SonicWall Capture Security appliance 1000

SonicWall Capture Security appliance™ (CSa) rende disponibili Capture Advanced Threat Protection™ (ATP) e l'analisi del malware mediante sandboxing in ambienti interni per i clienti che, per esigenza di conformità e scelte politiche, non possono inviare i file per l'analisi a cloud esterni, o che preferiscono che tutti i loro dati restino all'interno della loro organizzazione. CSa 1000 è in grado di analizzare i file sospetti provenienti da altri prodotti SonicWall per effettuare un rilevamento rapido e di precisione elevata delle minacce sconosciute, e consentendo al cliente di conservare i file in azienda. Inoltre, la funzionalità API REST su CSa mette i vantaggi di una capacità analitica decisamente elevata a disposizione degli esperti delle minacce, dei sistemi di sicurezza di terzi e di qualsiasi stack software che può essere integrato con API pubblicate.

CSa utilizza per l'analisi dinamica una combinazione di controlli basati sulla reputazione, l'analisi statica dei file e l'engine brevettato Real-Time Deep Memory Inspection™ (RTDMI) di SonicWall per garantire non solo il miglior tasso di rilevamento possibile dei file dannosi, ma anche l'efficacia del rilevamento stesso nel minor tempo possibile. L'ecosistema di prodotti di sicurezza di SonicWall, già completamente integrato con l'analisi di ATP Capture effettuata nel cloud è in grado di attuare la sicurezza in linea con funzioni come Block Until Verdict.

Le stesse funzioni sono supportate quando i prodotti SonicWall vengono collegati a quelli della serie CSa al posto di Capture ATP nel cloud.

RTDMI

L'engine di analisi dei file RTDMI (Real-Time Deep Memory Inspection) di SonicWall in attesa di brevetto è un nuovo metodo di analisi dei file sospetti attraverso il monitoraggio del comportamento delle applicazioni in memoria. RTDMI può vedere attraverso qualsiasi tecnica di offuscamento o di crittografia che i malware moderni sono in grado di mettere in atto per aggirare l'analisi di rete e della sandbox, ottenendo un rilevamento estremamente preciso degli attacchi portati da documenti, file eseguibili, file di archivio e tutta una serie di altri tipi di file.

Protezione in tempo reale

La combinazione dei controlli di reputazione e d'intelligence globale, dell'analisi statica e della tecnologia RTDMI consente di ottenere i risultati con una rapidità sufficiente a consentire l'impiego di tecnologie come Blocco fino al verdetto nei prodotti SonicWall. Questa funzione consente di attuare una politica d'ispezione dei file sul firewall per evitare che i file sospetti vengano scaricati dall'utente finale fino a quando l'ispezione non viene completata e non viene emesso un verdetto da Capture ATP o da CSa.

Vantaggi:

- Ispezione basata sulla memoria con RTDMI
- Analisi multi-fase con controllo della reputazione, analisi statica e analisi dinamica
- Accesso API per l'analisi delle minacce
- Supporto di un'ampia varietà di file
- Supporto del blocco fino al verdetto
- Efficacia con sicurezza elevata
- Reportistica e accesso basato sui ruoli

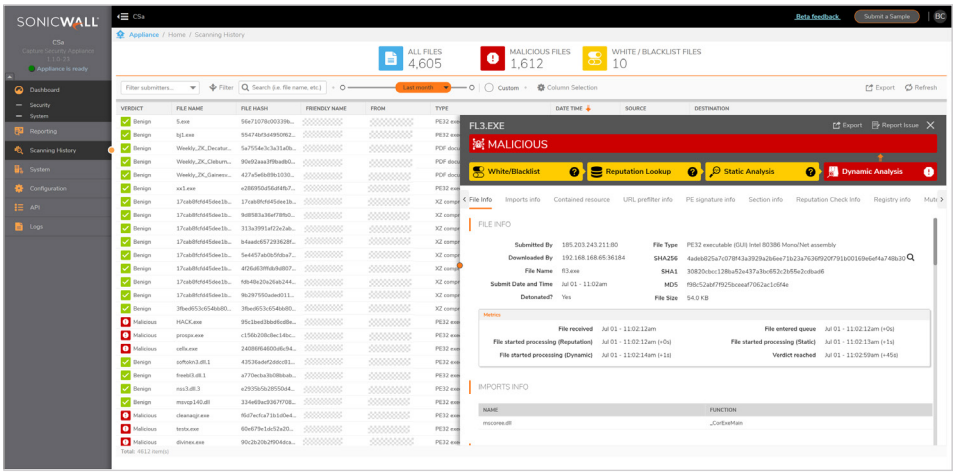
1. La capacità di analisi dipende dalla connettività di rete, dai tipi di file, dai livelli di compressione e può variare rispetto ai dati pubblicati.
2. Anche se non esiste un limite rigido, il numero di dispositivi dipende dal numero di file trasmessi da ognuno. Il numero consigliato alla data di pubblicazione è di circa 250 dispositivi.
3. Tutte le serie TZ, NSa e SuperMassive che possono eseguire SonicOS 6.5.4.6 o successive. Non supportato sulle serie SuperMassive 9800 e NSsp 12000.

La fiducia e i vantaggi dei grandi numeri

- CSa abbina la tecnologia Capture ATP di SonicWall - un servizio affidabile basato sul cloud utilizzato da oltre 150.000 clienti in tutto il mondo - ad un formato compatto.
- CSa viene regolarmente aggiornato per quanto riguarda l'intelligenza per mantenerlo sincronizzato con l'intelligenza delle minacce acquisita a livello globale tramite l'analisi dei file di SonicWall Capture ATP.

Reportistica, analisi e amministrazione

- CSa fornisce informazioni sui file inviati da qualsiasi fonte tramite un pannello di controllo di facile uso e lo storico dell'analisi dei file, per quanto riguarda frequenza, origine, verdetti e altri dati relativi ai file inviati per l'analisi
- Le funzioni di reportistica forniscono una visione globale della protezione ATP a livello dell'intera organizzazione, con possibilità di programmare report regolari configurati in funzione dei diversi ruoli
- Gli amministratori possono concedere un accesso granulare a CSa 1000 a tutta una serie di ruoli, con la possibilità di limitare l'accesso a qualsiasi parte dell'interfaccia utente
- Gli analisti delle sicurezza possono accedere alla cronologia delle scansioni e modificare gli elenchi di autorizzazione e di blocco e i dispositivi autorizzati e segnalare eventuali falsi positivi o falsi negativi sospetti
- Gli amministratori a livello di rete possono accedere alla configurazione operativa dell'apparecchiatura anche in presenza, per ragioni di riservatezza, di limitazioni alla consultazione dei file inviati e delle loro fonti



Funzioni

- Ricerca reputazione e verdetto globale (configurabile)
- Analisi statica e dinamica con RTDMI
- Elenchi di autorizzazione e blocco su hash e dominio
- Reportistica programmata configurabile
- Amministrazione basata sui ruoli (ruoli configurabili)
- Gestione: HTTPS o SSH tramite interfaccia di gestione dedicata o interfaccia di rete regolare
- Accesso alla console SSH
- Registrazione e avvisi
- Segnalazione falsi positivi e falsi negativi con automatismi elenchi di autorizzazione e di blocco
- Connettività diretta o tramite VPN (IP indirizzabile)
- Funzionamento a rete chiusa
- Supporto API REST per la presentazione e l'analisi dei file
- Sistema operativo potenziato con avvio sicuro e catena di fiducia per anti-manomissione
- Registrazione locale

1. La capacità di analisi dipende dalla connettività di rete, dai tipi di file, dai livelli di compressione e può variare rispetto ai dati pubblicati.
2. Anche se non esiste un limite rigido, il numero di dispositivi dipende dal numero di file trasmessi da ognuno. Il numero consigliato alla data di pubblicazione è di circa 250 dispositivi.
3. Tutte le serie TZ, NSa e SuperMassive che possono eseguire SonicOS 6.5.4.6 o successive. Non supportato sulle serie SuperMassive 9800 e NSsp 12000.

Opzioni di installazione

- L'utilizzo di SonicWall CSa è rapido e semplice e per iniziare richiede la configurazione delle reti di base, della reportistica e dell'accesso da parte dei dispositivi autorizzati
- CSa è stato progettato con IP indirizzabile e può quindi essere utilizzato dovunque a condizione che sia raggiungibile da dispositivi che invieranno i file per l'analisi

Esistono tre metodi d'impiego principali per CSa 1000:

Ufficio e ubicazione singoli

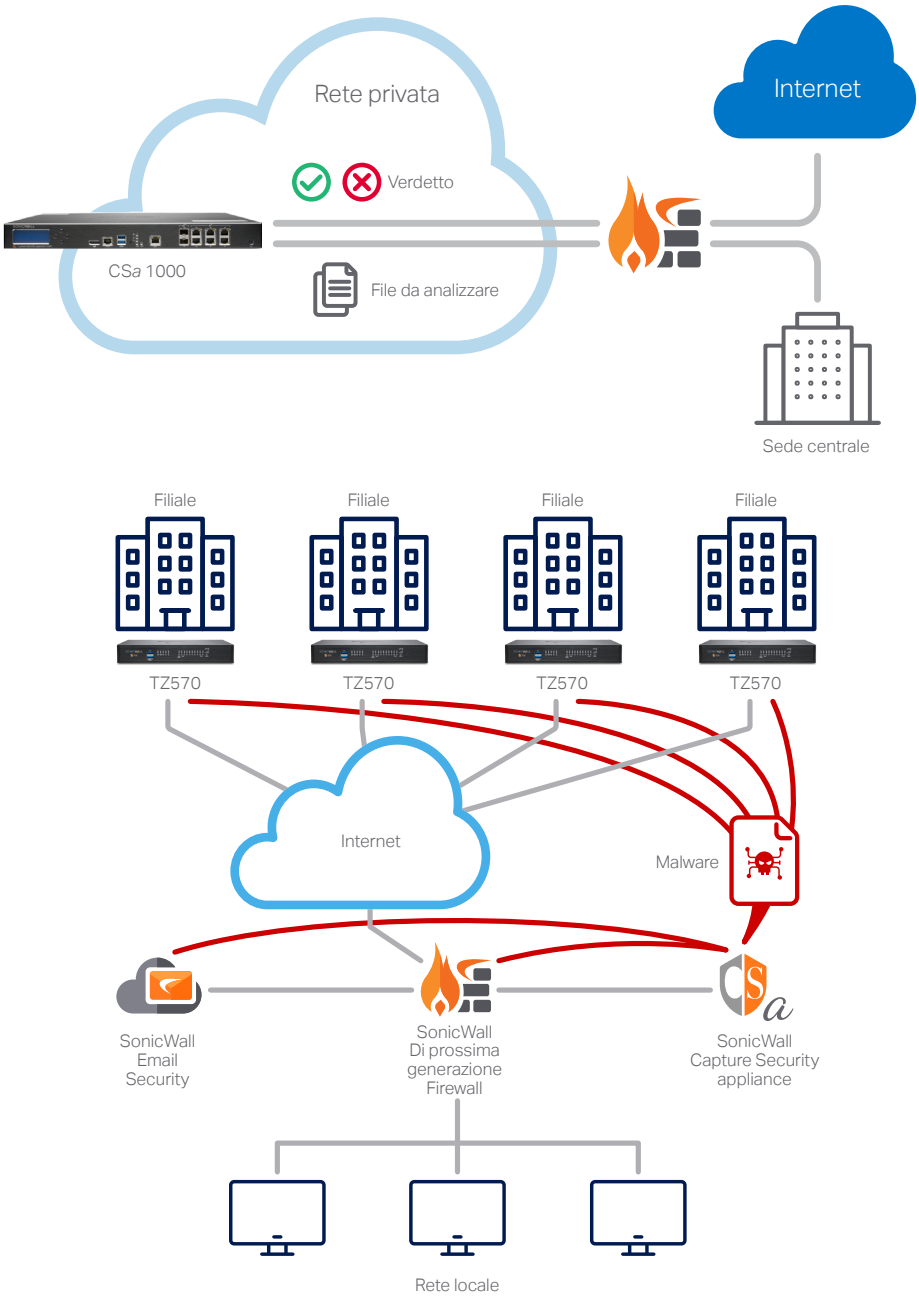
- CSa può essere utilizzato dovunque nella rete, purché i prodotti che lo utilizzeranno possano raggiungerlo attraverso un IP[1]
- Una volta installato CSa, i firewall e i sistemi di sicurezza della posta elettronica (altre soluzioni imminenti) possono essere configurati per reindirizzare i file sospetti per l'analisi ATP verso CSa anziché verso il cloud

Aziende distribuite e plurisede

- È possibile configurare più uffici e filiali per condividere l'accesso a un unico dispositivo CSa, utilizzato nel data center della sede centrale o in un data center remoto raggiungibile da tutti i dispositivi
- L'accesso può avvenire direttamente tramite Internet o VPN
- La configurazione di massa dei sistemi SonicWall perché puntino a CSa può essere effettuata tramite GMS o soluzioni di gestione NSM centralizzate basate sul cloud per una maggiore rapidità di configurazione e di installazione

Gateway API REST

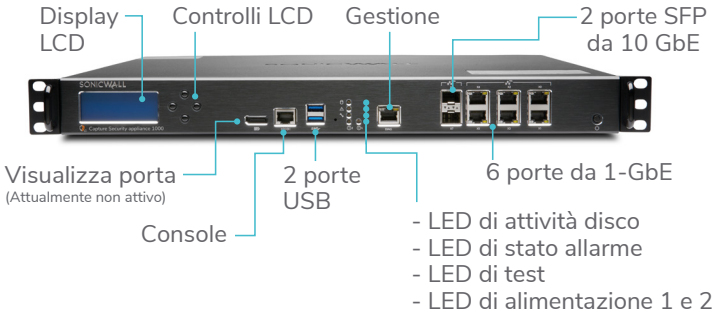
- La serie CSa è dotata di un'interfaccia API REST che può essere utilizzata per inviare i file per l'analisi e i risultati delle interrogazioni da parte dei responsabili dell'intelligenza delle minacce tramite propri script, integrazioni su portali web e altri prodotti di sicurezza
- Istruzioni su come iniziare a utilizzare lo scripting API per CSa ed esempi di codice sono disponibili su https://github.com/sonicwall

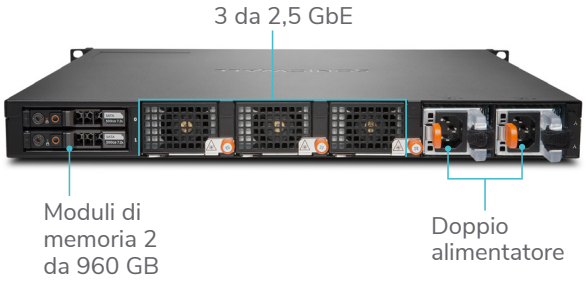


* [1]*I firewall di SonicWall richiedono anche l'accesso tramite UDP sulla porta 2259*

1. La capacità di analisi dipende dalla connettività di rete, dai tipi di file, dai livelli di compressione e può variare rispetto ai dati pubblicati.
2. Anche se non esiste un limite rigido, il numero di dispositivi dipende dal numero di file trasmessi da ognuno. Il numero consigliato alla data di pubblicazione è di circa 250 dispositivi.
3. Tutte le serie TZ, NSa e SuperMassive che possono eseguire SonicOS 6.5.4.6 o successive. Non supportato sulle serie SuperMassive 9800 e NSsp 12000.

CSa 1000





Specifiche di SonicWall Csa 1000

FUNZIONI	
Throughput di ricerca della reputazione e delle minacce globali (numero di file/ora) [1]	12.000
Throughput di mix di file reali (numero di file/ora)[1]	2.500
Throughput di analisi dinamica (RTDMI) (numero di file/ora) [1]	300
Dimensione massima dei file	100 MB
Numero massimo di dispositivi supportati[2]	Basato sulla performance
Massima profondità di scansione archivi	3
Supporto API REST	Sì
Dispositivi SonicWall supportati	TZ, NSa e SuperMassive (con sistema operativo SonicOS 6.5.4.6 o successivo)[3] Email Security 10.X Serie NSsp 15000 - Imminente Serie NSv (7.X e successiva) - Imminente
Tipi di file supportati	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip
Periodo di conservazione dei dati	Illimitato, limitato dalla capacità di memoria
Dischi fissi	2 SATA da 1 TB; RAID 1
Interfacce	6 porte 1GE, 2 porte 10 Gb SFP+, 2 USB, 1 console
Gestione porte dedicata	Sì (X0)
Certificazioni	FIPS 140-2 imminente
CARATTERISTICHE DEL PRODOTTO	
Fattore di forma	1U
Dimensioni	43 x 41,5 x 4,5 cm
Peso dell'apparecchiatura	8 kg
Accelerazione dati crittografia (AES-NI)	Sì
MTBF (a 25°C) in ore	129.601
Alimentazione	Doppia alimentazione, sostituibile a caldo
Tensione d'ingresso	100-240 VCA, 1,79 A
Potenza assorbita	114 W
Dissipazione di calore totale	389 BTU
Condizioni ambientali	RAEE, RoHS UE, RoHS Cina
Tolleranza agli urti (non operativo)	110 g, 2 msec
Emissioni	FCC, ICES, CE, C-Tick, VCCI; MIC
Sicurezza	TUV/GS, UL, CE PSB, CCC, BSMI, schema CB
Temperatura di funzionamento	da 0 °C a 40 °C
TPM	Sì

1. La capacità di analisi dipende dalla connettività di rete, dai tipi di file, dai livelli di compressione e può variare rispetto ai dati pubblicati.
2. Anche se non esiste un limite rigido, il numero di dispositivi dipende dal numero di file trasmessi da ognuno. Il numero consigliato alla data di pubblicazione è di circa 250 dispositivi.
3. Tutte le serie TZ, NSa e SuperMassive che possono eseguire SonicOS 6.5.4.6 o successive. Non supportato sulle serie SuperMassive 9800 e NSsp 12000.

Prodotto	SKU
Capture Security Appliance CSA 1000	02-SSC-2853
Capture Security Appliance CSA 1000 with Intelligence Updates and Support Bundle – 1 anno	02-SSC-5637
Capture Security Appliance CSA 1000 with Intelligence Updates and Support Bundle – 3 anni	02-SSC-5638
Capture Security Appliance CSA 1000 with Intelligence Updates and Support Bundle – 5 anni	02-SSC-5639

Servizi (necessari per il funzionamento di CSa 1000. Tutti i dispositivi che inviano file a CSa devono avere una licenza Capture ATP)	SKU
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 1 ANNO	02-SSC-4712
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 2 ANNI	02-SSC-4713
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 3 ANNI	02-SSC-4714
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 4 ANNI	02-SSC-4715
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 5 ANNI	02-SSC-4716
INTELLIGENCE UPDATES, ACTIVATION AND SUPPORT FOR SONICWALL CSA 1000 6 ANNI	02-SSC-4717

Attivazione API REST (questo servizio è necessario solo per il funzionamento delle API REST. Dev'essere applicato oltre al servizio di aggiornamento, attivazione e supporto dell'intelligenza)	SKU
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 1 ANNOYR	02-SSC-4706
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 2 ANNI	02-SSC-4707
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 3 ANNI	02-SSC-4708
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 4 ANNI	02-SSC-4709
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 5 ANNI	02-SSC-4710
REST API ACTIVATION FOR SONICWALL CAPTURE APPLIANCE CSA 1000 6 ANNI	02-SSC-4711

1. La capacità di analisi dipende dalla connettività di rete, dai tipi di file, dai livelli di compressione e può variare rispetto ai dati pubblicati.
2. Anche se non esiste un limite rigido, il numero di dispositivi dipende dal numero di file trasmessi da ognuno. Il numero consigliato alla data di pubblicazione è di circa 250 dispositivi.
3. Tutte le serie TZ, NSa e SuperMassive che possono eseguire SonicOS 6.5.4.6 o successive. Non supportato sulle serie SuperMassive 9800 e NSsp 12000.

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 www.sonicwall.com.

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

Datasheet-CSa-US-COG-2099