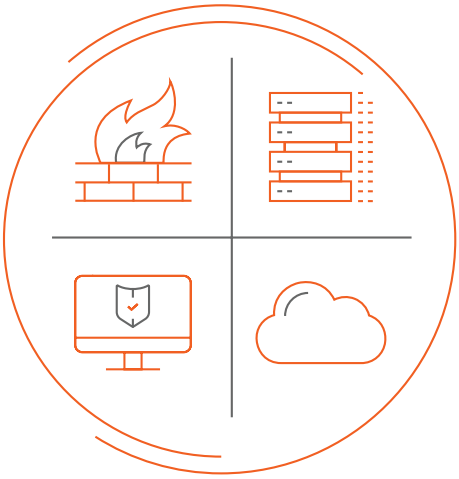
SONICWALL®

SonicWall Managed Detection and Response (MDR)

Protezione per i vostri endpoint, garantita dalla nostra competenza.



Managed Detection and Response (MDR) è un servizio completo che include monitoraggio delle minacce 24x7, ricerca proattiva, rilevamento e risposta alle minacce. Il servizio MDR di SonicWall, fornito da Solutions Granted, utilizza analisi avanzate, intelligence delle minacce e competenze umane per fornire indagini e risposte sofisticate e approfondite agli incidenti. Sono inoltre disponibili la convalida degli incidenti e servizi di risposta remota come il contenimento delle minacce. In questo modo avete la certezza di essere nelle mani migliori anche nel peggiore scenario possibile.

- Rilevamento di minacce avanzate agli endpoint che potrebbero eludere le altre vostre difese
- Servizi di sicurezza proattivi per i vostri clienti grazie a un SOC 24x7 gestito da esperti con le più recenti informazioni sulle minacce
- Prevenzione della diffusione di ransomware con isolamento automatico della rete e interruzione dei processi ransomware
- Riduzione dell'affaticamento da avvisi e dei falsi positivi
- Integrazione con SonicWall Capture Client per una piattaforma di gestione unificata semplice da utilizzare o abbinamento a servizi Windows Defender o SentinelOne esistenti

"Il SOC di Solutions Granted ha rilevato attività anomale sul server di un cliente alle 2 di notte. Siamo riusciti a contenere la violazione nella fase iniziale. Dormo sonni più tranquilli, sapendo che Solutions Granted sorveglia le mie reti".

DAN BROWNE, CEO, DMB NETWORKS

Scopri i vantaggi di una vera partnership con un fornitore di sicurezza: maggiore visibilità sul tuo ecosistema e risposte rapide dal nostro SOC presidiato 24x7x365.

Per conoscere l'ampia gamma di vantaggi riservati ai partner SonicWall SecureFirst, contattaci subito!

partnerdevelopment@sonicwall.com

TECNOLOGIE COMPROVATE. PROTEZIONE SUPERIORE.

Ecco come SonicWall MDR migliora la sicurezza e ottimizza le risorse:

DISTRIBUZIONE BASATA SU AGENTE

Presso gli endpoint vengono installati degli agenti leggeri che offrono un accesso costante e continuo e consentono il monitoraggio e la raccolta di dati in tempo reale.

RILEVAMENTO BASATO SU ANOMALIE

Mediante l'euristica, l'analisi statistica e il machine learning, l'agente individua qualsiasi evento o caratteristica atipica di un artefatto o di un file, facilitando il rilevamento di minacce avanzate o zero-day.

Il rilevamento basato su anomalie include:

- Monitoraggio in tempo reale di processi e script
- Analisi continua della memoria in diretta
- Rilevamento di attacchi basati su PowerShell o altre tecniche tipo Living Off the Land (LOTL)
- Prevenzione dell'abuso di account degli utenti e di strumenti di amministrazione legittimi
- Blocco di minacce che utilizzano movimenti laterali

RILEVAMENTO BASATO SUL COMPORTAMENTO

Il motore di analisi comportamentale ispeziona i processi e gli eventi legittimi per rilevare eventuali comportamenti sospetti. Queste anomalie vengono poi catalogate in base alle tattiche, tecniche e procedure (TTP) di attacco note, descritte nella matrice MITRE ATT&CK. Concentrandosi su 20 delle più comuni tecniche ATT&CK, SonicWall MDR è estremamente efficace nel rilevare e bloccare le minacce.

ANALISI DI STATO FORENSE

L'agente può raccogliere e analizzare dati dagli endpoint in tempo reale, inclusa la memoria volatile e non volatile. Ciò consente l'ispezione proattiva di migliaia di host per rilevare compromissioni attuali e passate e aiuta a identificare la causa principale degli attacchi rilevati. L'analisi può essere condotta senza agente o tramite l'agente ARR.

L'analisi di stato forense include:

- Processi e script attivi
- Triage della memoria volatile in tempo reale
- Registro ed esecuzione automatica (chiavi di esecuzione, cartelle di avvio, file lnk, schtask/cron, ecc.)
- Artefatti di esecuzione (shimcache, amcache, prefetch)
- Sottoversione del sistema operativo (hook delle API, controlli disabilitati)
- Triage del registro eventi locale
- Account privilegiati
- Applicazioni installate e vulnerabilità
- Connessioni host attive e listener

MONITORAGGIO CONTINUO, RISPOSTA E ANALISI FORENSE DEGLI ENDPOINT

La ricerca proattiva e il monitoraggio delle minacce avanzate aggiungono un ulteriore livello di sicurezza. Questa funzionalità identifica i comportamenti principali rilevati durante e dopo un attacco. L'analisi forense automatizzata consente ai nostri esperti di verificare in modo proattivo l'integrità degli endpoint e di determinare rapidamente la causa principale una volta rilevata una violazione. MDR semplifica e accelera l'identificazione, l'indagine e la risposta a cyber attacchi sofisticati.

SonicWall

SonicWall fornisce soluzioni di cybersecurity stabili, scalabili e senza soluzione di continuità per la 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 possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

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