SONICWALL

SonicWall Capture Client

Le minacce in continua espansione del ransomware e di altri attacchi malware dannosi hanno dimostrato che le soluzioni di protezione dei client non possono essere valutate esclusivamente in base alla conformità dell'endpoint. La tecnologia antivirus tradizionale utilizza un approccio controverso basato sulle segnature, che non è riuscito a tenere il passo delle tecniche di malware e di evasione emergenti. Inoltre, con la proliferazione del telelavoro, della mobilità e del BYOD, c'è urgente necessità di avere una protezione coerente degli endpoint dovunque si trovino.

SonicWall Capture Client è un endpoint unificato caratterizzato da funzioni di protezione multiple. Tramite l'engine di protezione dai malware di prossima generazione messo a punto da SentinelOne, Capture Client utilizza tecniche avanzate di protezione dalle minacce, come l'apprendimento automatico, l'integrazione della sandbox di rete e il ripristino dei sistemi all'ultima configurazione non compromessa. Inoltre consente l'ispezione approfondita del traffico TLS crittografato (DPI-SSL) sui firewall SonicWall tramite l'installazione e la gestione di certificati TLS affidabili.

Capture Client coabita con il client Global VPN di SonicWall, e le politiche per tutti i prodotti possono essere gestite da un'unica consolle nel cloud. Capture Client può essere facilmente integrato in qualsiasi client installato tramite politiche di gruppo Microsoft Active Directory, altre tecniche di installazione software di terzi o ancora mediante fornitura di URL personalizzati, dove i client possono effettuare il download e l'autoinstallazione in modo silente senza ulteriori interventi.

Inoltre, grazie all'integrazione con i firewall SonicWall, Capture Client consente un'installazione zero-touch su client non protetti con funzioni di attivazione opzionali.

Caratteristiche e vantaggi

Monitoraggio comportamentale continuo del client: contribuisce a definire un profilo completo delle attività dei file, delle applicazioni, dei processi e di rete, il che rende possibile la protezione dai malware basati o meno su file e fornisce una visione a 360 gradi degli attacchi, con la relativa intelligenza azionabile per le indagini.

Tecniche di protezione multilivello di tipo euristico: comprendono l'intelligenza del cloud, l'analisi statica avanzata e la protezione comportamentale dinamica, il che contribuisce alla protezione e al contrasto contro i malware noti e non.

Nessuna esigenza di scansioni regolari e di aggiornamenti periodici: massimo livello di protezione in qualsiasi momento senza penalizzare la produttività degli utenti. Capture Client esegue una scansione completa al momento dell'installazione e successivamente effettua il monitoraggio continuo per individuare attività sospette.

Integrazione di Capture Advanced Threat Protection (ATP): trasferisce automaticamente i file sospetti per l'analisi avanzata in sandbox tramite manipolazione del codice che l'endpoint non è in grado di eseguire. Blocca un maggior numero di minacce prima che vengano eseguite, come il malware a scoppio ritardato. Gli amministratori possono anche consultare il database delle valutazioni dei file di Capture ATP senza bisogno di caricarli sul cloud per l'analisi.

Vantaggi:

- Gestione indipendente basata su cloud
- Sinergia con i firewall SonicWall
- Attuazione delle politiche di sicurezza
- Gestione dei certificati DPI-SSL
- Monitoraggio continuo del comportamento
- Determinazione accurata tramite apprendimento automatico
- Tecniche multilivello basate su metodi euristici
- Intelligenza delle vulnerabilità delle applicazioni
- Capacità di ripristino esclusive
- Facilità di inserimento white list/ blanck list
- Sandbox cloud Capture Advanced Threat Protection (ATP) per analisi automatica dei malware
- Condivisione dell'intelligenza delle minacce per la verifica manuale dei file senza bisogno di trasferimento
- Filtraggio dei contenuti
- Controllo dispositivi

Capacità di ripristino esclusive: supporta anche politiche che non si limitano ad eliminare completamente la minaccia, ma riportano il cloud preso di mira allo stato precedente l'inizio dell'attività del malware, il che elimina l'esigenza di ripristino manuale in caso di ransomware e di attacchi simili in ambiente Windows.

Intelligenza delle vulnerabilità delle applicazioni: mette a disposizione degli amministratori la possibilità di catalogare tutte le applicazioni nei singoli endpoint protetti e gli eventuali rischi ad esse associati. Il rischio è basato sulla presenza di eventuali vulnerabilità conosciute con informazioni dettagliate sulle CVE e sui livelli di gravità dichiarati per quella versione, mettendo a disposizione degli amministratori l'intelligenza azionabile per definire le priorità degli aggiornamenti e ridurre la superficie di attacco degli endpoint.

Integrazione opzionale con firewall SonicWall di 6ª generazione e successivi: consente l'installazione zero-touch e la conformità avanzata dell'endpoint, oltre ad abilitare l'attivazione dell'ispezione deep packet del traffico crittografato (DPI-SSL) installando certificati affidabili sui singoli endpoint.

Filtraggio dei contenuti: consente alle organizzazioni di bloccare gli indirizzi IP e i domìni dei siti dannosi, e di aumentare la produttività degli utenti riducendo l'ampiezza di banda o limitando l'accesso a contenuti web dubbi o improduttivi.

Controllo dispositivi: consente alle organizzazioni di impedire ai dispositivi potenzialmente infettati di collegarsi agli endpoint grazie a politiche granulari di inserimento nelle white list.

Gestione centralizzata e reportistica di protezione del client: la consolle di gestione SonicWall basata su cloud funge da unico pannello di controllo per la gestione a livello del client, compresi la protezione contro il malware di prossima generazione, la gestione dei certificati DPI-SSL e il filtraggio dei contenuti

La consolle di gestione è una piattaforma multi-tenant basata su cloud, offerta senza maggiorazione di costo, Prevede la reportistica sulla protezione dei client e la gestione delle politiche, supportando politiche di controllo accessi minuziose, compresa la possibilità di assegnare le politiche sulla base degli attributi di Microsoft Active Directory. Ciò consente ai fornitori di servizi gestiti (MSP) di effettuare la gestione e la reportistica sui client di diversi clienti, mentre i singoli clienti possono effettuare la gestione e la reportistica solo dei loro client.

La consolle di gestione funge inoltre da piattaforma di indagine, contribuendo a individuare la causa profonda delle minacce malware rilevate e fornendo intelligenza azionabile per impedire che le stesse si ripresentino. Ad esempio, gli amministratori possono visualizzare agevolmente quali applicazioni sono in funzione su un client, il che a sua volta può contribuire a individuare le macchine che possano eseguire software vulnerabile o non autorizzato.

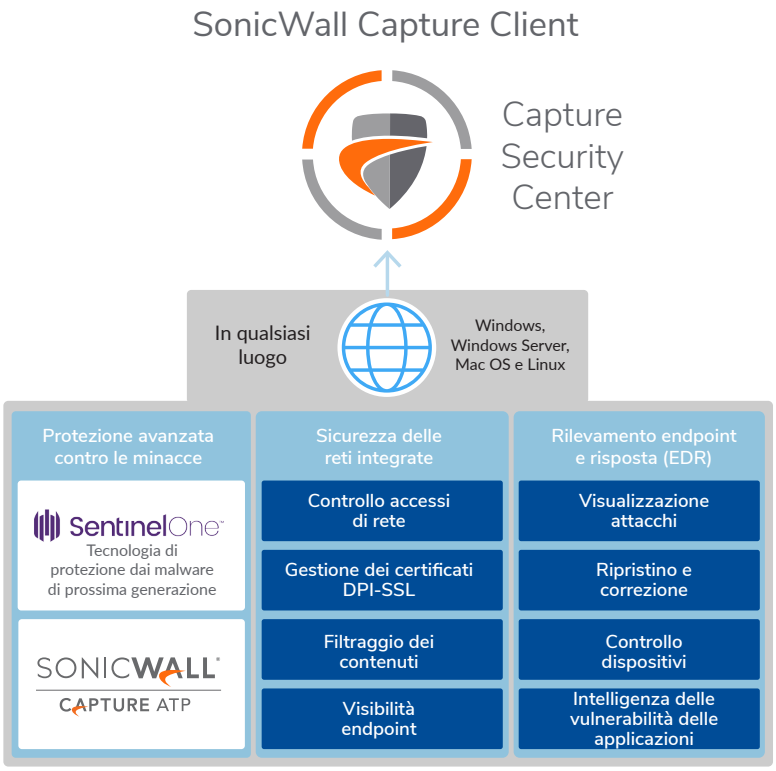
Offerte e supporto piattaforme

SonicWall Capture Client è disponibile in due versioni:

SonicWall Capture Client Basic contiene tutte le funzioni di protezione e rimedio contro i malware di prossima generazione tipiche di SonicWall, con possibilità di supporto DPI-SSL.

SonicWall Capture Client Advanced contiene tutte le funzioni della versione Basic sopra riportate, più funzionalità di ripristino avanzate, integrazione Capture ATP, visualizzazione degli attacchi, intelligenza delle vulnerabilità delle applicazioni e filtraggio dei contenuti.

Entrambe le offerte sono disponibili per Windows 7 (e versioni successive) e per Mac OSX.



CONFRONTO DELLE FUNZIONI		
Funzione	**Basic**	**Advanced**
Gestione cloud, reportistica e analisi (CSC)	✓	✓
Sicurezza delle reti integrate		
Visibilità endpoint	✓	✓
Installazione certificati DPI-SSL	✓	✓
Filtraggio dei contenuti	–	✓
Protezione avanzata contro le minacce		
Antimalware di prossima generazione	✓	✓
Capture Advanced Threat Protection Sandboxing	–	✓
Rilevamento endpoint e risposta		
Visualizzazione attacchi	–	✓
Ripristino e correzione	–	✓
Controllo dispositivi	–	✓
Intelligenza delle vulnerabilità delle applicazioni	–	✓

REQUISITI DI SISTEMA
Sistemi operativi
Windows 7 e versioni successive
Windows Server 2008 R2 e versioni successive
Mac OS/OSX 10.10 e versioni successive
Hardware
1 GHz Dual-core CPU o migliore
1 GB RAM o maggiore se richiesta dal sistema operativo (consigliati 2 GB)
2 GB di spazio libero su disco

SKU CAPTURE CLIENT		
Prodotto	Validità	SKU
ADVANCED		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED 10000 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED 10000 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1463
BASIC		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1510
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1511
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1512
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1513
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1514
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1515
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1516
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1517
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1444
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1445
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1446
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1447
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1448
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1449
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1450
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1451
SONICWALL CAPTURE CLIENT ADVANCED 10000 ENDPOINTS con assistenza 24X7	3 anni	02-SSC-1452
SONICWALL CAPTURE CLIENT ADVANCED 10000 ENDPOINTS con assistenza 24X7	1 anno	02-SSC-1453

SonicWall

SonicWall fornisce soluzioni di cibersicurezza illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cibersicurezza per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare il sito www.sonicwall.com.

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

© 2020 SonicWall Inc. TUTTI I DIRITTI RISERVATI. SonicWall è un marchio o un marchio depositato di SonicWall Inc. e/o delle sue controllate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi depositati appartengono ai rispettivi proprietari.
Datasheet-NetworkSecurityAppliance-US-VG-2139