SANGFOR

Sangfor Ransomware Solution Sales Guide

The most complete solution for ransomware protection

Sangfor Ransomware Incident Response Solution Key Features & Values

Pre-Attack Prevention

• Border protection prevents viruses from invading from outside, closes risky transmission ports, updates protection rules, and interrupts transmission.

• Endpoint protection prevents viruses from invading endpoints, and improves security baselines for endpoint port openings, weak passwords, and vulnerabilities.

Mid-Attack Detection

• After a virus invades, it scans horizontally and spreads. Continuous monitoring can detect intrusions the first time and stop losses quickly.

Post-Attack Response

• When a ransomware or malicious attack is discovered, it is necessary to isolate the lost host firstly to control the incident and avoid repeated infections; then, it is necessary to check and kill at a fixed point to remove the virus files.

• Sangfor IR service is also a unique value for ransomware solution compares with other vendors.

Sales Scenarios for Target Customers

Who Buys Sangfor Ransomware Solutions?

SME (50 – 300 employees)

Challenges

• Existing AV solutions are unable to keep pace with evolving threats like ransomware.

• NGFW & Endpoint Security often have separated policy management.

• Time consuming deployment of endpoint agents on each employee machine.

• As more business elements are deployed, there is no security baseline construction covering this new business. Various high-risk vulnerabilities continue to emerge, and security risks hide in the network.

• Lack of in-depth monitoring of network perimeter and endpoints. Lacking the ability to monitor and coordinate evidence, locate the real source of attacks, prevent the ransomware from moving laterally and develop into a serious security incident.

• Fragmented data reports. Side network equipment collects data from network traffic and endpoint software, meaning fragmented data can't be collaboratively analyzed.

Solutions: NGAF + Endpoint Secure + Platform-X + HCI

- Built-in ransomware honeypot with Endpoint Secure.
- Integrate Endpoint Secure with NGAF to provide single pane of glass management tosimplify network & endpoint security operations.
- One-click agent deployment saves 40% on project life cycle.

Enterprise (> 300 employees)

Challenges

- Difficulty managing business assets (many servers)
- It is difficult to configure an overly complex security system strategy
- Difficulty visualizing traffic between business assets
- Difficulty with immediate response to threat or attack
- Overlapping policy exposes critical assets to risk
- Lengthy threat location processing

Solutions: NGAF + Endpoint Secure + Cyber Command + HCI

- NGAF integrated asset management provides traffic visibility between business assets & network zones.
- Real-time network traffic analytics look into high risk applications & ports.
- Reduce attack surface by providing recommendations on associated firewall policy.
- Use Cyber Command to easily manage & monitor all Sangfor security products and ransomware protections and provide security orchestration for over 300 third-party security and networking products.

Competition Analysis

Sophos Ransomware Solution Advantages

01

- Intercept X provides advanced protection technology that stops ransomware at endpoints and servers at multiple stages of the attack chain.

02

- Sophos XG Firewall is packed with advanced protection to detect and block ransomware attacks and stop hackers moving laterally around your network to escalate privileges.

03

• Synchronized Security with Intercept X and XG Firewall are great on their own, but even better with Synchronized Security. If anything triggers either product, XG Firewall and Intercept X work together to automatically isolate the affected devices – preventing the threat from spreading further.

04

• Expert 24/7 Monitoring for organizations that don't have the expertise, resources, or desire to monitor their network 24/7. Managed Threat Response (MTR) service is a dedicated, round-the-clock team of threat hunters and response experts who constantly scan for, and act on, suspicious activity.

Sangfor Ransomware Solution Advantages

01

• **Network perimeter defense:** Sangfor NGAF builds a layer 2 - layer 7 complete defense system. NGAF provides various types of vulnerability detection and protection, risk port detection, malware filtering, botnet and DDOS attack detection, and provides comprehensive security protection for user network boundaries.

02

• **Endpoint protection:** Sangfor Endpoint Secure provides endpoint virus detection and killing, intrusion prevention, vulnerability management, rapid response and other protection functions. The Endpoint Secure platform integrates multiple new detection engines including genetic and sandbox detection and machine learning and prediction to achieve a high ransomware detection rate.

03

• **Security operation platform:** Sangfor Cyber Command adopts a big data analysis architecture, collecting network security traffic and other product security logs. It also combines artificial intelligence, machine learning, and UEBA analysis technology to centrally analyze and display the security situation of the entire network, and to assist users in locating security risks, security incidents and lost hosts.

04

• **Integrated response protection system:** In addition to collecting traffic logs of the entire network for centralized operation analysis, Sangfor Cyber Command can also intelligently integrate security devices like firewalls, behavior management, Endpoint Secure to block and isolate security incidents.

05

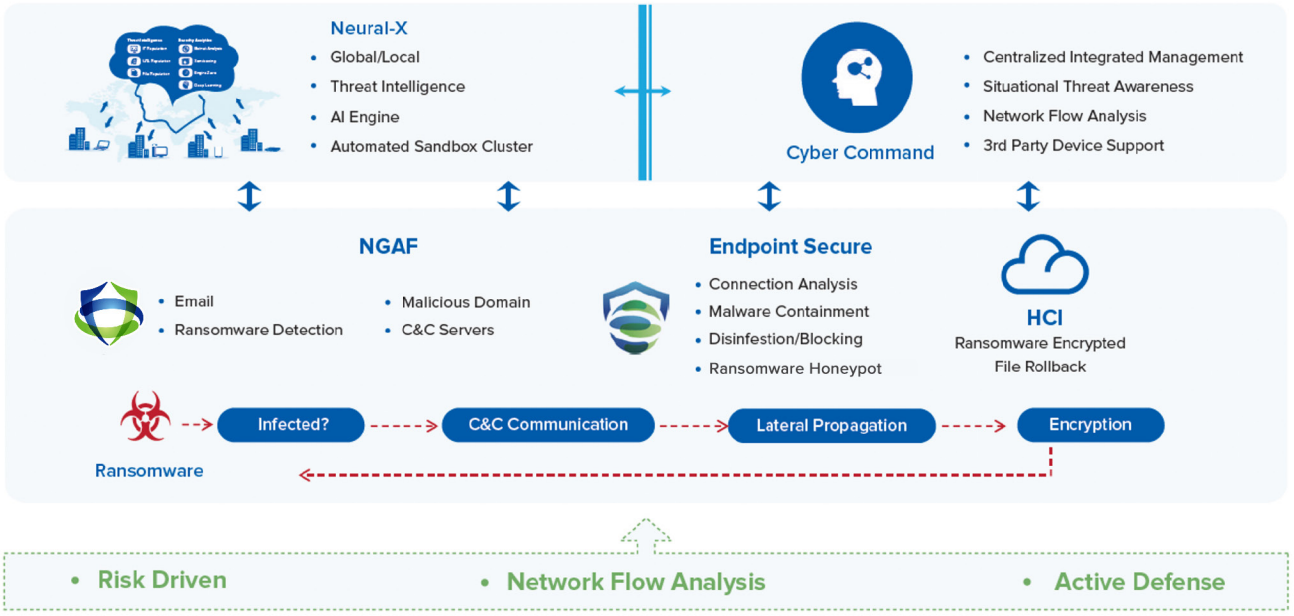
• Sangfor Endpoint Secure has specially developed targeted solutions for ransomware by inserting bait files into the victims' file directory, capturing ransomware encryption behavior. Once the bait files are encrypted, all file operations are ended immediately. Sangfor Endpoint Secure will locate any ransomware and kill them across the entire network. This is the last protective barrier for ransomware, ensuring that business system data will not be encrypted.

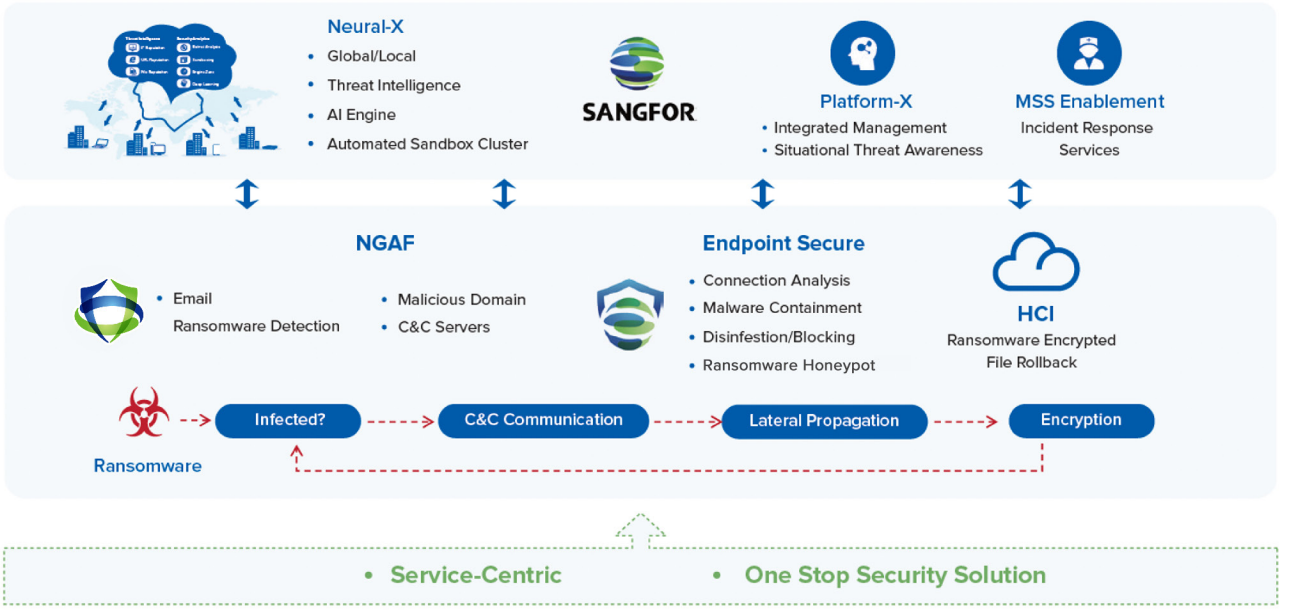
06

• Sangfor IR service provides incident response services including damage control, event analysis, malware family and type determination, kill chain determination, Indicator Of Compromise (IOC) identification, problem eradication and assistance in service recovery when an organization suffers malware, ransomware or crypto mining attacks, or Advanced Persistent Threat (APT). It helps users stop losses quickly, and minimize the impact of security incidents.

07

• Data backup and recovery mechanisms: Sangfor HCI built-in data backup mechanism can restore data to distributed storage EDS. Users no longer need to purchase backup software separately. Once assets are attacked by ransomware, the backup mechanism can recover data to any time node in the week before encryption, making it the best asset backup and restoration mechanism.





Sangfor Ransomware Solution vs Other Vendors

(Features Comparison)

Sophos Ransomware Solution	Sangfor Ransomware Solution
Managed Threat Response + Sophos Intercept X + Sophos XG Firewall	**SME Anti-Ransomware Solution:** ES + NGAF + Platform-X + HCI (optional) + Incident Response **Enterprise Anti-Ransomware Solution:** ES + NGAF + Cyber Command + HCI (optional) + Incident Response

Features	Sangfor Ransomware Solution	Sophos Ransomware Solution
AV Protection		
AI Behavior Analysis	✓	✓
Signature Database	✓	✓
In-Memory Protection	✓	✓
Fileless Attack Protection	✓	✓
Pre-Execution ML Detection	✓	✓
Application Whitelist	✓	✓
AV Scan CPU Resource Control	✓	✗
On-Premise Sandbox	✓	✗
Cloud Sandbox	✓	✗
Vulnerability Protection		
Host Based IPS/Firewall	✓	✓
Realtime Vulnerability Scanning	✓	✗
Scheduled Vulnerability Scanning	✓	✗
Rule-Based Virtual Patching	✓	✗
Scan-Based Virtual Patching	✓	✗
Exploit Detection	✓	✓

Detection & Response	Sangfor Ransomware Solution	Sophos Ransomware Solution
Detection & Response		
Device Control	✓	✓
DLP	IAG	✓
Realtime Visual Endpoint Connection Analysis	✓	✗
Ransomware Protection (blocking)	✓	✓
Ransomware Protection (file backup)	Built-in backup feature in HCI	✓
Ransomware Protection (stop encryption)	✓	✗
One-Click Network-Wide File Kill	✓	✗
Local Microsegmentation/ Isolation	✓	✓
Network/Remote Microsegmentation	✓	✓
Direct Firewall Integration	✓	✗
Cloud Backup	Built-in backup feature in HCI	✗
Support Services		
Normal Business Hours	✓	✓
24/7 Phone & Chat	Optional	Optional
Malware Removal Service (once)	✓	Optional
Malware Removal Service (unlimited)	Optional	✗
Security Health Check Service (annual)	✓	✗
Managed Detection & Response (MDR)	Optional	Optional
Incident Response Service	✓	✗
Other features		
Engine Zero (AI powered anti-malware, AV)	✓	✗
Sandbox	✓	✓
Neural-X (Cloud based TI)	✓	✓
Security visibility & Reporting	✓	✗ Requires View Subscription
EDR, File encryption & correlation	✓	✓
Simplified Security Operation	✓	✗

How Do You Sell Sangfor Ransomware Solution?

Sangfor Ransomware Solution Promotion Campaign & Strategy

- Ransomware solution bundle gets a higher discount than single product purchase
- Incident response service will be free if you choose a total Sangfor ransomware solution

Ideal Partners

- Non-Fortinet core partners, carrying multiple NGFW brand like Sophos and WatchGuard
- Traditional AV reseller with low profit margin
- Typical solution integrator who wants to expand their business by offering security managed services
- Partners who need free IR support

Why partners choose the Sangfor ransomware solution

- Higher profit margin vs other vendors
- In-country presales & post sales 24/7 project support
- Sangfor NGAF is the only FW vendor who provides complementary Incident Response services
- Sangfor provides the most completed and cost-effective ransomware solution

Case Studies

Customer A: Government

Country	Ransomware	Response Timeline
China	WannaCry	Recover back ups (1 hour) - Confirm ransomware strain and infected files (30 mins) - Install Endpoint Secure to remediate ransomware (2 hours)

Customer B: Education

Country	Ransomware	Response Timeline
Malaysia	GandGrab V2.1	Recover back ups (5 mins with Sangfor HCI) - Confirm ransomware strain and infected files (30 mins) - Install Endpoint Secure to mitigate ransomware(2 hours)

Customer C: Enterprise

Country	Ransomware	Response Timeline
UAE	Phobos	Confirm ransomware strain and infected files (30 mins) - Installed Endpoint Secure to remediate ransomware (2 hours) - Vulnerability scanning (2 hours)

SANGFOR

Make IT Simpler, More Secure and Valuable !

www.sangfor.com