SANGFOR

SANGFOR NETWORK SECURE NEXT-GENERATION FIREWALL

Smarter AI-Powered Network Defense

Gartner

Visionary in 2022 Gartner® Magic Quadrant™ for Network Firewalls

FROST & SULLIVAN BEST PRACTICES AWARDS

2023 Asia-Pacific (APAC) Next-generation Firewall (NGFW) Company of the Year Award by Frost & Sullivan

CRO CYBER RATINGS.ORG

Recommended Rating in CyberRatings.org's Enterprise Firewall Test

Converged Security Solution with Full Security Coverage

Sangfor Network Secure elimina il 99% delle minacce sul perimetro

Sangfor Network Secure (precedentemente noto come NGAF) è un firewall di nuova generazione che utilizza tecnologie avanzate per filtrare e ispezionare i tracciati della rete e delle applicazioni alla ricerca di minacce. Incorpora informazioni sulle minacce provenienti dall'esterno della rete e si integra con altri strumenti di sicurezza per aumentare le capacità di rilevamento e risposta. Sangfor Network Secure è una soluzione veramente sicura, integrata e semplificata. Fornisce una visibilità completa del perimetro della rete, la protegge dalle intrusioni e offre facilità di funzionamento e di manutenzione per gli amministratori.

Gartner peerinsights

FAVORABLE REVIEW

5.0 ★★★★★ June 22, 2023

Sangfor NGAF Firewall secure our network!

We use Sangfor NGAF Firewall for Primary security devices in our office, which always protect our endpoints and servers from ransomware, malware and threats, also gives us alert if we had any security issue

Read Full Review

Source: Gartner Peer Insights

CARATTERISTICHE E FUNZIONALITÀ

Engine Zero/ Neural-X/ NGWAF/ IoT Security/ Cloud Deception: Protezione avanzata alimentata dall'intelligenza artificiale

Sangfor Network Secure offre funzionalità avanzate di rilevamento delle minacce basate sull'intelligenza artificiale per proteggersi da un panorama di minacce in continua evoluzione. Con oltre 450.000 nuove varianti di malware registrate ogni giorno, i metodi di rilevamento tradizionali, come quello basato su firme e regole, stanno diventando sempre meno efficaci. Al contrario, Network Secure sfrutta le tecnologie IA, tra cui il motore di ispezione del malware Engine Zero e la piattaforma di threat intelligence Neural-X, per raggiungere un tasso di rilevamento del malware del 99,76% sia per le minacce note che per quelle sconosciute.

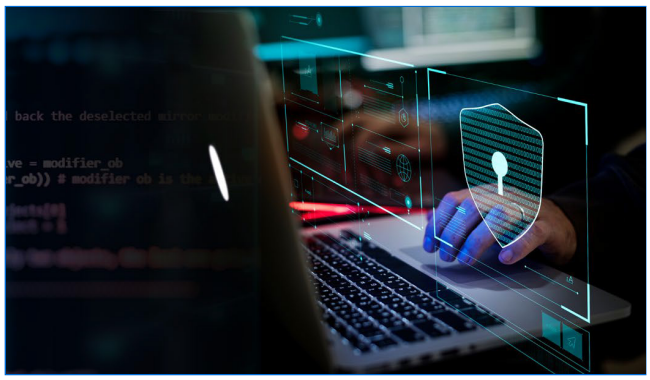
Sangfor Network Secure ha, inoltre, presentato le più recenti funzionalità di sicurezza IoT, tra cui l'individuazione delle risorse, il controllo dei dispositivi non autorizzati e le funzionalità dedicate alla sicurezza delle intrusioni.

Sangfor Network Secure è il primo NGFW con tecnologia di cloud deception. Gli amministratori impiegano solo 5 minuti per configurare tool che individuano e bloccano in modo proattivo le intrusioni e i movimenti laterali della rete.

Sangfor Network Secure offre protezione delle applicazioni web con un modulo integrato di Next-Generation Web Application Firewall (NGWAF). Il motore WISE del sistema combina analisi semantica e l'apprendimento automatico per difendersi da un'ampia gamma di attacchi alle applicazioni web, compresi gli attacchi zero-day.

Contact Us To Know More

Sangfor Technologies sales@sangfor.com marketing@sangfor.com

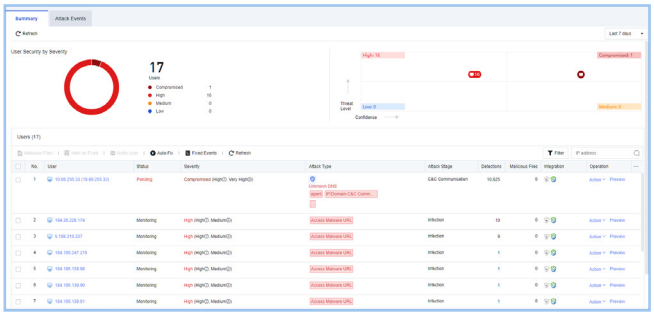


Integrazione di Sangfor Endpoint Secure Rilevamento e risposta alle minacce migliorati

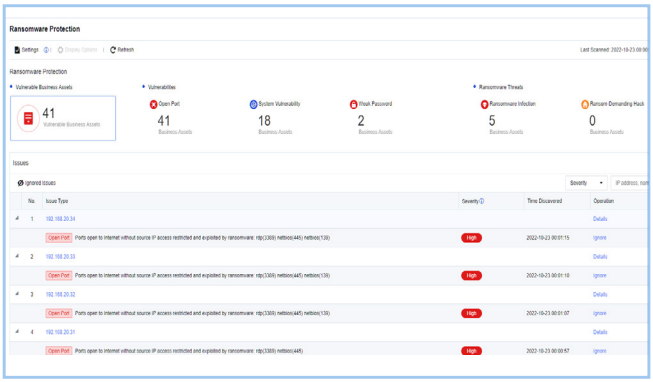
Sangfor Network Secure si integra perfettamente con Sangfor Endpoint Secure per migliorare il rilevamento delle minacce. Correlando i dati provenienti sia dalla rete che dai dispositivi endpoint, il sistema offre una visione olistica dell'attività di rete. Queste informazioni vengono presentate attraverso un'interfaccia grafica intuitiva, che facilita l'identificazione delle minacce nascoste. Il sistema integrato offre inoltre funzioni come la "one-click quarantine" e la "one-click virus scan" per semplificare la risposta.

SOC Lite: Operatività e manutenzione della sicurezza semplificate

Il SOC Lite di Sangfor Network Secure è stato progettato per semplificare e snellire le operazioni e la manutenzione della sicurezza. È dotato di tre funzioni chiave: una configurazione guidata iniziale, un ottimizzatore di policy e la gestione delle risorse. SOC Lite offre una visione intuitiva della sicurezza degli utenti, delle risorse e delle minacce ransomware, permettendo ai team di sicurezza di identificare rapidamente qualsiasi minaccia. Vengono fornite indicazioni essenziali per dare risposte tempestive e appropriate.



Panoramica sulla sicurezza degli utenti



Panoramica sulle minacce ransomware

Gestione degli asset

CASI D'USO

- **Sicurezza perimetrale:** Network Secure è distribuito come gateway della rete e funge da prima linea di difesa. Utilizza il rilevamento delle minacce informatiche basato sull'intelligenza artificiale e le informazioni sulle minacce in tempo reale per bloccare il 99% delle minacce in entrata sul perimetro della rete.
- **Firewall di secondo livello:** integra il firewall esistente con un firewall di nuova generazione dotato di rilevamento delle minacce basato su IA, threat intelligence di ultima generazione, NGWAF e cloud deception, per rendere più difficile la penetrazione nella rete da parte degli aggressori.
- **Protezione da ransomware:** Network Secure si integra con Sangfor Endpoint Secure per offrire protezione in ogni fase della kill chain del ransomware.
- **SD-WAN sicura:** la SD-WAN integrata di Network Secure fornisce una connessione di rete sicura e affidabile per le filiali e i lavoratori remoti.