SANGFOR NGAF NEXT GENERATION FIREWALL

Smarter Security Powered By Artificial Intelligence

The World First Fully Integrated NGFW + WAF

- One Management Panel for All Security Operations
- Security Expertise Enablement Through Visualization
- Do More With Less. Minimum 50% of TCO Reduction
- Reduce Security Hardware Footprint Up to 70%
- All-in-One Integrated Endpoint Security Management

Listed In

Gartner

Magic Quadrant for Enterprise Network Firewalls

Certified by

ICSA labs CERTIFIED FIREWALL - CORPORATE

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 insular 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?

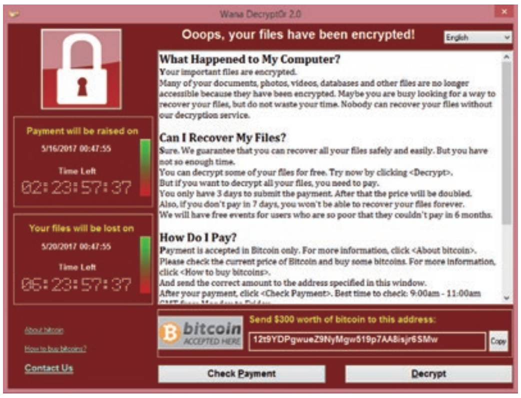
Ethics has never played the greatest role in the process of evolution and the IT industry is no exception. Information is the newest global business currency and sensitive data like financial information and confidential corporate information is understandably the target of coevolving corrosive elements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

The security market has responded with many granular security solutions but less than 40% of enterprises have progressed to Next Generation Firewall protection methods. Those organizations who are protected by Firewall or IPS often neglect to evolve their security protection into the realm of Web Application Firewall 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 NGFW & IPS is becoming too general and reactive with the increasing number of evolving web vulnerabilities.

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

More and more varients are now being spread such as XBash, which are focus on data system destruction and crypto currency 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's offered with no consideration given to (or no idea of) true needs.



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

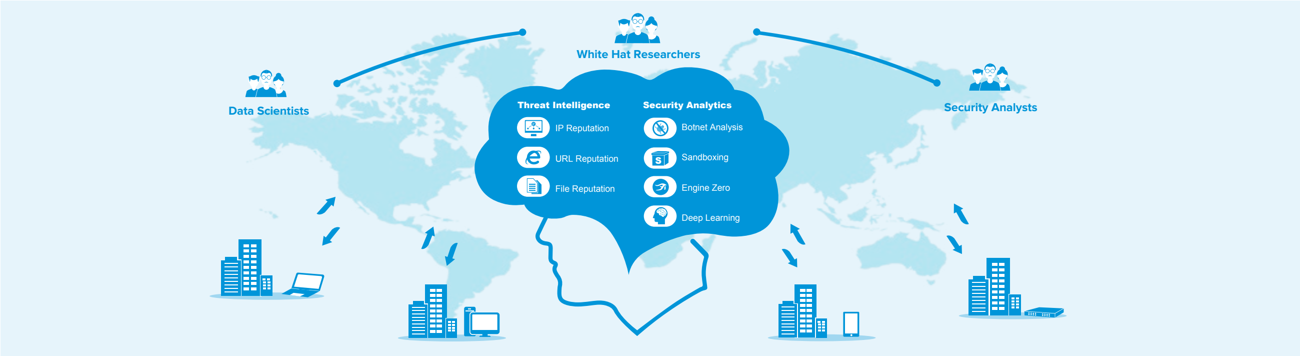
SANGFOR Next Generation Application Firewall

Sangfor NGAF is a converged security solution providing protection against IPS, advanced threat, malware, viruses, ransomware and web-based attacks using integrated security features like FW, IPS, AV, Anti-malware, APT, URL filtering, Cloud Sandbox, and WAF. Sangfor NGAF uses its own Cloud Sandbox to isolate possible emerging threats that haven't yet been added to any security database, making it especially effective against 0-day attacks.

Neural-X, Sangfor's newest security innovation, is at the core of a sophisticated web of Sangfor developed network security elements like threat intelligence, deep learning, WAF, ZSand, Botnet Malware Detection and Engine Zero. As a cloud-based intelligence and analytic platform powered by Artificial Intelligence (AI), Neural-X empowers and expands security detection capabilities for Sangfor's network, endpoint, and security-as-a-service offerings.

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 analytic 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.

Engine Zero

Engine Zero is an underlining malware detection engine that is built upon a set of powerful artificial intelligence technology, and enhanced by a team of data scientists, security analysts and white hat researchers. This engine is one of many malware inspection engines embedded in Sangfor's network security solutions, end point solution and Neural-X cloud platform. It is very efficient and utilizes very little resource. Only such efficiency can provide malware inspection for known and zero-day attacks on the network gateway with almost no impact on performance. In recent tests (July 2018), our malware detection rate scored the highest in terms of accuracy, surpassing other vendors and open source alternatives.

Threat Intelligence

Neural-X is at the core of Intelligent threat detection and defense. Threat Intelligence is organized, analyzed and refined information that enables organizations to understand, assess and prevent against known and severe risks from external sources.

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.

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 names goes, it can learn by itself by obersving and processing milllions of data so that it can make more accurate & faster predictions.

One of the way Neural-X uses deep learning is to break down cryptic domain names into vectors that are machine readable. In-depth analysis of vector association detects domain names used by malwares of similar families. Over time the deep learning function will begin to operate and learn independently – thus maintaining a proactive approach to malware

Botnet Detection

Hackers are becoming more sophisticated by abandoning fixed IP addresses and use dynamic domain names instead. These cryptic domain names are used to connect botnets to their controller using secret algorithms. They are notoriously difficult to detect because DNS queries behave similarly to the average user. Neural-X uses advanced flow analysis, visual calculation and deep learning technology to uncover botnets. It is able to uncovered significantly more malicious domain names compared to popular sources such as VirusTotal. So far, it has ncovered over a million malicious domain names and this list is growing daily.

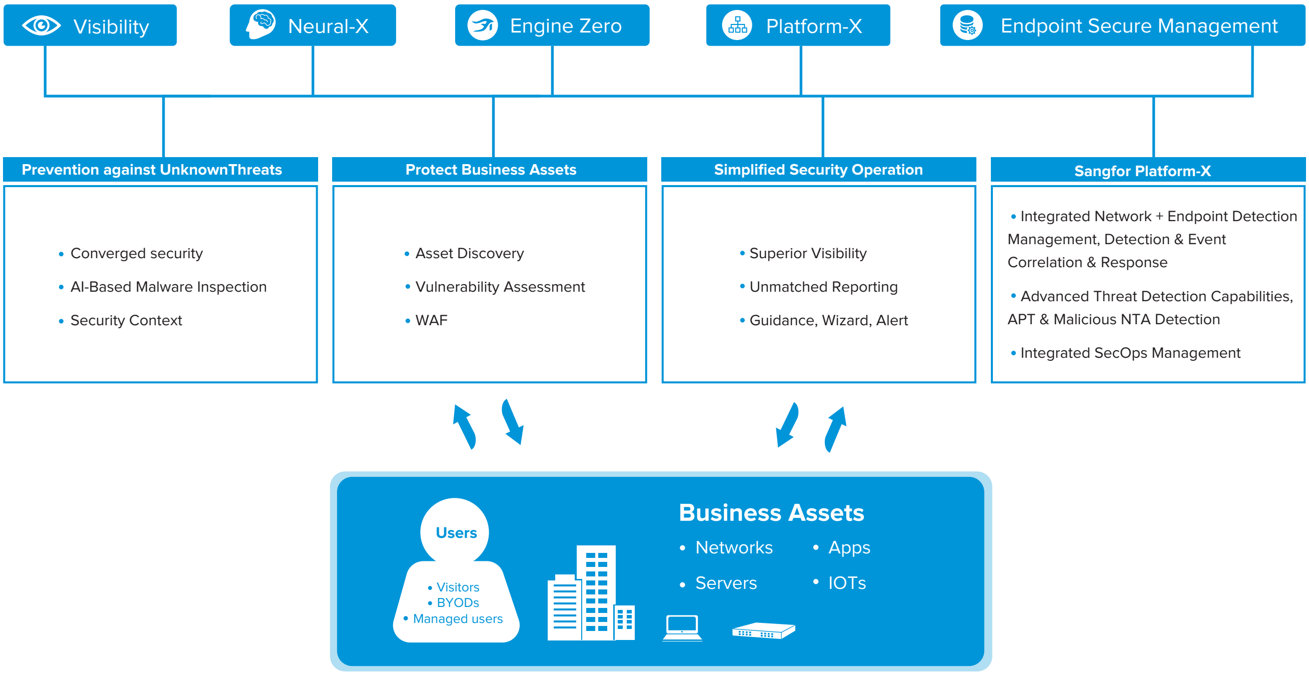
Next Generation Web Application Firewall

The Next Generation WAF engine, which is integrated in Sangfor's next-gen firewall, was developed to protect against new web-based attacks such as SQL injection, web shells, struts2 injection, and deserialization flaws. Sangfor's NGWAF engine uses machine- and deep-learning to analyze attack behaviors. It enhances detection rates and decreases false positives from traditional SNORT-based detection engines. By modeling attack behaviors, a threat model is created to easily manage the applications' system threats.

Sangfor
Concept of Security

Network Security has not experienced an equal evolution in all verticals – security experts have differing opinions, expectations and needs across different sectors and different locations. While some define network security as protection against unauthorized access to files and data, others focus on firewall, anti-virus and botnet detection. Traditional security solutions have limited visibility of users, traffic and IT assets with no real-time or post-event detection capabilities. With increasing attacks on the application layer, network security needs to evolve further to keep up with emerging threats.

Sangfor Technologies has a new concept of network security to counter new and more dangerous threats. We go further to provide a complete protection solution for all users against all threats, internal or external, existing or future. Sangfor's evolutionary adaptation of network security follows 4 fundamental points which form the core of our market strategy:



Visibility | Neural-X | Engine Zero | Platform-X | Endpoint Secure Management

Prevention against UnknownThreats
- Converged security
- AI-Based Malware Inspection
- Security Context

Protect Business Assets
- Asset Discovery
- Vulnerability Assessment
- WAF

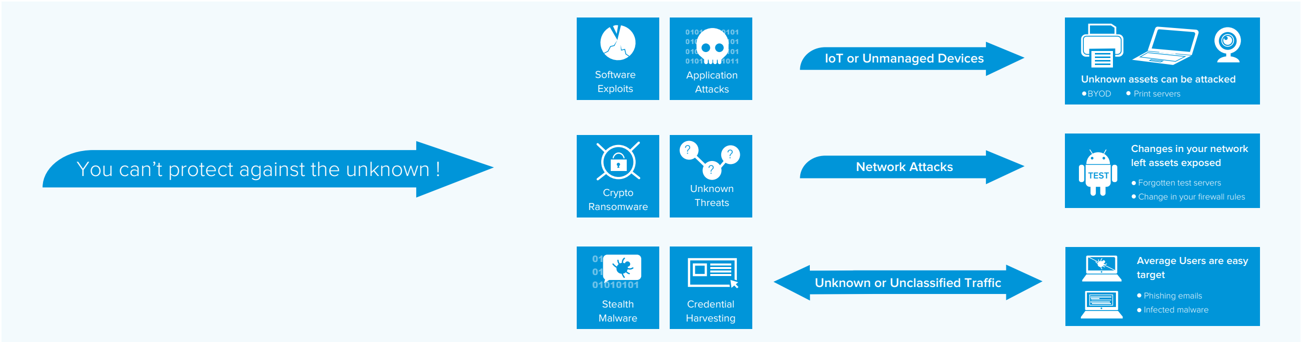
Simplified Security Operation
- Superior Visibility
- Unmatched Reporting
- Guidance, Wizard, Alert

Sangfor Platform-X
- Integrated Network + Endpoint Detection Management, Detection & Event Correlation & Response
- Advanced Threat Detection Capabilities, APT & Malicious NTA Detection
- Integrated SecOps Management

Business Assets
- Networks
- Apps
- Servers
- IOTs

Users
- Visitors
- BYODs
- Managed users

Prevention against Unknown Threats



Sangfor NGAF is a converged security solution, which provides protection against advanced persistent threats (APT), malware (virus, ransomware) and web-based attacks. Sangfor NGAF has integrated complete security features, such as Firewall, Intrusion Prevent System (IPS), Anti-Virus (AV), Anti-Malware engine, APT Protection (Advanced Persist Threats), URL filtering, Cloud Sandbox and Web Application Firewall.

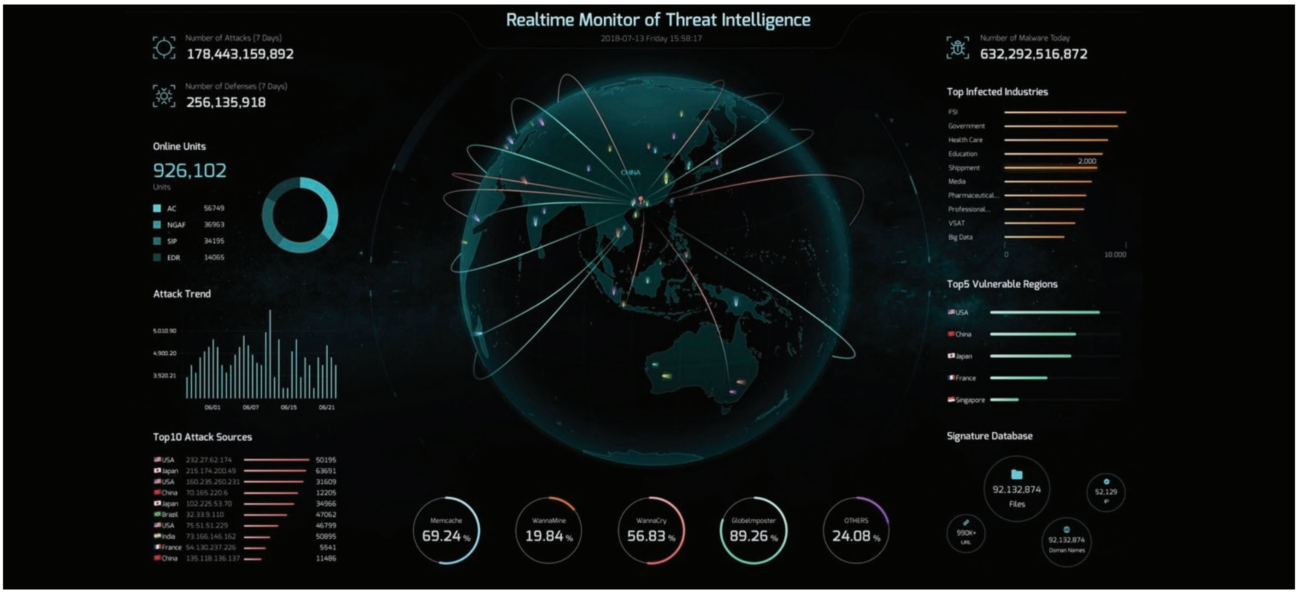
Sangfor NGAF uses its own Cloud Sandbox to help users isolate potential emerging & new threats that haven' t been included in any security database, which is especially useful against 0-day attacks.

The human element is still one of the weakest elements in any organization security operation team. With thousands of logs, it is almost impossible to go through each one of them. This is why many NGFW will filter all logs and only shows the ones with the highest level of importance. However even with this, it is still possible to make errors.

That is why Sangfor is now going further and has implemented artificial intelligence in all of its security innovations, such as malware detection "Engine Zero", Next generation WAF and new Botnet detection engines.

All these engines are sharing the same threat intelligence, which is provided by Sangfor cloud-based Neural-X platform. Using machine learning, it can detect the new unknown threat without any existing signature in advance and prevent any harms to your organization.

Real-Time Monitor of Threat Intelligence



Realtime Monitor of Threat Intelligence

2018-07-13 Friday 15:58:17

Number of Attacks (7 Days) 178,443,159,892

Number of Defenses (7 Days) 256,135,918

Online Units 926,102 Units

AC	56749
NGAF	36963
SIP	34195
EDR	14065

Number of Malware Today 632,292,516,872

Top10 Attack Sources

USA	232.27.62.174	50195
Japan	215.174.200.49	63691
USA	160.235.250.231	31609
China	70.165.220.6	12205
Japan	102.225.53.70	34966
Brazil	32.33.9.110	47062
USA	75.51.51.229	46799
India	73.166.146.162	50895
France	54.130.237.226	5541
China	135.118.136.137	11486

Signature Database

92,132,874 Files

52,129 IP

990K+ URL

92,132,874 Domain Names

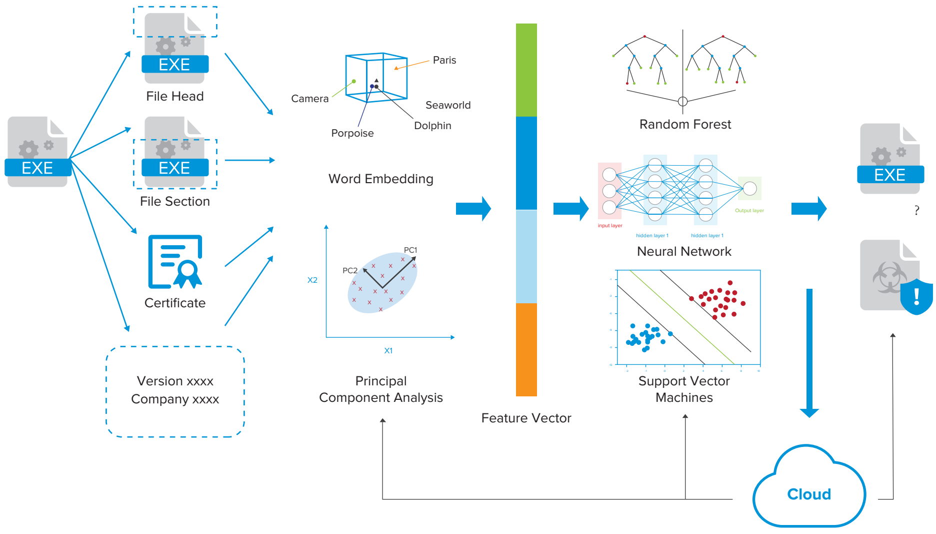
Intelligence Sources

- Over 20,000 connected network gateways provide IOC that includes malicious URL, IP, domain names and malware hashes with the number of participating gateways doubling every year.
- Third party threat intelligence feed.
- Sangfor security R&D into both white hat and black hat communities.

Real Case Scenario

If Sangfor NGAF detects an unusual outbound connection on 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 C&C server, it' s likely the server has been compromised. NGAF can be programmed to block these C&C communications so no further damage can be caused and to also send alerts to firewall operators for further investigation and processing.

AI Powered Detection Engine



AI Detection Engine

Engine Zero VS Traditional Detection Technologies

Traditional detection technologies mainly include MD5, virus signatures, rule matching, virtual execution and sandbox. In theory, their detection ability becomes stronger from MD5 to sandbox, with the performance decreasing and cost increasing. Compared to these traditional technologies, Engine Zero has the following advantages:

- Strong generalization ability to detect unknown viruses or new variants. Thanks to the generalization ability of machine learning, Engine Zero can identify unknown viruses or new variants of known viruses without having to see samples. However, traditional solutions need to get samples first, which can cause lag. A detailed explanation of this can be found in Section 2.2.1.

- Fast speed. Near-linear scan speed close to MD5.

- 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.

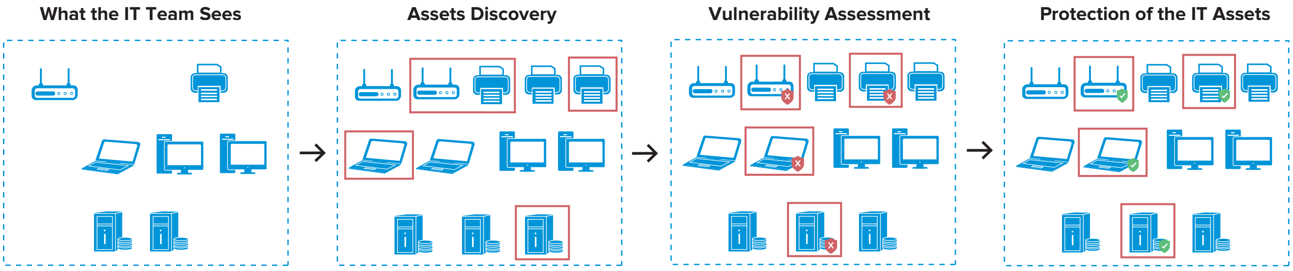
- High degree of automation. Engine Zero's model can automatically learn and extract features without human intervention. The model evolves in the cloud, with the detection ability and automation degree improved. However, traditional detection technologies require virus experts to manually extract virus fingerprints and signatures, which is not only costly but also lagged. It may cause the virus to appear for a long time since the traditional anti-virus vendors can update the virus database.

The insufficient traditional detection solutions also have unique value. For example, they can response to the black-and-white list mechanism more quickly. Therefore, the design of Engine Zero will also adopt some traditional technologies to form a malicious file detection solution based on AI and traditional technologies.

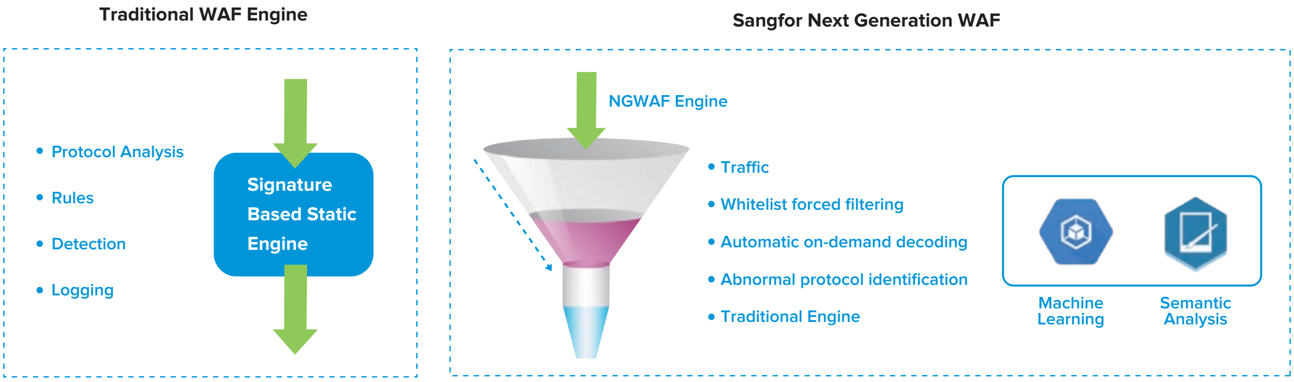
$ Protection of Business Assets

Sangfor NGAF is good at discovering and protecting business assets. Sangfor NGAF can automatically discover your organization' IT assets, discover the system vulnerabilities in real-time, and continuously protect the IT assets.

Moreover, with its proactive protection, Sangfor NGAF is capable of applying virtual patching, identify weak passwords, and hidden applications in all IT assets.



With its Next Generation WAF engine, which use learning and semantic analysis, will help to protect against the most common attacks such as webshell, struts2 injection, and deserialization flaws. It can also learn to analyze the attacks and the attack behaviors. It' ll enhance the detection rate and decrease the false positive of the traditional SNORT based detection engine. With the modeling of the attack behaviors, the threat model will be created for customers to easy manage the application system threats.


Traditional WAF Engine
Protocol Analysis
Rules
Detection
Logging
Signature Based Static Engine
Sangfor Next Generation WAF
NGWAF Engine
Traffic
Whitelist forced filtering
Automatic on-demand decoding
Abnormal protocol identification
Traditional Engine
Machine Learning
Semantic Analysis

- Unable to detect unknown threats and exploits
- Easy to bypass
- Common false positive SQL injection detection-Low-level performance

- Comprehensively surpasses sort rules to identify unknown threats and high-risk vulnerabilities
- Automatically learns by modeling normal business traffic, reducing false positives by 62.4%

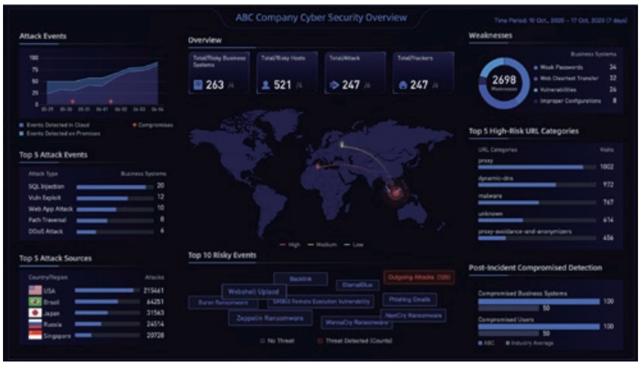
Simplified Security Operation

Even small or mid-sized organization without a specialized IT security team often receive thousands of alerts per week, requiring the IT department to dedicate man-hours to investigation and analysis, and increasing operational costs. The IT nightmare is just beginning, as they are now responsible for limiting downtime, identifying the root cause and taking action to mitigate damages and prevent future attack from the same source. Those organizations 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.

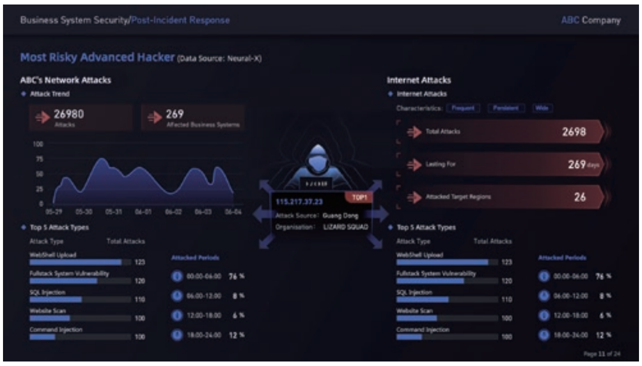
Sangfor NGAF provides reliable and effortless security with easy deployment and simplified operation and maintenance features, enabling an effective and safe IT environment. The NGAF Configuration Wizard streamlines security policy deployment while integrated intuitive reporting tools provide end-to-end visibility of the overall security of an organization from business systems to endpoints.

Sangfor NGAF simplifies daily security operations by helping to identify real and risky security events among thousands of alerts and providing guidance and suggestions for the best solution.

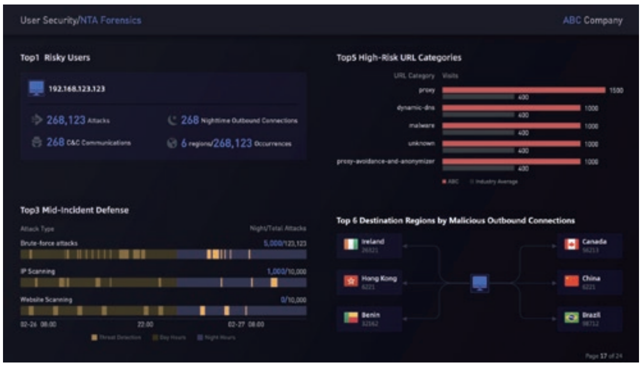
These expansive visibility components allow the IT department and business owners to execute proactive checks of their system online or offline, thus providing a secure environment for all business systems.



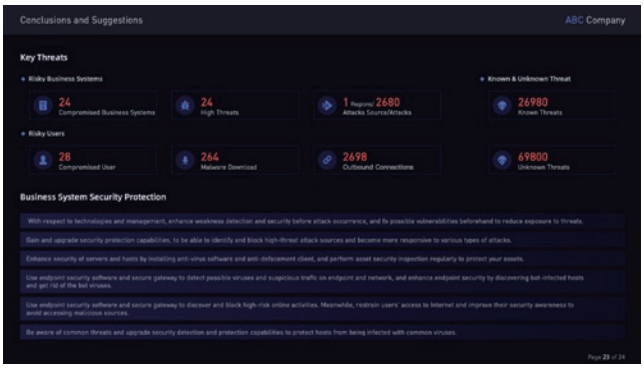
Executive Report for the Management Team



Simplified Daily Operation



User Security Overview



Conclusion and Suggestions

Security Visibility

Security is growing increasingly complex with malicious traffic intermingling with legitimate traffic and authorized users both at risk of attack and (knowingly or unknowingly) a potential risk to the network. Sangfor believes that visibility of the entire network is the foundation of solid network management. Administrators need to clearly see and understand all risks to information assets and track users and behaviours in order to recognize security threats and eliminate them in a timely manner.

Data and statistics on past and current threats is vital, but there is also a need for further analysis of the correlation between users, behaviours and business systems. By evolving security into a 360° view of the network, users can gain a better understanding of where the attack originated, the attack process, repair any damage and proactively defend against further attacks.

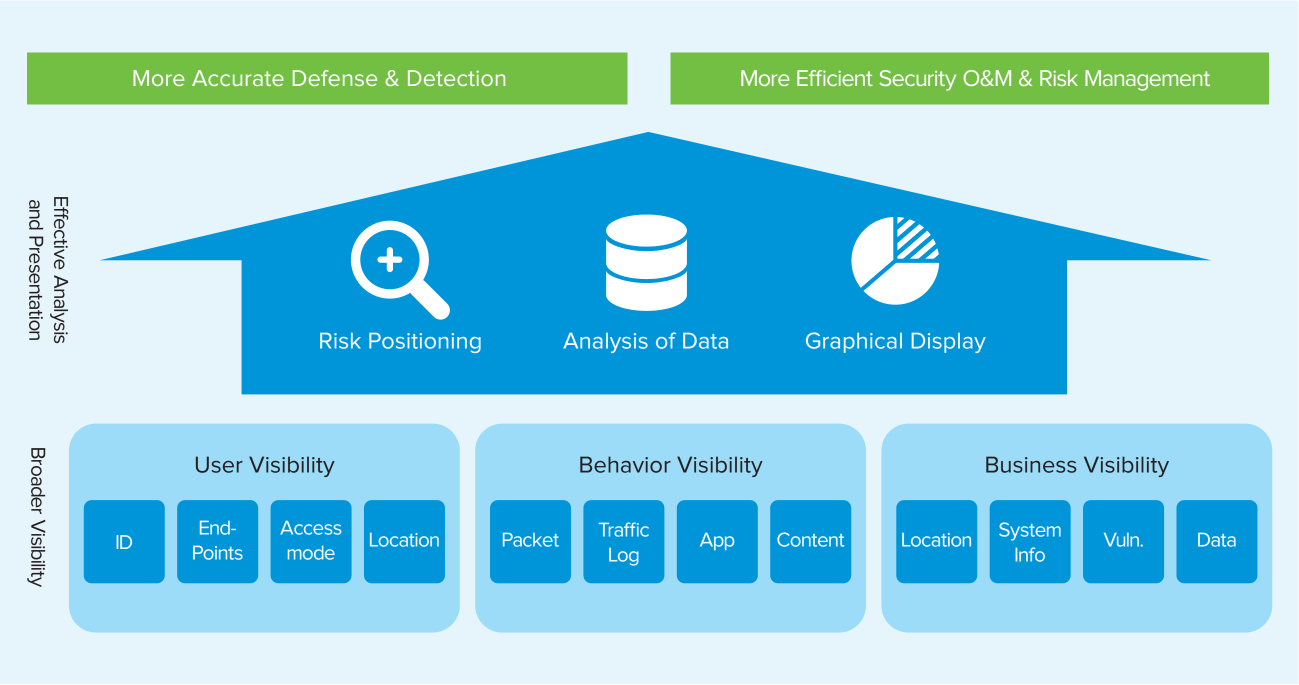
Sangfor NGAF Reporting Tools give our customers an extensive overview of their network with just a few clicks. Information like online user identity, server or abnormal traffic and attack status and source are just a few of the visibility resources provided.

Effective Analysis & Presentation: Risk Positioning | Analysis of Data | Graphical Display.

Broader Visibility: User | Behaviour | Business | Threats | Risks | Security Events.

Neural-X is at the core of NGAF intelligent threat detection and defence. Neural-X uses deep learning and in-depth analysis of vector association to detect domain names used by malware of similar families. The deep learning function is designed to operate and learn independently – thus maintaining a proactive, innovative and highly visible approach to malware detection, identification and elimination.

Intelligence is the key to visibility and Sangfor NGAF and Neural-X aim to provide a wholistic view of the network with comprehensive visibility from endpoints to business systems.



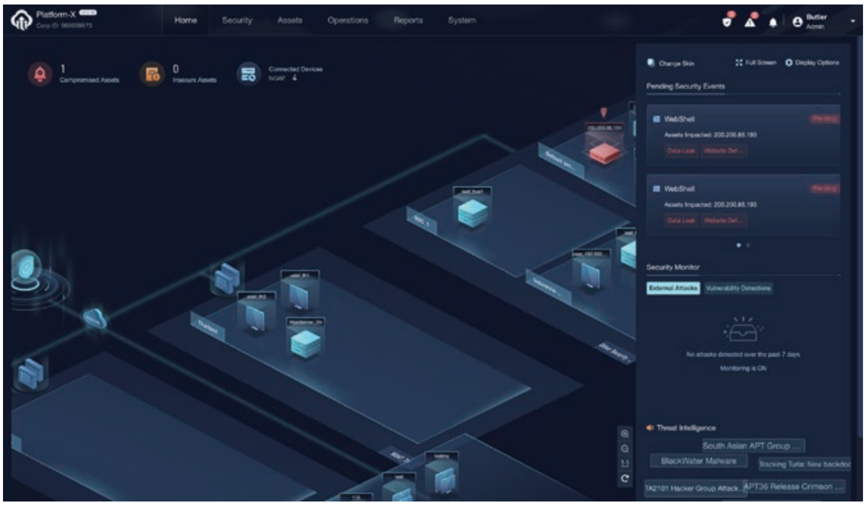
Sangfor Platform-X

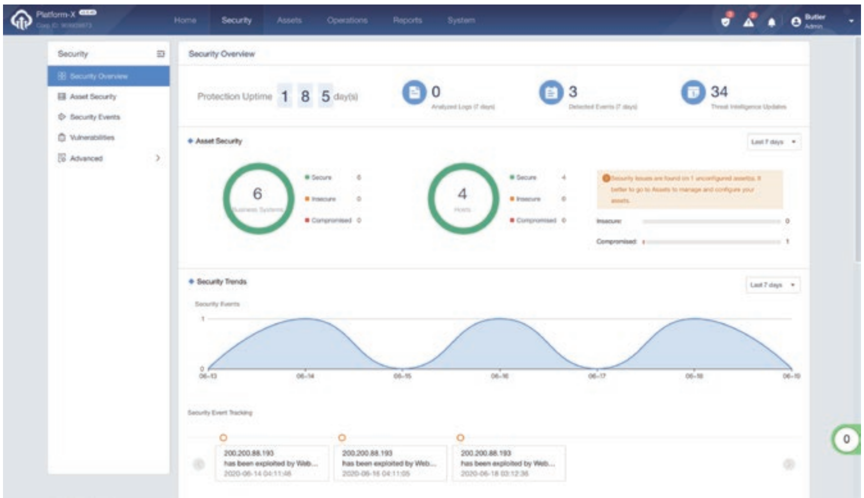
Sangfor Platform-X is a cloud-based security management platform, equipped to manage all Sangfor security products in the cloud by collecting, analyzing and displaying all security logs. Through integration with Sangfor's cloud-based security solution, Neural-X, Platform-X enables comprehensive security and detection by alerting administrators to attacks or threats in real-time, thus vastly simplifying security operations.

Visible Centralized Security
Platform-X unifies security device log collection, provides analysis and displays results. In addition, it provides topology-based security incident monitoring, security status evaluation and reporting, correlated incident detection and processing between security devices.

Shared Threat Intelligence
Collaboration of in-depth big data analytics, security analysts and white-hat researchers, has equipped Platform-X to effectively identify advanced attacks and potential threatening behavior, and provide critical indicators for investigation and threat identification.

Unified Device Management
Platform-X provides unified hardware status monitoring, firmware upgrade, policy synchronization, and remote login without password.





SANGFOR NGAF Product Family

Model	AF-1000-B1080*	AF-1000-B1120*	M4500-F-I	M5100-F-I	M5150-F-I	M5200-F-I	M5250-F-I	M5300-F-I	M5400-F-I
Profile	Desktop	1U	Desktop	1U	1U	1U	1U	1U	1U
RAM	2G	2G	4G	4G	4G	4G	4G	8G	8G
HD Capacity	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64 GB	SSD 128 GB
Firewall Throughput[1]	1.05 Gbps	1.75 Gbps	2 Gbps	2.8 Gbps	3.5 Gbps	4.9 Gbps	5.5 Gbps	12 Gbps	20 Gbps
NGFW Throughput[2]	800 Mbps	1 Gbps	1.4 Gbps	2.5 Gbps	2.5 Gbps	2.8 Gbps	2.8 Gbps	5 Gbps	8.4 Gbps
IPS + WAF Throughput (HTTP)	N/A	700 Mbps	1.2 Gbps	1.4 Gbps	1.4 Gbps	2.1 Gbps	2.1 Gbps	3.85 Gbps	5.6 Gbps
Threat Protection[3] Throughput	600 Mbps	800 Mbps	1 Gbps	1.8 Gbps	1.8 Gbps	2.1 Gbps	2.1 Gbps	4.2 Gbps	5.6 Gbps
IPsec VPN Throughput	100 Mbps	100 Mbps	250 Mbps	250 Mbps	250 Mbps	375 Mbps	375 Mbps	1 Gbps	1.25 Gbps
Max IPsec VPN Tunnels	100	100	300	300	300	500	500	1000	1500
Concurrent Connections (TCP)	800,000	800,000	250,000	750,000	1,000,000	1,200,000	1,800,000	2,000,000	2,500,000
New Connections (TCP)	15,000	18,000	10,000	20,000	25,000	30,000	50,000	80,000	110,000

[1] 1518 Bytes UDP Packets.
[2] NGFW is measured with Firewall, Bandwidth Management, IPS, Application Control.
[3] Threat Prevention is measured with Firewall, Bandwidth Management IPS, Application Control, Anti Virus.

Power and Hardware Specifications

Model	AF-1000-B1080*	AF-1000-B1120*	M4500-F-I	M5100-F-I	M5150-F-I	M5200-F-I	M5250-F-I	M5300-F-I	M5400-F-I
Support Dual Power Supplies	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Power [Watt] (Max)	60W	40W	60W	60W	40W	40W	40W	60W	150W
Temperature	0~45°C								
System Weight	1.5Kg	3.85Kg	2.0Kg	3.85Kg	3.85Kg	3.85Kg	4.24Kg	4.5Kg	6.1Kg
System Dimensions (mm^3)	175 x 275 x 45	300 x 430 x 45	175 x 275 x 45	300 x 430 x 45	300 x 430 x 45	300 x 430 x 45	300 x 430 x 45	300 x 430 x 45	400 x 430 x 45
Relative Humidity	5%~95% non-condensing								
Compliance & Certificates	CE, FCC								

Network Interfaces

Model	AF-1000-B1080*	AF-1000-B1120*	M4500-F-I	M5100-F-I	M5150-F-I	M5200-F-I	M5250-F-I	M5300-F-I	M5400-F-I
Bypass (Copper)	N/A	1 pair	N/A	1 pair	1 pair	1 pair	2 pairs	1 pair	3 pairs
10/100/1000 Base-T	3	6	4	4	6	6	6	6	6
1G Fiber SFP	N/A	N/A	N/A	N/A	N/A	N/A	2	2	N/A
10G Fiber SFP+	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2
Serial Port	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1
USB Port	2	2	2	2	2	2	2	2	2
Network Modules	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	2

1. “Optional Interface & 10G Fiber SFP” allows upgrading interfaces according to your requirement.
2. M5100-F-I are available with 6 interfaces platforms with corresponding cost.
3. All performance values are “up to” and vary depending on the system configuration.

*Only available for specific regions. Please contact us for more information.

4. 1 x network module can be customized to add one more NIC: 4x GE RJ45 | 4x GE SFP | 8x GE RJ45 | 8x GE SFP | 4x GE RJ45 & 4x GE SFP | 2x 10GE SFP+.

SANGFOR NGAF Product Family

Model	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I	AF-2000-B3100*	AF-2000-B3200*	AF-2000-B3300*
Profile	2U	2U	2U	2U	2U	2U	2U	2U
RAM	8G	16G	16G	24G	32G	96G	128G	192G
HD Capacity	1T + 64G MSATA	1T + 64G MSATA	1T + 64G MSATA	1 TB +4G CF	1 TB +4G CF	1T+SSD 64GB	1T+SSD 64GB	1T+SSD 64GB
Firewall Throughput[1]	25 Gbps	50 Gbps	67 Gbps	105 Gbps	140 Gbps	140 Gbps	180 Gbps	240 Gbps
NGFW Throughput[2]	12.6 Gbps	23 Gbps	31 Gbps	56 Gbps	84 Gbps	90 Gbps	120 Gbps	140 Gbps
IPS + WAF Throughput (HTTP)	8.4 Gbps	14 Gbps	21 Gbps	42 Gbps	56 Gbps	63 Gbps	84 Gbps	126 Gbps
Threat Protection[3] Throughput	9.1 Gbps	18 Gbps	26.5 Gbps	50.4 Gbps	67.2 Gbps	79.4 Gbps	91.2 Gbps	105 Gbps
IPsec VPN Throughput	2 Gbps	3 Gbps	3.75 Gbps	5 Gbps	5 Gbps	7 Gbps	10 Gbps	15 Gbps
Max IPsec VPN Tunnels	3,000	4,000	5,000	10,000	10,000	15,000	20,000	30,000
Concurrent Connections (TCP)	3,000,000	4,000,000	8,000,000	12,000,000	16,000,000	20,000,000	32,000,000	35,000,000
New Connections (TCP)	220,000	300,000	330,000	450,000	600,000	650,000	800,000	900,000

[1] 1518 Bytes UDP Packets.
[2] NGFW is measured with Firewall, Bandwidth Management, IPS, Application Control.
[3] Threat Prevention is measured with Firewall, Bandwidth Management IPS, Application Control, Anti Virus.

Power and Hardware Specifications

Model	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I	AF-2000-B3100*	AF-2000-B3200*	AF-2000-B3300*
Support Dual Power Supplies	√	√	√	√	√	√	√	√
Power [Watt] (Max)	150W	150W	150W	500W	500W	860W	860W	860W
Temperature	0~45°C							
System Weight	12.95Kg	12.95Kg	12.95Kg	20.0Kg	20.0Kg	24Kg	24Kg	24Kg
System Dimensions (mm^3)	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90
Relative Humidity	5%~95% non-condensing							
Compliance & Certificates	CE, FCC							

Network Interfaces

Model	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I	AF-2000-B3100*	AF-2000-B3200*	AF-2000-B3300*
Bypass (Copper)	3 pairs	3 pairs	3 pairs	2 pairs	4 pairs	2 pairs	2 pairs	4 pairs
10/100/1000 Base-T	6	6	10	4	8	4	4	8
1G Fiber SFP	4	4	4	4	8	4	8	8
10G Fiber SFP+	2	2	2	2	4	8	8	8
Serial Port	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1
USB Port	2	2	1	2	2	2	2	2
Network Modules	1	1	1	5	4	2	2	2

1. M5100-F-I are available with 6 interfaces platforms with corresponding cost.
2. All performance values are "up to" and vary depending on the system configuration.

*Only available for specific regions. Please contact us for more information.

3. 1 x network module can be customized to add one more NIC: 4x GE RJ45 | 4x GE SFP | 8x GE RJ45 | 8x GE SFP | 4x GE RJ45 & 4x GE SFP | 2x 10GE SFP+.

vNGAF
SANGFOR Virtual NGAF (HCI PLATFORM)

Model	vAF100	vAF200	vAF400	vAF800	vAF1600
NGFW / WAF Throughput	200 Mbps	400 Mbps	800 Mbps	1600 Mbps	3200 Mbps
Concurrent Connection (TCP)	500,000	1,000,000	2,000,000	4,000,000	4,000,000
New Connections (TCP)	10,000	20,000	50,000	80,000	80,000

System Requirements

System Requirements	vAF100	vAF200	vAF400
Virtualization Platform	SANGFOR HCI	SANGFOR HCI	SANGFOR HCI
CPU	Min. 1-Core Processor	Min. 2-Core Processor	Min. 4-Core Processor
Memory	2GB	4GB	8GB
Disk Space	32GB	32GB	32GB

System Requirements	vAF800	vAF1600
Virtualization Platform	SANGFOR HCI	SANGFOR HCI
CPU	Min. 8-Core Processor	Min. 8-Core Processor
Memory	16GB	16GB
Disk Space	32GB	32GB

SANGFOR NGAF Product Features

Firewall

- Networking
  - Policy routing, static routing, RIP v1/2, OSPF, BGP, and GRE.
  - Application policy-based forwarding, NAT (1-1 NAT, many-to-one NAT, NAT46, NAT64, and many-to-few NAT), VLAN tagging
  - IPv6 & IPv4 supported
  - Support multi cast traffic, SNMP v3, and Syslog server with UTF-8 format
  - Intelligent Dos/ DDos prevention
  - ARP spoofing prevention
  - HA fail-over time less than 1 second
  - Support at least 10000 security policies
  - Policies basis with “first come first match”
  - Provide management via SSH, HTTPS, CLI, and Web-based GUI
- SSL VPN
- IPsec VPN
  - IPSec Protocol: AH, ESP
  - D-H Group: MODP768 Group(1), MODP1024 Group(2), MODP1536 Group(5)
  - IPSec Authentication Algorithm: MD5, SHA-1. SHA-2
  - IPSec Encryption Algorithm: DES, 3DES, AES-192, AES-256. SANGFOR_DES
  - Auto VPN, support creating and manage VPN connection from Central Management Console Support SDWAN path selection policy
- SD-WAN
  - Intelligent Routing: Specific application routing, support routing based on remaining bandwidth, and best quality routing based on QOE detection
  - Dynamic Routing: RIP, OSPF, BGP
  - Tunnel Failover: Supports failure second-level switchover
  - Easy to deploy with step by step email instructions
  - Visualization of equipment operating status and geographic location distribution
  - Visualization of VPN link status and delay
  - Configuration batch management-support
  - Support for GRE
  - Support access to the centralized management platform (Central Manager), for unification management of branch appliances
  - Support for SD-WAN networking solution, rapid deployment of VPN through Sangfor Central Manager
  - Support for IPv6 services to meet the needs of user networks with IPv6 requirements

Threats Prevention

- Full SSL inspection
  - SSL inspection to all security modules including IPS, WAF, ATP, Access control, etc.
- Cross-module intelligent correction
  - Policy association of IPS, WAF and APT prevention modules.
  - Cross-module visibility reporting analysis
- Threats prevention
  - APT (Advanced Persistent Threat), Remote Access Trojan, Botnet, malware detection
  - Cloud-based Sandbox threats analysis
  - AI based malware detection engine, covering threats type of Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, Hacktool, Virus, etc.
  - Use cloud intelligence to prevent unknown and advanced threat.
- Anti-virus
  - Scan and kill viruses infecting HTTP, FTP, SMTP and POP3 traffic as well as viruses infecting compressed data packets
  - Support remove virus from detected malicious files
- Email security
  - Categorize and filter various forms of malicious emails.
  - Support detection deep into email body and attachments.
  - Support place warning messages into email title to avoid users from opening malicious emails

IPS

- IPS signature database
  - Prevention against vulnerability exploits towards various system, application, middleware, database, explorer, telnet, DNS, etc.
  - Employ cloud-based analysis engine
  - Allow custom IPS rules
  - Database update once a week
- Certificate and partnership
  - Common Vulnerabilities and Exposures (CVE) compatibility certificated
  - Microsoft Active Protections Program (MAPP) partnership

Risk Assessment and Security Service

- Risk assessment
  - Scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc.
- Web scanner
  - On-demand scanning of targeted website/URL to discover the system vulnerabilities.
- Real-time vulnerability scanner
  - Discover vulnerabilities in real-time and protection against 0-days attacks
- SANGFOR threat intelligence service
  - Threat intelligence to deliver the latest vulnerabilities, malware and security incidents information with advisory alerts for policy creation

Web Application Firewall

- Web-based attack prevention
  - Support SNORT based and semantic detection engine to
  - Defend against the 10 top major web-based attacks identified by the Open Web Application Security Project (OWASP)
  - Web-based attack rules database
  - Support custom WAF rules
- Parameters protection
  - Proactive protection of automatic parameter learning
- Application hiding
  - Hide the sensitive application information to prevent hackers from mounting targeted attacks with the feedback information from the applications
- Password protection
  - Weak password detection and brute-force attack prevention
- Privilege control
  - File upload restriction of file type blacklist
  - Specify access privilege of sensitive URL such as the admin page for risk prevention
- Buffer overflow detection
  - Defend against buffer overflow attacks
- Detection of HTTP anomalies
  - Analyze anomalies of the fields of the HTTP protocol via single parsing
- Secondary authentication for server access
  - Server access verification by IP address restriction and mail authentication

Data Leakage Prevention

- Data leakage detection and prevention
  - Control and detection over multiple types of sensitive information (customizable)including user information, email account information, MD5 encrypted passwords, bank card numbers, identity card numbers, social insurance accounts, credit card numbers, and mobile phone numbers
- File downloading control
  - Restrict suspicious file downloading

User Access Management

- User identity:
  - Mapping by IP, MAC, IP/MAC binding, hostname and USB-Key. User account import from CSV file and LDAP Server.
  - SSO integration with AD domain, proxy, POP3 and WEB
- Internet content classification
  - Cloud-based URL/APP classification engine
- Access control
  - Policy configuration oriented toward users and applications for web filter, application control and bandwidth management

Visibility Reporting

- Built-in report center
  - Full visibility to network, endpoint and business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats and behaviours
  - Threats analysis for specific attack by Description, Target, Solution
  - Support visualization into cyber kill chain
  - Business Systems based reporting
- Report subscription
  - Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis

Deployment

- Configuration Wizard
  - Guideline for deployment and policy configuration
- Deployment
  - Gateway (Route mode) | Bridge mode | Bypass mode | Multiple Bridge mode (2- 4 bridges) | Virtual Wire
- High Availability
  - Active-Active | Active-Passive
- Bypass
  - Hardware bypass in the event of hardware failure
- Central Management
  - Support central management of multiple NGAFs
  - Support quick deployment from Central Management Console

COMPANY PROFILE

Sangfor Technologies is a leading global vendor of IT infrastructure solutions, specializing in Cloud Computing & Network Security with a wide range of products & services including: Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Firewall, Internet Access Management, Endpoint Protection, Ransomware Protection, Managed Detection and Response, WAN Optimization, SD-WAN and many others.

Sangfor takes customers' business needs and user experience seriously, placing them at the heart of our corporate strategy. Constant innovation and commitment to creating value for our customers helps them achieve sustainable growth. Established in 2000, Sangfor currently has 5,000 + employees with more than 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy and the USA.

CONTINUOUS INNOVATION & EXCELLENT SERVICE

Sangfor invests at least 20% of its yearly revenue in R&D, improving current products and developing new solutions in their four R&D centers in the USA & China. So far, Sangfor has applied for more than 1,000 patents with more patent applications scheduled for 2020. This dedication to innovation enables Sangfor to release new and updated versions of products every quarter and launch new products yearly or bi-yearly.

Sangfor also emphasizes excellent service. With three Customer Service Centers in Malaysia & China, Sangfor's total customer service capacity exceeds 250 technicians and providers.

With thousands of certified engineers and 24x7 online support 365 days a year, Sangfor customers enjoy fast and personalized on-site service support.

At present, Sangfor has more than 100,000 customers worldwide, many of them Fortune 500 companies, governmental institutions, universities and schools.

AWARDS & ACHIEVEMENTS

- "Technology Fast 500 Asia Pacific Region" Award for 8 consecutive years from 2005 to 2012 by Deloitte
- Sangfor SSL VPN No. 1 in Network Security market in China, Hong Kong & Taiwan according to F&S
- No. 1 for Secure Content Management Hardware and VPN Hardware segment in China according to IDC
- Sangfor NGAF WAF recommended by NSS labs (2014)
- "Most Promising Network Security Solution" in June 2016 by Singapore NetworkWorld Asia
- "Readers Choice Awards for Enterprise Security" in October 2016 by Computerworld Malaysia
- Member of various technology alliances including VirusTotal
- "Next Gen" Award for Sangfor Endpoint Secure by Cyber Defense Magazine (2019)
- SAP Certified for Cloud and Infrastructure Operations and SAP HANA Operations (2019)
- ICSA Labs certification for Sangfor Next Generation Firewall (2020)

Gartner Magic Quadrant

SSL VPN	SWG	WOC
2010-2011	2011-2019	2013-2016
NGFW	**X86 Server**	**HCI**
2015-2019	2016	2019

SANGFOR NGAF - NEXT GENERATION FIREWALL

SANGFOR INTERNATIONAL OFFICES

SANGFOR SINGAPORE
8 Burn Road # 04-09, Trivex,
Singapore (369977)
Tel: (+65) 6276 9133

SANGFOR HONG KONG (CHINA)
Unit 04, 6/F, Greenfield Tower, Concordia Plaza, No.1 Science
Museum Road, Tsim Sha Tsui East, Kowloon, Hong Kong
Tel: (+852) 3427 9160

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

SANGFOR MALAYSIA
No. 47-10 The Boulevard Offices, Mid Valley City, Lingkaran
Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3 2201 0192

SANGFOR THAILAND
6th Floor, 518/5 Maneeya Center Building, Ploenchit Road,
Lumpini, Patumwan, Bangkok, 10330 Thailand
Tel: (+66) 22517700

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati,
122 Metro, Manila, Philippines.
Tel: +63(0) 9175081244 / +63(0) 9171179346

SANGFOR VIETNAM
OTX2-0327 Sunrise City, 27 Nguyen Huu Tho,
Tan Hung Ward, Dist. 7, HCMC, Vietnam.
Tel: (+84) 28 62700133

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
C-80 (C-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE
Tel: +971-52-9606471

SANGFOR PAKISTAN
D203, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: +92 3142288929

SANGFOR ITALY
Sede Legale ed Operativa via E. Berlinguer, 9 20834 Nova
Milanese MB Italia
Tel: +393400616767

SANGFOR USA
46721 Fremont Blvd, Fremont, CA 94538, USA
Tel: +1 (510) 573-0715

AVAILABLE SOLUTIONS

IAM	Simplify User & Network Management
NGAF	Smarter Security Powered By AI
Endpoint Secure	The Future of Endpoint Security
Cyber Command	Powerful Intelligent Threat and Detection Platform
SD-WAN	Boost Your Branch Business With Sangfor
WANO	Enjoy a LAN Speed on your WAN
HCI	Driving Hyperconvergence to Fully Converged
aCLOUD	Enterprise Cloud Built on HCI
VDI	Ultimate User Experience that Beats PC
aBOS	The World First NFV Converged Gateway
CM	Centralized Management Platform

SANGFOR

www.sangfor.com

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

Our Social Networks :

https://twitter.com/SANGFOR

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

https://www.facebook.com/Sangfor

https://plus.google.com/+SangforTechnologies

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

NGAF_BR_P_NGAF-Brochure_20201013