SANGFOR

SANGFOR ATHENA NGFW

NEXT GENERATION FIREWALL

Smarter AI-Powered Network 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 SynergAI

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

CRO CYBER RATINGS.ORG

Recommended Ratings in CyberRatings.org's Enterprise Firewall Test

Sangfor Technologies
AF8.0.47.1004
RECOMMENDED
Enterprise Firewall
April 2023
CRO 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 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 Athena NGFW

Sangfor Athena NGFW (previously known as Sangfor Network Secure) 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. Athena NGFW 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 Athena EPP, 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

Athena NGFW 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.

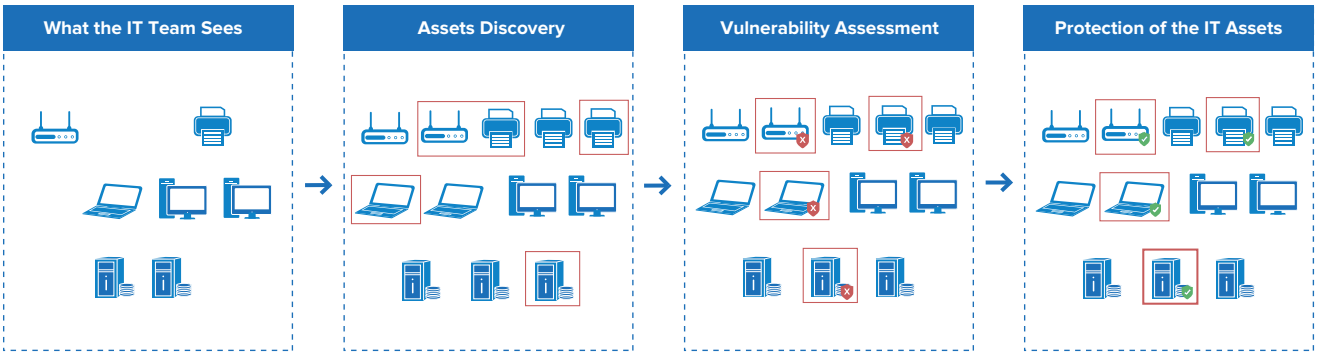
Sangfor advocates an innovative and more encompassing concept of network security. We go above and beyond, providing a comprehensive security solution that covers all threats, be they pre-attack or post-attack, originating externally or internally, current or future.

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

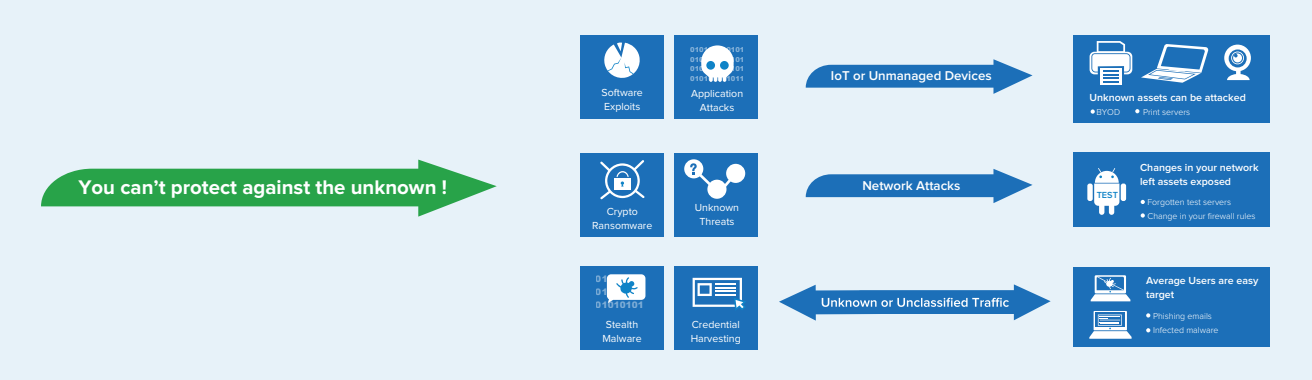
1. Protect Business Assets

Athena NGFW 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, Athena NGFW offers proactive protection of assets through remedial features like virtual patching.



2. Comprehensive Threat Protection



Athena NGFW 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

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.

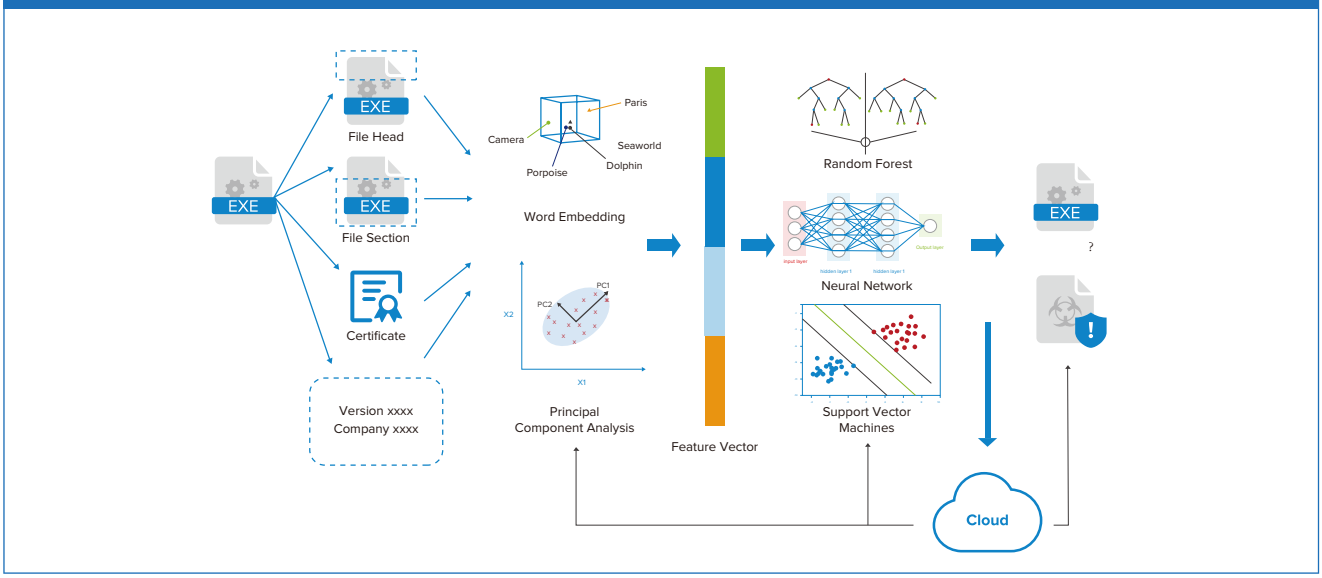
• Sangfor security R&D actively monitors both white hat and black hat communities.

Real Case Scenario

When Athena NGFW 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. Athena NGFW 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



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:

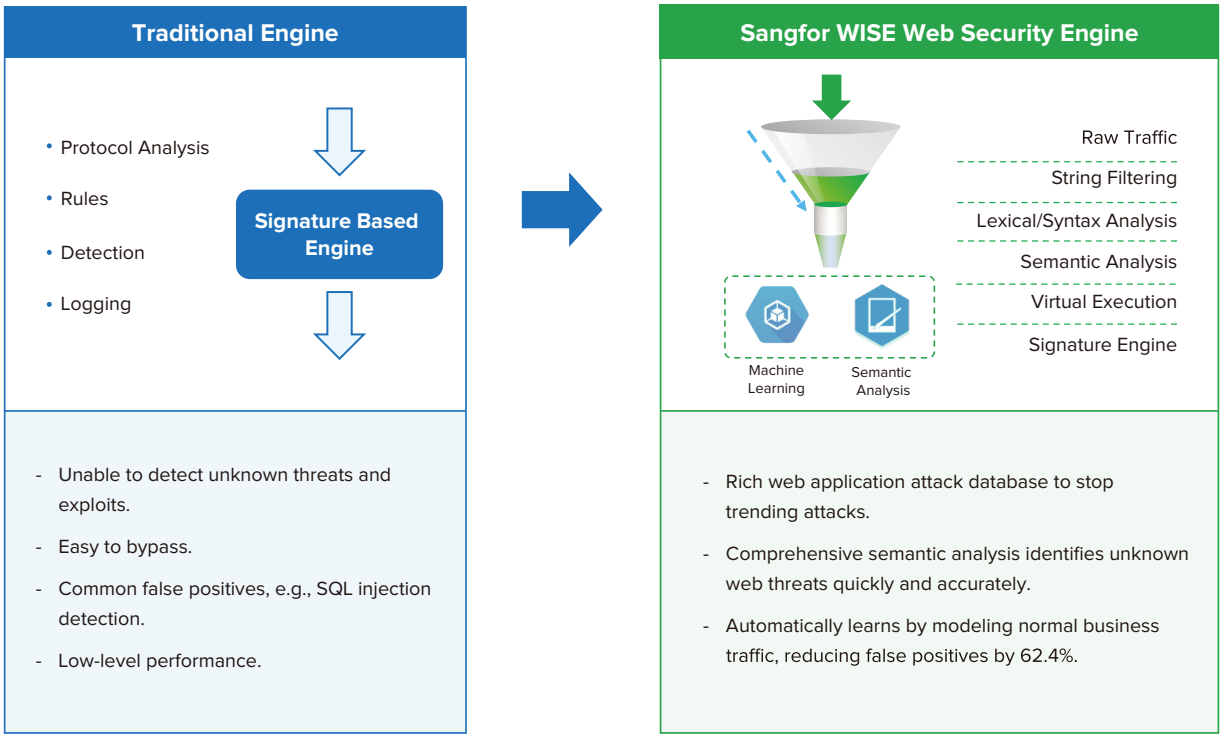
- **Strong generalization:** Thanks to the generalization of machine learning, Engine Zero can identify unknown viruses or new variants of known viruses without prior knowledge. However, traditional solutions need to get samples first, which creates a lag between when new malware is created and when 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

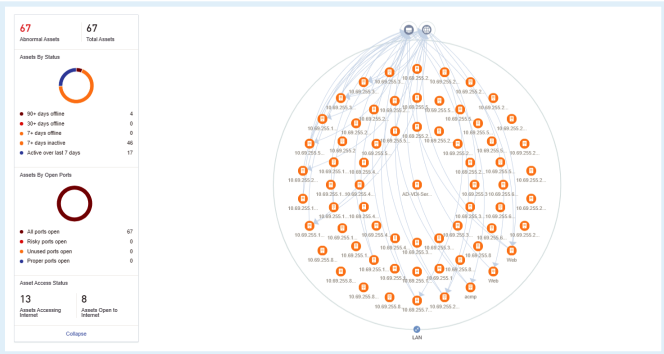


3. Simplified Security Operation

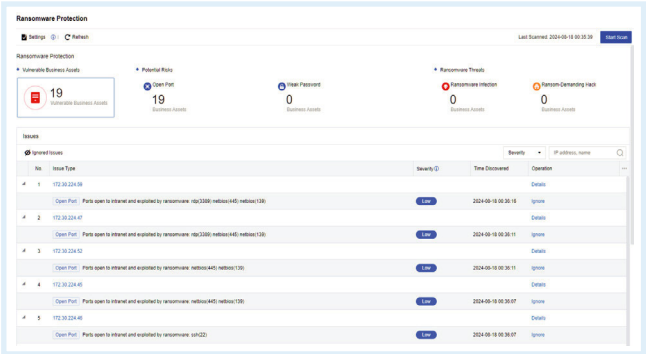
Even small or mid-sized organizations without a dedicated IT security team often receive thousands of alerts per week, requiring the IT department to allocate man-hours to investigation and analysis, thus increasing operational costs. This is the IT operator's nightmare, as they are now tasked with identifying 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.

Athena NGFW 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.
Athena NGFW 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.

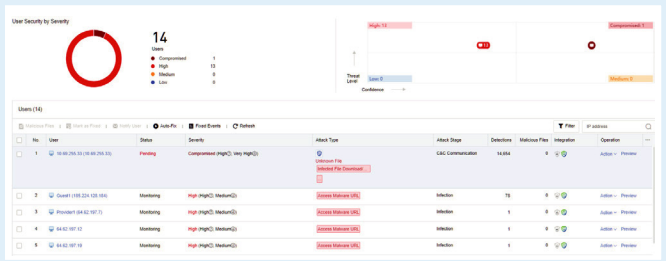
Expansive assets and IoT visibility components allow the IT department and business owners to execute proactive checks of their business systems. These checks help IT operators quickly grasp the security posture of assets, including their online/offline status and the presence of illegal network access and potential risks, enabling them to make informed decisions to close any loopholes.
Furthermore, Athena NGFW 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.



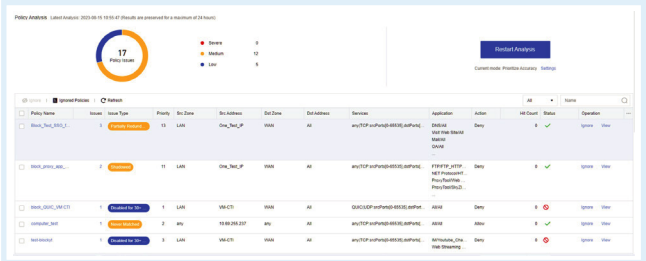
Asset Discover & Risk Management



Ransomware Threat Monitoring



User Security Overview



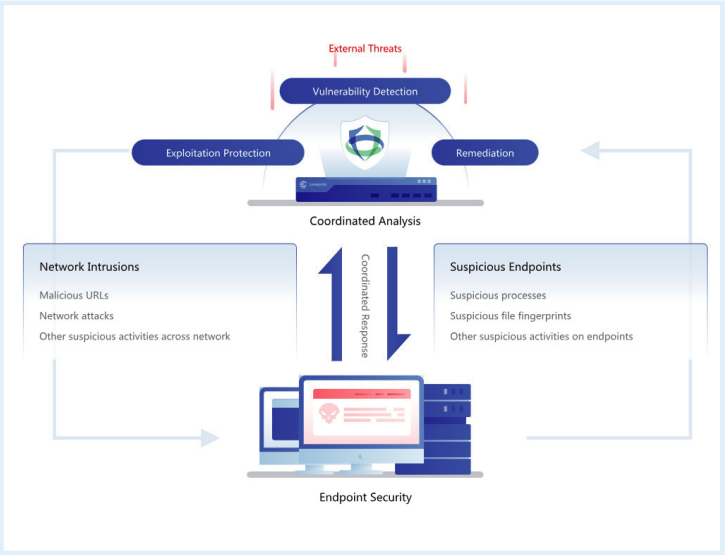
Smart Policy Optimizer

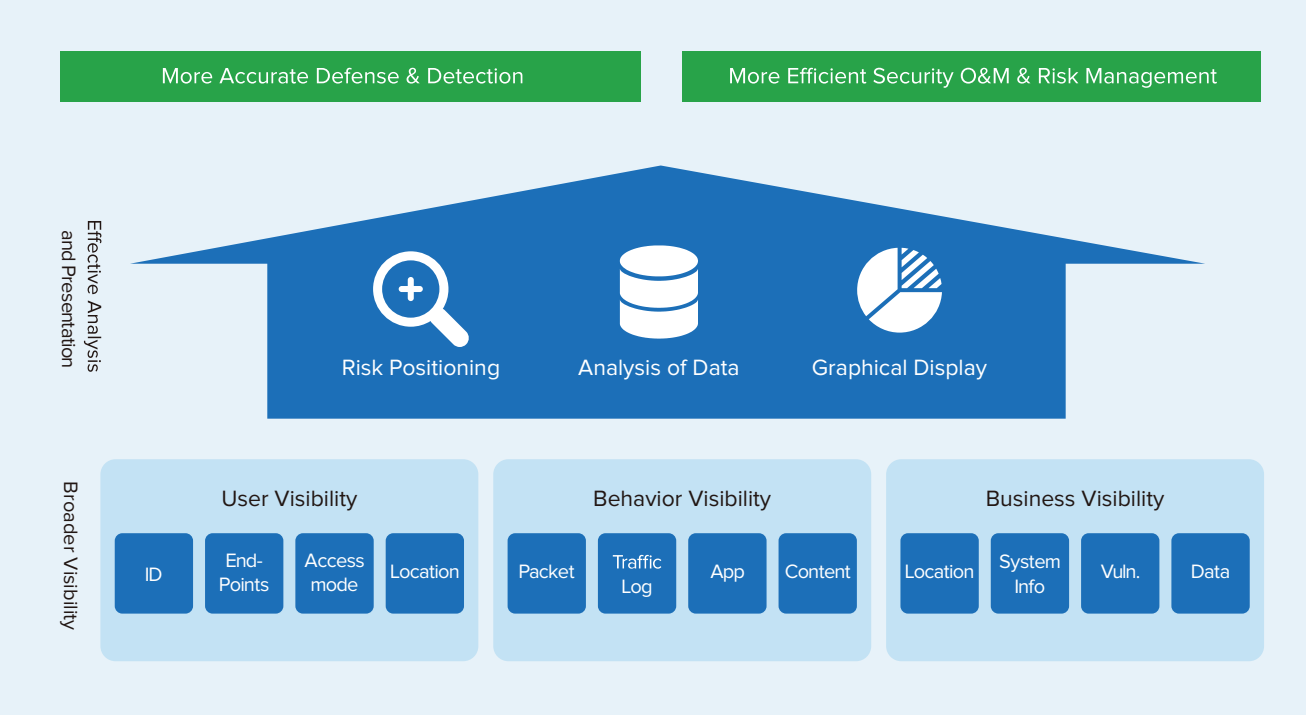
4. Security Synergy

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 Athena NGFW & Athena EPP integration, a seamless collaboration empowered by native built-in APIs. This integration enables Athena NGFW and Athena EPP 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 Athena NGFW. 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 Athena NGFW dashboard with a single click.

The synergy created between Athena NGFW and Athena EPP significantly enhances threat detection and response and simplifies operations with minimal investment.





Sangfor Athena NGFW Product Family

Performance (Measured by Enterprise Mix Traffic)

	NSF-1030A-I	NSF-1050A-I	NSF-1060A-I	NSF-1100A-I	NSF-1200A-I	NSF-3100A-I
Firewall Throughput [1,2]	2Gbps	10Gbps	20Gbps	20Gbps	20Gbps	30Gbps
Application Control Throughput [1,3]	1.1Gbps	5Gbps	6Gbps	10Gbps	12.5Gbps	15Gbps
NGFW throughput [1,4]	1Gbps	1.2Gbps	2.6Gbps	3.2Gbps	4Gbps	7Gbps
Threat Prevention Throughput [1,5]	850Mbps	1.1Gbps	1.7Gbps	2.2Gbps	2.8Gbps	6Gbps
Web Application Protect Throughput [1,6]	-	-	650Mbps	1.1Gbps	1.2Gbps	1.5Gbps
IPsec VPN Throughput [1,7]	900Mbps	600Mbps	1.8Gbps	1.8Gbps	2.2Gbps	3.5Gbps
Max IPsec VPN Tunnels	100	100	100	1000	1,000	4,000
Concurrent Connections	800,000	800,000	1,000,000	2,000,000	2,000,000	4,000,000
New Connections	30,000	20,000	90,000	90,000	90,000	180,000
Virtual Domains (Recommended/Max)	1/1	1/6	3/6	3/6	5/10	5/10

Hardware Specification

	NSF-1030A-I	NSF-1050A-I	NSF-1060A-I	NSF-1100A-I	NSF-1200A-I	NSF-3100A-I
Form Factor	Desktop	Desktop	Desktop	1U	1U	1U
RAM	4GB	4GB	4GB	8GB	8GB	16GB
Storage	64GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	256GB SSD
Power Supply Type	Single AC	Single AC	Single AC	Dual AC	Dual AC	Dual AC
Power Consumption (Max)	24W	24W	24W	60W	60W	150W
Operation Temperature	0°C – 45°C					
Humidity	5% - 90% non-condensing					
System Weight	2.7kg	3.08kg	3.08kg	7.96kg	7.96kg	8.78kg
Length x Width x Height (mm)	175 x 275 x 44.5	175 x 275 x 44.5	175 x 275 x 44.5	400 x 430 x 44.5	400 x 430 x 44.5	450 x 440 x 44.5
Hardware Bypass (Copper)	N/A	N/A	N/A	2	2	4
10/100/1000 Base-T	6	8	8	8	8	16
1G SFP	2	2	N/A	N/A	N/A	N/A
10G SFP+	N/A	N/A	2	2	2	6
Network Slots (In Use/Total)	N/A	N/A	N/A	0/1	0/1	0/2
Management Interface	N/A	1	1	1	1	1
Serial Port	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45
USB Port	2	2	2	2	2	2
Certificates	CE, FCC, ROHS					

Remarks

1. All throughput performance data is measured under laboratory conditions with firmware version 8.0.107. Actual performance may vary based on configuration and network environment.

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

3. Application Control throughput is measured with Firewall and Application Control enabled.

4. NGFW Throughput is measured with Firewall, Application Control, and IPS enabled

5. Threat Prevention Throughput is measured with Firewall, Application Control, IPS, and Anti-Virus enabled.

6. Web Application Protection Throughput is measured with Firewall, Application Control, IPS, and WAF enabled.

7. IPsec VPN Throughput includes Sangfor-to-Sangfor device connection and Sangfor-to-3rd party device connection scenarios with 512 Byte packets.

Sangfor Athena NGFW Product Family

Performance (Measured by Enterprise Mix Traffic)

	NSF-3200A-I	NSF-3400A-I	NSF-7100A-I	NSF-7200A-I	NSF-7300A-I	NSF-7500A-I
Firewall Throughput [1,2]	40Gbps	55Gbps	70Gbps	70Gbps	80Gbps	170Gbps
Application Control Throughput [1,3]	20Gbps	28Gbps	35Gbps	40Gbps	50Gbps	80Gbps
NGFW throughput [1,4]	9Gbps	14Gbps	19Gbps	22Gbps	30Gbps	65Gbps
Threat Prevention Throughput [1,5]	7Gbps	10.5Gbps	13Gbps	16Gbps	26Gbps	50Gbps
Web Application Protect Throughput [1,6]	2Gbps	7Gbps	10Gbps	10.5Gbps	11Gbps	30Gbps
IPsec VPN Throughput [1,7]	4Gbps	7Gbps	10Gbps	10Gbps	10Gbps	40Gbps
Max IPsec VPN Tunnels	6000	10,000	20,000	20,000	20,000	25,000
Concurrent Connections	4,100,000	10,000,000	25,000,000	25,00,000	27,000,000	50,000,000
New Connections	180,000	500,000	600,000	600,000	600,000	1,500,000
Virtual Domains (Recommended/Max)	5/10	10/20	24/48	24/48	24/48	25/225

Hardware Specification

	NSF-3200A-I	NSF-3400A-I	NSF-7100A-I	NSF-7200A-I	NSF-7300A-I	NSF-7500A-I
Form Factor	1U	2U	2U	2U	2U	2U
RAM	16GB	48GB	48GB	48GB	48GB	192GB
Storage	256GB SSD	128GB + 960GB SSD	128GB + 960GB SSD	128GB + 960GB SSD	128GB + 960GB SSD	480GB + 960GB SSD
Power Supply Type	Dual AC	Dual AC	Dual AC	Dual AC	Dual AC	Dual AC
Power Consumption (Max)	150W	300W	300W	300W	300W	800W
Operation Temperature	0°C – 45°C					
Humidity	5% - 90% non-condensing					
System Weight	8.78kg	21kg	21kg	21kg	21kg	21.6kg
Length x Width x Height (mm)	450 x 440 x 44.5	600 x 440 x 89	600 x 440 x 89	600 x 440 x 89	600 x 440 x 89	600 x 440 x 89
Hardware Bypass (Copper)	4	2	2	2	2	4
10/100/1000 Base-T	16	4	4	4	4	8
1G SFP	N/A	4	4	4	4	8
10G SFP+	6	8	8	8	8	8
Network Slots (In Use/Total)	0/2	0/2	0/4	0/4	0/4	4/8
Management Interface	1	1	1	1	1	1
Serial Port	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45
USB Port	2	2	2	2	2	2
Certificates	CE, FCC, ROHS					

Remarks

1. All throughput performance data is measured under laboratory conditions with firmware version 8.0.107. Actual performance may vary based on configuration and network environment.

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

3. Application Control throughput is measured with Firewall and Application Control enabled.

4. NGFW Throughput is measured with Firewall, Application Control, and IPS enabled

5. Threat Prevention Throughput is measured with Firewall, Application Control, IPS, and Anti-Virus enabled.

6. Web Application Protection Throughput is measured with Firewall, Application Control, IPS, and WAF enabled.

7. IPsec VPN Throughput includes Sangfor-to-Sangfor device connection and Sangfor-to-3rd party device connection scenarios with 512 Byte packets.

Sangfor Athena NGFW Product Family

Virtual Appliance Specification

	vNSF100	vNSF200	vNSF400	vNSF800	vNSF1600
vCPU Core Required	2 vCores	2 vCores	4 vCores	8 vCores	8 vCores
Memory Required	4GB	4GB	8GB	16GB	16GB
Storage Required	120GB	120GB	120GB	120GB	120GB
Threat Prevention Bandwidth[1]	100 Mbps	200 Mbps	400 Mbps	800 Mbps	1600 Mbps
Supported Platforms	Sangfor HCI, VMware ESXi 6.5 or higher				

Remarks

1.Threat Prevention Throughput is measured with Firewall, Application Control, IPS, and Anti-Virus enabled.

SANGFOR

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
380 Jln Besar,
#08-04/05 ARC 380, Singapore 209000
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
Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav.
B 10-11 Kuningan, Setia Budi, Kecamatan Setiabudi, Kota Jakarta
Selatan, Daerah Khusus Ibukota Jakarta 12910, Indonesia
Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA
Suite 11.01 & 11.02 , Level 11 of Centrepoint North, Mid Valley City,
Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3645

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

SANGFOR PHILIPPINES
Unit 14B 14th Floor, Rufino Pacific Tower, 6784 Ayala Avenue,
Makati City, Philippines
Tel: (+63) 9688998920

SANGFOR VIETNAM
Unit 11.01 MB Sunny Tower, 259 Tran Hung Dao Street,
Co Giang Ward, District 1, Ho Chi Minh City, Vietnam
Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA
305, 76, Yeonmujang-gil, Seongdong-gu,
Seoul, Republic of Korea.

SANGFOR UAE
Office #718, Publishing Pavilion, Production City, Dubai, UAE
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
Office No.210, 2nd Floor, "The Forum",
Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton, Karachi, Pakistan
South Region: (+92) 321 2373991
North Region: (+92) 304 5170714
Central Region: (+92) 314 519 8386

SANGFOR ITALY
Sede Principale: Via Marsala 36B, 21013, Gallarate (VA)
Sede a Roma: Via del Serafico, 89-91, 00142 Roma RM
Tel: (+39) 0331-6487-73

SANGFOR TÜRKIYE
A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk,
Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul
Tel: (+90) 216-5156969

SANGFOR LATAM OFFICE
Torre Onyx Segundo Piso, Av. Río San Joaquin 406, Amp Granada,
Miguel Hidalgo, C.P. 11529, Ciudad de México, CDMX.

SANGFOR SAUDI ARABIA OFFICE
Office 505, Al Dhabab Complex 5th Floor, 6347 Anas Ibn Aous,
Al Murabba, Riyadh.

SANGFOR OFFERINGS

Cybersecurity

Athena NGFW - Next Generation Firewall
Smarter AI-Powered Perimeter Defense

Athena EPP - Endpoint Protection Platform
The Future of Endpoint Security

Athena SWG - Secure Web Gateway
Secure User Internet Access Behaviour

Athena NDR - Network Detection and Response
Intelligent Detection and Response Platform

Athena XDR - Extended Detection and Response
The Best Fusion of SecOps and GenAI

Athena MDR - Managed Threat Detection & Response Service
The Cyber Guardian of Your Business

Athena SASE - Secure Access Service Edge
The Smarter, Simpler, and More Secure Way to Connect

Simplified Security Operations Solution
Run Full-fledged SecOps Minus the Complexity

Anti-Ransomware Solution
Block Ransomware in 3 Seconds

Secure SD-WAN Solution
Build a Secure and Efficient Enterprise Network

Secure Hybrid Work Solution
Simplify Access. Strengthen Security. Power Hybrid Work.

Cloud Computing

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

VMware Alternative
The Ideal Platform to Streamline Your off-VMware Journey

aDesk - Virtual Desktop & Virtual App Solutions
Seamless Experience, Secure and Efficient

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

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

Sales: sales@sangfor.com
Marketing: marketing@sangfor.com
Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com

Copyright © 2026 Sangfor Technologies. All Rights Reserved.