SANGFOR
SANGFOR

SANGFOR NETWORK SECURE
NEXT GENERATION FIREWALL

Smarter AI-Powered Perimeter Defense

The World's First Fully Integrated NGFW + NGWAF + SoC Lite

- One Management Panel for All Security Operations
- Security Expertise Enablement Through Visualization
- Do More With Less. Minimum 50% of TCO Reduction Efficiently

- Stop Emerging Cyber Threats
- Eradicate Ransomware with Sangfor XDDR Synergy

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

Sangfor Technologies
AF8.0.47.1004
RECOMMENDED
Enterprise Firewall
April 2023
Cyber Ratings.org

FROST & SULLIVAN BEST PRACTICES AWARDS
2023 ASIA-PACIFIC NEXT-GENERATION FIREWALL COMPANY OF THE YEAR
SANGFOR

New World. New IT. New Security.

The World's First Fully Integrated NGFW + NGWAF + SoC Lite

The IT industry is constantly evolving. The Internet has given IT trends like cloud computing, BYOD, and IoT adaptive advantage over previous traditional methods of connection, with business-critical applications and IT services hosted remotely and accessible 24/7 on an endless array of devices in an endless number of locations. These adaptable trends survive because they are the fittest, but is network security evolving at the same pace?

Ethics has never played the greatest role in the process of evolution and the IT industry is no exception. Information is the newest global business currency and sensitive data like financial information and confidential corporate information is understandably the target of coevolving corrosive elements like defacement, ransomware, and malware.

It is estimated that more than 90% of enterprise firewalls will be NGFWs, replacing traditional firewalls. But those organizations who are protected by NGFWs often neglect to evolve their security protection into the realm of Web Application Firewall (WAF) or more comprehensive and proactive methods of protection. WAF and deep-learning security components are often seen as an additional investment with few monetary benefits, while the protection offered by NGFWs is becoming too general and reactive amid the continuous evolution of cyber threats.

In 2017, a new variation of ransomware called WannaCry infected more than 99 countries, attacking governments, schools, hospitals, and other industries. It was this incident that made ransomware well-known to the public.

Ransomware is malicious software that cyber-criminals use to hold your files (or computer) for ransom and require you to pay a certain amount of money to get them back by encrypting your files. Since it was discovered, Ransomware has been growing at a tremendous speed with more and more users being infected, both companies and consumers. Ransomware critically affects the productivity and reputation of many companies, many of whom have to pay in the end.

More and more variants are now being spread such as XBash, which are focused on data system destruction and cryptocurrency mining. Application security is no longer optional. Between increasing attacks and regulatory pressures, organizations must establish effective processes and capabilities for securing their applications and APIs (source: OWASP, 2017). With risk awareness & cost concerns delaying the evolution of true organizational security, many businesses are simply taking what is offered with no consideration given to (or no idea of) true needs.

Sangfor Network Secure

Sangfor Network Secure (previously known as Sangfor NGAF) is a converged security solution that provides protection against advanced persistent threats (APT), malware, ransomware, IoT threats, and web-based attacks. It integrates security features including Firewall, Application Control, URL Filtering, Intrusion Prevention System (IPS), Anti-malware, Cloud Sandbox, and WAF. Sangfor Network Secure also harnesses the power of Sangfor Engine Zero (AI-enabled malware inspection engine) and Neural-X (threat intelligence and analytics platform) to detect and isolate emerging threats that haven't yet been added to any security database, making it especially effective against 0-day attacks.

Smart World, Safe World with Sangfor Innovations

Neural-X is at the center of a sophisticated web of Sangfor-developed network security elements. As a cloud-based intelligence and analytics platform powered by Artificial Intelligence (AI), Neural-X powers and expands security detection capabilities for Sangfor's network, endpoint, and security-as-a-service offerings.

Neural-X contains dozens of interconnected components designed to work together seamlessly to keep your system both safe and secure including Engine Zero, threat intelligence, deep learning, sandboxing, and botnet detection.
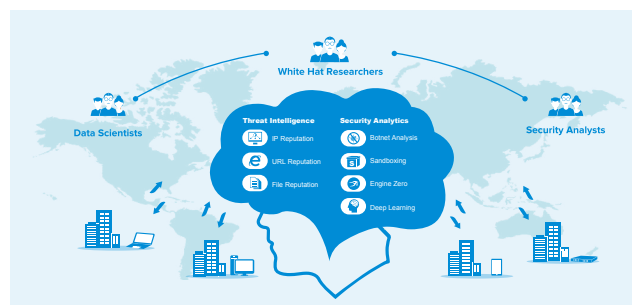
Sangfor Engine Zero

Sangfor Engine Zero is a malware detection engine built upon powerful artificial intelligence technology and is continuously enhanced by a team of data scientists, security analysts, and white hat researchers. This engine is one of several malware inspection engines embedded in Sangfor's security products and the Neural-X cloud threat intelligence platform. It is highly efficient and utilizes minimal resources. Only such efficiency can provide malware inspection for both known and zero-day attacks on the network gateway without impacting performance. In a recent ransomware test conducted by AV-Test, Sangfor Endpoint Secure, powered by Engine Zero, achieved a perfect 100% success rate across all the tests, demonstrating the engine's ability to detect advanced real-world threats.

Sangfor Neural-X

Neural-X lies at the core of Sangfor's intelligent threat detection and defense. Threat intelligence consists of organized, analyzed, and refined information that enables organizations to understand, assess, and guard against known and emerging risks from external sources.

Deep Learning

Deep learning is a complex element of machine learning inspired by the function of interconnecting neurons in the human brain. It is part of Artificial Intelligence and can be considered as an evolution to Machine Learning. As the name goes, it can learn by itself by observing and processing millions of data so that it can make more accurate & faster predictions. One of the ways Neural-X uses deep learning is to break down cryptic domain names into vectors that are machine-readable. An in-depth analysis of vector association detects domain names used by malware of similar families. Over time the deep learning function will begin to operate and learn independently – maintaining a proactive approach against malware.

Sangfor ZSand

Sangfor ZSand is a virtual dynamic execution technology (sandboxing) designed to detect unknown malware. Sangfor ZSand detonates suspected malware in a safe and controlled environment and monitors the abnormal behaviors of these files for future recognition and prevention. In recent tests, it has accurately detected ransomware families including GandCrab, Zusy, GlobeImposter, and LockCrypt. ZSand shares all data with Neural-X threat intelligence making it possible to identify and study malware with no known previous signature, reducing the risk of future zero-day attacks, detection, identification, and elimination within Neural-X.

Botnet Detection

Hackers are becoming more sophisticated by abandoning fixed IP addresses and using dynamic domain names instead. These cryptic domain names are used to connect a network of compromised computers called botnets to their controller using secret algorithms. Botnets are notoriously difficult to detect because DNS queries mimic the behavior of normal internet users. Neural-X uses advanced flow analysis, visual calculation, and deep learning technology to detect botnets. It is able to uncover significantly more malicious domain names compared to popular sources such as VirusTotal. So far, it has identified over a million malicious domain names, and this list is growing daily.

Next Generation Web Application Firewall

Sangfor Network Secure is the world's first NGFW integrated with a dedicated Next-Generation Web Application Firewall (NGWAF) to protect against both network and web-based attacks, including SQL injection, web shells, cross-site scripting (XSS), and deserialization flaws. The Sangfor Web Intelligent & Semantic Engine (WISE) employs machine learning and semantic analysis to scrutinize attack behaviors, enhancing detection rates and reducing false positives when compared to traditional SNORT-based detection engines. Threat models of attack behaviors are established to facilitate the streamlined management of application-related security threats.
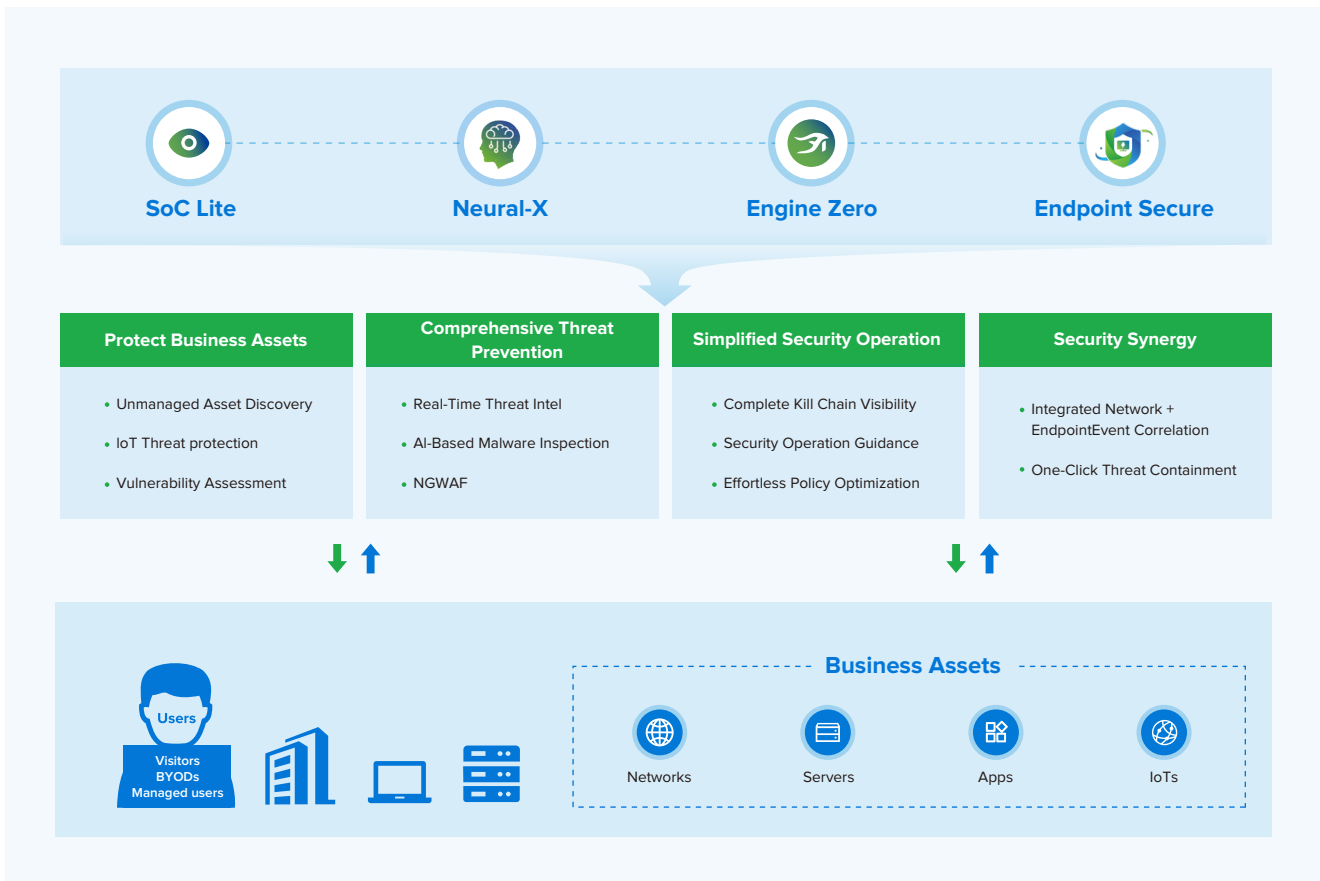
Sangfor's Concept of Security

Network Security has not evolved equally across verticals and locations. Security professionals from different industries and regions have differing opinions, expectations, and needs when it comes to network security. Some define it as protection against unauthorized access to files and data, while others emphasize the prevention of malware infection.

However, security solutions based on these traditional functions of network security offer limited visibility to users, traffic, and IT assets and lack real-time or post-compromise detection capabilities. As the volume and complexity of cyber-attacks increases, network security must evolve to keep up with emerging threats.

Sangfor advocates an innovative and more encompassing concept of network security. We go above and beyond, providing a comprehensive security solution that covers all threats, be they pre-attack or post-attack, originating externally or internally, current or future.

Sangfor's revolutionary approach to network security is grounded in four fundamental principles:

SoC Lite	Neural-X	Engine Zero	Endpoint Secure

Protect Business Assets	Comprehensive Threat Prevention	Simplified Security Operation	Security Synergy
• Unmanaged Asset Discovery	• Real-Time Threat Intel	• Complete Kill Chain Visibility	• Integrated Network + EndpointEvent Correlation
• IoT Threat protection	• AI-Based Malware Inspection	• Security Operation Guidance	• One-Click Threat Containment
• Vulnerability Assessment	• NGWAF	• Effortless Policy Optimization	

Users

Visitors
BYODs
Managed users

Business Assets

Networks   Servers   Apps   IoTs

1. Protect Business Assets

Sangfor Network Secure excels at discovering and protecting business assets to minimize the risks of compromise. It automatically discovers unmanaged IT assets and identifies risks such as system vulnerabilities, weak passwords, and unauthorized applications.

Additionally, Sangfor Network Secure offers proactive protection of assets through remedial features like virtual patching.

What the IT Team Sees	Assets Discovery	Vulnerability Assessment	Protection of the IT Assets
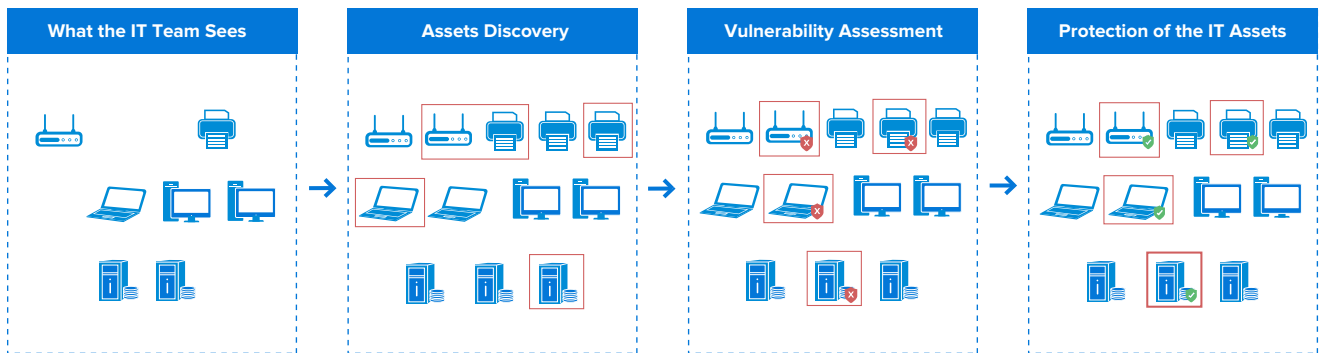
2. Comprehensive Threat Protection
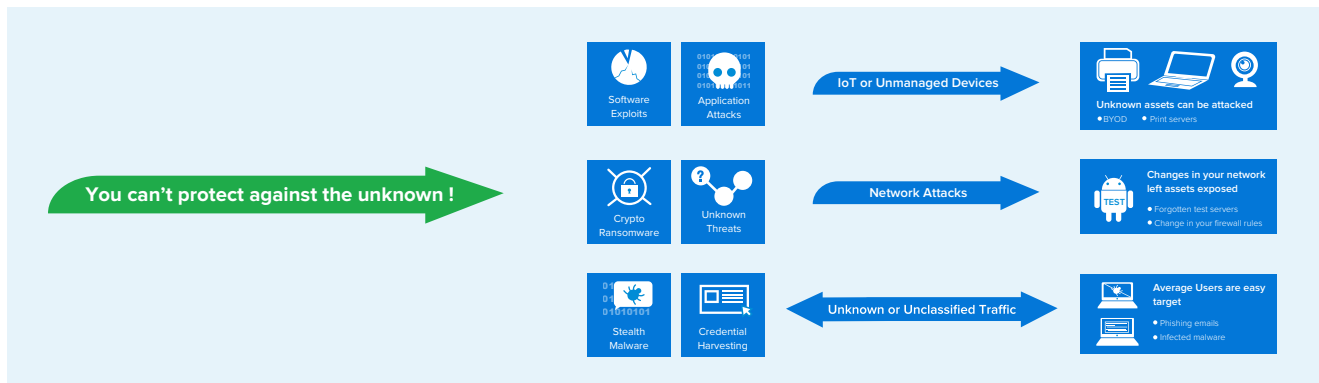
Sangfor Network Secure is a converged security solution that integrates multiple security features, including Firewall, Intrusion Prevent System (IPS), Anti-Virus (AV), Anti-Malware, APT (Advanced Persist Threat) Protection, IoT Security, URL filtering, Cloud Sandbox, and Web Application Firewall. These ensure comprehensive coverage against a wide array of security threats like ransomware, APT attack, and web exploits.

Protection against new malware and zero-day attacks is by far the most critical, as these threats have not been included in any signature database. Moreover, these advanced threats are typically in the possession of highly sophisticated and well-resourced threat actors, who are more capable of causing significant damage.

Sangfor effectively addresses these threats by implementing artificial intelligence in all of its security innovations, including Engine Zero, the Web Intelligent & Semantic Engine for NGWAF, Botnet Detection, and more. For example, Engine Zero is continuously trained on tens of millions of malware samples using advanced machine-learning algorithms to learn the evolving characteristics of malware. This has enabled it to recognize potential new malware and zero-day attacks with a significant degree of accuracy.

All Sangfor detection engines sharing the same threat intelligence provided by Sangfor's cloud-based Neural-X platform. Using machine learning, it can accurately detect new threats without any known signatures, empowering the proactive defense of your organization.
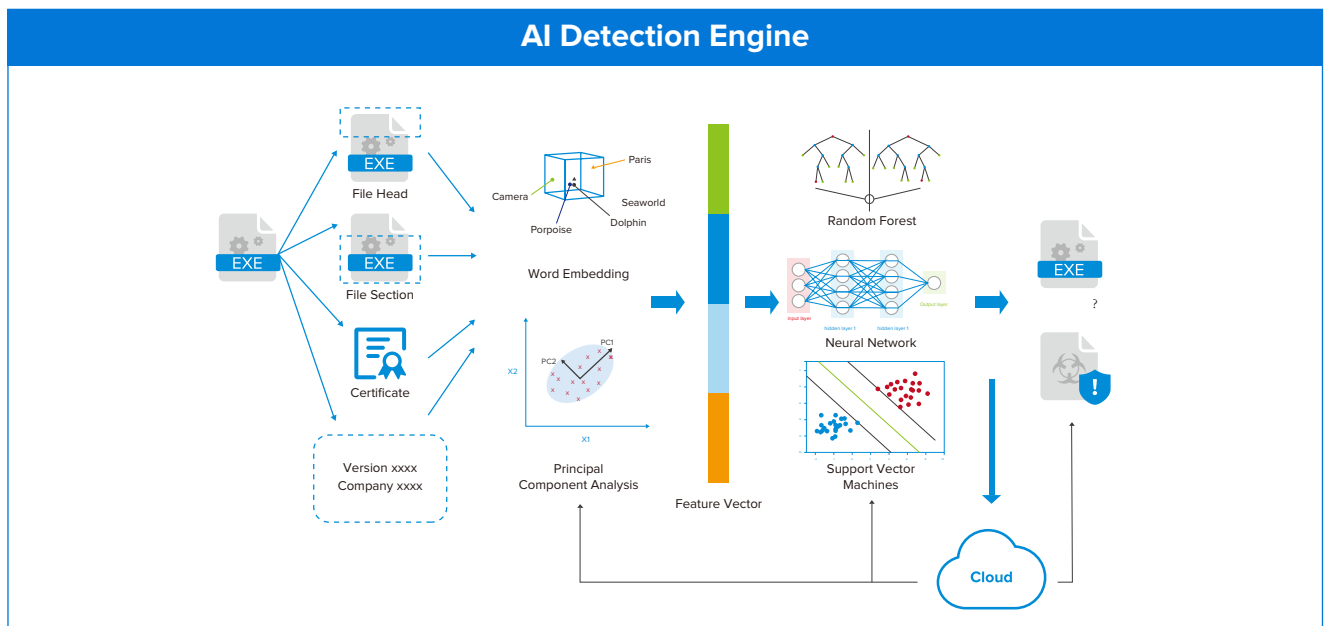
Real-Time Threat Intelligence Monitor

Global Cyber Attack Trends

283,130,752
Detections Today

172,181,239
Total Blocks Today

Top 5 Attack Types

Botnet

Web Atta...

Vulnerabi...

DDoS

Sensitive ...

Hot Topics

2023-04-23	Vulnerabilities
Cyrus IMAPD pop3d popsubf...	
2023-04-09	Vulnerabilities
PHP Code Execution Backdoo...	
2023-03-15	Vulnerabilities
Oracle9iAS Oracle Web Cache...	
2023-03-11	Vulnerabilities
D-Link Central WiFiManager ...	
2023-02-05	Vulnerabilities
Jenkins Remote Code Executi...	
2022-12-01	Security Event
Apache APISIX Remote Code ...	
2022-11-16	Security Event
HTTP Protocol Stack Remote ...	
2022-11-14	Security Event
Remote Code Execution Vuln...	
2022-11-03	Security Event
Oracle Access Manager Remo...	
2022-10-26	Security Event
Fortinet Authentication Bypas...	

□ Attack Source ⊙ Attack Target

Live Attacks

Timestamp	Attack Source	Attacker IP	Attack Target	Attack Type
2023-08-14 17:38:13	China	49.122.*.36	India	Vulnerability Attack
2023-08-14 17:38:14	France	195.154.*.130	China	DDoS
2023-08-14 17:38:15	United States of America	18.53.*.65	France	Botnet
2023-08-14 17:38:16	Chile	190.114.*.179	China	Web Attack
2023-08-14 17:38:18	Greece	5.54.*.10	United States of America	Sensitive Information

Intelligence Sources

• Over 20,000 connected network gateways provide IOCs that include malicious URLs, IPs, domain names, and malware hashes, with the number of participating gateways doubling every year.

• Third-party threat intelligence feeds.

• Sangfor security R&D actively monitors both white hat and black hat communities.

Real Case Scenario

When Sangfor Network Secure detects an unusual outbound connection from a server connected to the internet, it sends the suspicious DNS address to Neural-X for verification. If threat intelligence has classified this particular DNS as a known command & control (C2) server, it's likely the server has been compromised. Network Secure can be programmed to block these C2 communications so that no further damage is caused and alert security operators for further investigation and processing.

Engine Zero AI Powered Detection Engine

AI Detection Engine

EXE

EXE
File Head

EXE
File Section

Certificate

Version xxxx
Company xxxx

Camera
Paris
Porpoise
Seaworld
Dolphin
Word Embedding

PC1
PC2
X2
X1
Principal Component Analysis

Feature Vector

Random Forest

Neural Network

Support Vector Machines

EXE
?

Cloud

Engine Zero vs Traditional Detection Technologies

Traditional detection technologies mainly include signature-based detection (hashes, virus signatures, etc.), rule matching, virtual execution, and sandboxing. The threat detection capability of these technologies improves from signature-based detection to sandboxing. However, performance generally decreases and costs increase the more advanced the detection technology. Compared to these traditional technologies, Engine Zero has the following advantages:

▪ **Strong generalization:** Thanks to the generalization of machine learning, Engine Zero can identify unknown viruses or new variants of known viruses without prior knowledge. However, traditional solutions need to get samples first, which creates a lag between when new malware is created and when it can be detected.
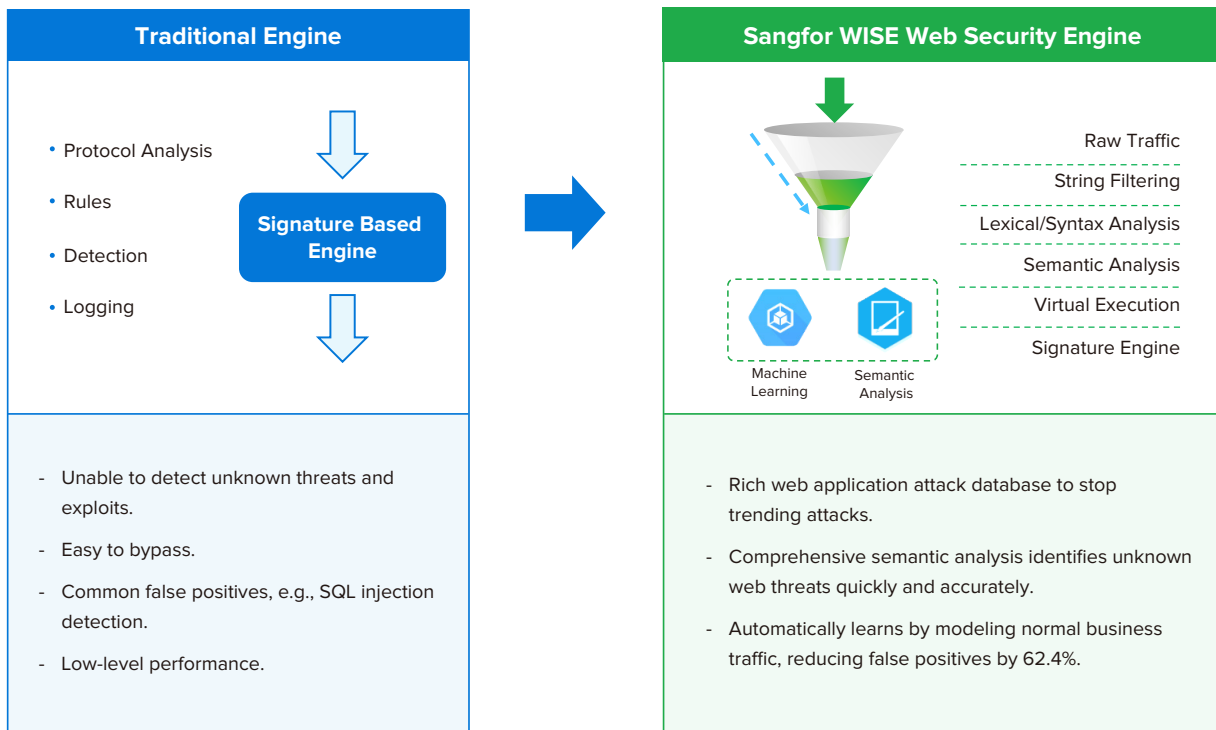
▪ **Rapid speed:** Near-linear scan speed close to signature-based detection using hashes.

Low memory occupation: In terms of resource cost, Engine Zero only occupies less than 200MB of memory, which is smaller than the known traditional engines.

▪ **A high degree of automation:** Engine Zero's AI model can automatically learn and extract features without human intervention. The model evolves in the cloud, with continuously improving detection and automation capabilities. However, traditional detection technologies require experts to manually extract virus fingerprints and signatures, which is not only costly but may also result in missed detections. "New" viruses may have been around for a long time before traditional anti-virus vendors update the virus database.

Despite the insufficiencies of traditional detection solutions, they still have a unique value. For example, they can respond rapidly using a blacklist and whitelist mechanism. As a result, Engine Zero combines advanced AI and traditional detection technologies to deliver both exceptional performance and detection accuracy.

The Only NGFW with Enterprise-Grade WAF

| Traditional Engine	Sangfor WISE Web Security Engine
• Protocol Analysis • Rules • Detection • Logging **Signature Based Engine**	Raw Traffic String Filtering Lexical/Syntax Analysis Semantic Analysis Virtual Execution Signature Engine Machine Learning Semantic Analysis
- Unable to detect unknown threats and exploits. - Easy to bypass. - Common false positives, e.g., SQL injection detection. - Low-level performance.	- Rich web application attack database to stop trending attacks. - Comprehensive semantic analysis identifies unknown web threats quickly and accurately. - Automatically learns by modeling normal business traffic, reducing false positives by 62.4%.

3. Simplified Security Operation

Even small or mid-sized organizations without a dedicated IT security team often receive thousands of alerts per week, requiring the IT department to allocate man-hours to investigation and analysis, thus increasing operational costs. This is the IT operator's nightmare, as they are now tasked with identifying the root cause of security incidents and taking action to mitigate damage and prevent future attacks from the same source, despite a lack of expertise. Additionally, organizations that are still using traditional security solutions without any intelligent or automated reporting tools are at a severe disadvantage. Without 360° visibility and clear analytics and reports, effective security becomes exponentially more difficult.

Sangfor Network Secure provides reliable and effortless security with easy deployment and simplified operation and maintenance features, enabling an effective and safe IT environment. The built-in Configuration Wizard streamlines security policy deployment, while the integrated SoC Lite module provides end-to-end visibility of the overall security of the organization, from business systems to endpoints.
Sangfor Network Secure simplifies daily security operations by identifying actual and risky security events among thousands of alerts and providing guidance and suggestions on the best solution. Dedicated dashboards are provided for trending threats such as ransomware to help administrators obtain timely updates.

Expansive assets and IoT visibility components allow the IT department and business owners to execute proactive checks of their business systems. These checks help IT operators quickly grasp the security posture of assets, including their online/offline status and the presence of illegal network access and potential risks, enabling them to make informed decisions to close any loopholes.
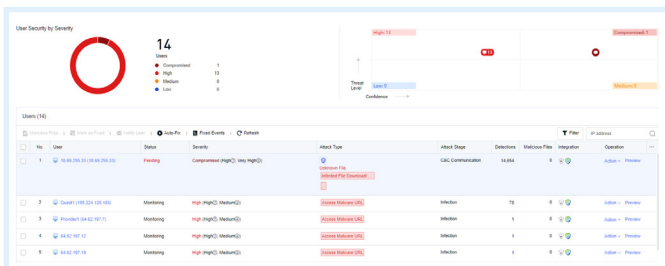Furthermore, Sangfor Network Secure features a built-in smart policy optimizer that empowers administrators to swiftly identify duplications, conflicts, and misconfigurations among thousands of policies with just a single click.
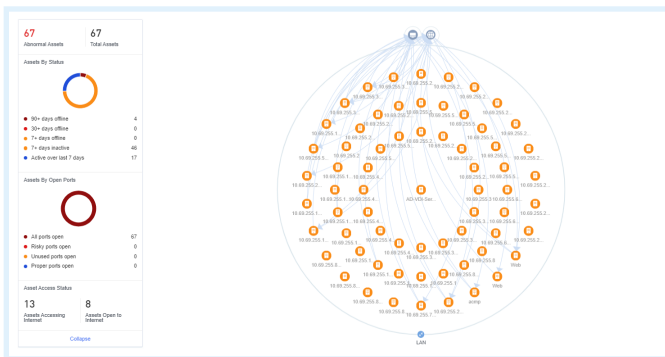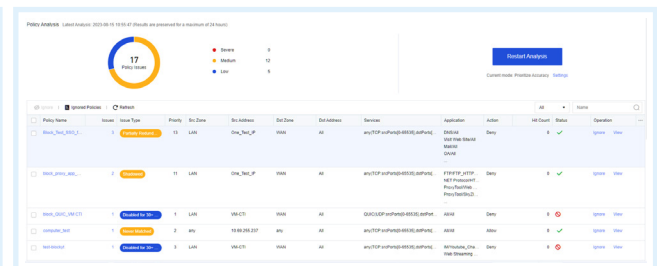

Asset Discover & Risk Management
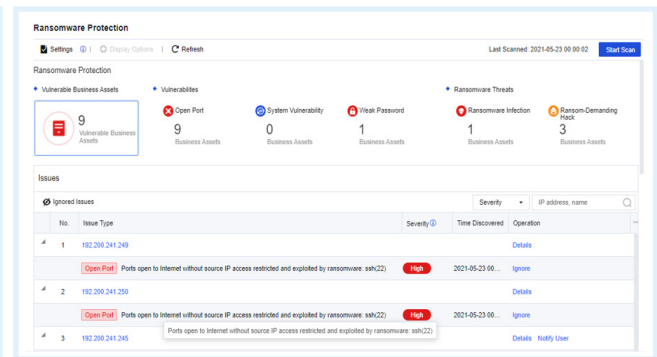
Ransomware Threat Monitoring

User Security Overview
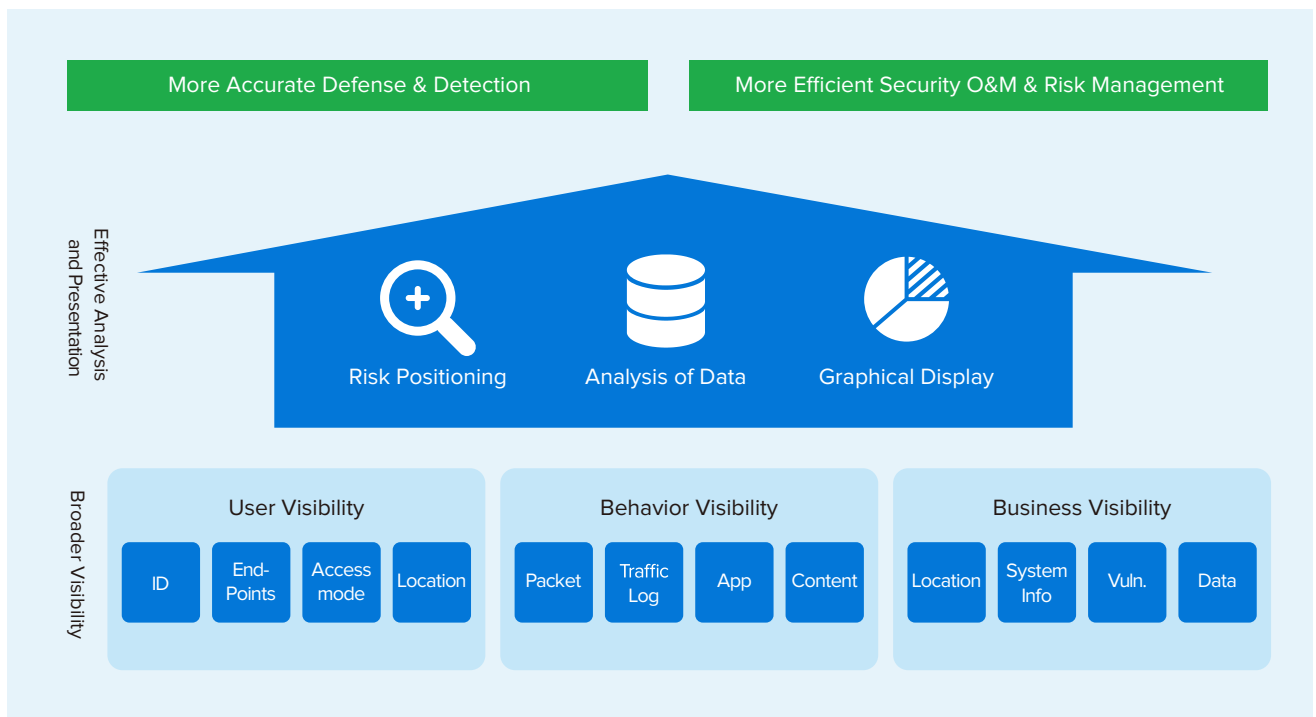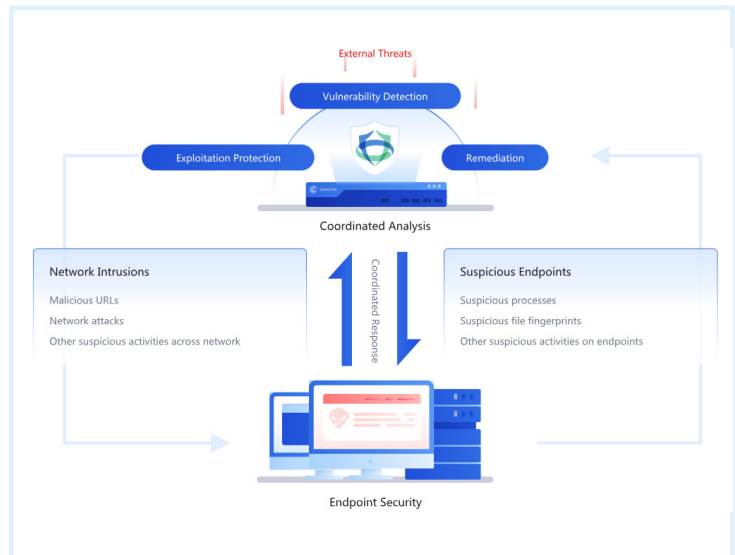

Smart Policy Optimizer

4. Security Synergy

In sophisticated threats, such as ransomware and crypto mining attacks, establishing command & control (C2) communication between the compromised endpoint and the attacker's infrastructure is an essential stage in the kill chain. However, accurately identifying compromised clients exhibiting C2 behavior in day-to-day operations, whether through firewall detection or manual investigation, is a formidable challenge, especially in the DHCP environment. Sangfor recognizes this challenge and innovatively addresses it via orchestrating network and endpoint protection.

Introducing Sangfor Network Secure & Endpoint Secure integration, a seamless collaboration empowered by native built-in APIs. This integration enables Sangfor Network Secure and Endpoint Secure to exchange threat intelligence and correlate events to improve the detection of C2 communication and other stealthy behavior. Findings are consolidated on a single dashboard in Network Secure. This dashboard offers a comprehensive overview of threats, including malicious domains, names of affected clients and processes, and recommended mitigation strategies. Security administrators can choose to quarantine malicious processes or initiate virus scans directly from the Network Secure dashboard with a single click.

The synergy created between Sangfor Network Secure and Endpoint Secure significantly enhances threat detection and response and simplifies operations with minimal investment.

External Threats

Vulnerability Detection

Exploitation Protection — Remediation

Coordinated Analysis

Network Intrusions
Malicious URLs
Network attacks
Other suspicious activities across network

Coordinated Response

Suspicious Endpoints
Suspicious processes
Suspicious file fingerprints
Other suspicious activities on endpoints

Endpoint Security

| More Accurate Defense & Detection | More Efficient Security O&M & Risk Management |

Effective Analysis and Presentation

Risk Positioning — Analysis of Data — Graphical Display

Broader Visibility

User Visibility				Behavior Visibility				Business Visibility			
ID	End-Points	Access mode	Location	Packet	Traffic Log	App	Content	Location	System Info	Vuln.	Data

Sangfor Network Secure Product Family

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

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

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