SONICWALL

Tutto si può vedere dalle nostre finestre

Volete sapere come? Una soluzione olistica integrata per la gestione totale della sicurezza.

SONICWALL CAPTURE SECURITY CENTER

con architettura true Single-Sign-On (SSO) e Single-Pane-of-Glass (SPOG). Tenete completamente sotto controllo il vostro ecosistema di sicurezza con una soluzione gestionale modulare.

Capture Security Center (CSC) ha tutto ciò che serve per una gestione completa ed accessibile da un'unica interfaccia con tantissime funzioni. Contiene tutto ciò che occorre, compresi strumenti analitici e di reportistica, sicurezza delle reti wireless, della posta elettronica, degli endpoint e del cloud, Risk Meters e gestione delle apparecchiature.

CSC è una soluzione SaaS che consente una maggiore flessibilità, con una visione a 360° dell'intero ecosistema di sicurezza SonicWall. Si contraddistingue per l'integrazione funzionale che consente un miglior rendimento ed una maggiore flessibilità operativa con un'interfaccia true SPOG. Risposte consapevoli a qualsiasi minaccia, rapide e in tempo reale, da qualsiasi sede e da qualsiasi dispositivo collegato ad Internet, con reportistica dettagliata e statistiche approfondite.

CSC supporta anche le strategie di ciberdifesa più ampie grazie alla conformità con i requisiti di livello di servizio per i Security Operation Center (SOC). Consente una gestione unificata della sicurezza, la conformità e altre strategie di gestione del rischio, il tutto da un'unica applicazione collegata ad Internet.

Capture Security Center è un'applicazione true SPOG per la gestione olistica e integrata ed è compresa nella maggior parte dei firewall e dei servizi cloud di SonicWall.

Maggiore efficienza e flessibilità operativa

Essere più efficienti. Lavorare più velocemente, in modo più intelligente e con minore sforzo.

CAPTURE SECURITY CENTER È PIÙ EFFICIENTE

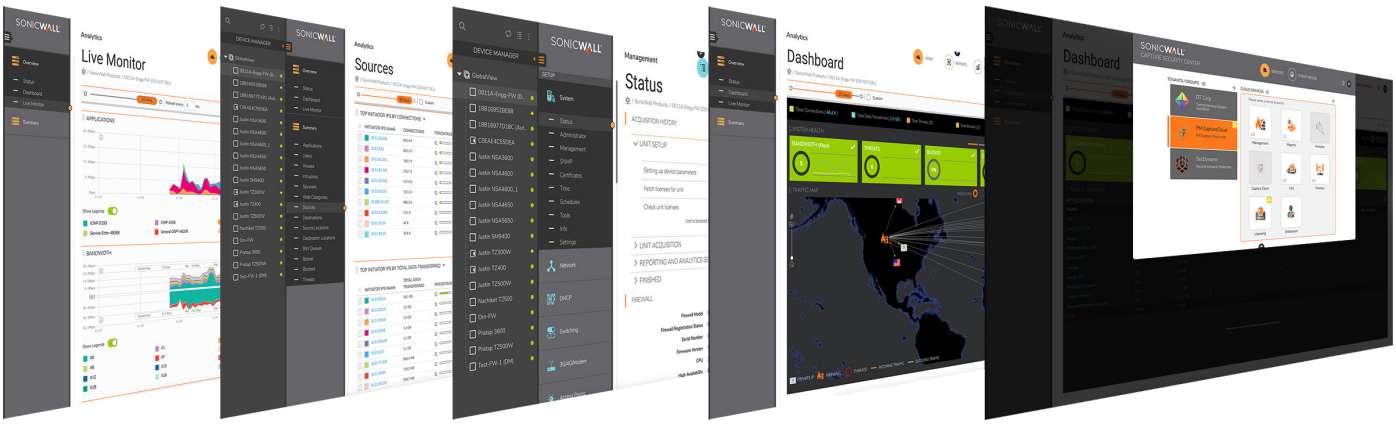
Gestire più funzioni in modalità SPOG. Riguarda qualsiasi cosa a livello di infrastrutture di sicurezza e di rete, tra cui architettura, ciberminacce e problemi di conformità.

CSC è uno strumento di gestione della produttività modulare in grado di coordinare meglio la gestione.

L'architettura SSO consente di gestire ogni aspetto operativo della rete, dalla sicurezza del cloud all'endpoint. La concezione nativa per il cloud consente di avere a disposizione tutto ciò che serve in una semplice infrastruttura comune. Tutte le attività risultano facilitate e più efficaci.

Ridurre tempi e costi di esecuzione delle attività quotidiane. Eliminare i silos di sicurezza non necessari e conseguire un'efficienza di tipo "see-and-click" per tutti i flussi di lavoro essenziali. Utilizzare nuove funzioni non appena si rendono disponibili.

Gestire l'intero stack di sicurezza SonicWall da un'unica postazione. Individuare le lacune ed i rischi di sicurezza grazie ai Risk Meters e a precisi strumenti analitici. Rispondere più rapidamente con informazioni sulle minacce per le quali il fattore tempo è fondamentale e con indicazioni in funzione delle situazioni specifiche. Semplificare il flusso di lavoro gestionale, ridurre le errate configurazioni e gli errori umani ed effettuare facilmente il provisioning dei firewall, degli switch e degli access point remoti presso le filiali tramite l'installazione Zero-Touch.



La concezione cloud nativa migliora l'efficienza e la flessibilità operativa. Ridurre i silos di sicurezza, aumentare la produttività di tutto l'ambiente di rete, il tutto da un'unica applicazione.

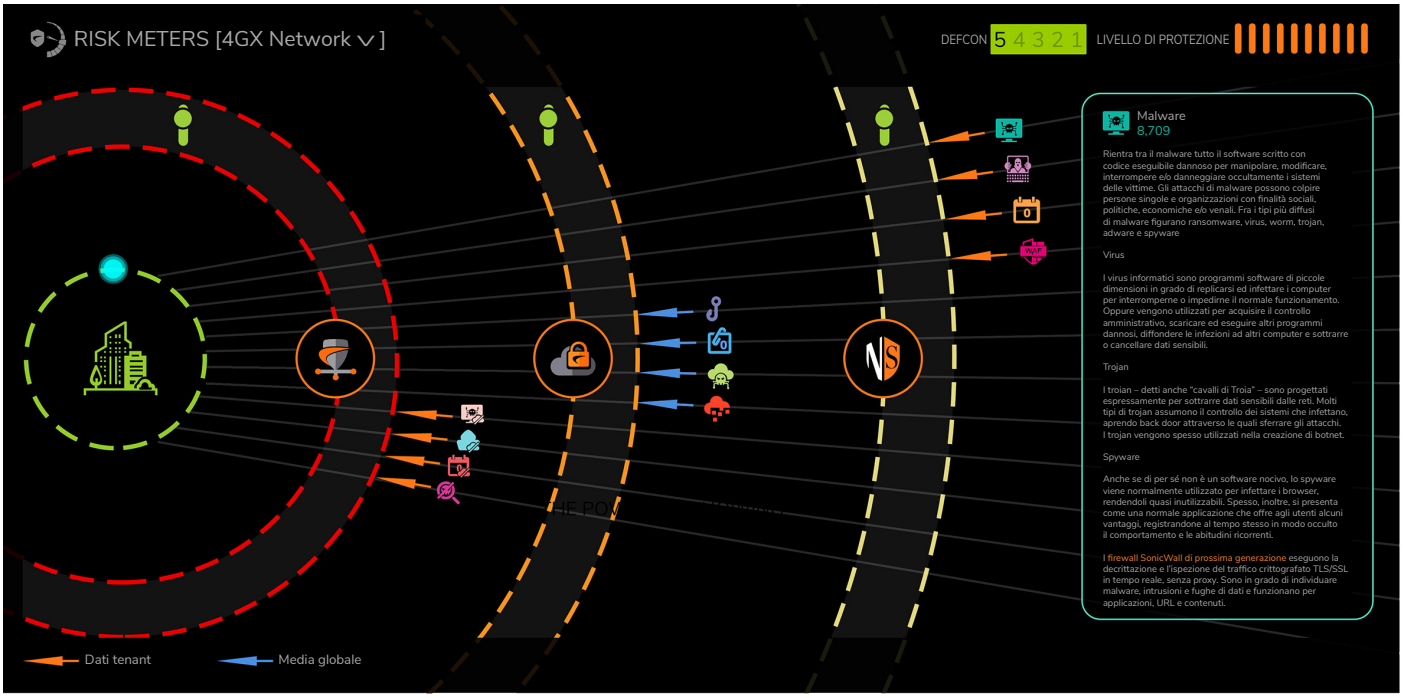
SONICWALL

Intelligenza sincronizzata delle ciberminacce per tutta la rete

La sicurezza prima di tutto. Studiare i rischi e le minacce in tempo reale e con dati reali.

CAPTURE SECURITY CENTER UTILIZZA L'INTELLIGENZA DELLE MINACCE

Unite i dati personalizzati basati sulle condizioni del momento delle risorse di sicurezza con l'intelligenza delle ciberminacce. Difendete le vostre reti con dati reali in tempo reale.



Risk Meters visualizza automaticamente i dati delle minacce e i punteggi di rischio confrontando i dati delle minacce reali con l'attuale livello di protezione. Evidenzia le falle dei livelli di difesa e prende decisioni di sicurezza in tempo reale. Guida la pianificazione di sicurezza, le politiche e le decisioni di budget sulla base di punteggi logici.

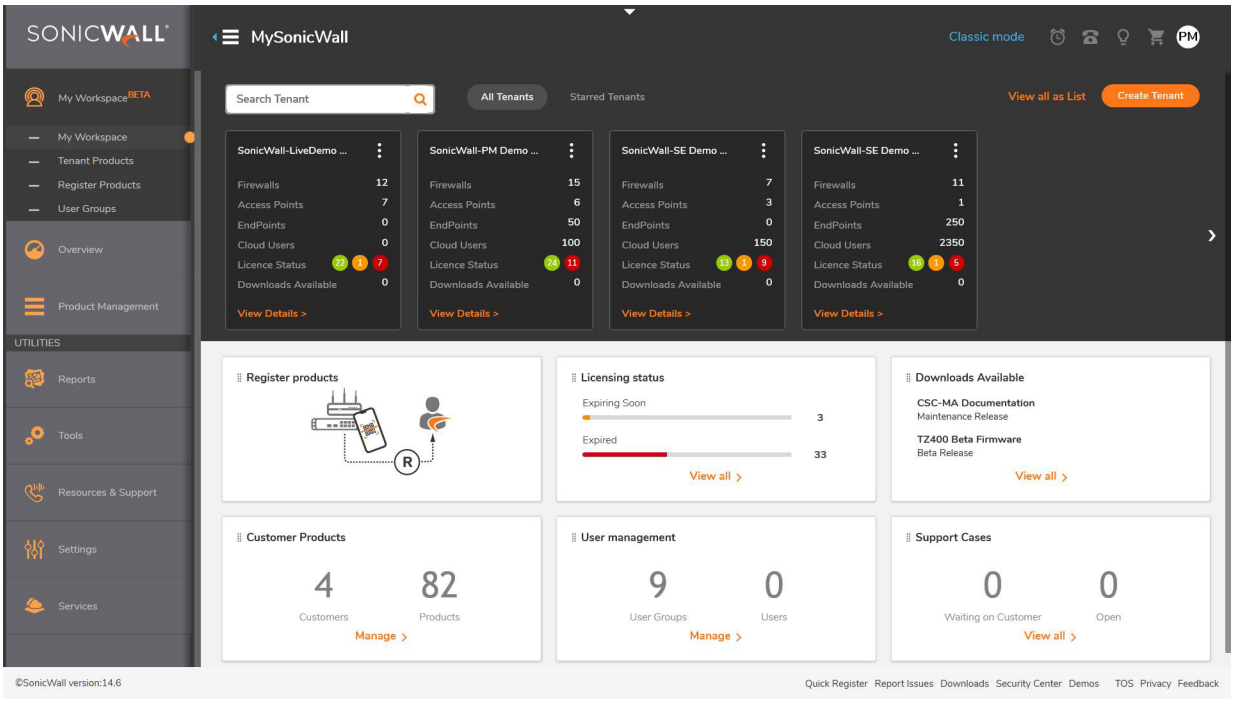
Con **SonicWall Risk Meters** è possibile personalizzare la valutazione della sicurezza sulla base di requisiti specifici dell'infrastruttura di rete. Visualizzare le minacce a carico della rete proiettate in tempo reale, con analisi in modalità grafica. Si tratta di una risorsa integrata che consente ai responsabili della sicurezza di visualizzare i vettori delle minacce e individuare le azioni da adottare per difendere la rete. Tenere sotto controllo le minacce alla rete provenienti da web, cloud, applicazioni, endpoint, dispositivi mobili, database e IoT. Visualizzare le lacune di sicurezza, riconoscere gli attacchi in arrivo, monitorare tutte le possibili origini, compresi i servizi di terzi e adottare le opportune misure difensive. Prevenire attacchi imprevisti e migliorare la sicurezza della rete in funzione di ciò che accade in tempo reale.

Gestire la sicurezza senza attriti.

Avere la situazione sotto controllo. Effettuare tutte le attività di sicurezza da un'unica postazione.

CAPTURE SECURITY CENTER È SINONIMO DI COMPLETEZZA

Usufruire di potenti punti di osservazione simultanea degli ambienti di sicurezza per semplificare i processi gestionali e contabili, velocizzare la presa di decisioni, migliorare l'assistenza e correggere le lacune di sicurezza.



Accessibile dalla consolle di Capture Security Center in ambiente cloud, SonicWall My Workspace consente di eseguire le complesse attività di sicurezza in modo più semplice e più efficace. Il flusso di lavoro sistematico consente di prendere in carico, configurare e gestire in modo semplice e rapido più tenant nelle università, nelle filiali e nei gruppi funzionali, effettuare registrazioni cumulative dei prodotti, attivare licenze e supporto e avviare prove dei prodotti on-demand.

I flussi di lavoro dei tenant consentono l'accesso istantaneo ai responsabili della sicurezza delle organizzazioni, compreso il controllo di accesso granulare e basato sui ruoli per i prodotti gestiti da Capture Security Center. Un pannello di controllo intuitivo consente la visibilità e la conoscenza istantanee di prodotti la cui licenza sta per scadere o che richiedono aggiornamenti software o firmware. Contattare, collaborare e comunicare con i tenant e facilitare, tenere sotto controllo e risolvere problemi e interventi di assistenza attraverso un portale di autoassistenza integrato.

Riepilogo delle caratteristiche di CSC

Gestione

- Accesso in modalità SPOG alla maggior parte delle funzioni
- Sessioni utente contemporanee multiple
- Gestione centralizzata della sicurezza e delle reti
- Pannello di controllo universale
- Gestione dei firewall
- Gestione degli switch SonicWall
- Gestione wireless
- Configurazione unificata delle politiche
- Definizione delle politiche a livello di gruppo
- Replica delle politiche da un dispositivo a un altro o a un gruppo di dispositivi
- Gestione e flusso di lavoro degli ordini di variazione
- Zero-Touch Deployment
- Configurazioni dei dispositivi preimpostate in modalità Zero-Touch
- Installazione e configurazione VPN
- Monitoraggio e allerta dei dispositivi attivi
- Visualizzazione e intelligenza delle applicazioni
- Supporto API, CLI e SNMP
- Gestione Capture Client
- Gestione Cloud App Security
- Gestione sicurezza della posta elettronica in hosting
- MySonicWall e MyWorkspace
- Risk Meters
- Security Center
- Cloud App Security – Attività informatiche nascoste
- Gestione licenze
- Gestione basata sui ruoli (utenti, gruppi)
- Backup dei file con le preferenze per i firewall

Monitoraggio

- Monitoraggio e allerta dei dispositivi
- Flusso dati IPFIX in tempo reale
- Monitoraggio attivo dispositivi e allerte
- Gestione relay SNMP
- Monitoraggio stato VPN e firewall
- Risk Meters

Reportistica

- Memorizzazione firewall centralizzata
- Reportistica basata su Syslog o su IPFIX
- Reportistica PDF personalizzata programmata
- Reportistica minacce multiple
- Reportistica incentrata sull'utente
- Reportistica dell'uso delle applicazioni
- Reportistica botnet
- Reportistica geolocalizzazione
- Reportistica indirizzi MAC
- Reportistica Capture ATP
- Reportistica rogueware access point wireless
- Reportistica CAS (Cloud App Security)
- Reportistica Capture Client
- Reportistica larghezza di banda e servizi in base alle interfacce

Statistiche

- Attività basate sugli utenti
- Uso delle applicazioni
- Visibilità dei diversi prodotti con Capture Client
- Visualizzazione dinamica in tempo reale
- Funzionalità di ricerca (drill-down) e pivoting

Licenze e abbinamenti

I servizi basati sul cloud sono disponibili nelle seguenti formulazioni di pacchetti.

1. CSC Basic Management (Lite)

Questa versione è l'ideale per il backup/ripristino dei sistemi o delle preferenze dei firewall e per l'upgrade del firmware. Tutti i firewall con abbonamento AGSS o CGSS possono beneficiare di questa funzione di gestione base attivata per contribuire a gestire i firewall.

2. CSC Management

Questa opzione di abbonamento a pagamento abilita tutte le funzioni di gestione, comprese Workflow Automation e Zero-Touch Deployment.

3. CSC Management and Reporting

Questa opzione di licenza è l'ideale per realtà di grandi dimensioni, con numerosi firewall installati in diverse sedi distanti tra loro gestite a livello di gruppo o in modalità tenant, come le organizzazioni mid-market, le imprese distribuite, le organizzazioni del settore pubblico e accademico con numerosi distretti e sedi universitarie e i fornitori di servizi gestiti (MSP).

Oltre alle funzionalità di gestione complete, questo abbonamento consente una reportistica completa per l'esecuzione di riesami e verifiche periodiche o a richiesta della sicurezza e delle prestazioni della rete, utilizzando il pannello di controllo universale interattivo a video con diagrammi e tabelle dal vivo, o off-screen con l'esportazione programmata dei report.

4. Statistiche CSC

Si tratta di un potente servizio integrativo per tutte le opzioni di abbonamento Capture Security Center. L'attivazione del servizio consente l'accesso completo agli strumenti e ai servizi SonicWall Analytics e SonicWall Cloud App Security per lo svolgimento di analisi investigative e la ricerca delle minacce di rete grazie a funzionalità complete di drill-down e pivoting. CSC Analytics comprende anche 30 giorni di memorizzazione dei registri di roll over e 365 giorni di reportistica.

Modelli di firewall supportati

Capture Security Center è disponibile per clienti con firewall SOHO-W, SOHO 250, SOHO 250W, TZ Series, NSA Series, NSa 2650-6650 e NSv Series. Per SuperMassive 9000 Series, NSa Series e NSsp da 12400 a 12800, l'opzione di abbonamento a CSC Management viene attivata automaticamente nell'ambito della corrispondente attivazione dell'abbonamento ad AGSS.

CAPTURE SECURITY CENTER			
	Gestione	Reporting[4]	Analytics[4]
FW entry-level	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100	SOHO-W, SOHO 250, SOHO 250W TZ Series, NSv 10-100
FW di fascia media:	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400	NSA Series, NSa Series, NSv 200-400
FW di fascia alta	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600	SuperMassive 9000 series, NSsp 12000 series, NSa 9250-9650, NSv 800-1600

[4] *Il supporto per Reporting e Analytics per i FW di fascia alta è disponibile solo su On_prem Analytics.*

	Funzioni	CSC Management Lite	CSC Management	CSC Management and Reporting	Analisi SaaS	Analisi in sede
Gestione	Backup/ripristino – sistema firewall	Sì	Sì	Sì	Sì	Sì[2]
	Backup/ripristino – preferenze firewall	Sì	Sì	Sì	Sì	Sì[2]
	Aggiornamento firmware	Solo da file locale	Solo da file locale o MySonicWall	Sì	Solo da file locale	Solo da file locale[3]
	Programmazione attività	-	Sì	Sì	-	-
	Gestione di gruppo semplificata	-	Sì	Sì	-	-
	Eredità – avanti/indietro	-	Sì	Sì	-	-
	Installazione zero-touch[1]	-	Sì	Sì	-	-
	Download segnatura firewall offline	-	Sì	Sì	-	-
	Flusso di lavoro	-	Sì	Sì	-	-
	Licenze cumulative: ricerca, condivisione, elenco codici di attivazione utilizzati	-	Sì	Sì	-	-
Reportistica (basata su Netflow/IPFix)	Programmazione report, monitoraggio dal vivo, riepilogo pannelli di controllo	-	-	Sì	Sì	Sì
	Download report: Applicazioni, Threat, CFS, Utenti, Traffico, Origine/ Destinazione (reportistica di flusso 1 anno)	-	-	Sì	Sì	Sì
Statistiche (basate su Netflow/IPFix)	Indagini di rete di tipo forense e ricerca delle minacce tramite drill-down e pivot	-	-	-	Sì	Sì
	Cloud App Security – Attività informatiche nascoste	-	-	-	Sì	No
	Conservazione dati	-	-	-	Traffico 30 giorni	1 anno
Supporto tecnico		Solo Web Case	Supporto 24x7	Supporto 24x7	Supporto 24x7	Supporto 24x7

[1] *Supportata per SOHO-W con firmware 6.5.2+; TZ, NSA series e NSa 2650-6650 con firmware 6.5.1.1+. Non supportata per SOHO o NSv series.*
[2] *Richiede il servizio AGSS/CGSS o qualsiasi servizio Capture Security Center a pagamento*
[3] *Richiede una licenza di assistenza 24x7*

Informazioni per l'ordinazione

Prodotto	SKU
SonicWall Capture Security Center Management per TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 – 100 1 anno	01-SSC-3664
SonicWall Capture Security Center Management per TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 – 100 2 anni	01-SSC-9151
SonicWall Capture Security Center Management per TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 – 100 3 anni	01-SSC-9152
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 1 anno	01-SSC-3665
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 2 anni	01-SSC-9214
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 3 anni	01-SSC-9215
SonicWall Capture Security Center Management per TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 – 100 1 anno	01-SSC-3435
SonicWall Capture Security Center Management per TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 – 100 2 anni	01-SSC-9148
SonicWall Capture Security Center Management per TZ Series, SOHO-W, SOHO 250, SOHO 250W, NSv 10 – 100 3 anni	01-SSC-9149
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 1 anno	01-SSC-3879
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 2 anni	01-SSC-9154
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 3 anni	01-SSC-9202
SonicWall Capture Security Center Analytics per SOHO-W, SOHO 250, SOHO250W, TZ Series, NSv 10 – 100 1 anno	02-SSC-0171
SonicWall Capture Security Center Management per NSA 2600 – 6600, NSa 2650 – 6650 e NSv 200 – 400 1 anno	02-SSC-0391

Internet Browser

- Microsoft® Internet Explorer versione 11.0 o successiva (non usare in modalità compatibilità)
- Mozilla Firefox versione 37.0 o successiva
- Google Chrome versione 42.0 o successiva
- Safari (ultima versione)

Dispositivi SonicWall supportati gestiti da Capture Security Center

- Dispositivi SonicWall Email Security Serie SuperMassive E10000 e 9000, E-Class NSA, NSsp Series, NSa Series, TZ Series, SOHO-W, SOHO 250, SOHO 250W
- Certificazione SonicWall Network Security Professional Serie NSv
- SonicWall Endpoint Security – Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)
- SonicWall Email Security
- SonicWall Web Application Firewall
- SonicWall Secure Mobile Access: SMA serie 100

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-CaptureSecurityCenter-US-COG-2315