SonicWall Capture Client con motore SentinelOne

L'aumento costante delle minacce ransomware e di altri attacchi basati su malware ha dimostrato che l'efficacia delle soluzioni per la 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. Questo nuovo tipo di minacce richiede un approccio diverso per la protezione dei client. Inoltre, con la diffusione di fenomeni come il telelavoro, la mobilità e il BYOD, è più che mai indispensabile garantire una protezione costante degli endpoint, ovunque essi siano.

SonicWall Capture Client è una soluzione unificata che offre molteplici funzionalità di protezione per gli endpoint. Dotato di un motore di protezione contro il malware di nuova generazione basato su SentinelOne, Capture Client adotta tecniche di protezione avanzate contro le minacce come l'apprendimento automatico e il ripristino di sistema. Inoltre consente l'ispezione approfondita del traffico TLS crittografato (DPI-SSL) sui firewall SonicWall mediante l'installazione e la gestione di certificati TLS affidabili.

Capture Client coesiste con i servizi Content Filtering Client e Global VPN Client di SonicWall. Le policy per tutti i prodotti possono essere gestite da un'unica console di controllo basata sul cloud. Capture Client può essere aggiunto con facilità a qualsiasi client implementato tramite policy di gruppo di Microsoft Active Directory o con qualsiasi altra tecnica di implementazione di software terzi, oppure mediante il rilascio di URL ad hoc dai quali i client possono scaricarlo e installarlo automaticamente, senza alcun intervento aggiuntivo. Una volta integrato con i firewall SonicWall, Capture Client viene implementato sui client non protetti in maniera pressoché impercettibile.

Caratteristiche e vantaggi

Il monitoraggio continuo del comportamento del client aiuta a creare un profilo completo delle attività relative a file, applicazioni, processi e alla rete. Ciò garantisce una protezione contro malware sia basati su file che di tipo fileless, fornendo una visione a 360 gradi sugli attacchi e informazioni di intelligence concrete per ulteriori analisi.

Le tecniche di protezione multilivello basate su metodi euristici, che includono intelligence nel cloud, analisi statica avanzata e protezione comportamentale dinamica, contribuiscono alla protezione contro malware noti e sconosciuti e agevolano l'attuazione di misure di rimedio.

L'assenza di scansioni a intervalli regolari o aggiornamenti periodici garantisce il massimo livello di protezione in ogni momento, senza limitare la produttività degli utenti.

Le capacità di ripristino esclusive supportano policy che non solo rimuovono completamente la minaccia, ma ripristinano anche il client colpito riportandolo a com'era prima che il malware entrasse in azione. In questo modo non occorre effettuare un ripristino manuale in caso di attacchi ransomware e simili.

La console di gestione basata su cloud riduce la complessità di amministrazione, migliorando al contempo la capacità di implementare e attuare la protezione degli endpoint, ovunque essi siano.

L'integrazione con i firewall SonicWall di nuova generazione permette un'implementazione zero-touch e una

Vantaggi:

- Gestione indipendente basata su cloud
- Sinergia con i firewall SonicWall
- Applicazione di policy di sicurezza
- Gestione dei certificati DPI-SSL
- Monitoraggio continuo del comportamento
- Determinazione accurata grazie al machine learning
- Tecniche multilivello basate su metodi euristici
- Capacità di ripristino esclusive

maggiore conformità degli endpoint. Consente inoltre di eseguire l'ispezione approfondita dei pacchetti di traffico crittografato (DPI-SSL) applicando certificati affidabili ad ogni terminale.

Gestione centralizzata e creazione di rapporti sulla protezione dei client

La console SonicWall basata sul cloud funge da unico pannello di controllo per la gestione di tutte le policy dei client, incluse quelle per la protezione contro i malware di nuova generazione, la gestione dei certificati DPI-SSL, il filtraggio dei contenuti e la VPN.

La console di gestione è una piattaforma multi-tenant basata su cloud che viene offerta senza costi aggiuntivi. Offre funzionalità di gestione delle policy e reportistica sulla protezione dei client, con il supporto per policy granulari di controllo degli accessi. Ciò permette ai fornitori di servizi gestiti (MSP) di amministrare i client di più clienti e fornire i report corrispondenti. Allo stesso tempo, ogni cliente può gestire e ottenere report solo per i propri client.

La console funge inoltre da piattaforma di analisi per esaminare le cause profonde alla base delle minacce malware rilevate, fornendo informazioni utili su come evitare che le minacce si ripresentino. Un amministratore può ad esempio vedere con facilità le applicazioni in esecuzione su un client e, in tal modo, individuare le macchine che utilizzano software vulnerabili o non autorizzati.

Versioni disponibili e piattaforme supportate

SonicWall Capture Client è disponibile in due versioni:

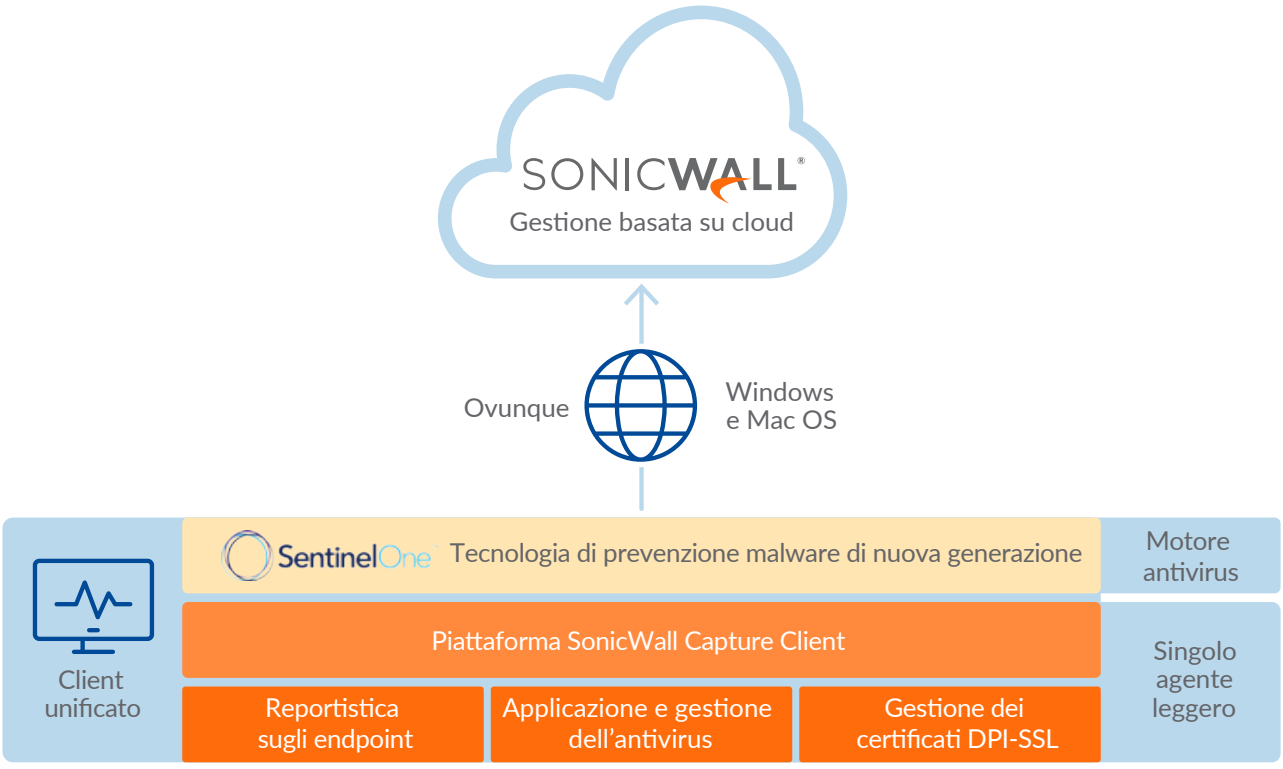
SonicWall Capture Client Basic offre tutte le funzionalità SonicWall di nuova generazione per la protezione e la correzione del malware, oltre al supporto per l'ispezione DPI-SSL.

SonicWall Capture Client Advanced offre tutte le funzionalità della versione Basic sopra elencate, con in più capacità di ripristino avanzate.

Entrambe le versioni sono disponibili per Windows 7 o superiori e per Mac OSX.

Informazioni su SonicWall

Da oltre 25 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 difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.



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

Datasheet-CaptureClient-US-KJ-MKTG1820