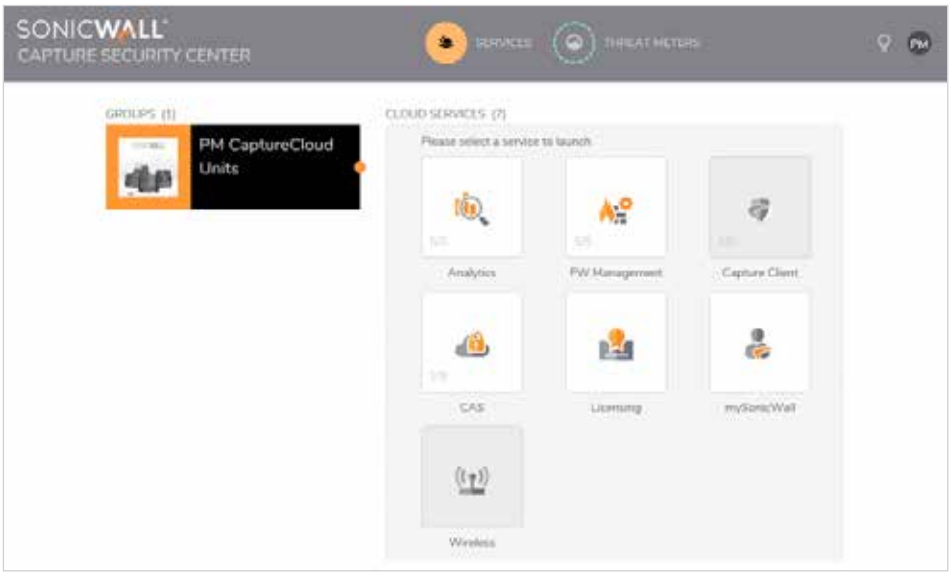
SONICWALL CAPTURE SECURITY CENTER

Gestione unificata, reporting e analisi forniti via cloud per la protezione di rete, endpoint e cloud

SonicWall Capture Security Center è un software di gestione della sicurezza aperto, scalabile e basato su cloud, disponibile come conveniente soluzione as-a-service per imprese e fornitori di servizi di vario tipo e dimensioni. Offre la massima visibilità, agilità e capacità di gestire centralmente l'intero ecosistema di sicurezza SonicWall con maggiore chiarezza, precisione e velocità – il tutto da un unico pannello di controllo. Questa architettura orientata al cloud e ai servizi unifica e connette i servizi di sicurezza e gli strumenti di gestione SonicWall per aiutare a ottenere migliori efficienze operative ed elasticità, supportando al contempo una strategia di difesa informatica più ampia.

Basato su processi aziendali e requisiti dei livelli di servizio, Capture Security Center consente ai Security Operation Center (SOC) di creare le basi per una strategia unificata di governance della sicurezza, conformità e gestione dei rischi. Mediante un approccio olistico e connesso all'orchestrazione della sicurezza, Capture Security Center combina tutti gli aspetti operativi della protezione di rete, endpoint e cloud attraverso un framework di gestione semplice e comune. Semplifica e, in molti casi, automatizza varie attività per consentire un migliore coordinamento della sicurezza e processi decisionali migliori, riducendo la complessità, il tempo e le spese richiesti per eseguire le operazioni di sicurezza e le attività di gestione. Queste attività comprendono il provisioning e la configurazione di firewall e endpoint, il monitoraggio, la creazione di report, l'applicazione di patch, il controllo e l'analisi del traffico e dei dati, che è uno strumento prezioso per rilevare e reagire ai problemi di sicurezza prima che si verifichino.



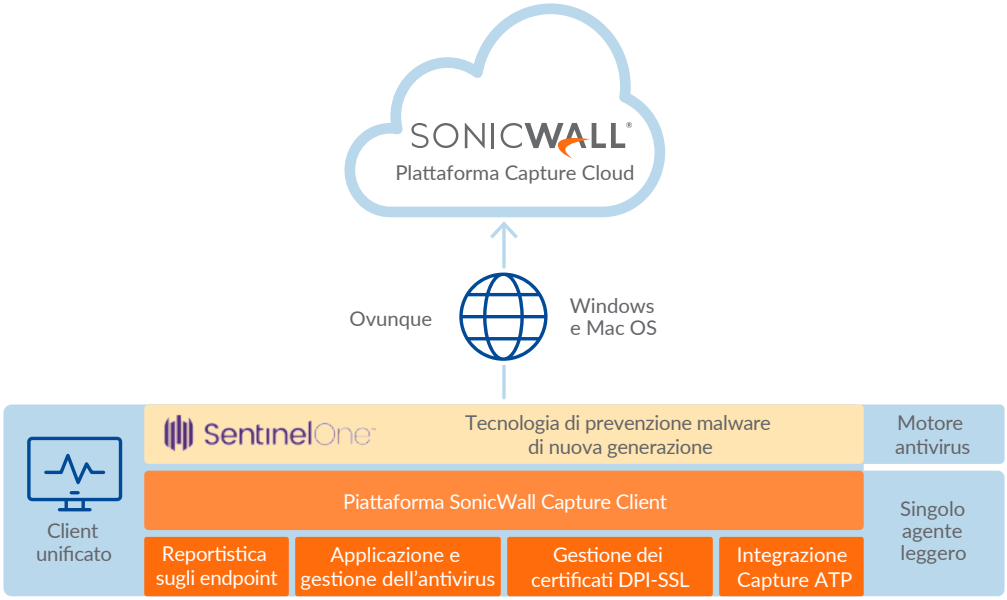
Vantaggi:

- Programma unificato per la governance della sicurezza, la conformità e la gestione del rischio
- Una console di gestione e facile integrazione per tutte le vostre soluzioni SonicWall
- I flussi di lavoro automatizzati assicurano la conformità ai requisiti di sicurezza e una gestione delle policy priva di errori
- Implementazione e provisioning remoti zero-touch dei firewall SonicWall in modo semplice e veloce
- Visibilità e consapevolezza situazionale dell'ambiente di sicurezza della rete da un unico pannello
- Analisi investigative e forensi approfondite dei dati di sicurezza arricchiti
- Riduzione dei tempi di risposta agli eventi imprevisti grazie all'intelligence delle minacce in tempo reale

Capture Security Center offre l'accesso Single Sign-On per la registrazione delle licenze, il provisioning e la gestione di tutti i vostri servizi per la sicurezza di rete, endpoint e cloud. Questi servizi includono Firewall Management, Analytics, Capture Client e Cloud Application Security. La nostra visione di unificare l'intera gamma di servizi per la sicurezza del portafoglio SonicWall in un unico strumento di gestione facilmente integrabile include i servizi di sicurezza per web, wireless, email, mobile e IoT.[1] La combinazione di questi servizi cloud fornisce una difesa informatica multilivello fondamentale, intelligence delle minacce, analisi, collaborazione e comuni funzionalità di gestione, reporting e analisi che interagiscono in modo sincrono. Con gli aggiornamenti software e il supporto inclusi in un servizio di abbonamento attivo, l'accesso alle innovazioni e ai miglioramenti più recenti è immediato. In questo modo è possibile gestire i rischi legati alla sicurezza, rispettare gli obblighi normativi e difendersi dalle vulnerabilità e le minacce più recenti in modo automatizzato. Grazie a scalabilità e flessibilità illimitate, Capture Security Center si adatta prontamente e on demand a modifiche della capacità e a cambiamenti aziendali.

Capture Client

Dal Capture Security Center è possibile accedere a SonicWall Capture Client, una piattaforma client unificata che offre diverse funzionalità per la protezione degli endpoint. Dotato di un motore di protezione contro il malware di nuova generazione con tecnologia SentinelOne, Capture Client applica tecniche di protezione avanzate contro le minacce come l'apprendimento automatico e il ripristino di sistema. In tal modo protegge dai 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. In combinazione con i firewall SonicWall, Capture Client offre anche visibilità sul traffico crittografato mediante la gestione di certificati SSL attendibili utilizzati per l'ispezione Deep Packet del traffico SSL/TLS.



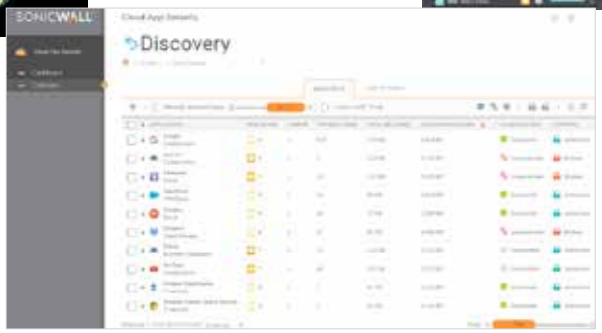
[1] *I servizi di sicurezza per web, wireless, email, dispositivi mobili e IoT saranno completamente integrati in questa piattaforma e segnalati negli annunci di prodotto futuri.*

Cloud App Security

L'abbonamento in bundle SonicWall Capture Security Center Analytics offre ai clienti visibilità sullo shadow IT e controllo sull'utilizzo delle applicazioni cloud. SonicWall Cloud App Security fornisce funzionalità simili a CASB. Consente agli amministratori di rilevare l'uso di applicazioni rischiose, monitorare l'attività degli utenti e impostare policy di autorizzazione/blocco per le applicazioni IT approvate e non approvate sui firewall gestiti, per proteggere i dati sensibili.

Rilevamento dello shadow IT, visibilità in tempo reale e classificazione e controllo delle applicazioni sono le caratteristiche principali del servizio Cloud App Security. Il servizio garantisce l'adozione sicura delle applicazioni SaaS senza compromettere la produttività dei dipendenti e con un costo totale di proprietà ridotto.

1. **Rilevamento dello shadow IT:** utilizza i file di log esistenti del firewall per automatizzare la ricerca nel cloud e identificare le applicazioni utilizzate e il loro potenziale di rischio.
2. **Visibilità delle applicazioni in tempo reale:** consente di monitorare l'utilizzo in tempo reale con un dashboard intuitivo che fornisce dettagli sulle applicazioni in uso, il volume di traffico, le attività degli utenti e il luogo di utilizzo.
3. **Classificazione e controllo delle applicazioni:** classifica le applicazioni cloud non gestite in Applicazioni approvate (dall'IT) e Applicazioni non approvate (dall'IT), e imposta policy di autorizzazione/blocco basate sul punteggio di rischio delle applicazioni.



Automazione dei flussi di lavoro

Mediante l'automazione nativa dei flussi di lavoro, Capture Security Center aiuta i SOC a conformarsi ai requisiti di controllo e gestione delle modifiche delle policy dei firewall previsti da varie normative quali PCI, HIPAA e GDPR. Consente la modifica delle policy del firewall mediante una serie di rigorose procedure di configurazione, comparazione, convalida, revisione e approvazione delle policy prima della loro implementazione. I gruppi di approvazione sono flessibili per consentire la conformità alle varie procedure di autorizzazione e controllo previste da diversi tipi di organizzazioni. L'automazione dei flussi di lavoro applica in modo programmatico le policy di sicurezza approvate per migliorare l'efficienza operativa, ridurre al minimo i rischi ed eliminare gli errori.

Capture Security Center offre un approccio olistico alla governance della sicurezza, alla conformità e alla gestione del rischio.

1. CONFIGURAZIONE E CONFRONTO

Capture Security Center configura gli **ordini di modifica** delle policy e le differenze in base a **codici colore** per offrire confronti chiari

2. CONVALIDA

Capture Security Center esegue una **convalida dell'integrità della logica delle policy**

3. REVISIONE E APPROVAZIONE

Capture Security Center invia e-mail ai revisori e registra un **audit trail di approvazione/disapprovazione** delle policy

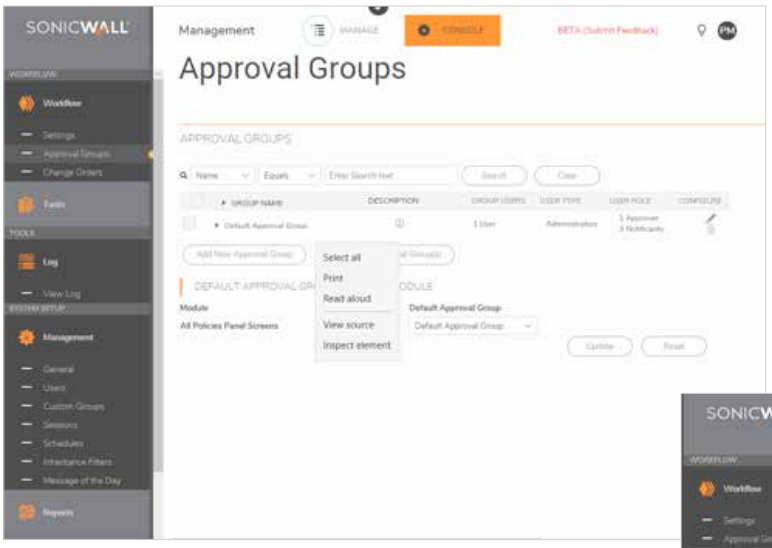
4. IMPLEMENTAZIONE

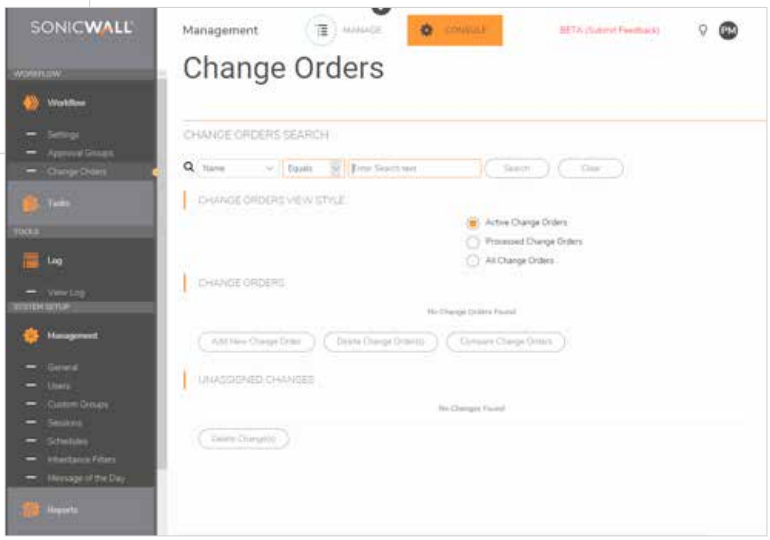
Capture Security Center implementa le modifiche alle policy immediatamente o **in modo pianificato**

5. CONTROLLO

I log delle modifiche consentono un **controllo** accurato delle policy e dati di **conformità** esatti

Automazione dei flussi di lavoro: cinque passaggi per una perfetta gestione delle policy





Implementazione zero-touch

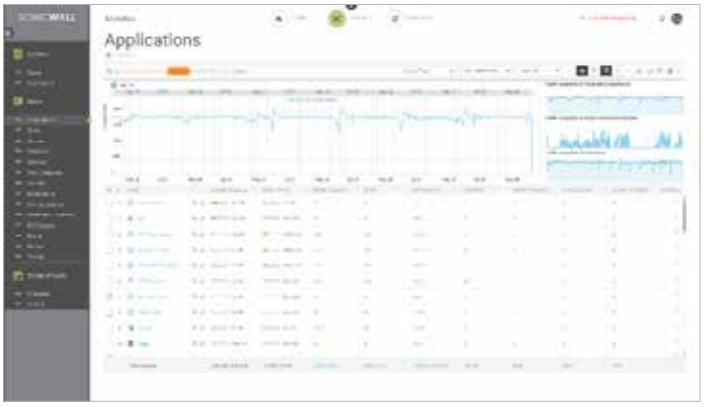
Nel Capture Security Center è integrato il servizio Zero-Touch Deployment, che semplifica e velocizza il processo di provisioning dei firewall SonicWall presso sedi remote e filiali. Il processo richiede un intervento minimo da parte dell'utente ed è completamente automatizzato per rendere operativi i firewall su vasta scala in quattro semplici passaggi. Questo riduce significativamente il tempo, i costi e la complessità associati all'installazione e alla configurazione, mentre la protezione e la connettività vengono applicate in modo immediato e automatico.

FASE 1	**REGISTRAZIONE DEL FIREWALL** Registrare il nuovo firewall in MySonicWall utilizzando il numero seriale e il codice di autenticazione assegnati.
FASE 2	**CONNESSIONE DEL FIREWALL** Collegare il firewall alla rete utilizzando il cavo Ethernet fornito in dotazione all'unità.
FASE 3	**ACCENSIONE DEL FIREWALL** Accendere il firewall dopo aver collegato il cavo di alimentazione e averlo inserito in una presa a muro standard. Alle unità viene automaticamente assegnato un IP WAN tramite il server DHCP. Una volta stabilità la connettività, l'unità viene automaticamente rilevata, autenticata e aggiunta al Capture Security Center e tutte le licenze e configurazioni vengono sincronizzate con MySonicWall e License Manager.
FASE 4	**GESTIONE DEL FIREWALL** L'unità è ora operativa e gestita tramite la console di gestione centrale basata su cloud di Capture Security Center, che si occupa degli aggiornamenti del firmware, delle patch di sicurezza e delle modifiche alla configurazione a livello di gruppo.

Implementazione zero-touch: quattro semplici passaggi per rendere operativo il firewall

Reporting

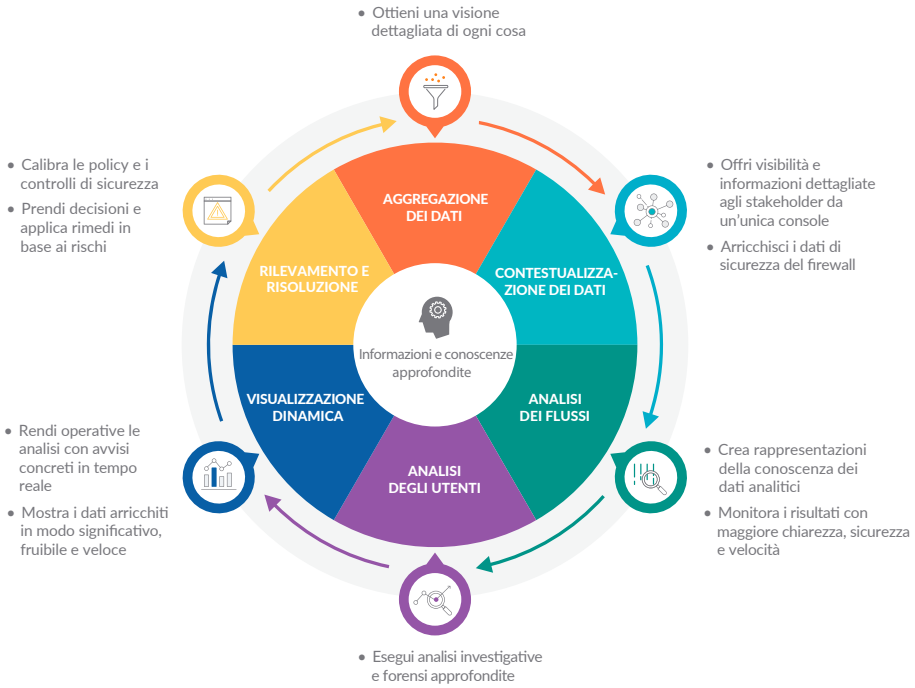
Capture Security Center offre più di 140 report predefiniti e la flessibilità di creare report personalizzati utilizzando una qualsiasi combinazione di dati verificabili per acquisire i risultati di vari casi d'uso. Questi risultati includono un quadro generale e informazioni dettagliate su eventi di rete, attività degli utenti, minacce, problemi operativi e prestazionali, efficacia della sicurezza, rischi e lacune di sicurezza, preparazione alla conformità e analisi a posteriori. Ogni report è progettato sulla base degli input collettivi ricevuti da clienti e partner di SonicWall nell'arco di numerosi anni. Ciò fornisce maggiore granularità, contesto e conoscenza dei dati Syslog e IPFIX/NetFlow necessari ai SOC per monitorare, misurare e garantire un funzionamento efficace della rete e delle misure di sicurezza.

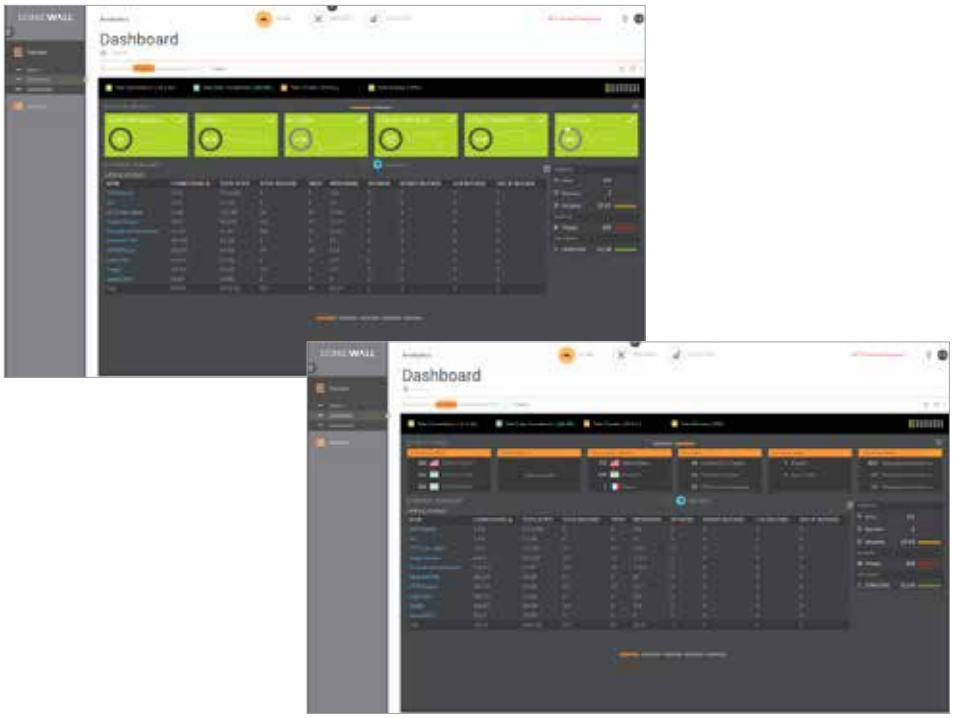


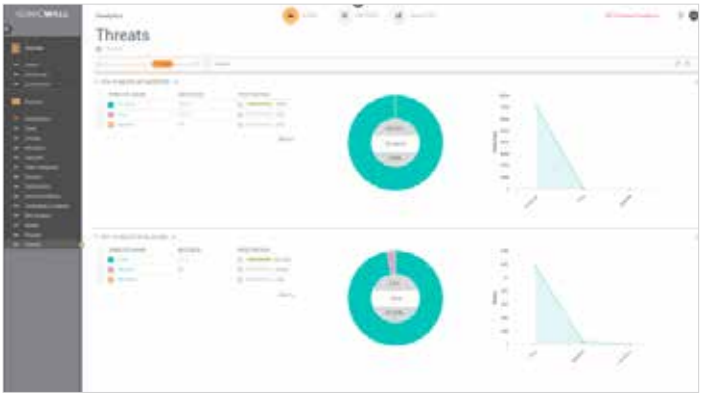
Analisi

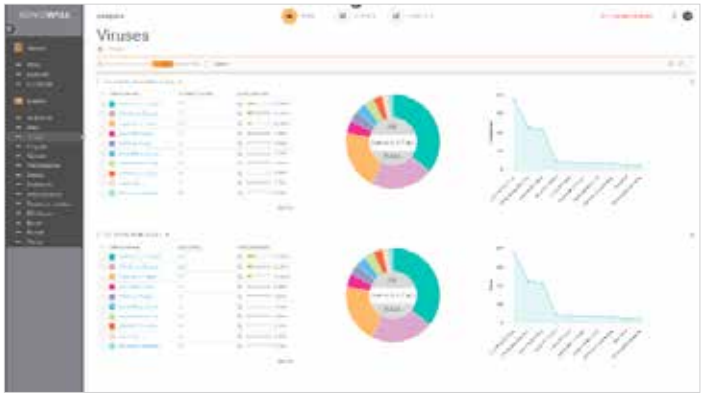
SonicWall Analytics è un motore di analisi dei big data con capacità di intelligence che automatizza l'aggregazione, la normalizzazione, la correlazione e la contestualizzazione dei dati di sicurezza che passano attraverso tutti i firewall gestiti. Fornisce alle aziende informazioni dettagliate in tempo reale su tutto quello che succede nelle loro reti. I risultati, presentati in modo strutturato, significativo, fruibile e facilmente utilizzabile, consentono ai team addetti alla sicurezza e ad analisti, revisori, dirigenti di alto livello e stakeholder di rilevare, interpretare, assegnare priorità, prendere decisioni e adottare misure difensive e correttive appropriate.

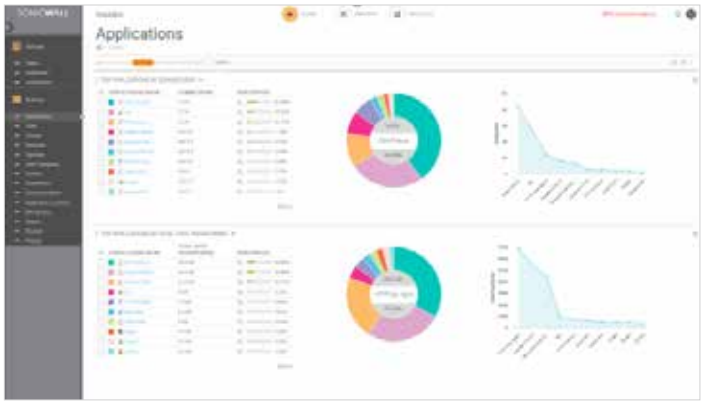
Analytics presenta visualizzazioni, monitoraggio e avvisi in tempo reale dei dati di sicurezza arricchiti in un unico pannello di controllo. I potenti strumenti di Analytics offrono ai clienti la completa autorità, agilità e flessibilità per eseguire ampie analisi investigative con drill-down per il traffico di rete, le attività degli utenti, gli eventi di sicurezza, il profilo delle minacce, l'uso delle applicazioni e altri innumerevoli dati contestuali del firewall. Questa profonda visibilità, conoscenza e comprensione dell'ambiente di sicurezza fornisce ai clienti informazioni preziose e la capacità non solo di scoprire i rischi per la sicurezza ma anche di orchestrarne la risoluzione, monitorando i risultati con maggiore chiarezza e velocità. Analytics consente ai clienti di rendere operative le analisi di sicurezza e di integrarle nei processi aziendali per trasformare i dati in informazioni, le informazioni in conoscenza e la conoscenza in decisioni per ottenere una completa automazione della sicurezza.











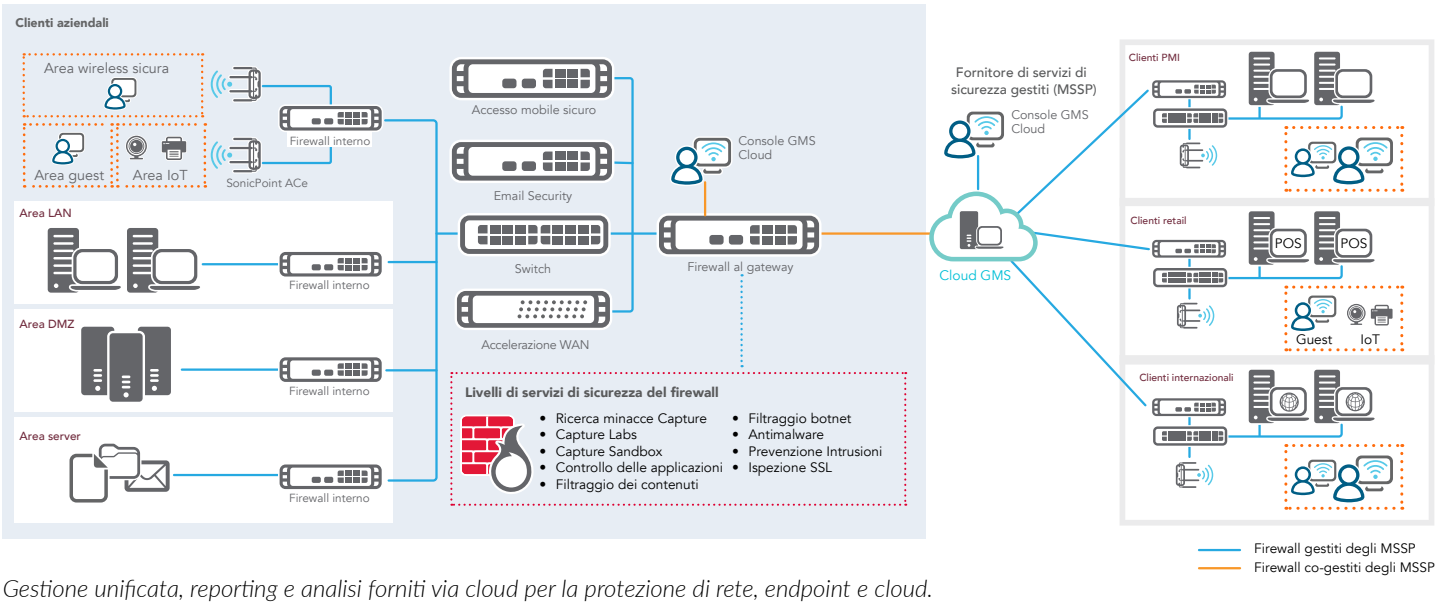
SONICWALL®

Architettura cloud scalabile

L'architettura distribuita di Capture Security Center favorisce la disponibilità e scalabilità illimitate del sistema. Per supportare le esigenze di grandi imprese, operatori di telecomunicazioni, compagnie telefoniche e service provider con un solido ecosistema multi-tenant, Capture Security Center è scalabile su richiesta per supportare migliaia di dispositivi di sicurezza SonicWall gestiti, indipendentemente dalla loro posizione.

Per il cliente ciò si traduce in dashboard universali altamente interattivi con monitoraggi in tempo reale, report e dati analitici per aiutarlo a prendere decisioni intelligenti sulle politiche di sicurezza, favorendo la collaborazione, la comunicazione e il trasferimento di conoscenze nell'infrastruttura di sicurezza condivisa. Una visione globale dell'ambiente di sicurezza aziendale e la condivisione di informazioni sulla sicurezza in tempo reale con le persone giuste in azienda consentono di creare policy e controlli di sicurezza accurati, per realizzare una strategia di protezione più solida e adattiva.

Capture Security Center offre una piattaforma di gestione, analisi e reporting completa e scalabile per imprese distribuite e fornitori di servizi (compagnie telefoniche, operatori di telecomunicazioni e MSP).



Gestione unificata, reporting e analisi forniti via cloud per la protezione di rete, endpoint e cloud.

Funzionalità di gestione e monitoraggio della sicurezza	
Funzionalità	Descrizione
Gestione centralizzata della sicurezza e della rete	Aiuta gli amministratori a implementare, gestire e monitorare un ambiente di rete distribuito.
Configurazione di policy federate	Semplice configurazione delle policy per migliaia di firewall SonicWall, punti di accesso wireless, soluzioni di email security, dispositivi di accesso remoto sicuro e switch da una postazione centralizzata.
Gestione degli ordini di modifica e flusso di lavoro	Garantisce la correttezza e la conformità delle modifiche alle policy applicando un processo di configurazione, comparazione, convalida, revisione e approvazione delle policy prima della loro implementazione. I gruppi di approvazione sono configurabili dagli utenti per assicurare la conformità alle policy di sicurezza aziendali. Tutte le modifiche alle policy vengono registrate in un formato verificabile, garantendo così la conformità del firewall ai requisiti normativi. Tutti i dettagli granulari di ogni modifica effettuata sono registrati in ordine cronologico per facilitare il rispetto della conformità, gli audit trail e la risoluzione di problemi.
Implementazione zero-touch	Semplifica e velocizza l'implementazione e il provisioning dei firewall SonicWall in remoto attraverso il cloud. Distribuisce automaticamente le policy, esegue gli aggiornamenti del firmware e sincronizza le licenze.
Configurazione e implementazione VPN avanzate	Gli switch X-Series di Dell possono essere gestiti facilmente con i firewall delle serie TZ, NSa e SuperMassive, offrendo una gestione unificata dell'intera infrastruttura di sicurezza della rete.
Gestione offline	Semplifica e velocizza l'implementazione e il provisioning dei firewall SonicWall in remoto attraverso il cloud. Distribuisce automaticamente le policy, esegue gli aggiornamenti del firmware e sincronizza le licenze.
Gestione semplificata delle licenze	Semplifica la creazione di connessioni VPN e consolida migliaia di policy di sicurezza.
Dashboard universale	Widget personalizzabili, mappe geografiche e report basati sugli utenti.
Monitoraggio e notifica dei dispositivi attivi	Fornisce notifiche in tempo reale con funzionalità di monitoraggio integrate per semplificare la risoluzione dei problemi e consentire agli amministratori di adottare misure preventive e fornire interventi immediati.
Supporto SNMP	Le notifiche trap avanzate in tempo reale per tutti i dispositivi e le applicazioni abilitati per TCP/IP (Transmission Control Protocol/Internet Protocol) e SNMP migliorano notevolmente la risoluzione dei problemi grazie alla rapida identificazione e reazione agli eventi critici della rete.
Visualizzazione e intelligence delle applicazioni	Rapporti in tempo reale e storici sulle applicazioni in uso e sugli utenti che le utilizzano. I rapporti sono completamente personalizzabili con intuitive funzioni di filtraggio e drill-down.
Numerose opzioni di integrazione	Interfaccia di programmazione delle applicazioni (API) per i servizi Web, supporto per interfaccia a riga di comando (CLI) per la maggior parte delle funzioni e supporto per trap SNMP per fornitori di servizi e imprese.
Gestione di switch Dell Networking X-Series	Gli switch X-Series di Dell possono essere gestiti facilmente con i firewall delle serie TZ, NSa e SuperMassive, offrendo una gestione unificata dell'intera infrastruttura di sicurezza della rete.
Reporting	
Funzionalità	Descrizione
Rapporti Botnet	Sono disponibili quattro tipi di rapporti (tentativi, obiettivi, iniziatori e cronologia), contenenti informazioni di contesto sui vettori di attacco come ID delle botnet, indirizzi IP, paesi, host, porte, interfacce, iniziatore/obiettivo, origine/destinazione e utente.
Report GeoIP	Contiene informazioni sul traffico bloccato basate sul Paese di origine o di destinazione del traffico. Sono disponibili quattro tipi di rapporti (tentativi, obiettivi, iniziatori e cronologia), contenenti informazioni di contesto sui vettori di attacco come ID delle botnet, indirizzi IP, paesi, host, porte, interfacce, iniziatore/obiettivo, origine/destinazione e utente.
Report sull'indirizzo MAC	Nella pagina del rapporto viene visualizzato l'indirizzo MAC (Media Access Control), oltre a informazioni specifiche del dispositivo (MAC dell'iniziatore e del risponditore). Sono disponibili cinque tipi di rapporto: • Utilizzo dati > Iniziatori • Utilizzo dati > Risponditori • Utilizzo dati > Dettagli • Attività utente > Dettagli • Attività Web > Iniziatori
Report Capture ATP	Questo rapporto mostra informazioni dettagliate sul comportamento delle minacce per reagire a una minaccia o ad un'infezione.
Report conformi a HIPAA, PCI e SOX	I modelli di report predefiniti, conformi ai requisiti PCI, HIPAA e SOX, consentono di soddisfare i controlli di conformità della sicurezza.

Reporting (cont.)	
Funzionalità	Descrizione
Creazione di report su punti di accesso wireless non autorizzati	Visualizzazione di tutti i dispositivi wireless in uso e di comportamenti non autorizzati da connessioni di rete ad hoc o peer-to-peer tra gli host e associazioni accidentali per gli utenti che si collegano a reti vicine non autorizzate.
Rapporti intelligenti e visualizzazione delle attività	Gestione completa e creazione di report grafici per i firewall, le soluzioni di sicurezza e-mail e i dispositivi di accesso mobile sicuro SonicWall. Offre maggiore visibilità sui trend di utilizzo e gli eventi relativi alla sicurezza, rafforzando l'immagine di brand per i fornitori di servizi.
Sistema di logging centralizzato	Un unico strumento centralizzato per consolidare gli eventi di sicurezza e i log di migliaia di appliance o effettuare analisi forensi della rete.
Report in tempo reale o storici basati su syslog di nuova generazione	La rivoluzionaria architettura potenziata semplifica il laborioso processo di riepilogo dei dati, fornendo report quasi in tempo reale sui messaggi syslog in arrivo, con la possibilità di eseguire analisi drill-down dei dati e personalizzare ampiamente i report.
Report pianificati universali	Creazione automatica di report pianificati per diverse appliance di vario tipo, che vengono poi inviati per e-mail a destinatari autorizzati.
Analisi	
Funzionalità	Descrizione
Aggregazione dei dati	Il motore analitico basato su intelligence automatizza l'aggregazione, la normalizzazione, la correlazione e la contestualizzazione dei dati di sicurezza che passano attraverso tutti i firewall.
Contestualizzazione dei dati	Le analisi fruibili, presentate in modo strutturato, significativo e facilmente utilizzabile, consentono ai team addetti alla sicurezza, agli analisti e alle parti interessate di rilevare, interpretare, prioritizzare, prendere decisioni e adottare misure difensive appropriate.
Analisi in streaming	I flussi di dati sulla sicurezza di rete sono costantemente elaborati, correlati e analizzati in tempo reale, e i risultati sono illustrati visivamente in un dashboard dinamico interattivo.
Analisi degli utenti	L'analisi approfondita delle attività degli utenti offre la completa visibilità sulle loro tendenze di utilizzo, accesso e connessione nell'intera rete.
Visualizzazione dinamica in tempo reale	Mediante un unico pannello di controllo, il team dedicato alla sicurezza può eseguire approfondite analisi investigative e forensi dei dati di sicurezza con maggiore precisione, chiarezza e velocità.
Rapido rilevamento e correzione	Le funzionalità investigative consentono di monitorare le attività non sicure e di gestire ed eliminare i rischi con rapidità.
Analisi e rapporti sui flussi	Un agente di reporting sui flussi relativi all'analisi del traffico delle applicazioni e ai dati di utilizzo tramite i protocolli IPFIX o NetFlow consente il monitoraggio in tempo reale e cronologico. Gli amministratori dispongono così di un'interfaccia efficace ed efficiente per monitorare visivamente la propria rete in tempo reale, con la capacità di individuare le applicazioni e i siti web che richiedono più larghezza di banda, visualizzare l'utilizzo delle applicazioni per ogni utente e anticipare gli attacchi e le minacce diretti alla rete. • Visualizzatore in tempo reale personalizzabile con funzioni drag-and-drop • Schermata con report in tempo reale e filtraggio con un semplice clic • Dashboard sui flussi principali con pulsanti per la visualizzazione in base a categorie • Schermata con rapporti sui flussi, con cinque schede aggiuntive sugli attributi dei flussi • Schermata di analisi dei flussi con potenti funzioni di correlazione e pivoting • Visualizzatore di sessioni per analisi drill-down approfondite di singole sessioni e pacchetti.
Analisi del traffico delle applicazioni	Offre alle aziende informazioni dettagliate sul traffico delle applicazioni, sull'uso della larghezza di banda e sulle minacce alla sicurezza, oltre a potenti funzioni di risoluzione dei problemi e analisi forense.
Cloud App Security	
Funzionalità	Descrizione
Dashboard in tempo reale	Fornisce una rappresentazione visiva in tempo reale delle applicazioni in uso, del volume di traffico, delle attività degli utenti e del luogo di utilizzo.
App Discovery	Automatizza il rilevamento delle applicazioni cloud, utilizzando i file di log del vostro firewall SonicWall per identificare attività di shadow IT nella rete.
App Risk Assessment	Consente di prendere decisioni informate sulle applicazioni da bloccare/sbloccare in base alla valutazione dei rischi.
App Classification and Control	Classifica le applicazioni in Approvate e Non approvate e imposta policy per bloccare le applicazioni rischiose.

Riepilogo delle funzionalità

Gestione

- Accesso ubiquitario
- Avvisi e notifiche
- Strumenti di diagnostica
- Varie sessioni utente simultanee
- Gestione e pianificazione offline
- Gestione delle policy di sicurezza dei firewall
- Gestione delle policy di sicurezza VPN
- Gestione delle policy di sicurezza e-mail
- Gestione delle policy di accesso remoto sicuro/VPN SSL
- Gestione dei servizi di sicurezza a valore aggiunto
- Definizione di modelli di policy a livello di gruppi
- Replica delle policy da un dispositivo a un gruppo di dispositivi
- Replica delle policy dal livello di gruppo a un singolo dispositivo
- Ridondanza ed elevata disponibilità
- Gestione del provisioning
- Architettura scalabile e distribuita
- Viste di gestione dinamica
- Gestione unificata delle licenze
- CLI (Command Line Interface)
- Interfaccia di programmazione delle applicazioni (API) per i servizi Web
- Gestione basata sui ruoli (utenti, gruppi)
- Dashboard universale
- Backup dei file di preferenze per le appliance firewall

Monitoraggio

- Flussi di dati IPFIX in tempo reale
- Supporto SNMP
- Monitoraggio e avvisi per i dispositivi attivi
- Gestione relay SNMP
- Monitoraggio stato VPN e firewall
- Monitoraggio e avvisi syslog in tempo reale

Reporting

- Serie completa di report grafici
- Creazione di report sulla conformità
- Creazione di report personalizzabili con funzioni drill-down
- Sistema di logging centralizzato
- Creazione di report su minacce multiple
- Creazione di report incentrati sull'utente
- Creazione di report sull'utilizzo delle applicazioni
- Creazione di report granulari sui servizi
- Nuova intelligence degli attacchi
- Report su larghezza di banda e servizi per ogni interfaccia
- Creazione di report per firewall SonicWall UTM
- Creazione di report per appliance VPN SSL SRA SonicWall
- Report universali pianificati
- Report Syslog e IPFIX di nuova generazione
- Creazione di report quasi in tempo reale flessibili e granulari
- Creazione di report sulla larghezza di banda per utente
- Creazione di report sull'attività VPN del client
- Riepilogo dettagliato del report sui servizi tramite VPN
- Creazione di report su punti di accesso wireless non autorizzati
- Creazione di report sui firewall per applicazioni Web (WAF) SRA per le PMI
- Report per Cloud App Security (CAS)
- Report per Capture Client

Analisi

- Aggregazione dei dati
- Contestualizzazione dei dati
- Analisi in streaming
- Analisi degli utenti
- Visualizzazione dinamica in tempo reale
- Rapido rilevamento e correzione

Licenze e pacchetti

Capture Security Center (CSC)		Livello di licenza			
		CSC Management Lite	CSC Management	CSC Management and Reporting	CSC Analytics
Requisito della licenza	Disponibile per i clienti con abbonamento AGSS/CGSS attivo	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS	AGSS/CGSS
Gestione	Pannello di controllo	✓	✓	✓	
	Backup/ripristino	✓	✓	✓	
	Pianificazione attività		✓	✓	
	Gestione firewall di gruppo		✓	✓	
	Ereditarietà (forward/reverse)		✓	✓	
	Zero touch		✓	✓	
	Download di firme firewall offline		✓	✓	
	Flusso di lavoro		✓	✓	
Reporting	Monitoraggio in tempo reale, dashboard di riepilogo			✓	
	Report scaricabili: applicazioni, minacce, CFS, utenti, traffico, ecc.			✓	
	Report pianificati			✓	
Analisi	Analytics (conservazione per 30 giorni)				✓
	Cloud App Security (conservazione per 30 giorni)				✓

Informazioni per l'ordinazione di Capture Security Center

Prodotto	SKU
SonicWall Capture Security Center Management per TZ Series, NSv 10 - 100, 1 anno	01-SSC-3664
SonicWall Capture Security Center Management per TZ Series, NSv 10 - 100, 2 anni	01-SSC-9151
SonicWall Capture Security Center Management per TZ Series, NSv 10 - 100, 3 anni	01-SSC-9152
SonicWall Capture Security Center Management per NSA 2600 - 6650 e NSv 200 - 400, 1 anno	01-SSC-3665
SonicWall Capture Security Center Management per NSA 2600 - 6650 e NSv 200 - 400, 2 anni	01-SSC-9214
SonicWall Capture Security Center Management per NSA 2600 - 6650 e NSv 200 - 400, 3 anni	01-SSC-9215
SonicWall Capture Security Center Management and Reporting per TZ Series, NSv 10 - 100, 1 anno	01-SSC-3435
SonicWall Capture Security Center Management and Reporting per TZ Series, NSv10 - 100, 2 anni	01-SSC-9148
SonicWall Capture Security Center Management and Reporting per TZ Series, NSv 10 - 100, 3 anni	01-SSC-9149
SonicWall Capture Security Center Management and Reporting per NSA 2600 - 6650 e NSv 200 - 400, 1 anno	01-SSC-3879
SonicWall Capture Security Center Management and Reporting per NSA 2600 - 6650 e NSv 200 - 400, 2 anni	01-SSC-9154
SonicWall Capture Security Center Management and Reporting per NSA 2600 - 6650 e NSv 200 - 400, 3 anni	01-SSC-9202
SonicWall Capture Security Center Analytics per TZ Series, NSv 10 - 100, 1 anno	02-SSC-0171
SonicWall Capture Security Center Analytics per NSA 2600 - 6650 e NSv 200 - 400, 1 anno	02-SSC-0391

Browser

- Microsoft® Internet Explorer 11.0 o superiore (non usare la modalità di compatibilità)
- Mozilla Firefox 37.0 o superiore
- Google Chrome 42.0 o superiore
- Safari (versione più recente)

Appliance SonicWall gestibili da Capture Security Center

- Appliance di sicurezza di rete SonicWall: NSa 2600 fino a NSa 6650 e TZ Series
- Appliance di sicurezza di rete SonicWall virtuali: NSv 10 fino a NSv 400
- SonicWall Endpoint Security - Capture Client
- SonicWall Cloud Security – Cloud App Security (CAS)

Informazioni su SonicWall

Da oltre 26 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-CaptureSecurityCenter-US-VG-MKTG2657