Sangfor NGAF

Branch Office Protection with Sangfor NGAF

www.sangfor.com

SANGFOR

Branch Office Protection

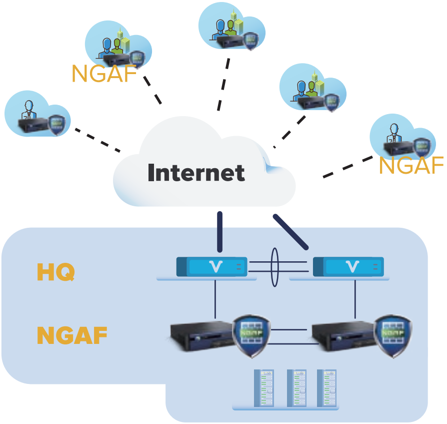
01

Branched-based enterprises are tasked with dealing with the complexities of how to build a stable, secure and reliable network between headquarters and branches, while taking into account economic considerations.

When headquarters implements comprehensive threat protection for the branch network, it also needs to ensure the security of information transmission between the branch offices and headquarters, simplify equipment operation and maintenance in a multi-security equipment scenario and reduce personnel operation and maintenance costs.

Problems and Challenges Faced by Traditional Protection

- Branch security systems are weak and make the entire organizational network vulnerable.
- Branch security systems cannot be managed uniformly making branch security risks uncontrollable and unpredictable.
- Branches often lack full-time security operation and maintenance staff.
- Security capabilities need to be enhanced and updated continuously.



Traditional Branch Security

Gateways with no security features can easily become a vulnerable security risk.

Traditional firewalls can’t detect application layer attacks and are unable to detect or defend against most ransomware.

Traditional gateways cannot implement security auditing oradapt to network multi-traffic management.

Sangfor NGAF in Branch Offices

Sangfor next-generation firewall establishes 2-7 layers of network security protection, and monitors branch security risks continuously to detect ransomware.

Unified management and quick implementation of branch security systems.

Comprehensive network IT visualization, operation and maintenance with dynamic perception capabilities.

Internet can be audited and user behavior tracked

Advantages of Branch Office Protection with Sangfor NGAF

Unified Branch Management:

Meets overall security requirements of rapid deployment, unified management, network-wide monitoring, centralized analysis, intelligent operation & maintenance and offers comprehensive protection.

Branch Risk Closed Loop:

Risk perception, defense, detection, response, security posture awareness, traceability positioning and prevention of the spread of any risks from branches to HQ.

Enhanced Security Capabilities:

Local and cloud collaboration powered by an AI engine to defend against unknown and advanced threats.

End to End User Management

Visibility of Assets

- Identify core business system assets
(example: application software, users, devices and content).

Visibility of Threats and Risks

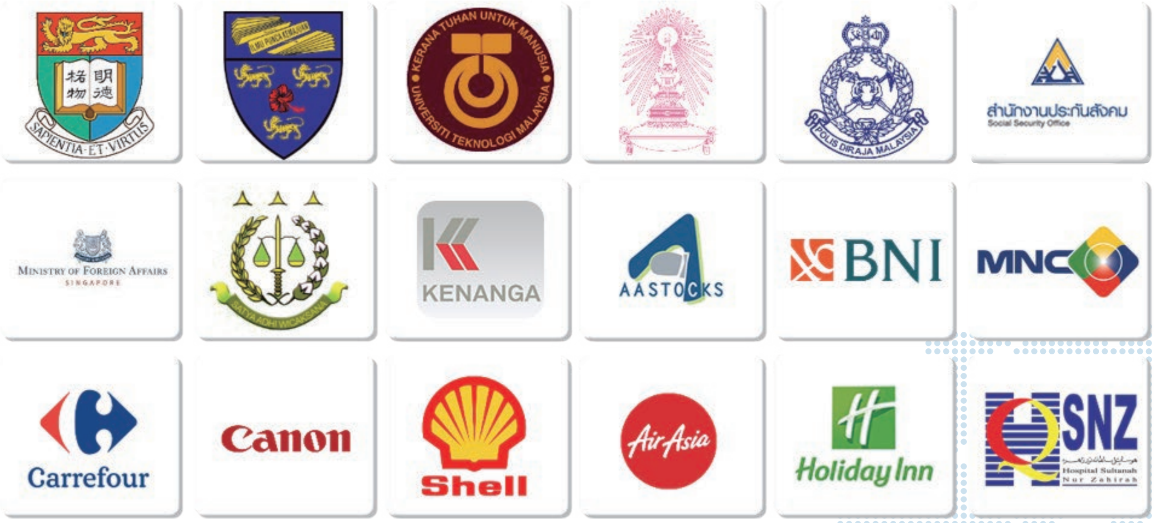
- Identify vulnerabilities and risks to business assests.

Visiblity of User Behavior

- Distinguish between common and uncommon user behavior, identify potential risks and respond to threats in real-time.

- Easily distinguish between legitimate users and malicious users.

Notable Customers


格物 明德
SAPIENTIA·ET·VIRTUS
KERANA TUHAN UNTUK MANUSIA
UNIVERSITI TEKNOLOGI MALAYSIA
POLIS DIRAJA MALAYSIA
สำนักงานประกันสังคม
Social Security Office
Ministry of Foreign Affairs
Singapore
SATYA ADHI WICAKSANA
KENANGA
AASTOCKS
BNI
MNC
Carrefour
Canon
Shell
AirAsia
Holiday Inn
SNZ
Hospital Sultanah Nur Zahirah