

SonicWall Analytics

Trasforma i dati in informazioni immediatamente fruibili

SonicWall Analytics trasforma i dati di traffico dei firewall in informazioni concrete sugli utenti, le applicazioni e le reti, permettendo di limitare i rischi di sicurezza con maggiore precisione e velocità. Il tutto da un'unica interfaccia. Basato su un'architettura cloud-native ad alte prestazioni, il motore di analisi elabora un'enorme quantità di dati grezzi provenienti da migliaia di nodi firewall su larga scala per offrire la massima trasparenza e visibilità sulla sicurezza attraverso un pannello di controllo.

Con la creazione di grafici semantici e diagrammi Analytics aiuta a diminuire i tempi di processo e facilita il lavoro degli analisti. Le funzionalità di drill-down aggiuntive consentono ai responsabili della sicurezza di analizzare ed eliminare punti di dati critici per intervenire tempestivamente sui rischi nascosti e adottare policy basate sull'evidenza contro attività rischiose degli utenti man mano che procedono nel processo di rilevamento.

Grazie alla visibilità e al controllo completi, gli analisti di sicurezza possono vedere ogni cosa ovunque e gestire meglio il rischio, mentre gli addetti alla gestione degli incidenti possono concentrarsi sulla pianificazione di azioni di risposta rapida per le applicazioni e gli utenti più importanti, senza dover reagire a ogni evento. Analytics è scalabile e offre l'agilità e l'elasticità del cloud per soddisfare i più complessi requisiti aziendali.

CARATTERISTICHE PRINCIPALI

Azienda

- Massima trasparenza sulla sicurezza
- Istantanee in tempo reale sul livello di sicurezza
- Rispetto delle normative di conformità interne
- Pianificazione e creazione di budget accurati per la cyber sicurezza
- Riduzione di CAPEX e OPEX

Personale operativo

- Comprensione immediata dei dati di sicurezza
- Informazioni su ogni attività di rete e degli utenti con relativi allarmi
- Creazione di policy di difesa accurate
- Scalabilità e performance per la massima agilità nel cloud

Sicurezza

- Rilevamento dei rischi nascosti
- Capacità di intervento precoce
- Reazione tempestiva alle attività non sicure degli utenti
- Aiuta gli analisti a gestire meglio il rischio
- Semplifica la risoluzione dei problemi



Maggiori informazioni su SonicWall Analytics

www.sonicwall.com/analytics



Vedere ogni cosa ovunque

Analytics offre una visione completa dell'intero ambiente di sicurezza SonicWall a livello di tenant, gruppi o dispositivi. Il pannello di controllo offre l'analisi e il monitoraggio statici in quasi tempo reale di tutto il traffico di rete e delle comunicazioni di dati che attraversano l'ecosistema dei firewall. Tutti i dati di log vengono registrati, aggregati, contestualizzati con modalità facilmente fruibili che permettono di scoprire, interpretare e valutare i dati per adottare le necessarie misure di difesa grazie a informazioni basate sui dati.

Analytics offre un'ampia gamma di report predefiniti e la flessibilità di creare report personalizzati per usi o intenti specifici con qualsiasi combinazione di dati sul traffico, per poi riceverli su base regolare. Permette di creare report con dati storici fino a un anno prima per l'analisi del traffico e il rilevamento di lacune di sicurezza e anomalie, in modo da monitorare e misurare i dati attraverso un centro operativo di sicurezza e di rete.



Figura 1.0 Pannello di controllo

Comprendere l'esposizione al rischio

Le funzioni di drill-down e pivoting consentono di esaminare in dettaglio modelli specifici e tendenze relativi al traffico in entrata/in uscita, all'uso delle applicazioni, all'accesso di utenti e dispositivi, alle minacce e molto altro ancora. Mediante una combinazione di report e analisi su endpoint, reti, utenti e applicazioni è possibile analizzare o reagire proattivamente ad allarmi, anomalie e attività rischiose degli

utenti. La massima trasparenza della sicurezza migliora la consapevolezza e permette di rilevare i rischi, coordinare le policy, applicare misure di sicurezza coerenti e monitorare costantemente i risultati nel proprio ambiente.

Implementazione flessibile con servizi SaaS, virtuali o IaaS

Analytics offre opzioni d'installazione flessibili per soddisfare al meglio i diversi requisiti operativi.

Analytics è disponibile come servizio SaaS gestito in hosting da SonicWall, accessibile tramite Internet e senza bisogno di manutenzione. L'opzione SaaS offre una flessibilità illimitata con scalabilità on-demand, riducendo allo stesso tempo i costi operativi. I tipici costi per l'acquisto di hardware e software, l'installazione personalizzata, la manutenzione ordinaria, gli aggiornamenti, l'ammortamento degli asset e il ritiro dei prodotti vengono sostituiti da un costo annuale di abbonamento contenuto e prevedibile.

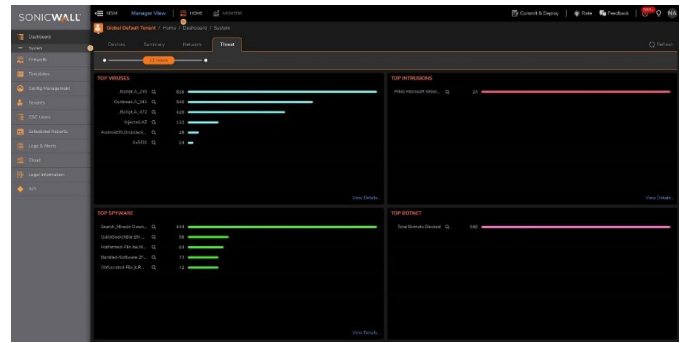


Figura 2.0 Riepilogo delle minacce

Per ottenere il controllo e la conformità completi del sistema è possibile installare la versione software di Analytics in azienda su una piattaforma virtuale a scelta, come VMware e Microsoft Hyper-V. In questo modo si ottengono tutti i vantaggi operativi ed economici della virtualizzazione, come scalabilità del sistema, velocità di provisioning e riduzione dei costi.

Riepilogo delle funzionalità

Funzionalità	Descrizione
Agregazione dei dati	Consente di automatizzare l'aggregazione e la normalizzazione dei dati di sicurezza che passano attraverso tutti i firewall.
Contestualizzazione dei dati	I dati dei firewall possono essere elaborati, arricchiti e visualizzati in modo strutturato, significativo e facilmente fruibile, per consentire 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 e caricati in tempo reale, e i risultati sono illustrati visivamente in un dashboard dinamico e interattivo.
Analisi degli utenti	Mostra una panoramica completa sull'utilizzo di Internet e delle applicazioni web da parte del personale tramite un pannello di controllo. Consente un'analisi granulare dei dati storici per stabilire misure basate su dati concreti contro le attività rischiose degli utenti nel web.
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.
Analisi della sicurezza	Visibilità in tempo reale e rapido rilevamento delle minacce. Consente agli analisti di sicurezza e agli addetti alla gestione degli incidenti di cercare, identificare e analizzare i problemi.
Visualizzazione dinamica in tempo reale	Mediante un unico pannello di controllo, gli analisti della sicurezza possono 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 rapidamente i rischi con misure adeguate.
Report sulla produttività (richiedono la licenza AGSS/CGSS attiva sui firewall di generazione 6/6.5, o la licenza Essential Protection sui firewall di generazione 7)	<p>Forniscono informazioni dettagliate sull'uso delle risorse Internet in tutta l'organizzazione e consentono di generare potenti snapshot e report dettagliati sul comportamento di accesso a Internet degli utenti. I rapporti raccolgono dati relativi all'indirizzo dei siti web e alla data in cui l'utente li ha visitati, calcolano il tempo trascorso dagli utenti su ogni sito e verificano se questi siti sono stati consultati durante l'orario di lavoro oppure no. I report sulla produttività classificano le attività web degli utenti in gruppi di produttività quali produttivo, improduttivo, accettabile, inaccettabile, o altri gruppi personalizzabili, permettendo all'azienda di comprendere meglio i modelli di utilizzo di Internet e ottimizzare la produttività del personale.</p> <p>Ad esempio, con le informazioni sul tempo trascorso dagli utenti su siti web non aziendali, i responsabili HR possono gestire e rispondere a potenziali violazioni delle regole del codice di comportamento dei dipendenti. Un caso simile è applicabile a tutti gli altri gruppi funzionali.</p>

Funzionalità	Descrizione
Report VPN	Forniscono un riepilogo delle risorse aziendali utilizzate nel tunnel VPN, della larghezza di banda consumata e degli utenti responsabili (nome utente e indirizzo IP). Gli amministratori di rete possono usare queste informazioni per monitorare le applicazioni business-critical, controllare o strutturare il traffico e pianificare un incremento della capacità.
Analisi e rapporti sui flussi	<p>Monitoraggio in tempo reale e cronologico grazie all'agente di reporting del flusso per l'analisi del traffico delle applicazioni e ai dati di utilizzo tramite i protocolli IPFIX o NetFlow. Un'interfaccia intuitiva ed efficace consente agli amministratori di 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'uso delle applicazioni per ogni utente e anticipare le minacce e gli attacchi diretti alla rete.</p> <ul style="list-style-type: none"> • 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 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.
Report grafici dettagliati	Forniscono visibilità su attacchi ai firewall, uso della larghezza di banda, produttività dei dipendenti, attività sospette in rete e analisi del traffico delle applicazioni.
Report basati su syslog	Semplificano il riepilogo dei dati, offrendo report quasi in tempo reale sui messaggi syslog in arrivo. L'accesso diretto ai dati grezzi sottostanti garantisce una migliore granularità delle analisi e la personalizzazione dei report.
Report pianificati	Forniscono un unico modello base per tutti i report pianificati. Un report può combinare diagrammi e tabelle per diverse unità. I report possono essere pianificati e inviati in diversi formati a uno o più analisti.
Report immediati	Diverse viste personalizzabili per visualizzare diversi report di riepilogo in un'unica pagina. Gli utenti possono consultare facilmente dati essenziali della rete e analizzare in poco tempo le informazioni contenute in svariati report.
Report dettagliati sulle minacce	Raccolgono informazioni sugli attacchi e forniscono l'accesso immediato alle attività delle minacce rilevate dai firewall SonicWall mediante i servizi di gateway anti-virus, anti-spyware, prevenzione delle intrusioni, controllo e intelligence delle applicazioni.
Nuova intelligence degli attacchi	Fornisce report granulari su determinati tipi di attacco o tentativi d'intrusione e sull'indirizzo di origine dell'attacco, per poter reagire rapidamente alle minacce ricorrenti.
Report su punti di accesso wireless non autorizzati	Mostrano tutti i dispositivi wireless in uso e i 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.
Report di Capture ATP	Dashboard intuitivo per l'analisi delle minacce e report con risultati dettagliati dell'analisi per i file che sono stati inviati al servizio, con informazioni come sorgente e destinazione, e un riepilogo accurato della reazione del malware dopo la detonazione.
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 GeolP	Contengono informazioni sul traffico bloccato in base al 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	<p>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:</p> <ul style="list-style-type: none"> • Utilizzo dati > Iniziatori • Utilizzo dati > Risponditori • Utilizzo dati > Dettagli • Attività utente > Dettagli • Attività Web > Iniziatori
Sistema di logging centralizzato	Un unico strumento centralizzato per consolidare gli eventi di sicurezza e i log di tutti gli apparati gestiti o effettuare analisi forensi della rete.
Architettura cloud-native	Consente di raccogliere, combinare, elaborare, riprocessare, estrarre, correlare e caricare enormi quantità di dati da decine di migliaia di nodi firewall, sfruttando la velocità e l'elasticità del cloud.

Licenze e pacchetti

	Funzionalità	Analytics SaaS	Analytics on-premise
Gestione	Backup/ripristino – sistema firewall	Sì	Sì*
	Creazione di report (basati su Netflow/ IPFIX)	Sì	Sì*
	Analisi (basate su Netflow/ IPFIX)	Solo da file locali	Solo da file locali
Reporting	Report pianificati, monitoraggio in tempo reale, dashboard di riepilogo	Sì	Sì
	Download di report, applicazioni, minacce, CFS, utenti, traffico, origine/destinazione (report sui flussi per 1 anno)	Sì	Sì
Analisi (basate su Netflow/ IPFIX)	Analisi forensi della rete e ricerca minacce con drill-down e pivoting	Sì	Sì
	Cloud App Security – Rilevamento dello shadow IT	Sì	No
	Conservazione dei dati	30 giorni	1 anno
Supporto tecnico		Supporto 24x7	Supporto 24x7**

*Richiede il servizio AGSS/CGSS o un servizio Capture Security Center a pagamento

**Richiede una licenza di supporto 24x7

Requisiti minimi di sistema

Per SonicWall Analytics in modalità SaaS tramite Network Security Manager:

Appliance SonicWall supportate:

- Appliance di sicurezza di rete SonicWall: Serie NSA, serie NSa, appliance della serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Appliance di sicurezza di rete SonicWall virtuali: NSv 10 fino a NSv 400

Firmware SonicWall supportato:

- SonicWall SonicOS 6.0 o superiore

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)

Per l'installazione on-premise di SonicWall Analytics:

Appliance virtuale

- Hypervisor: VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2016
- RAM consigliata: illimitata (minimo 8 GB)
- Hard disk: Base OVA 65 GB con montaggio esterno
- vCPU: 4/illimitate
- Interfaccia di rete: 1
- Guida alla compatibilità VMware

Appliance SonicWall supportate:

- Appliance di sicurezza di rete SonicWall: Serie SuperMassive E10000 e 9000, Serie NSA, serie NSa, appliance della serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Appliance di sicurezza di rete SonicWall virtuali: Serie NSv



Maggiori informazioni su SonicWall Analytics

www.sonicwall.com/analytics

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative che si adattano perfettamente alla nuova "normalità iperdistribuita", in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibile economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni potete visitare www.sonicwall.com o seguirci su [Twitter](#), [LinkedIn](#), [Facebook](#) e [Instagram](#).



SonicWall, Inc.

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

SONICWALL®

© 2021 SonicWall Inc. TUTTI I DIRITTI RISERVATI

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari. Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. SALVO QUANTO SPECIFICATO NEI TERMINI E NELLE CONDIZIONI STABILITI NEL CONTRATTO DI LICENZA DI QUESTO PRODOTTO, SONICWALL E/O LE SUE AFFILIATE NON SI ASSUMONO ALCUNA RESPONSABILITÀ ED ESCLUDONO GARANZIE DI QUALSIASI TIPO, ESPLICITE, IMPLICITE O LEGALI, IN RELAZIONE AI PROPRI PRODOTTI, INCLUSE, IN VIA ESEMPLIFICATIVA, QUALSIASI GARANZIA IMPLICITA DI COMMERCIALIZZABILITÀ, IDONEITÀ A SCOPI SPECIFICI O VIOLAZIONE DI DIRITTI ALTRUI. SONICWALL E/O LE SUE AFFILIATE DECLINANO OGNI RESPONSABILITÀ PER DANNI DI QUALUNQUE TIPO, SIANO ESSI DIRETTI, INDIRETTI, CONSEGUENZIALI, PUNITIVI, SPECIALI O INCIDENTALI (INCLUSI, SENZA LIMITAZIONI, DANNI PER MANCATO GUADAGNO, INTERRUZIONI DELL'ATTIVITÀ O PERDITE DI DATI) DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE DOCUMENTO, ANCHE NEL CASO IN CUI SONICWALL E/O LE SUE AFFILIATE SIANO STATE AVVERTITE DELL'EVENTUALITÀ DI TALI DANNI. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riserva il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.