SANGFOR

SANGFOR NETWORK SECURE

NEXT GENERATION FIREWALL

Smarter AI-Powered Perimeter Defense

Il primo NGFW + NGWAF + SOC Lite al mondo completamente integrato

- Un unico pannello di gestione per tutte le operazioni di sicurezza
- Abilitazione alla sicurezza attraverso la visualizzazione
- Riduzione minima del 50% del TCO
- Bloccare le minacce informatiche emergenti
- Eliminare ransomware in sinergia con Sangfor XDDR

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

Cyber Ratings .org

Recommended Ratings in CyberRatings.org's Enterprise Firewall Test

Nuovo mondo. Nuova IT. Nuova sicurezza.

Il settore IT è in continua evoluzione. Internet ha dato vita a nuove tendenze come il cloud computing, BYOD e IOT, che hanno dei vantaggi rispetto ai precedenti metodi di connessione, con applicazioni business-critical e servizi IT ospitati in remoto e accessibili 24/7 su una serie infinita di dispositivi in un numero infinito di posizioni. Queste tendenze sopravvivono perché sono le migliori, ma la sicurezza della rete sta evolvendo allo stesso ritmo?

L'etica non ha mai svolto un ruolo così importante nel processo di evoluzione. Le informazioni sono la valuta aziendale globale più recente e i dati sensibili, come le informazioni finanziarie e le informazioni aziendali riservate, sono l'obiettivo di attacchi come defacement, ransomware e malware.

Il mercato della security ha risposto con molte nuove soluzioni, ma solo meno del 40% delle imprese ha progredito con metodi di protezione che vanno oltre il Next Generation Firewall. Quelle organizzazioni che sono protette da Firewall o IPS spesso trascurano di evolvere la loro protezione di sicurezza con metodi più completi e proattivi. In questo panorama, la protezione offerta da NGFW & IPS sta diventando troppo generale e troppo poco efficiente.

Nel 2017, una nuova variante del ransomware chiamata WannaCry ha infettato più di 99 paesi, attaccando governi, scuole, ospedali e altri settori. È stato questo incidente che ha reso ransomware ben noto al pubblico.

Il ransomware è un software dannoso che i cyber-criminali utilizzano per prendere i file (o computer) per poi richiedere il pagamento di una certa quantità di denaro per riaverli. Da quando è stato scoperto, ransomware è cresciuto a una velocità enorme con sempre più utenti infettati, sia aziende sia consumatori. Ransomware colpisce criticamente la produttività e la reputazione di molte aziende, molti dei quali alla fine sono costrette a pagare il riscatto per evitare danni.

Sempre più varianti sono ora diffuse come XBash, che si concentrano sulla distruzione dei sistemi di dati e sull'estrazione di valute crittografiche. La sicurezza delle applicazioni non è più facoltativa. Tra attacchi crescenti e pressioni normative, le organizzazioni devono stabilire processi e scegliere tecnologie efficaci per proteggere le loro applicazioni e APIs (fonte: OWASP, 2017). Con la consapevolezza del rischio e le preoccupazioni sui costi che ritardano l'evoluzione della vera sicurezza organizzativa, molte aziende stanno semplicemente acquistando ciò che viene offerto senza però prendere in considerazione i bisogni reali.

Sangfor Network Secure

Sangfor Network Secure (prima conosciuto come Sangfor NGAF) è una soluzione di sicurezza convergente che fornisce protezione contro minacce avanzate, malware, virus, minacce IoT, ransomware e attacchi web-based. Esso integra funzionalità di sicurezza integrate come firewall, IPS, AV, Anti malware, APT, URL filtering, Cloud Sandbox e WAF. Sangfor Network Secure utilizza il potere di Sangfor Engine Zero (Motore di rilevamento malware basato su IA) e di Neural-X (piattaforma di analisi e threat intelligence) per rilevare e isolare possibili minacce emergenti, rendendolo infatti particolarmente efficace contro gli attacchi 0-day.

Un mondo intelligente e sicuro con le innovazioni Sangfor

Neural-X è un'innovazione in ambito di sicurezza firmata Sangfor. In qualità di piattaforma analitica e intelligente, basata sul cloud e sull'intelligenza artificiale (IA), Neural-X potenzia ed espande le capacità di rilevamento della sicurezza per le tecnologie di rete, endpoint e sicurezza.

Neural-X contiene decine di componenti interconnessi e progettati per lavorare insieme mantenendo il sistema sicuro e protetto includendo Engine Zero, threat intelligence, deep learning, sandboxing e botnet detection.

Sangfor Engine Zero

Engine Zero è un motore di rilevamento malware costruito su una potente tecnologia basata su intelligenza artificiale e curato da un team di "scienziati dei dati", analisti di sicurezza e ricercatori white hat. Esso è una tecnologia di ispezione malware incorporato nelle soluzioni di sicurezza di rete di Sangfor, nella soluzione endpoint e nella piattaforma cloud Neural-X.

È molto efficiente e utilizza pochissime risorse. Può fornire l'ispezione malware per attacchi noti e zero-day con quasi nessun impatto sulle prestazioni. In alcuni test recenti condotti da AV-Test, Sangfor Endpoint Secure, alimentato da Engine, ha ottenuto un successo del 100% in termini di precisione e detection delle minacce.

Sangfor Neural-X

Neural-X è al centro del rilevamento intelligente delle minacce e della difesa. La Threat Intelligence consente alle organizzazioni di comprendere, valutare e prevenire i rischi noti e gravi, provenienti da fonti esterne.

Next Generation Web Application Firewall

Sangfor Network Secure è il primo NGFW al mondo integrato con un Web Application Firewall di nuova generazione (NGWAF) per proteggere dai nuovi attacchi web-based come SQL injection, web shell, cross-site scripting (XSS) e deserialization flaws.

Il Sangfor Web Intelligent & Semantic Engine di Sangfor utilizza l'apprendimento automatico e l'analisi semantica per analizzare i comportamenti di attacco. Migliora i tassi di rilevamento e diminuisce i falsi positivi rispetto ai tradizionali motori di rilevamento basati su SNORT. Modellando i comportamenti di attacco, viene creato un modello di minaccia per gestire facilmente le minacce di sistema delle applicazioni.

Sangfor ZSand

Sangfor ZSand è una tecnologia di esecuzione dinamica virtuale (sandboxing) progettata per rilevare malware sconosciuti. Sangfor ZSand fa esplodere i malware sospetti in un ambiente sicuro e controllato e monitora i comportamenti anomali di questi file per il riconoscimento e la prevenzione futura. Nei test recenti, ha rilevato con precisione le famiglie ransomware tra cui GandCrab, Zusy, GlobeImposter e LockCrypt. ZSand condivide tutti i dati con Neural-X rendendo possibile identificare e studiare malware senza alcuna firma precedente nota, riducendo il rischio di futuri attacchi.

Botnet Detection

Gli hacker stanno diventando sempre più sofisticati; stanno abbandonando gli indirizzi IP fissi optando per nomi di dominio dinamici. Questi nomi di dominio criptici sono usati per collegare le botnet al loro controller usando algoritmi segreti. Sono notoriamente difficili da rilevare perché le query DNS si comportano in modo simile all'utente medio. Neural-X utilizza l'analisi di flusso avanzata, il calcolo visivo e la tecnologia di deep learning per scoprire botnet. È in grado di scoprire nomi di dominio significativamente più dannosi rispetto alle fonti popolari come Virustotal. Finora, ha scoperto oltre un milione di nomi di dominio dannosi e questa lista sta crescendo ogni giorno.

Deep Learning

Il deep learning è un elemento complesso di apprendimento automatico. Fa parte del mondo dell'intelligenza artificiale e può essere considerata un'evoluzione del Machine Learning. Può imparare da solo osservando ed elaborando milioni di dati in modo che possa fare previsioni più accurate e più veloci.

Neural-X utilizza il deep learning per scomporre i nomi di dominio criptici in vettori leggibili da una macchina. Con un'analisi approfondita rileva nomi di dominio utilizzati da malware e simili. Nel corso del tempo la funzione di deep learning inizierà a funzionare in modo indipendente - mantenendo così un approccio proattivo al malware.

Il concetto di security secondo Sangfor

Il mondo della sicurezza della rete non ha avuto un'evoluzione uguale per tutti. Gli esperti di sicurezza hanno opinioni, aspettative ed esigenze diverse, tra diversi settori e diversi luoghi. Mentre alcuni definiscono la sicurezza di rete come la protezione contro l'accesso non autorizzato a file e dati, altri si concentrano sul firewall, anti-virus e rilevamento botnet. Le soluzioni di sicurezza tradizionali hanno una visibilità limitata di utenti, traffico e asset e non hanno capacità di rilevamento in tempo reale o post-evento.

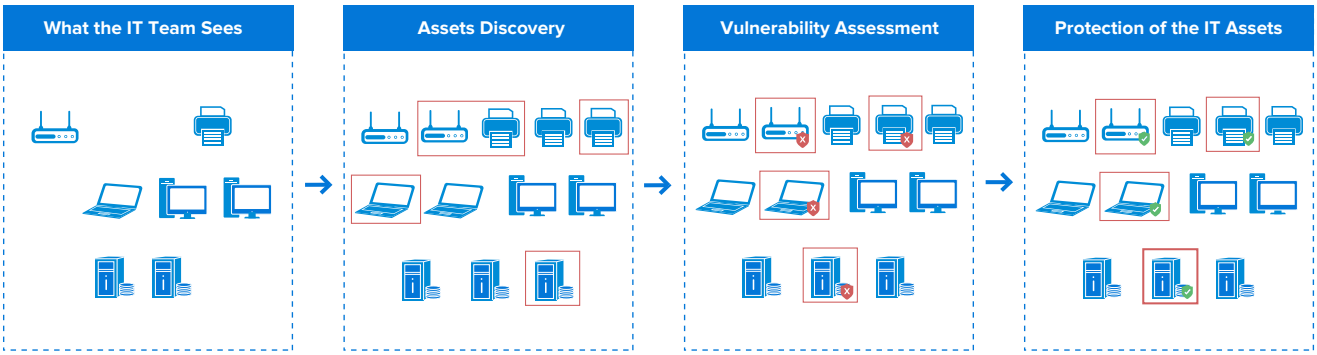
Con l'aumento degli attacchi a livello delle applicazioni, la sicurezza della rete deve evolversi ulteriormente per tenere il passo con le minacce emergenti. Sangfor Technologies ha un nuovo concetto di sicurezza di rete che contrasta le minacce nuove e più pericolose. Andiamo oltre per fornire una protezione completa e una soluzione per tutti gli utenti contro tutte le minacce, interne o esterne, esistenti o future.

L'approccio rivoluzionario di Sangfor alla sicurezza delle reti si basa su quattro principi fondamentali:

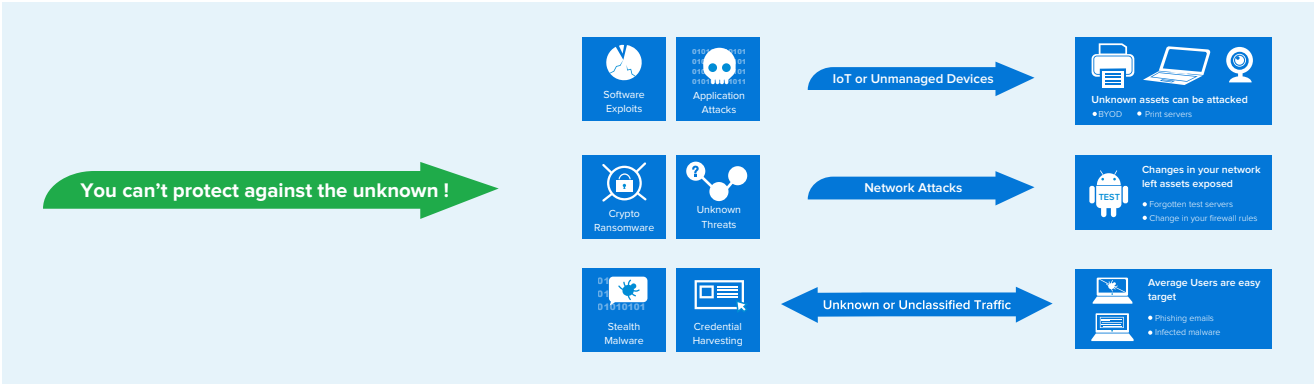
1. Proteggere gli asset aziendali

Sangfor Network Secure eccelle nella scoperta e protezione degli asset aziendali per ridurre al minimo i rischi di compromessi. Rileva automaticamente le risorse IT non gestite e identifica rischi, quali vulnerabilità del sistema, password deboli e applicazioni non autorizzate.

Inoltre, Sangfor Network Secure offre una protezione proattiva delle risorse attraverso funzionalità correttive come le patch virtuali.



2. Protezione completa contro le minacce



Sangfor Network Secure è una soluzione di sicurezza convergente che integra più funzionalità di sicurezza, tra cui Firewall, Intrusion Prevent System (IPS), Anti-Virus (AV), Anti-Malware, APT (Advanced Persist Threat) Protection, IoT Security, URL filtering, Cloud Sandbox, e Web Application Firewall. Questi garantiscono una copertura completa contro una vasta gamma di minacce alla sicurezza come ransomware, attacchi APT ed exploit web.

La protezione contro nuovi malware e attacchi zero-day è di gran lunga la più critica, in quanto queste minacce non sono state incluse in nessun database di firme. Inoltre, queste minacce avanzate sono in genere in possesso di attori altamente sofisticati e dotati di risorse adeguate, che sono in grado di causare i danni più significativi.
Sangfor affronta efficacemente queste minacce implementando l'intelligenza artificiale in tutte le sue innovazioni di sicurezza, tra cui Engine Zero, il Web Intelligent & Semantic Engine per NGWAF, Botnet Detection e altro ancora. Ad esempio, Engine Zero viene continuamente addestrato su decine di milioni di campioni di malware utilizzando algoritmi di apprendimento automatico avanzati per apprendere le caratteristiche in evoluzione del malware. Questo ha permesso di riconoscere potenziali nuovi malware e attacchi zero-day con una significativa precisione.

Tutti i motori di rilevamento Sangfor condividono la stessa intelligence sulle minacce fornita dalla piattaforma Neural-X basata su cloud di Sangfor. Utilizzando il machine learning, è in grado di rilevare con precisione le nuove minacce senza alcuna firma nota, consentendo la difesa proattiva della vostra organizzazione.

Real-Time Threat Intelligence Monitor

Fonti di intelligence

•Oltre 20.000 gateway di rete connessi forniscono IOCs che includono URL dannosi, IP, nomi di dominio e hash malware, con il numero di gateway che partecipano raddoppiando ogni anno.

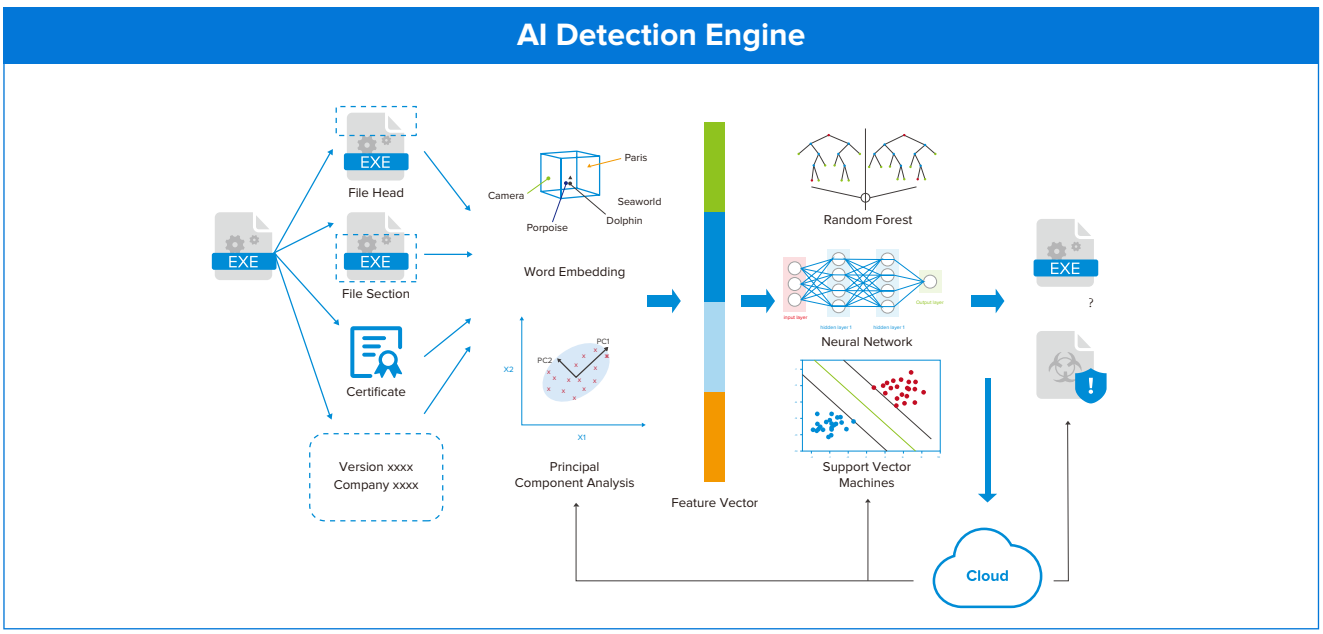
•Fonti di intelligence sulle minacce di terze parti. L'intelligence sulle minacce.

•R&D di sicurezza di Sangfor controlla attivamente entrambe le comunità di white hat e black hat.

Scenario di caso reale

Quando Sangfor Network Secure rileva una connessione in uscita insolita da un server connesso a Internet, invia l'indirizzo DNS sospetto a Neural-X per la verifica. Se la threat intelligence ha classificato questo particolare DNS come un server noto di comando e controllo (C2), è probabile che il server sia stato compromesso. Network Secure può essere programmato per bloccare queste comunicazioni C2 in modo da non causare ulteriori danni e avvisare gli operatori di sicurezza per ulteriori indagini ed elaborazioni.

Engine Zero: motore di rilevamento alimentato da IA



Engine Zero vs tecnologie di rilevamento tradizionali

Le tecnologie di rilevamento tradizionali includono principalmente il rilevamento basato sulla firma (hash, firme di virus, ecc.), la rule matching, l'esecuzione virtuale e la sandboxing. La capacità di rilevamento delle minacce di queste tecnologie migliora dal rilevamento basato sulla firma alla sandbox. Tuttavia, le prestazioni generalmente diminuiscono e i costi aumentano quanto più avanzata è la tecnologia di rilevamento. Rispetto a queste tecnologie tradizionali, Engine Zero ha i seguenti vantaggi:

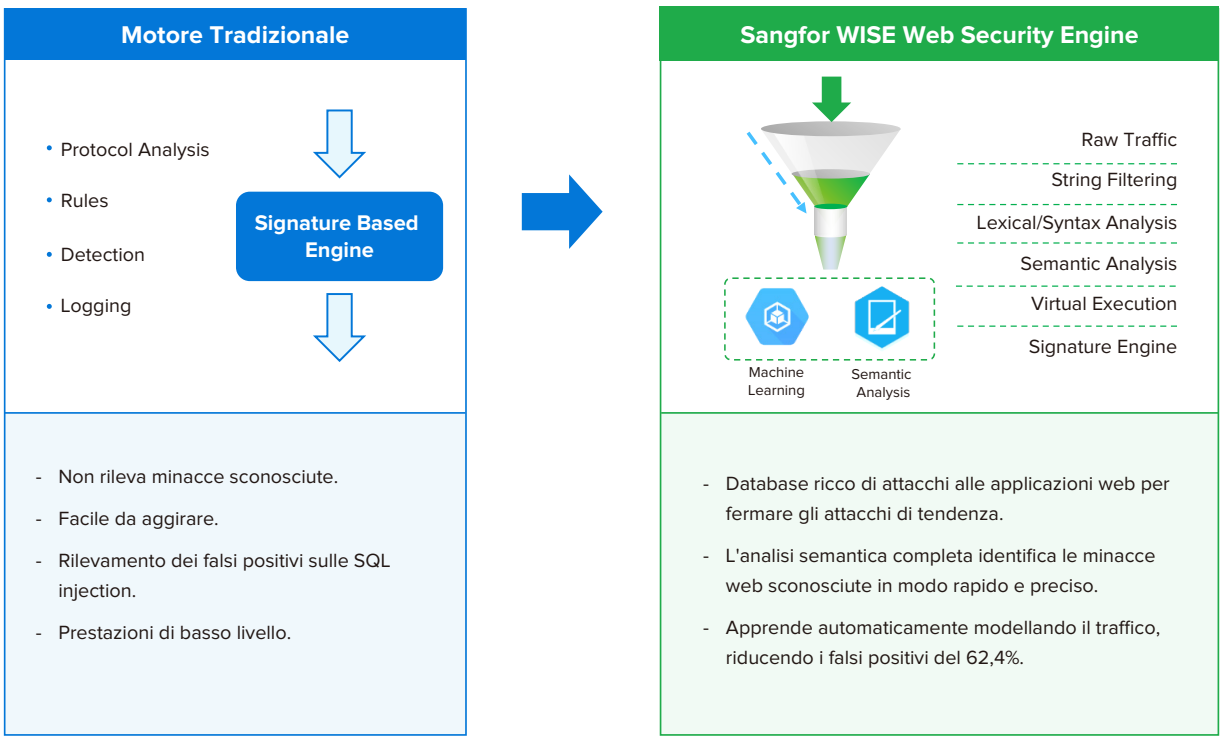
-Forte capacità di generalizzazione per rilevare virus sconosciuti o nuove varianti. Grazie alla capacità di generalizzazione dell'apprendimento automatico, Engine Zero è in grado di identificare virus sconosciuti o nuove varianti di virus noti senza dover vedere campioni. Invece, le soluzioni tradizionali devono ottenere prima i campioni, che possono causare dei ritardi.

-Speed veloce. Velocità di scansione quasi lineare, vicino a MD5.

-Elevato grado di automazione. Il modello Engine Zero può apprendere ed estrarre automaticamente le funzionalità senza l'intervento umano. Il modello si evolve nel cloud, migliorando la capacità di rilevamento e il grado di automazione. Tuttavia, le tecnologie di rilevamento tradizionali richiedono agli esperti di estrarre manualmente le impronte digitali e le firme dei virus, che non è solo costoso, ma causa anche ritardi in termini di tempo. Esso può far rimanere il virus per un lungo periodo di tempo fino a che i tradizionali fornitori di antivirus non aggiornano il database.

Le inefficaci soluzioni di rilevamento tradizionali hanno però un valore unico. Ad esempio, possono rispondere più rapidamente al meccanismo della blacklist. Pertanto, il design di Engine Zero adotterà anche alcune tecnologie tradizionali per formare una soluzione di rilevamento dei file dannosi basata sull'AI e sulle tecnologie tradizionali.

L'unico NGFW con WAF di livello enterprise



3. Operazioni di sicurezza semplificate

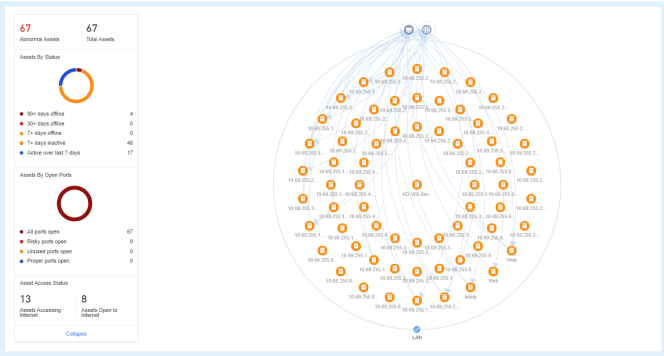
Anche le organizzazioni di piccole e medie dimensioni, senza un team di sicurezza specializzato, spesso ricevono migliaia di avvisi a settimana, richiedendo al reparto IT di dedicare ore di lavoro all'indagine e all'analisi, aumentando i costi operativi. Quelle organizzazioni che ancora utilizzano soluzioni di sicurezza tradizionali, senza strumenti di reporting intelligenti o automatizzati, sono in grave svantaggio. Senza una visibilità a 360 °, analisi e report chiari, la sicurezza efficace diventa esponenzialmente più difficile.

Sangfor Network Secure fornisce una sicurezza affidabile e senza sforzo con una facile implementazione, funzionamento semplificato e funzioni di manutenzione, che permettono all'ambiente IT di essere sicuro.

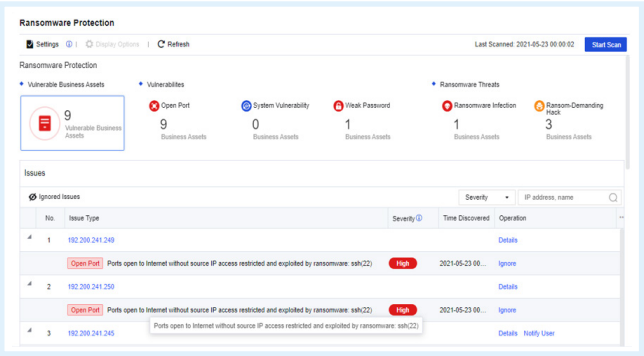
La Configurazione guidata integrata semplifica l'implementazione delle policy di sicurezza, mentre il modulo SoC Lite integrato offre visibilità end-to-end della sicurezza complessiva dell'organizzazione, dai sistemi aziendali agli endpoint.

Sangfor Network Secure semplifica le operazioni di sicurezza quotidiane identificando eventi di sicurezza reali e rischiosi tra migliaia di avvisi e fornendo indicazioni e suggerimenti sulla soluzione migliore. Dashboard dedicate sono fornite per le minacce di tendenza, come ransomware, per aiutare gli amministratori ottenere aggiornamenti tempestivi.

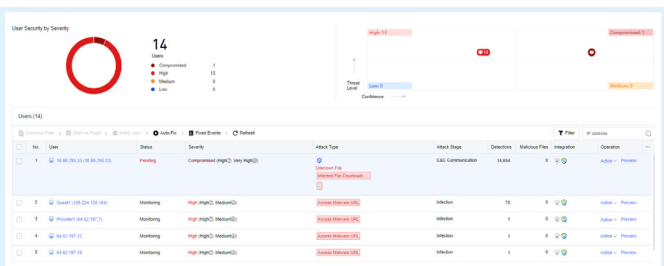
Asset e i componenti di visibilità IoT consentono al reparto IT e agli imprenditori di eseguire controlli proattivi dei loro sistemi aziendali. Questi controlli aiutano gli operatori a cogliere rapidamente la situazione di sicurezza delle risorse, incluso il loro stato online/offline e la presenza di accesso alla rete illegale e potenziali rischi, consentendo loro di prendere decisioni per chiudere eventuali scappatoie.
Inoltre, Sangfor Network Secure offre un ottimizzatore di policy intelligente integrato che consente agli amministratori di identificare rapidamente duplicazioni, conflitti ed errori di configurazione tra migliaia di policy con un semplice clic.



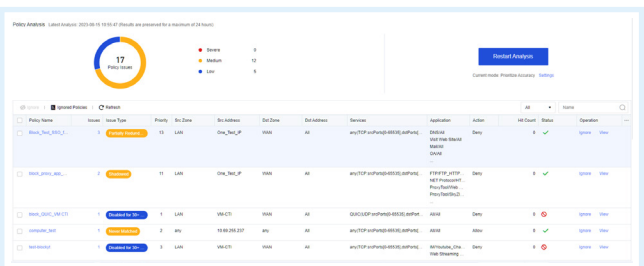
Asset Discover & Risk Management



Ransomware Threat Monitoring



User Security Overview

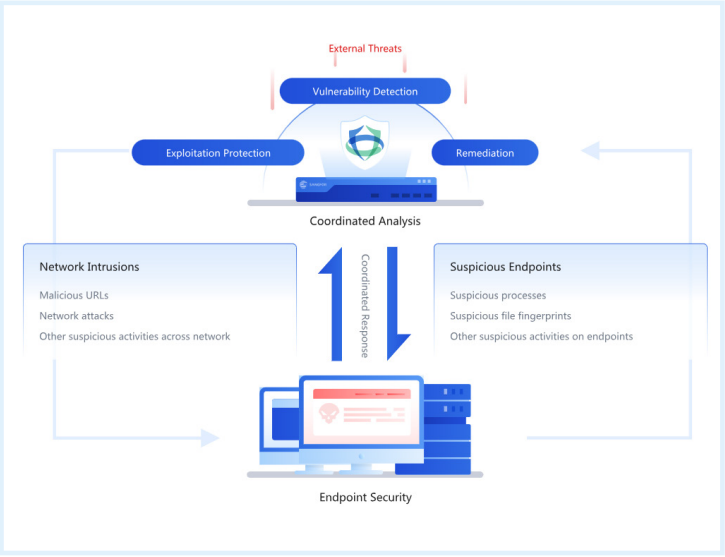


Smart Policy Optimizer

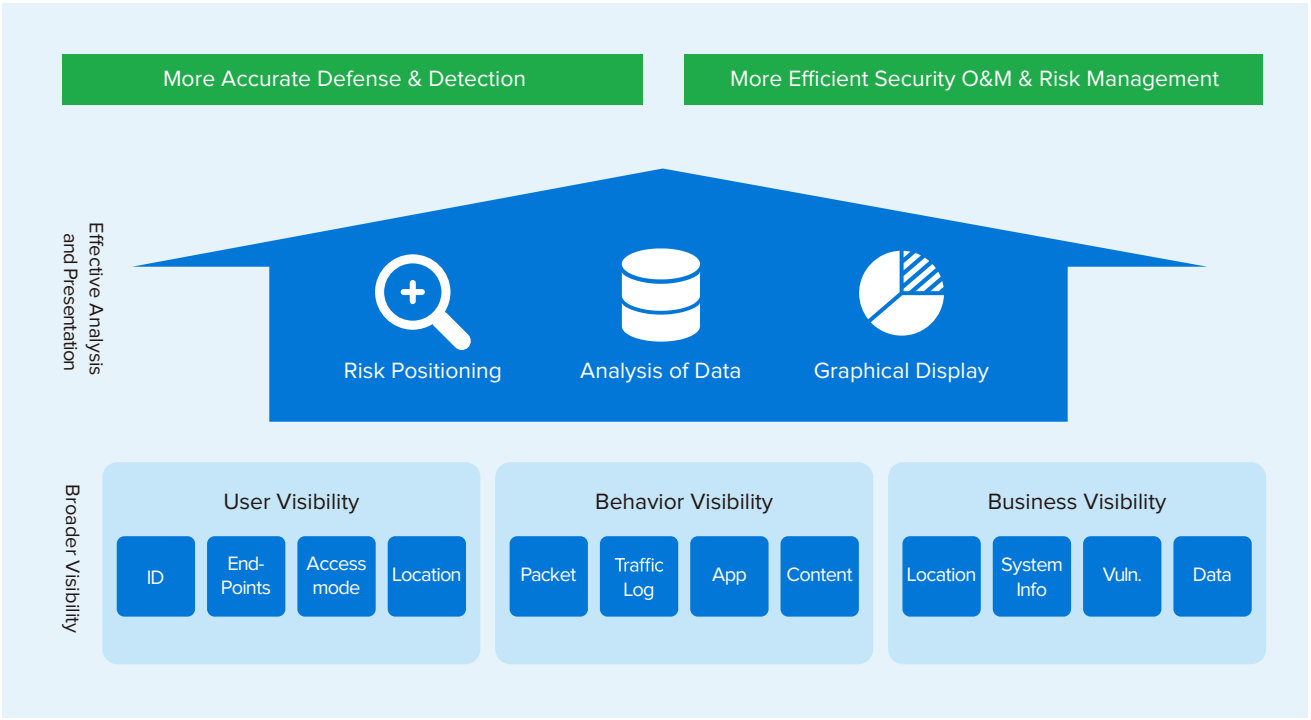
4. Sinergia di sicurezza

Nelle minacce sofisticate, come gli attacchi ransomware e crypto mining, stabilire il comando 6 di controllo (C2) di comunicazione tra l'endpoint compromesso e l'infrastruttura dell'attaccante è una fase essenziale nella kill chain. Tuttavia, identificare con precisione i clienti compromessi che mostrano il comportamento C2 nelle operazioni quotidiane, sia attraverso il rilevamento del firewall o l'indagine manuale, è una sfida difficile, specialmente nell'ambiente DHCP. Sangfor riconosce questa sfida e la affronta in modo innovativo orchestrando la rete e la protezione degli endpoint.

Introducendo l'integrazione di Sangfor Network Secure & Endpoint Secure, una collaborazione senza soluzione di continuità potenziata da APIs native integrate. Questa integrazione consente a Sangfor Network Secure ed Endpoint Secure di scambiare informazioni sulle minacce e di correlare gli eventi per migliorare il rilevamento delle comunicazioni C2 e di altri comportamenti furtivi. I risultati sono consolidati su un unico dashboard in Network Secure. Questa dashboard offre una panoramica completa delle minacce, inclusi i domini dannosi, i nomi dei clienti e dei processi interessati e le strategie di mitigazione consigliate. Gli amministratori della sicurezza possono scegliere di mettere in quarantena i processi dannosi o avviare la scansione dei virus direttamente dalla dashboard di Network Secure con un solo clic.



La sinergia creata tra Sangfor Network Secure e Endpoint Secure migliora significativamente il rilevamento e la risposta alle minacce e semplifica le operazioni con un investimento minimo.



SANGFOR Network Secure – Famiglie di prodotto

Performance

	NSF-1050A-I	NSF-1100A-I	NSF-3100A-I	NSF-7100A-I
Firewall Throughput [1,2]	10Gbps	20Gbps	30Gbps	70Gbps
Application Control Throughput [1,3]	6Gbps	12Gbps	20Gbps	40Gbps
NGFW throughput [1,4]	1.5Gbps	3Gbps	7Gbps	25Gbps
Threat Prevention Throughput [1,5]	820Mbps	1.5Gbps	3.6Gbps	15Gbps
Web Application Protect Throughput [1,6]	950Mbps	2.3Gbps	3.2Gbps	20Gbps
IPsec VPN Throughput [1,7]	600Mbps	1.5Gbps	3.5Gbps	10Gbps
Max IPsec VPN Tunnels	100	1000	4,000	20,000
Concurrent Connections	800,000	2,000,000	4,000,000	25,000.000
New Connections	20,000	90,000	180,000	600,000
Virtual Domains (Recommended/Max)	1/6	3/6	5/10	24/48

Hardware Specification

	NSF-1050A-I	NSF-1100A-I	NSF-3100A-I	NSF-7100A-I
Form Factor	Desktop	1U	1U	2U
RAM	4GB	8GB	16GB	48GB
Storage	128GB SSD	128G SSD	256G SSD	128G + 960G SSD
Power Supply Type	Single AC	Dual AC	Dual AC	Dual AC
Power Consumption (Max)	24W	40W	150W	300W
Operation Temperature	0°C – 45°C			
Humidity	5% - 90% non-condensing			
System Weight	3.08kg	7.96kg	8.78kg	21kg
Length x Width x Height (mm)	175 x 275 x 44.5	400 x 430 x 44.5	450 x 440 x 44.5	600 x 440 x 89
Hardware Bypass (Copper)	N/A	2	4	2
10/100/1000 Base-T	8	8	16	4
1G SFP	2	N/A	N/A	4
10G SFP+	N/A	2	6	8
Network Slots (In Use/Total)	N/A	0/1	0/2	0/4
Management Interface	1	1	1	1
Serial Port	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45
USB Port	2	2	2	2
Certificates	CE, FCC, ROHS			

Remarks

1. All throughput performance data is measured in the laboratory. The performance may vary depending on the actual configuration & network environment.

2. Firewall Throughput is measured with 1518 Bytes UDP packets.

3. Application Control throughput is measured with firewall and Application Control enabled. 64K HTTP packets

4. NGFW Throughput is measured with Firewall, Application Control, Bandwidth Management and IPS enabled. 64K HTTP packets

5. Threat Prevention Throughput is measured with Firewall, Application Control, Bandwidth Management, IPS, and Anti-Virus enabled. 64K HTTP packets

6. Web Application Protect Throughput is measured with Firewall, Application Control, Bandwidth Management, IPS and WAF enabled. 64K HTTP packets.

7. IPsec VPN Throughput include Sangfor to Sangfor device connection scenario and Sangfor to 3rd party device scenario.

SANGFOR NETWORK SECURE

INTERNATIONAL OFFICES

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-648773

SANGFOR HONG KONG (CHINA)
Unit 1612-16, 16/F, The Metropolis Tower, 10 Metropolis Drive, Hung Hom, Kowloon, Hong Kong
Tel: (+852) 3845-5410

SANGFOR INDONESIA
MD Place 3rd Floor, Jl Setiabudi No.7, Jakarta Selatan 12910, Indonesia
Tel: (+62) 21-2966-9283

SANGFOR MALAYSIA
No.45-10 The Boulevard Offices, Mid Valley City, Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3644

SANGFOR THAILAND
141 Major Tower Thonglor (Thonglor10) Floor 11 Sukhumvit Road, Kholngtan Nuea Wattana BKK, Thailand 10110
Tel: (+66) 02-002-0118

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati, 122 Metro, Manila, Philippines.
Tel: (+63) 0916-267-7322

SANGFOR VIETNAM
4th Floor, M Building, Street C, Phu My Hung, Tan Phu Ward, District 7, HCMC, Vietnam
Tel: (+84) 287-1005018

SANGFOR SOUTH KOREA
Floor 17, Room 1703, Yuwon bldg. 116, Seosomun-ro, Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

SANGFOR EMEA
D-81 (D-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE.
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
D44, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: (+92) 333-3365967

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi Techpark (Lobby B), Singapore 408564
Tel: (+65) 6276-9133

SANGFOR TURKEY
Turgut Ozal Street, Zentra Istanbul, First Floor, Office. 20 Çekmeköy / İstanbul, Postal Code: 34788
Tel:(+90) 546-1615678

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

Network Secure - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/AI Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
Seamless Experience, Secure and Efficient

Access Secure - Secure Access Service Edge
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

SANGFOR

https://twitter.com/SANGFOR

https://www.linkedin.com/company/sangfor-technologies

https://www.facebook.com/Sangfor

https://www.instagram.com/sangfortechnologies/

https://www.youtube.com/user/SangforTechnologies

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com

IT-Sangfor Network Secure_BR_P_Sangfor Network Secure-Brochure_20231009