SonicWall Capture Client

Blocca le violazioni a una velocità senza precedenti e in modo autonomo

La crescente minaccia posta dal ransomware e da altri attacchi basati su malware ha dimostrato che l'efficacia di una soluzione di protezione dei client non è misurabile solo in termini di compliance degli endpoint. La tecnologia antivirus tradizionale utilizza un approccio basato su firme ormai superato, che non è riuscito a tenere il passo con il malware e le tecniche di elusione emergenti.

Inoltre, con la diffusione di fenomeni come il telelavoro, la mobilità e il BYOD, è più che mai indispensabile garantire una protezione costante, il controllo delle vulnerabilità delle applicazioni, l'implementazione di policy web e altro ancora per gli endpoint, ovunque essi siano. SonicWall Capture Client è una soluzione unificata che offre molteplici funzionalità di protezione e di rilevamento e risposta (EDR) per gli endpoint.

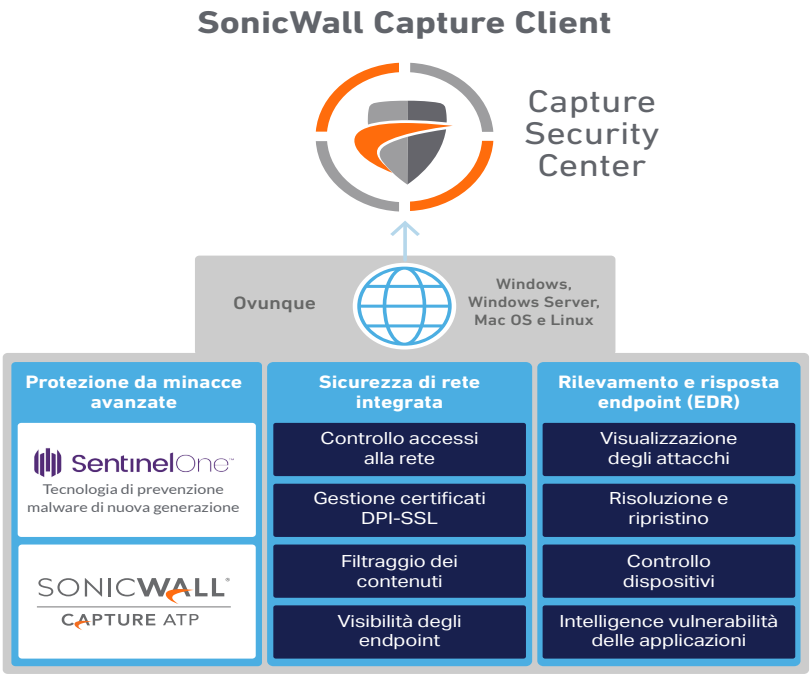
CARATTERISTICHE PRINCIPALI

- Rilevamento efficace e immediato delle minacce senza interferenze
- Gestione centralizzata e via cloud con funzionalità multi-tenant per rafforzare la sicurezza di rete e degli endpoint
- Soluzione semplice e intuitiva che consente a team di sicurezza e responsabili IT di bloccare le moderne minacce informatiche

Sicurezza degli endpoint su misura per le aziende

Leggi il documento: sonicwall.com

SCHEDA TECNICA



Capture Client applica la protezione dalle minacce avanzate basata sul comportamento, con tecnologia NGAV di SentinelOne.

L'integrazione con Capture ATP garantisce una maggiore efficacia in termini di sicurezza, tempi di risposta più rapidi e un TCO più basso.

Caratteristiche e vantaggi

Monitoraggio continuo del comportamento

- Profilo completo delle attività relative a file, applicazioni, processi e alla rete
- Protezione da malware basati su file o di tipo fileless
- Visione a 360 gradi degli attacchi con informazioni di intelligence concrete

Threat hunting con visibilità approfondita

- La funzionalità Deep Visibility consente di cercare minacce in base a indicatori di comportamento e indicatori di compromissione (IOC) sui dispositivi Windows, MacOS e Linux gestiti
- Ricerca e risposta automatizzate alle minacce con regole e avvisi personalizzati

Integrazione con Capture Advanced Threat Protection (ATP)

- I file sospetti sui dispositivi Windows vengono automaticamente sottoposti all'analisi sandbox avanzata
- Rilevamento delle minacce prima dell'esecuzione, come ad es. i malware ad attivazione ritardata
- Confronto con i verdetti sui file del database di Capture ATP, senza dover caricare i file nel cloud

Capacità di ripristino esclusive

- Supporto di policy per rimuovere completamente le minacce
- Ripristino autonomo di uno stato noto degli endpoint prima che vengano avviate attività dannose

Tecniche multilivello basate su metodi euristici

- Intelligence nel cloud, analisi statica avanzata e protezione comportamentale dinamica
- Protezione e risoluzione di malware noti e sconosciuti prima, durante o dopo un attacco

Intelligence delle vulnerabilità delle applicazioni

- Catalogazione di ogni applicazione installata e ogni rischio associato
- Analisi delle vulnerabilità note con dettagli sulle vulnerabilità ed esposizioni comuni (CVE) e sui livelli di gravità segnalati
- Questi dati sono utilizzabili per assegnare priorità alle patch e ridurre la superficie di attacco

Controllo in rete degli endpoint

- Aggiunta di controlli simili a quelli di un firewall sugli endpoint
- Base di regole di quarantena aggiuntiva per gestire i dispositivi infetti

Remote Shell[1]

- Elimina la necessità di avere un contatto fisico con i dispositivi per risolvere eventuali problemi, modificare le configurazioni locali ed eseguire indagini forensi

Nessuna necessità di scansioni o aggiornamenti periodici

- Massimo livello di protezione in ogni momento, senza limitare la produttività degli utenti
- Scansione completa all'installazione e monitoraggio continuo in seguito per rilevare attività sospette

Integrazione opzionale con i firewall SonicWall

- Possibilità di eseguire l'ispezione approfondita dei pacchetti di traffico crittografato (DPI-SSL) sugli endpoint
- Semplice installazione di certificati affidabili su ogni endpoint
- Gli utenti non protetti vengono indirizzati a una pagina di download di Capture Client prima di accedere a Internet da dietro un firewall

Filtraggio dei contenuti

- Blocca gli indirizzi IP e i domini di siti dannosi
- Aumenta la produttività degli utenti riducendo la larghezza di banda o limitando l'accesso a contenuti web non idonei o improduttivi

Controllo dei dispositivi

- Blocco dei dispositivi potenzialmente infetti per impedirne la connessione agli endpoint
- Utilizzo di policy di autorizzazione granulari

Funzionalità di Capture Client		
Funzionalità	Advanced	Premier
Gestione cloud, reportistica e analisi (CSC)	✓	✓
Integrazioni della sicurezza di rete		
Visibilità e implementazione degli endpoint	✓	✓
Distribuzione dei certificati DPI-SSL	✓	✓
Filtraggio dei contenuti	✓	✓
Protezione avanzata degli endpoint		
Antimalware di nuova generazione	✓	✓
Sandbox Capture Advanced Threat Protection	✓	✓
ActiveEDR (rilevamento e risposta degli endpoint)		
Visualizzazione degli attacchi	✓	✓
Risoluzione e ripristino	✓	✓
Controllo dei dispositivi	✓	✓
Intelligence e vulnerabilità delle applicazioni	✓	✓
Rilevamento di punti di accesso non autorizzati		✓
Controllo in rete degli endpoint		✓
ActiveEDR, ricerca e intelligence delle minacce		
Threat hunting con visibilità approfondita		✓
Remote Shell[1]		✓
Catalogo delle esclusioni		✓

[1] Remote shell sarà disponibile su richiesta in un nuovo account (con 2FA abilitato) direttamente sulla console S1.

Capture Client - Requisiti di sistema | SonicWall

Best practice per le attività globali di sicurezza degli endpoint per MSSP e aziende distribuite

Leggi il documento: www.sonicwall.com

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative 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