SonicWall Analytics

Trasforma i dati in informazioni, le informazioni in conoscenze, le conoscenze in decisioni e le decisioni in azioni

SonicWall Analytics offre una visione dettagliata di tutto quello che succede all'interno dell'ambiente di sicurezza di rete SonicWall – il tutto in un unico pannello di controllo. È basato su un potente motore analitico 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 e i punti di accesso wireless di SonicWall. Il dashboard interattivo dell'applicazione utilizza varie forme di diagrammi relativi a tempo/utilizzo e tabelle per creare rappresentazioni della conoscenza dei modelli di dati.

Analytics presenta i risultati in modo significativo, fruibile e facilmente utilizzabile. Ciò consente ai team responsabili della sicurezza e ad analisti, revisori e dirigenti di alto livello di individuare, interpretare, assegnare priorità e prendere decisioni basate su dati concreti, e di adottare misure difensive e correttive appropriate contro i rischi e le minacce man mano che si presentano durante il processo di rilevamento.

Analytics offre informazioni dettagliate in tempo reale e visibilità, autorità e flessibilità da un unico pannello di controllo ai soggetti interessati, che in questo modo possono eseguire analisi investigative e forensi approfondite sul traffico di rete, l'accesso degli utenti, la connettività, le applicazioni e il loro utilizzo, lo stato delle risorse di sicurezza, gli eventi di sicurezza, i profili delle minacce e altri dati relativi al firewall.

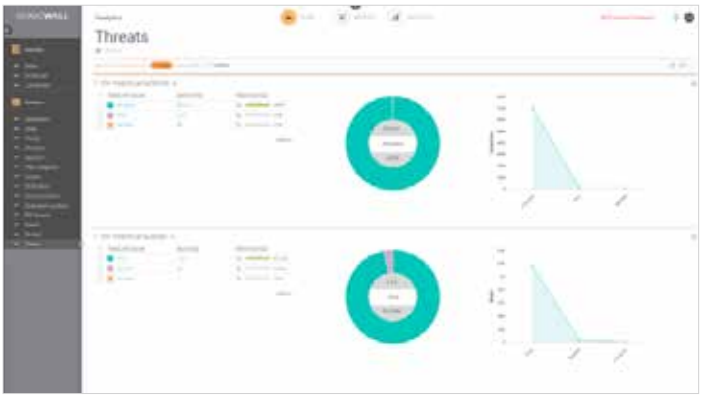
Vantaggi:

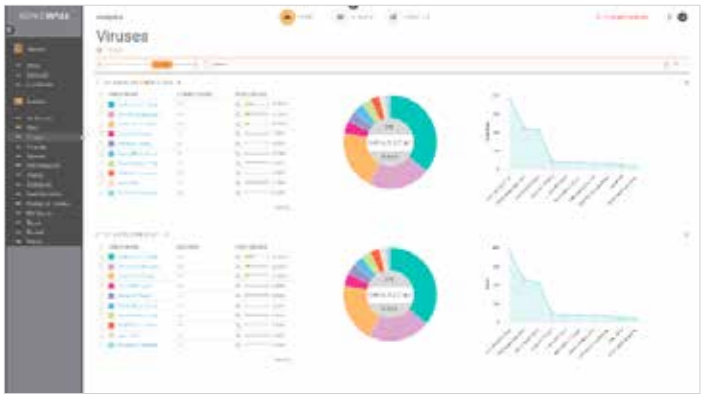
- Visibilità e completa consapevolezza situazionale dell'ambiente di sicurezza della rete in un unico pannello
- Completa autorità e flessibilità per eseguire analisi investigative e forensi approfondite
- Migliore conoscenza e comprensione dei rischi e delle minacce reali e potenziali
- Risoluzione dei rischi con maggiore chiarezza, sicurezza e velocità
- Riduzione dei tempi di risposta agli incidenti grazie all'intelligence delle minacce in tempo reale

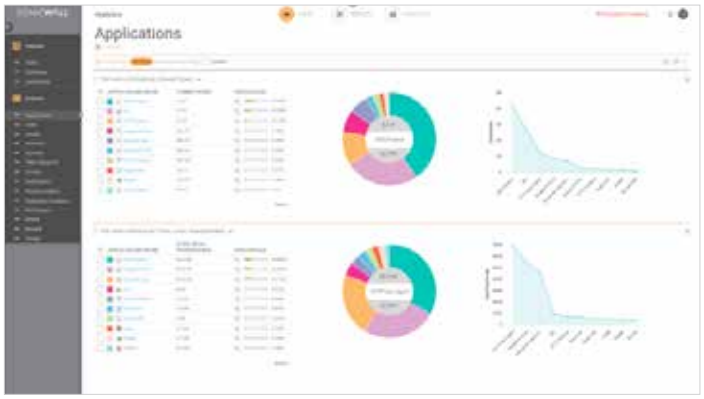
Partner Enabled Services
Serve aiuto per pianificare, ottimizzare o implementare una soluzione SonicWall? Gli Advanced Services Partner di SonicWall sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni: www.sonicwall.com/PES.

Questa profonda conoscenza e comprensione dell'ambiente di sicurezza fornisce le informazioni e la capacità per scoprire i rischi alla sicurezza, orchestrare la loro risoluzione e monitorare i risultati con maggiore chiarezza, sicurezza e velocità.

L'integrazione di Analytics nel processo aziendale aiuta a rendere operative le analisi, trasformando i dati in informazioni, le informazioni in conoscenze e le conoscenze in decisioni volte ad automatizzare la sicurezza.







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 la distribuzione 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 la distribuzione 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 sia per i fornitori di servizi che per le 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.
Rapporti 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.
Analytics	
Funzionalità	Descrizione
Aggregazione dei dati	Il motore analitico basato sull'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 imprese 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.

Riepilogo delle funzionalità

Dashboard di riepilogo con visualizzazioni e diagrammi

- Velocità della larghezza di banda
- Utilizzo della CPU
- Numero di connessioni
- Velocità di connessione al secondo
- Indice di rischio (scala da 1 a 10)
- Percentuale di blocco
- Connessioni totali
- Dati trasferiti totali
- Applicazioni principali
- Intrusioni principali
- Categorie URL principali
- Virus principali
- Numero di virus, intrusioni, spyware, botnet

Monitoraggio dei flussi in tempo reale con grafici ad aree/a barre

- Applicazioni
- Ingresso/uscita interfaccia, media, min, picco
  - Larghezza di banda
  - Velocità dei pacchetti
  - Dimensioni dei pacchetti
  - Velocità di connessione
- Utilizzo
  - Numero di connessioni
  - Monitoraggio multi-core

Dashboard di riepilogo principali con drill-down

- Applicazioni
- Utenti
- Virus
- Intrusioni
- Spyware
- Categorie web
- Fonti
- Destinazioni
- Luoghi di origine
- Luoghi di destinazione
- Code BW
- Botnet

Report con drill-down, esportazione in pdf/csv e invio di e-mail pianificate

- Applicazioni / Utenti / Sorgenti / Destinazioni
  - Connessioni
  - Connessioni totali bloccate
  - Connessioni bloccate in base a regola di accesso
  - Connessioni bloccate in base a minaccia
  - Connessioni bloccate in base a filtro botnet
  - Connessioni bloccate in base a filtro GeoIP
  - Connessioni bloccate con Content Filtering Service
  - Virus
  - Intrusioni
  - Spyware
  - Dati trasferiti totali
  - Dati inviati
  - Dati ricevuti
- Virus / Intrusioni / Spyware / Categorie Web / Località di origine / Località di destinazione / code BW
  - Connessioni
  - Dati trasferiti totali
  - Dati inviati
  - Dati ricevuti
- Botnet
  - Connessioni
- Esportazione
  - .pdf
  - .csv
- Report pianificati
  - Report sui flussi
  - Capture Threat Assessment (SWARM)
  - Giornaliero / Settimanale / Mensile
  - Archivio / Email / PDF

Analytics Session Viewer con drill-down, filtraggio, esportazione dei dati di singole sessioni

- Analisi del traffico in qualsiasi combinazione di:
  - Applicazione
  - Categoria di applicazione
  - Rischio dell'applicazione
  - Firma
  - Azione
  - IP iniziatore/risponditore
  - Paese iniziatore/risponditore
  - Porta iniziatore/risponditore
  - Byte iniziatore/risponditore
  - Interfaccia iniziatore/risponditore
  - Indice iniziatore/risponditore
  - Gateway iniziatore/risponditore
  - MAC iniziatore/risponditore
  - Protocollo
  - Velocità (kbps)
  - ID flusso
  - Intrusione
  - Virus
  - Spyware
  - Botnet
- Analisi Minacce / Bloccate in qualsiasi combinazione di:
  - Nome minaccia
  - Tipo di minaccia
  - ID minaccia
  - Applicazione
  - Categoria di applicazione
  - Rischio dell'applicazione
  - Firma
  - Azione
  - IP iniziatore/risponditore
  - Paese iniziatore/risponditore
  - Porta iniziatore/risponditore
  - Byte iniziatore/risponditore
  - Interfaccia iniziatore/risponditore
  - Indice iniziatore/risponditore
  - Gateway iniziatore/risponditore
  - MAC iniziatore/risponditore
  - Protocollo
  - Velocità (kbps)
  - ID flusso
  - Intrusione
  - Virus
  - Spyware
  - Botnet

Analisi URL / Bloccati in qualsiasi combinazione di:

- URL
- Categoria URL
- Dominio URL
- Applicazione
- Categoria di applicazione
- Rischio dell'applicazione
- Firma
- Azione
- IP iniziatore/risponditore
- Paese iniziatore/risponditore
- Porta iniziatore/risponditore
- Byte iniziatore/risponditore
- Interfaccia iniziatore/risponditore
- Indice iniziatore/risponditore
- Gateway iniziatore/risponditore
- MAC iniziatore/risponditore
- Protocollo
  - Velocità (kbps)
  - ID flusso
  - Intrusione
  - Virus
  - Spyware
  - Botnet

Analytics Flow Monitor – drill-down e pivoting dei parametri di flusso

- Applicazioni
  - Nomi
  - Categorie
  - Firme
- Utenti
  - Nome
  - Indirizzo IP
  - Nomi di dominio
  - Tipi di autenticazione
- Attività web
  - Siti web
  - Categorie web
  - URL
- Fonti
  - Indirizzi IP
  - Interfacce
  - Paesi
- Destinazioni
  - Indirizzi IP
  - Interfacce
  - Paesi
- Minacce
  - Intrusioni
  - Virus
  - Spyware
  - Spam
  - Botnet
- VoIP
  - Tipi di supporto
  - ID del chiamante
- Dispositivi
  - Indirizzi IP
  - Interfacce
  - Nomi
- Contenuti
  - Indirizzi email
  - Tipi di file
- Gestione della larghezza di banda
  - In entrata
  - In uscita
  - Tutta
  - URL
  - Sessioni
  - Pacchetti totali
  - Byte totali
  - Minacce

Grafici a stella – visualizzazioni punto-punto, drill-down e pivoting

- Sorgenti / Utenti / Luoghi / Dispositivi
  - Verso/da
    - » Destinazioni
    - » Applicazioni
    - » Attività web
    - » Minacce
  - Filtraggio in base a
    - » Numero di connessioni
    - » Dati trasferiti
    - » Pacchetti scambiati
    - » Numero di minacce
  - Evidenziazione per
    - » Minacce
    - » Dati > 1 MB
    - » Connessioni > 1000
    - » Pacchetti > 1000

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 e Reporting per TZ Series, NSv 10 - 100, 1 anno	01-SSC-3435
SonicWall Capture Security Center Management e Reporting per TZ Series, NSv 10 - 100, 2 anni	01-SSC-9148
SonicWall Capture Security Center Management e Reporting per TZ Series, NSv 10 - 100, 3 anni	01-SSC-9149
SonicWall Capture Security Center Management e Reporting per NSA 2600 - 6650 e NSv 200 - 400, 1 anno	01-SSC-3879
SonicWall Capture Security Center Management e Reporting per NSA 2600 - 6650 e NSv 200 - 400, 2 anni	01-SSC-9154
SonicWall Capture Security Center Management e 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 NS*a* 6650 e TZ Series
- Appliance di sicurezza di rete SonicWall virtuali: NSv 10 fino a NSv 400

Informazioni su SonicWall

Da oltre 27 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 rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, 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-Analytics-US-VG-MKTG4305

SONICWALL®