SANGFOR

SANGFOR NETWORK SECURE

Security Subscription Bundles

Continuously evolving cyber threats drive the evolution of security products and the creation of new security infrastructure, as threats can increasingly evade traditional defenses. Malicious software, having bypassed the defense perimeter, can fully exploit a flat internal network to cause severe infections, data theft, or even advanced persistent threats (APT).

Sangfor Network Secure (previously known as Sangfor NGAF) is a converged security solution that protects against APT attacks, malware, ransomware, IoT threats, and web-based attacks. Network Secure is available in various Security Subscription Bundles to provide both small and large enterprises with the most comprehensive and professional security protection!

Essential Bundle Primarily suits SMB customers and small branch sites. The Essential Bundle includes Stateful Firewall, IPS, and Application/URL Control modules. Sangfor Network Secure employs Deep Packet Inspection (DPI) and attack behavior analysis technologies to go beyond traditional firewalls to prevent application layer attacks. The SOC Lite module and security reporting tools help IT professionals identify business risks and take immediate action to mitigate damage.

Premium Bundle Primarily suits enterprise customers who require advanced attack prevention. To mitigate business risk from cyber threats, Sangfor Network Secure brings intelligent protection to the perimeter firewall, including Sangfor Engine Zero and Sangfor Neural-X, providing AI-powered malware detection and real-time Threat Intelligence (TI) feeds to augment threat detection. The Premium Bundle is designed for total threat protection capability against advanced and unknown threats.

Ultimate Bundle Primarily suits customers who require both Network and endpoint protection. By integrating Sangfor Network Secure and Endpoint Secure, you can realize one-stop threat discovery, analysis, mitigation, and the complete eradication of threats. Additionally, the Ultimate Bundle provides device monitoring and remote control via a centralized console, greatly simplifying device management.

Bundle Type	Essential Bundle	Premium Bundle	Ultimate Bundle
Stateful Firewall	Yes	Yes	Yes
Granular Application Control	Yes	Yes	Yes
URL Content Filtering	Yes	Yes	Yes
Intrusion Prevention System (IPS)	Yes	Yes	Yes
Botnet Prevention & Advanced Threat Prevention	Yes	Yes	Yes
Security Log & Reporting	Yes	Yes	Yes
SOC Lite	Yes	Yes	Yes
Sangfor Endpoint Secure Integration	Yes	Yes	Yes
Engine Zero: AI-powered Malware Inspection Engine	/	Yes	Yes
Neural-X: Cloud Threat Intelligence	/	Yes	Yes
Sangfor Endpoint Secure Agent × 30	/	/	Yes
Sangfor Endpoint Secure Manager (One per Customer)	/	/	Yes
Centralized Device Monitoring & Remote Control [1]	/	/	Yes
Web Application Firewall (WAF)	Optional	Optional	Optional
IoT Security	Optional	Optional	Optional

[1] Centralized Device Monitoring & Remote Control: include device online/offline status monitoring, CPU/Memory/Disk/Bandwidth usage monitoring, remote access web console & control.

SANGFOR

Sangfor Network Secure Highlighted Features Overview

Granular Application Control

Sangfor's continuous optimization and improvement give customers the most comprehensive application classification and identification database. Sangfor Network Secure provides granular control for applications like Microsoft Office 365, Facebook, and YouTube. Moreover, Sangfor keeps improving its capabilities to identify and control popular regional applications to provide the best user experience in regions like APAC and EMEA.

Engine Zero: AI-powered Malware Inspection Engine

Sangfor Engine Zero is a malware detection engine built upon powerful Artificial Intelligence (AI) technology. Engine Zero works right out of the box, eliminating both known and unknown malware without relying on traditional signatures while consuming little resources.

Neural-X: Cloud Threat Intelligence

Neural-X is a cloud threat intelligence (TI) platform that comprises various interconnected components, including threat intelligence, deep learning, sandboxing, file reputation, and botnet detection. These components work seamlessly together to enhance Network Secure's threat detection and response capabilities. Total awareness, identification, and protection make Sangfor Neural-X the most powerful and comprehensive TI solution available.

SOC Lite

Due to the lack of dedicated security experts, many small and medium-sized businesses often overlook proper security operations. This oversight can result in delayed responses to security issues, leaving potential risks and human errors unaddressed. Sangfor Network Secure is equipped with SOC Lite capability to simplify security operations.

Through automated analysis of security logs, SOC Lite provides a clear visualization of security issues and offers actionable recommendations for resolution. The policy optimizer also examines existing access control policies, identifying issues and vulnerabilities while suggesting modifications. With SOC Lite, users can proactively address security concerns and optimize their security posture quickly and efficiently.

Web Application Firewall (WAF)

Sangfor Network Secure is the world's first NGFW integrated with a dedicated Next-Generation Web Application Firewall (NGWAF). This allows it 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 compared to traditional signature detection engines.

Threat models of attack behaviors are established to facilitate the streamlined management of application-related security threats. Moreover, a passive vulnerability analysis reporting tool is built to provide a comprehensive web server vulnerability status with remediation recommendations to help the administrator harden the system.

Sangfor Endpoint Secure Integration

Sangfor Network Secure can seamlessly integrate with Sangfor Endpoint Secure. Via this integration, Network Secure and Endpoint Secure logs are correlated to locate the malicious processes related to advanced persistent threats (APTs). Administrators can see the forensic data on Network Secure and correlate it with the Endpoint Secure agent to quarantine the malicious processes in one click.

Security Log & Reporting

Sangfor Network Secure supports local security log retention and generates security reports. This feature facilitates daily security operations, troubleshooting, and compliance without relying on additional third-party log servers.

IoT Security

IoT devices are becoming one of the most significant sources of cyber-attacks. The common security issues relating to IoT devices include management complexity, lack of vulnerability fixes, and no dedicated protection. Sangfor Network Secure is equipped with IoT Security capability, which identifies the IoT devices in the network, deploys dedicated controls, and keeps log of the IoT devices' activities.