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 garantire una protezione coerente e l'attuazione delle politiche web per gli 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 multi-engine e il ripristino dei sistemi all'ultima configurazione non compromessa. Consente inoltre 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, per consentire ai client di 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.

Gestione centralizzata e reportistica sulla protezione dei client

La consolle di gestione e i pannelli di controllo globali di SonicWall basati sul cloud sono stati progettati per consentire agli MSSP uno sguardo d'insieme sulla salute dei tenant in un'ottica globale. Gli amministratori possono visualizzare lo stato di salute dei singoli tenant, valutato in base al numero di infezioni, alle vulnerabilità presenti, alla versione installata di Capture Client e a che cosa e chi viene maggiormente bloccato dal filtraggio dei contenuti. Il pannello di controllo può anche indicare quali dispositivi sono online e quali stanno funzionando.

La Politica globale consente agli amministratori di applicare una singola politica di base a tutti i tenant, semplificando così la definizione di nuovi tenant. Ciò consente anche agli MSSP di definire rapidamente le protezioni contro le nuove minacce per tutti i tenant oggetto della politica. Quando viene attivata la funzione Inheritance, tutti i nuovi tenant acquisiscono la Politica globale. Quando la funzione viene disattivata, è possibile definire politiche individuali e modificare quelle esistenti per i singoli tenant, per quanto riguarda qualsiasi aspetto, dal filtraggio dei contenuti alla protezione dai malware alla gestione dei certificati DPI-SSL.

Il supporto delle politiche di controllo minuzioso degli accessi, compresa la possibilità di attribuire politiche sulla base degli attributi Microsoft Active Directory e dei gruppi di utenti, consente ai fornitori di servizi gestiti (MSSP/MSP) di effettuare la gestione e la reportistica sui client di diversi clienti, mentre i singoli clienti possono effettuare la gestione e il reporting 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 intelligence 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

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
- Intelligence delle vulnerabilità delle applicazioni
- Capacità di ripristino esclusive
- Pannello di controllo per lo stato di salute globale per tutti i conduttori
- Facilità di definizione di politiche globali
- Facilità di elencazione di blocchi/autorizzazioni
- Sandbox cloud Capture Advanced Threat Protection (ATP) per analisi automatica dei malware
- Condivisione dell'intelligence delle minacce per la verifica manuale dei file senza bisogno di trasferimento
- Filtraggio dei contenuti
- Controllo dispositivi

le macchine che possano eseguire software vulnerabile o non autorizzato.

Caratteristiche e vantaggi

Monitoraggio continuo del comportamento

- Visualizzazione profili completi di file, applicazioni, processi e attività di rete
- Protezione contro il malware basato su file e quello senza file
- Visualizzazione degli attacchi a 360 gradi con intelligence azionabile

Tecniche multilivello basate su metodi euristici

- Utilizzo di intelligence del cloud, analisi statiche avanzate e protezione dinamica basata sui comportamenti
- Protezione e rimedi nei confronti del malware noto e di quello sconosciuto prima, durante o dopo gli attacchi

Nessuna necessità di scansioni regolari e aggiornamenti periodici

- Massimo livello di protezione in qualsiasi momento senza penalizzare la produttività degli utenti
- Scansione completa al momento dell'installazione e successivo monitoraggio continuo per individuare attività sospette

Integrazione Capture Advanced Threat Protection (ATP) (per dispositivi Windows)

- Caricamento automatico dei file sospetti sui dispositivi Windows per analisi avanzata nella sandbox
- Individuazione di minacce dormienti prima che vengano eseguite, come il malware a scoppio ritardato
- Riferimento al database dei verdetti dei file di Capture ATP senza doverli caricare sul cloud

Capacità di ripristino esclusive (per Windows)

- Politiche di supporto che eliminano completamente le minacce
- Ripristino degli endpoint a uno stato precedente l'inizio dell'attività dannosa
- Eliminazione dell'esigenza di ripristino manuale in caso di attacchi ransomware e simili

Intelligence della vulnerabilità delle applicazioni (per Window e MacOS)

- Catalogazione di tutte le applicazioni installate e degli eventuali rischi associati
- Esame delle vulnerabilità note con l'indicazione dei particolari delle CVE e dei livelli di gravità
- Utilizzo di questi dati per definire la priorità delle patch e ridurre la superficie d'attacco

Integrazione opzionale con i firewall SonicWall

- Abilitazione della forzatura dell'ispezione deep packet del traffico crittografato (DPI-SSL) sugli endpoint
- Facilità di installazione di certificati affidabili sui singoli endpoint
- Indirizzamento degli utenti non protetti a una pagina di Capture Client scaricata prima dell'accesso a Internet quando si è in presenza di un firewall

Filtraggio dei contenuti (per Windows e MacOS)

- Bloccaggio degli indirizzi IP e dei domini dei siti dannosi
- Miglioramento della produttività degli utenti riducendo l'ampiezza di banda o limitando l'accesso a contenuti web discutibili o non produttivi

Controllo dei dispositivi (per Windows e MacOS)

- Bloccaggio della connessione agli endpoint da parte di dispositivi potenzialmente infetti
- Utilizzo di politiche di elencazione delle autorizzazioni granulari

Offerte e supporto piattaforme

SonicWall Capture Client è disponibile in due versioni:

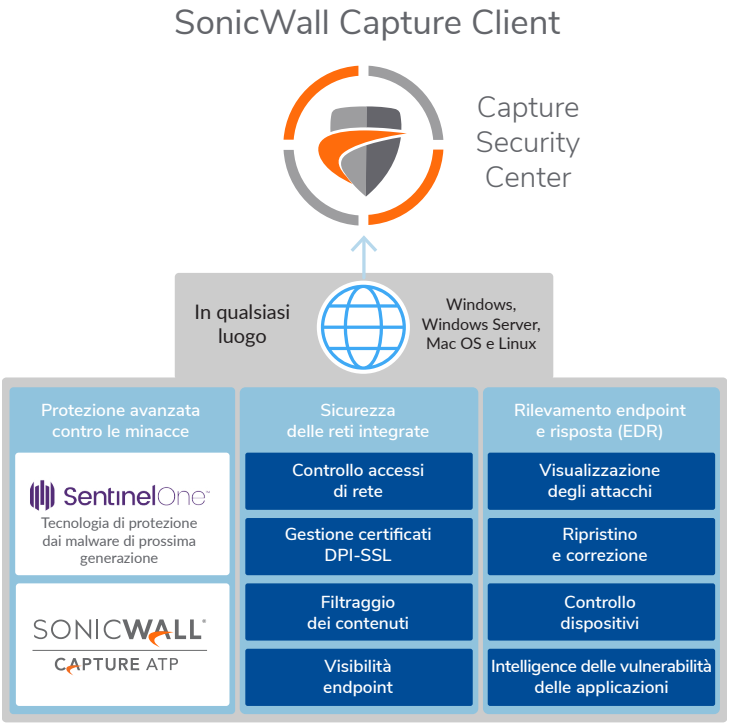
SonicWall Capture Client Basic contiene:

- Tutta la protezione SonicWall contro i malware di prossima generazione
- Funzioni di ripristino
- Supporto DPI-SSL

SonicWall Capture Client Advanced contiene:

- Tutte le funzioni di Basic
- Capacità di ripristino avanzate
- Integrazione Capture ATP
- Visualizzazione degli attacchi
- Intelligence delle vulnerabilità delle applicazioni
- Filtraggio dei contenuti

Entrambe le offerte sono disponibili per Windows 7 e versioni successive, Mac OSX e Linux (per ulteriori informazioni vedere più avanti, Requisiti di sistema).



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 degli attacchi	–	✓
Ripristino e correzione	–	✓
Controllo dispositivi	–	✓
Intelligence 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
Amazon Linux AMI
Red Hat Enterprise Linux RHEL v5.5-5.11, 6.5+, 7.0+
Ubuntu 12.04, 14.04, 16.04, 16.10
CentOS 6.5+, 7.0+
Oracle Linux OL (precedentemente conosciuto come Oracle Enterprise Linux o OEL) v6.5-6.9 e v7.0+
SUSE Linux Enterprise Server 12
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

SONICWALL®

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 cybersecurity 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 della cybersecurity 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

Datasheet-NetworkSecurityAppliance-US-VG-2889