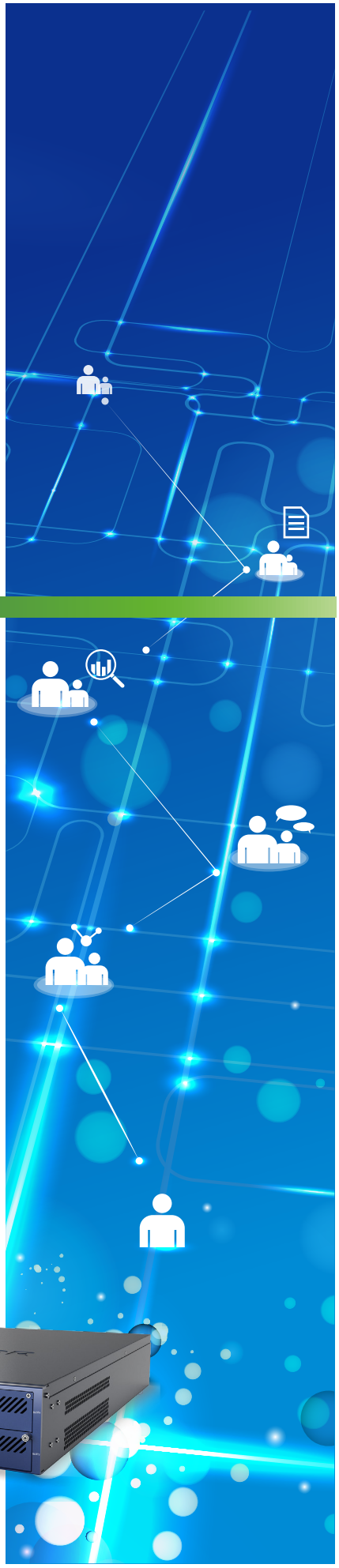
SANGFOR INTERNET ACCESS GATEWAY

Secure User Internet Access Behaviour



- ✓ *Detect and block unwanted behavior in encrypted traffic.*
- ✓ *Identify which applications are accessed by who and when.*
- ✓ *Boost user productivity through internet access compliance.*

SANGFOR

Sangfor
Internet Access Gateway Solution

Internet has become an increasingly vital platform for most businesses as an increasing number of business-critical applications are deployed over the Internet.

However, with great opportunities come great challenges. Improving user experience & work efficiency, blocking illegal endpoints, reducing bandwidth consumption, guarding intellectual property rights, protecting against malware and implementing internet access compliance have become the primary challenges for IT managers, who are often seen as an expense rather than an investment.

Furthermore, as BYOD (Bring Your Own Device) becomes more prevalent in the workplace, improved network management technologies are more important than ever for overwhelmed IT departments.

SANGFOR Internet Access Gateway (IAG) is a secure internet access solution that addresses enterprise network challenges by allowing users and networks to be managed in a simple and visible manner.

Simple & Intuitive Reporting

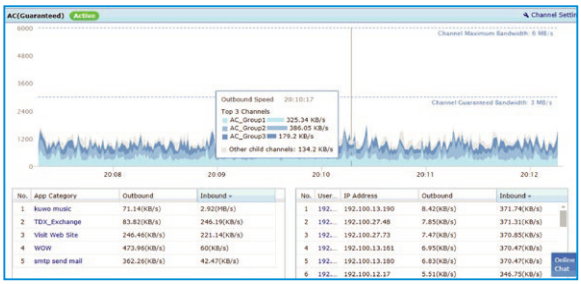
- **Advanced Report Center:** Accurate Traffic Reporting and Graphs
- **Content Visibility and Auditing:** Instant Messaging, Emails and Social Media

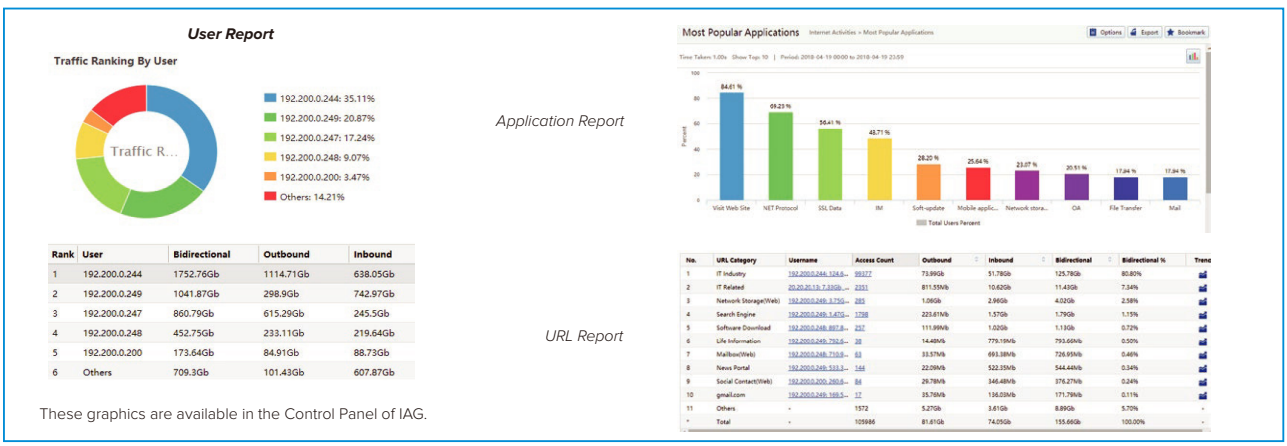
The old adage “You can't manage what you can't see” describes the challenges and risks of modern enterprise networks, making a comprehensive Report Center a critical component for IT departments to analyse network traffic. SANGFOR IAG includes an Advanced Report Center supporting numerous report customization options measuring traffic statistics, queries, ranking, times and behaviour of user & user groups, helping enterprises analyse the root causes of all network issues.

In addition, as information and data are becoming key business assets, enterprises are paying more attention to preventing potential information leakage and disruptive network activities. SANGFOR IAG boasts refined content and attachment auditing for corporate Instant Messaging programs.

• Advanced Report Center

IAG Advanced Report Center records, audits and counts all network behaviour to all unauthorized network behaviour of intranet users in easy-to-read graphical reports. With reports, curves and statistics, IT managers are provided with all the detailed information they need about their network, including Internet access activities, bandwidth consumption and viewed content. Reports are self-generating and sent automatically & regularly to an appointed e-mail address to effectively assist in the network design, security and optimization of bandwidth usage.





These graphics are available in the Control Panel of IAG.

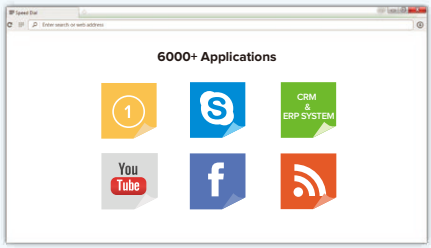
BM & User Access Management

- **Bandwidth Management:** Guaranteed Bandwidth for Critical Applications
- **User Access Management:** Avoid Abuse by Restricting Access & Devices
- **Application Control:** Protect Enterprises Against Unauthorized Applications
- **URL Filtering:** Monitor & Control Evasive Activities
- **Endpoint Control:** Management of Mobile Devices & Tablets
- **Illegal Wi-Fi Hotspot Detection:** Block Phishing Wi-Fi to Avoid Data Leakage

To solve these common issues SANGFOR IAG employs a URL & application database, which helps IT administrators effectively to enforce organization internet compliance by setting specific policies.

In addition, as the BYOD trend is becoming more and more popular, mobile devices should be also included in the enterprise network management policy. IAG empower IT administrators to ensure onboarding devices are identified and comply according to assigned acceptable user policy (AUP).

Sangfor IAG also detects and blocks illegal Wi-Fi hotspots to avoid any information leakage from laptops, smartphones or tablets. A wireless endpoint list will display which endpoint is using an illegal Wi-Fi hotspot allowing the IT team to decide whether to block it or not.



Note: Data from November 2022

700+ Cloud Applications | 300+ Web Applications

1,000+ Mobile Applications | Sangfor 300+ IAG R&D Staffs

- **Authentication based on SMS, Portal, Social Media & QR Code**
- **Push Advertising based on SMS, Portal & Social Media**

Authentication & Push Advertising based on SMS

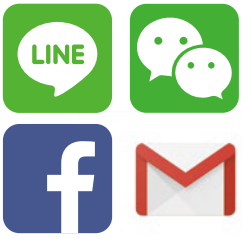
One of the quickest and most common way to collect customer information is by collecting phone numbers. When connecting to the Wi-Fi access point, the login page will ask the customer to insert a phone number to access the internet, allowing your business to send advertisements to your customers through SMS or phone call.

Authentication & Push Advertising based on Portal

Another common solution for collecting information is to redirect customers to a customized portal page after they have successfully connected to your Wi-Fi. This portal can be customized with any kind of information such as daily promotions, new products or services, etc.

Authentication & Push Advertising based on Social Media

Facebook, Line and WeChat are the fastest growing social media platforms in Asia. They can now be used as an authentication method for your Wi-Fi while simultaneously increasing your number of followers. More importantly, you can use push information to reach a larger potential customer base.



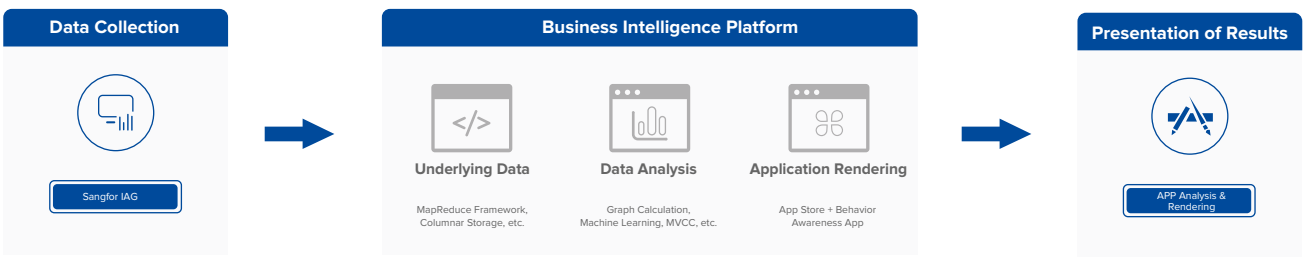
Authentication via QR Code

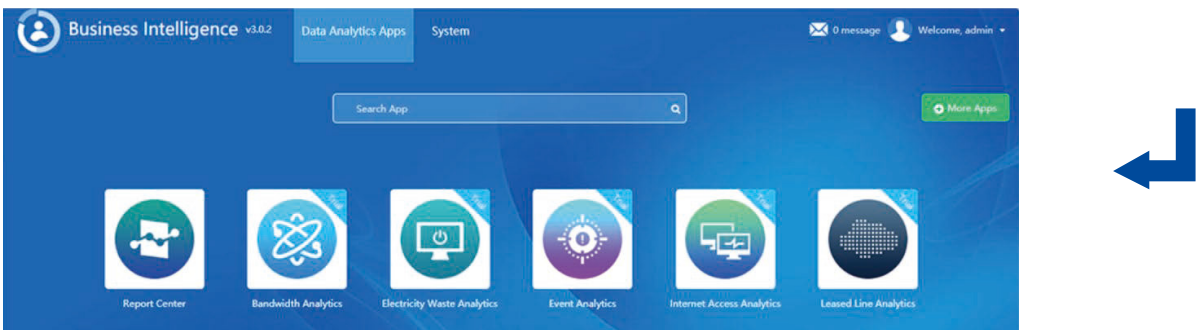
For companies receiving dozens of visitors per day, sharing the Wi-Fi password can become headache for the sta . With Sangfor IAG, you can create a QR code to allow your visitors to connect to the Wi-Fi simply by opening any QR code software and scan it. With this type of authentification, there is no need to change your Wi-Fi password every time and you can generate the QR Code according to each visitor group.

Business Intelligence Platform

The Look of Innovation

Sangfor Business Intelligence Platform (BI) is the newest major innovation within Sangfor IAG. It is based on IAG's massive internet log and conducts in-depth modelling analysis of internet usage trend. It constantly utilizes behavioural awareness applications in different scenarios and continuously uncovers valuable data, helping organizations understand behaviour risk and simplify O&M.

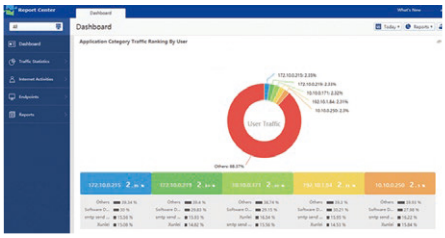




Work Smarter, Not Harder

Report Center

The Professional Report center has never been more simple, comprehensive or responsive. With a single dashboard and step-by-step analysis, you can simply see your network from top to bottom. Through analysis of traffic, duration, applications and URL's you can easily see customized reports on keywords, uploads, email and application use. Finally, proactively monitor your network with monthly base reports in 10 seconds giving you the 20/20 hindsight you need to plan ahead.



Bandwidth Analysis

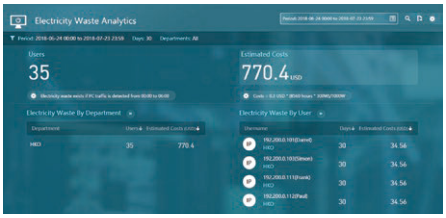
Give the people what they need! With Line Quality Analysis you can easily see what applications are utilizing the majority of your bandwidth and allocate or block bandwidth to individual applications with a single click.

Leased Line Analytics

It can provide a report on the quality of the leased line and help you with more informed decisions on when to expand the leased line bandwidth. It also provides visibility into the tunnel and the user to achieve awareness of the whole network.

Electricity Waste Analytics

We work 24/7 so you don't need too! When the lights go out at night and the last employee leaves the building, Off Hours PC Scan allows you to monitor any network users, heightening your network security while also reducing business cost by monitoring power consumption outside business hours.



Internet Access Analytics

Reduce your IT expenditure and make IT more valuable. See and control information and traffic for all branches with SANGFOR Overall Status Display. With easy to read reports on bandwidth and traffic distribution as well as e ciency-reducing applications and websites at all your branches and locations, simply point and click to optimize your bandwidth consumption and user experience.

Event Analytics

Customise your view and see what is most important to you! Automatically scan for specific keywords indicative of malware or abnormal user behaviour and be proactive in managing your potential risk.

Manage the SaaS Application in the Right Way

Discover → Manage → Control → Analyze

1. Discover Know the Risk

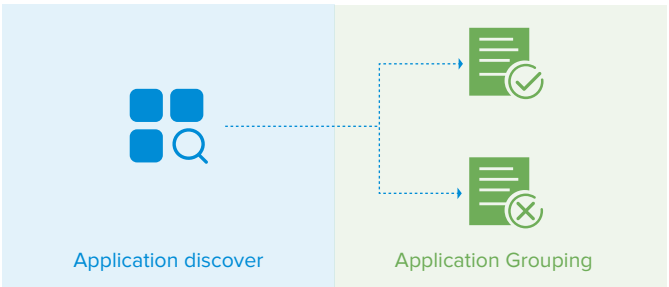
IAG with the built-in SaaS application database, identifies the most used applications, and also categorize them in group according to their security risks (sent emails, high bandwidth consumption, unproductive websites and applications, data leakage risk, etc.). The dashboard directly shows the applications and how much data had been used and how much files are transferred, making the IT administrators have a clear understanding of the applications in the network.

Applications | Users

App Catego

No.	Name	App Category	Tags	Sanction Status	Outgoing Files	Outbound(Bytes)	Inbound(Bytes)	Users
1	QQ Mail[brow...	Mail		New	4	31.89 KB	8.12 KB	1
2	Google Drive ...	Network storage	Disclosure Risk	New	0	2.24 MB	16.61 MB	15
3	NetEase_Mail...	Mail	Reduce the Efficiency of Work	New	0	1.05 MB	3.51 MB	1
4	Baidu Wangpa...	Network storage		New	0	721.42 KB	3.27 MB	5
5	Baidu_Wenku[...	Network storage	Reduce the Efficiency of Work	New	0	707.45 KB	2.09 MB	1
6	QQ Mail-Base	Mail	Reduce the Efficiency of Work	New	0	502.84 KB	441.16 KB	4
7	Baidu Wangpa...	Network storage		New	0	464.88 KB	1.4 MB	2
8	Sina_Mail_Base	Mail	Reduce the Efficiency of Work	New	0	113.78 KB	1.07 MB	1
9	Google Hango...	IM	Reduce the Efficiency of Work	New	0	105.82 KB	2.26 MB	9
10	Baidu Wangpa...	Network storage	Disclosure Risk	New	0	21.92 KB	44.07 KB	1
11	Baidu Wangpa...	Network storage	Reduce the Efficiency of Work	New	0	8.8 KB	1.88 KB	4
12	GitHub_Client	Network storage		New	0	5.33 KB	19.97 KB	1
13	Dropbox	Network storage	Disclosure Risk	New	0	4.52 KB	13.52 KB	1
14	Sohu Mail[sen...	Mail	Send Email	New	0	3.45 KB	2.21 KB	1
15	NetEase Mail[...	Mail		New	0	587 B	585 B	1

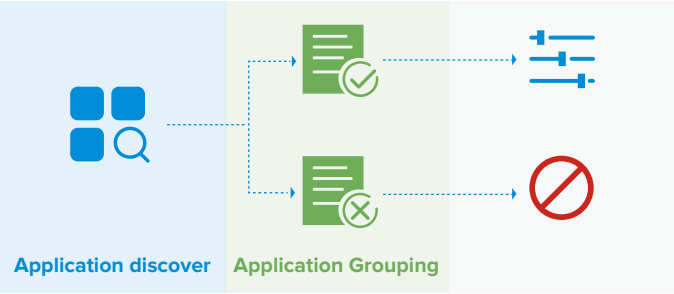
2.Grouping – Manage the Applications



- **Sanctioned–** These applications provide IT teams with security guarantee and are allowed to be used by the user.
- **Unsanctioned–** These applications are potentially dangerous and the IT administrators do not want users to use them due to security risk and data leakage risk.

The sanction status makes it easier for managing the applications in a proper way. Sanctioned applications are the ones known and approved by the IT administrators, while the unsanctioned one are not known but may be used by the user, which may a ect the user experience when all of them are blocked, or the ones that need to be monitored for a while.

3.Control the Risk



- **Control Policy–** Setup control policy over the applications.
- **Block–** These applications have been used in the network.

Sangfor IAG provides a granular control over the applications identified, together with the bandwidth control capabilities, providing much higher work productivity.

Create A Space For Work

The search engine is convenient to find the information you need, but it will also come out with inappropriate contents. Sangfor IAG can set Google, Bing and YouTube into default safe search mode, blocking inappropriate content that could a ect the organization reputation.

Improve Work Productivity

The SaaS application brings convenience but also bring troubles. It allows user to access work resources freely but also entertainment resources.

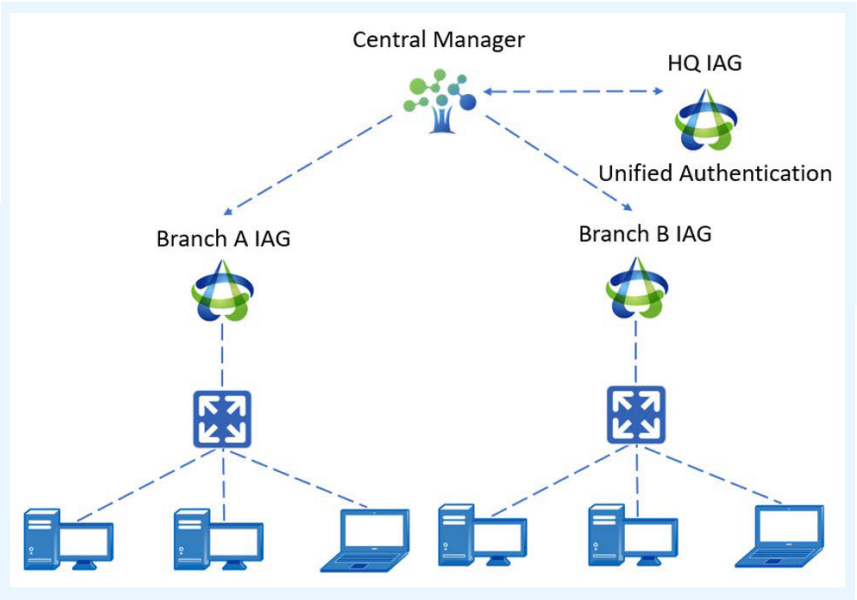
IAG can improve user productivity by allowing the user to only access specified work resources such as login Google Workspace and Office 365 with the enterprise user account, access, access Facebook company page for work purposes only, and block all other Facebook content.

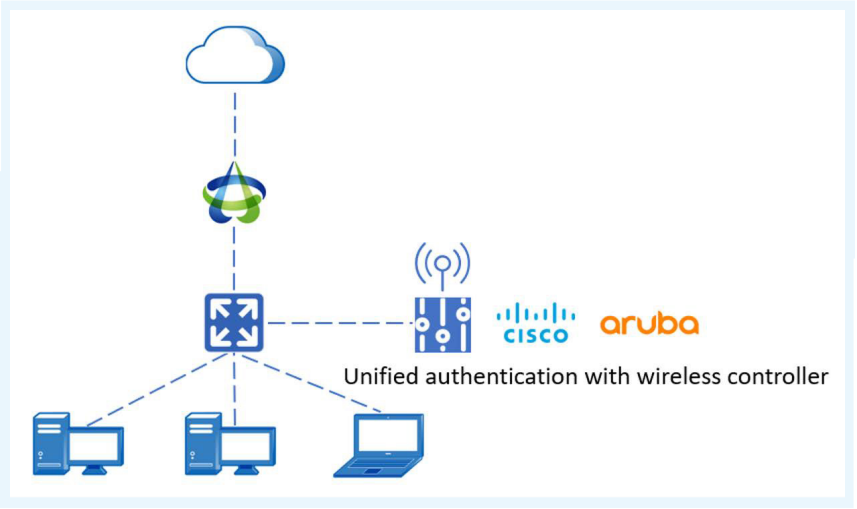
Unified Authentication and Wireless Controller Integration

Control Any Device - Anywhere

Success used to have its price, but now it doesn't! The issue of centralization and unification has become common as businesses expand and open new branches. In the past, various branches were individually responsible for management of their wired and wireless authentication, WIFI network and control policies.

User experience varied from branch to branch and WIFI connectivity did not roam with the user. SANGFOR IAG now provides centralized management capabilities which allow policies, restrictions and control to be exercised from a central platform, reducing operating costs and simplifying the IT management process. With the Central Manager system user experience is also improved by allowing roaming WIFI connectivity and unifying the information visible on each branch platform.





Real-Time Asset Management

IOT devices especially those are unknown has become another major dilemma among the administrators. Without standardized monitoring and enforcement policy, there is no way administrators can have current holistic view of total onboarding devices and compliance check to determine overall status.

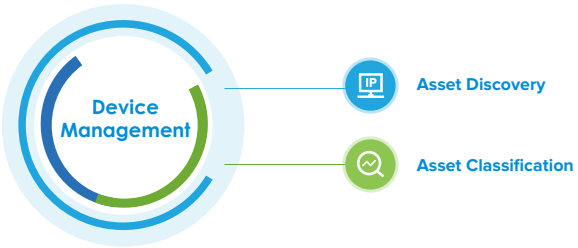
Sangfor real-time asset management is designed to tackle this problem with 2 main components:

Asset Discovery

It provides real-time status of what endpoint are running on your network and all this without any agent software. This allows administrators to build accurate inventory and up-to-date status about their network assets.

Asset Classification

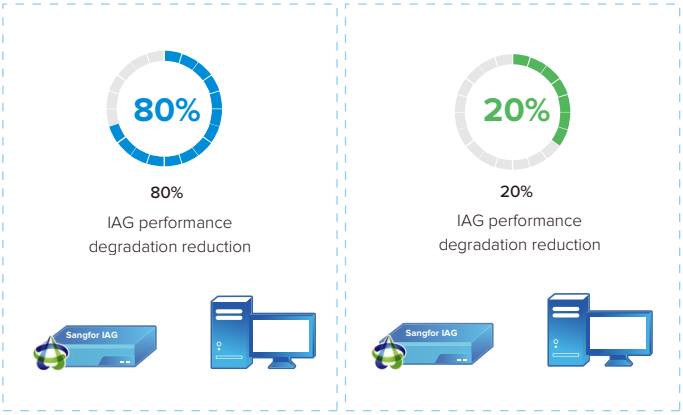
One of the crucial elements in asset management is the ability to identify any unknown IOT devices and perform classification to determine asset type.



SSL Decryption

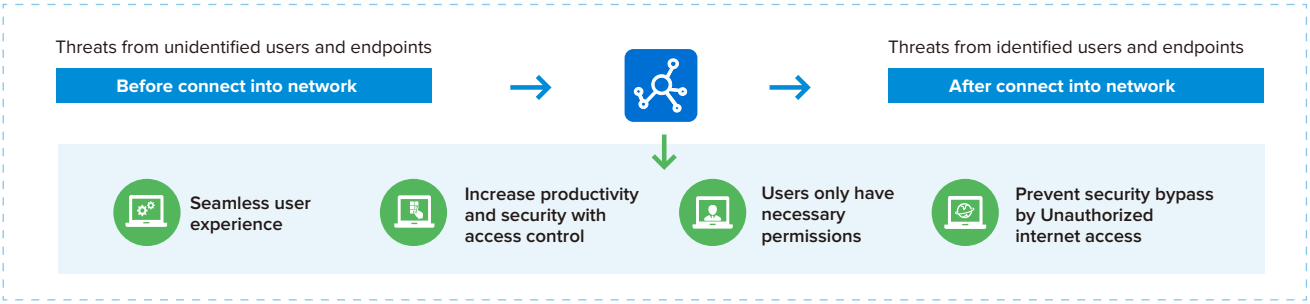
Typically, user always have to choose between having SSL decryption enabled with huge performance degradation and using internet access without any SSL decryption. IAG now provide another option to mitigate such performance degradation by using ingress client to perform SSL proxy decryption process.

With captive portal redirection, users will have the ability to deploy ingress client with ease along with root SSL certificate is distributed and installed together with ingress client. User can now plan their SSL decryption policy strategy without compromising performance loss by having use either IAG decryption, Ingress client decryption or running both for different network segments as an option.



Endpoint Security Posture

Endpoints are the most common target of cybersecurity attacks. One compromised endpoint within your organization can lead to widespread effects and disruption to your business. With endpoint security posture from IAG, you will get a complete picture of your current endpoints, whether compliant and non-compliant according to the organization policies. Also, this will identify risks associated with your organization's endpoint devices, such as using unauthorized network connections, changing MAC/IP addresses, and subsequently make a remediation action plan to address these risks.

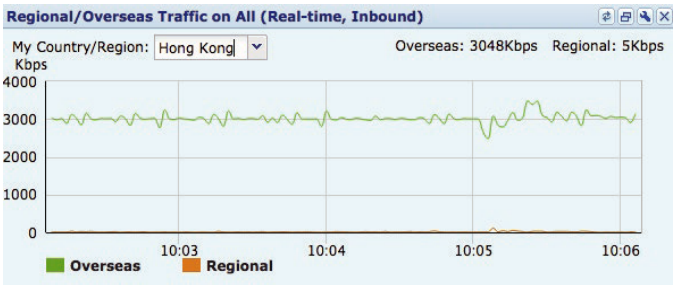


Advanced Bandwidth Management

Separate Management of International & Domestic Bandwidth

As businesses cross borders IT needs to be aware of usage patterns, bandwidth needs, potential risks and differing costs and challenges associated with individual international locations.

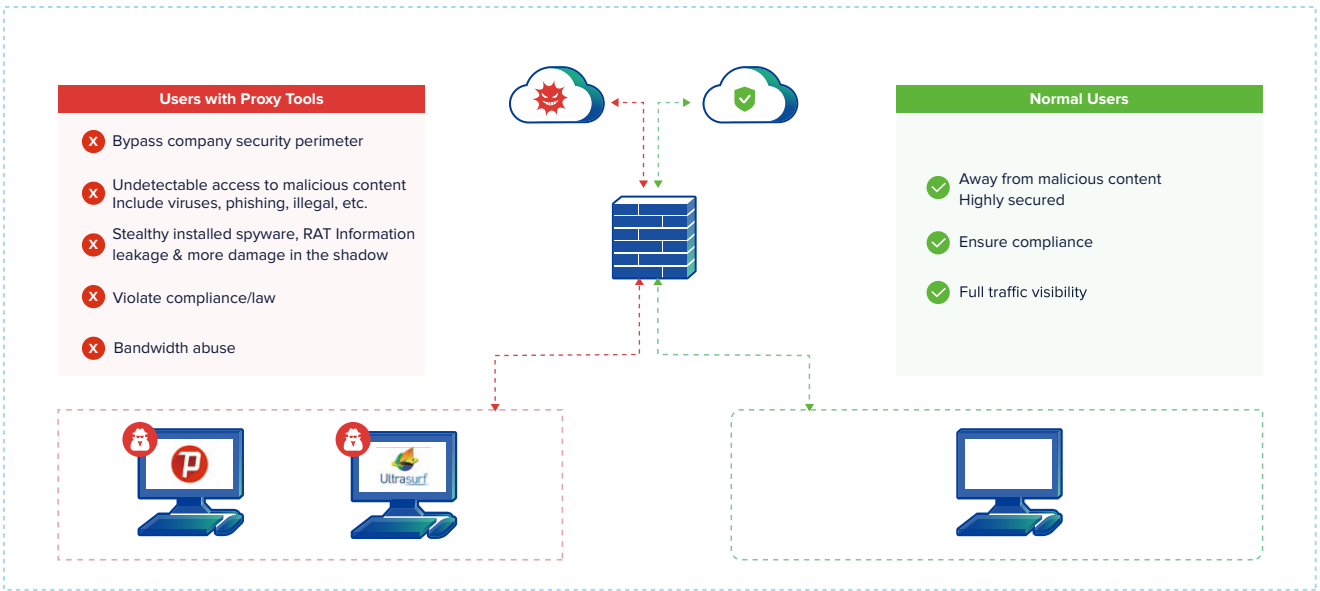
With Sangfor IAG, you can separate the bandwidth management for international and domestic internet access. This is especially important in countries where different fees for bandwidth usage apply but also improves international user experience and reduces risk of network security issues stemming from international locations by allowing full visibility and control of both domestic and international network traffic.



Proxy Avoidance Protection

Proxy avoidance is a tool constantly used by users to bypass network security perimeter and allowing them to access inappropriate content. Many organizations face issues where users access proxy avoidance applications to circumvent security protection and access web content that should be filtered.

Sangfor IAG working with Endpoint Secure to provide comprehensive detection and blocking capabilities on proxy avoidance protection. It has an extensive library of well-known anti-proxy applications, anonymous browsers and VPNs to create blocking/monitoring policies enforced by the Endpoint Secure Protect Agent.



SANGFOR IAG Product Family

Model	M5100-AC-I-S	M5200-AC-I	M5400-AC-I	M5500-AC-I	M5600-AC-I	M6000-AC-I	M6000-UPG[2]	M9000-AC-I	M10000-AC-I	M12000-AC-I
Profile	1U	1U	1U	1U	1U	2U	2U	2U	2U	2U
HD Capacity	128 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD	64 GB SSD + 960 GB SSD
Application Layer Throughput Options[1]	160Mbps	400Mbps	600Mbps	1Gbps	1.2Gbps	2Gbps	4Gbps	10Gbps	20Gbps	40Gbps
Recommended Concurrent Users	600	2,000	3,000	5,000	6,000	15,000	20,000	50,000	100,000	200,000

Power and Physical Specifications

Model	M5100-AC-I-S	M5200-AC-I	M5400-AC-I	M5500-AC-I	M5600-AC-I	M6000-AC-I	M6000-UPG[2]	M9000-AC-I	M10000-AC-I	M12000-AC-I
Support Dual Power Supplies	N/A	N/A	N/A	N/A	YES	YES	YES	YES	YES	YES
Power [Watt] (Typical)	40W	40W	40W	60W	150W	150W	150W	325W	325W	325W
Working Temperature	0℃~45℃	0℃~45℃	0℃~45℃	0℃~45℃	0℃~40℃	0℃~40℃	0℃~40℃	0℃~40℃	0℃~40℃	0℃~40℃
System Dimensions (W x L x H in mm)	430 x 300 x 44.5	430 x 375 x 44.5	430 x 400 x 44.5	430 x 400 x 44.5	430 x 400 x 44.5	440 x 600 x 89	440 x 600 x 89	440 x 600 x 89	440 x 600 x 89	440 x 600 x 89
System Weight	3.4 Kg	6.6Kg	6.6Kg	7.5Kg	9Kg	18.5Kg	18.5Kg	20.0Kg	20.0Kg	20.0Kg
Relative Humidity	5%~95% non-condensing									

Network Interfaces

Model	M5100-AC-I-S	M5200-AC-I	M5400-AC-I	M5500-AC-I	M5600-AC-I	M6000-AC-I	M6000-UPG[2]	M9000-AC-I	M10000-AC-I	M12000-AC-I
Bypass (copper)	1 pair	2 pairs	2 pairs	2 pairs	3 pairs	3 pairs	3 pairs	2 pairs	2 pairs	2 pairs
10/100/1000 Base-T	4	6	6	6	6	6	6	4	4	4
1G SFP	N/A	2	2	2	N/A	N/A	N/A	4	4	2
10GbE SFP+	N/A	N/A	N/A	N/A	2	2	2	2	4	4
Extended Slot Number	1	1	1	1	2	2	2	1	1	4
Serial Port	RJ45x1	RJ45x1	RJ45x1	RJ45x1	RJ45x1	RJ45x1	RJ45x1	RJ45x1	RJ45x1	RJ45x1
USB Port	2	2	2	2	2	2	2	2	2	2

Compliance and Certificates

Compliance	CE, FCC, IPv6 Ready

[1] Represents the maximum bidirectional flow (max. inbound + outbound flow).

[2] M6000-UPG is a license upgrade from M6000 with application layer bandwidth increased from 1G to 2G.

- Products specifications described herein are subject to change without prior notification.
- All performance values are “up to” and vary depending on the system configuration.

vIAG
Sangfor Virtual IAG (VMware & Sangfor HCI Platforms)

Model[2]	vIAG-50 vmIAG-50	vIAG-100 vmIAG-100	vIAG-200 vmIAG-200	vIAG-300 vmIAG-300	vIAG-700 vmIAG-700	vIAG-1000 vmIAG-1000	vIAG-2000
FW Throughput Options[1]	200 Mbps	500 Mbps	1 Gbps	1.4 Gbps	2.1 Gbps	3.0 Gbps	5.0 Gbps
Application Layer Throughput Options[1]	100 Mbps	200 Mbps	400 Mbps	600 Mbps	1.4 Gbps	2 Gbps	4 Gbps
Recommended Concurrent Users	500	1000	3000	5000	7000	10000	20000

[1] Represents the maximum bidirectional flow (max. inbound + outbound flow).

[2] vIAG = Virtual IAG based on Sangfor HCI | vmIAG = Virtual IAG based on VMware ESXi

System Requirements

vIAG & vmIAG System Requirements	vIAG-50 vmIAG-50	vIAG-100 vmIAG-100	vIAG-200 vmIAG-200
Virtualization Platform	Sangfor HCI/ VMWare ESXi	Sangfor HCI/ VMWare ESXi	Sangfor HCI/ VMWare ESXi
CPU	Min. 1 Virtual Core	Min. 1 Virtual Core	Min. 2 Virtual Cores
Memory	2GB	2GB	4GB
Disk Space	80GB	80GB	80GB

vIAG & vmIAG System Requirements	vIAG-300 vmIAG-300	vIAG-700 vmIAG-700	vIAG-1000, vIAG2000 vmIAG-1000
Virtualization Platform	Sangfor HCI/ VMWare ESXi	Sangfor HCI/ VMWare ESXi	Sangfor HCI/ VMWare ESXi
CPU	Min. 2 Virtual Cores	Min. 4 Virtual Cores	Min. 8 Virtual Cores
Memory	4GB	8GB	16GB
Disk Space	80GB	80GB	80GB

**SANGFOR IAG can co-exist alongside another internet security system or any other Sangfor solutions.*

Sangfor IAG Product Features

User Authentication and Management	
Mapping and Identifying Users	IP, MAC, IP/MAC binding, hostname, USB Key, SMS, QR-Code, Portal, WeChat, Facebook, Line, Gmail, Twitter.
User Accounts Importing	- Import user accounts information using CSV file, LDAP Server. - Synchronize user with LDAP, Database and H3C CAMS Server.
Integration and SSO Option	Active Directory/POP3/Proxy/Web Server, Radius, Third-party authentication device, Database Server.
New User Management	- Automatically map new user to its privileged groups in local database based on its IP range, subnet or external authentication server group. - Automatically map new users to a pre-defined privileged group as temporary accounts.
Account Attribution	Public (Share user login)/ Private (Single user login) account option.
WLAN Auth. Integration	Aruba, Cisco, CMCC 1.0, CMCC 2.0.
Access Control	
Application Control	Identify and control applications through application DB or port.
URL Filter	URL DB, keyword in web-page based control.
Search Engine Control	Managed by keywords.
Enhanced Email Control	Managed by source address, destination address, keywords in email, keywords in body/title, attachment, type/size/count based control.
Enhance IM Control	Corporate instant messaging (IM) is subject to content and attachment audits, while consumer-grade instant messaging (IM) is subject to attachment audit.
File Filter	Control HTTP, FTP upload and download activity based on true file type.
SSL Traffic Control	Certificate, text content based control and filter.
SSL Decryption	Gateway decryption and ingress client decryption.
Proxy Avoidance Protection	
Anti-Proxy	Detect and block proxy tools based on application signatures database and Endpoint Secure integration.
Asset Management	
Asset Discovery	- Identify and list of IOT devices based on endpoint type - Advance search and filter based on endpoint parameter - Export to csv
Asset Classification	Categorize endpoint type based on host, mobile endpoint, network device, dumb endpoint, medical equipment, network endpoint sharing and custom.
Endpoint Security Posture	
Ingress Client-based (Agent)	Login domain, operating system, process, file, registry, task, patch, access check, access control, external device control, windows account, software check, anti-defacement and anti-virus software related to update and database version.
Traffic-based (Agentless)	Endpoint verification and enforce update on outdated antivirus signatures including consumer-grade antivirus and corporate antivirus.
Illegal Wi-Fi Detection and Blocking	
Illegal Wi-Fi Detection and Blocking	Detect the endpoint information from every IP address.

Bandwidth Management (BM)	
BM Policy	Traffic guarantee/limit policy for uplink and/or downlink base on bandwidth percentage of the pipe, max bandwidth per user, user/application priority, exclusion policy.
BM Objects	Application type, website type, file type, user, schedule, destination IP, etc.
Separate BM Management	For International & Domestic Traffic.
Bandwidth Guarantee & Limitation	Allocate bandwidth resource according to business type & guarantee bandwidth for core business applications and restrict irrelevant traffic.
Multi-level SON Channel	Match the organizational structure to achieve finegrained bandwidth management.
Dynamic Bandwidth Management	- "Bandwidth Borrowing" among BM tunnel for full bandwidth utilization. - Specify a network flow thresholds as effective points of BM policy. - BM based on public IP (oversea). - Average allocation/free competition among users in a single traffic pipe.
Virtual Line	Manage and control to each physical line independently and effectively bridge mode.
Multiplexing and Intelligent Routing	Provide link load balancing in router mode.
Traffic Identification and Categorization	
Sangfor URL Database	- Leverage on-the-cloud infrastructure, dynamically categorizes millions URLs into the predefine categories. - Support configurable in-box cache footprint.
Application Database	Independent Internet application signatures database.
Intelligent Identification Rules	Identify P2P/Proxy tools/VOIP/SSL traffic intelligently through dynamic flow characteristics analysis.
File Type Identification	- By extension name. - By file type (data pattern).
Value-Added Services	
Big Data Mining	Record of online behavior data record, data modeling analysis and analytics report.
Report Center	
Report Objects	Application flow, user behavior counts, online duration per user & per application, virus and security, keywords, etc.
Graphical Reports	Counts, ranking, comparison, trends analysis with statistics, pie, bar, line chart, etc.
Real-Time Report	Real-time monitor of CPU/hard disk/traffic/connection/session status, online user information, traffic ranking, connection ranking, real-time utilization, visibility of bandwidth channels.
Content Log	Content log including corporate Instant Messaging (IM) chat, SMTP and webmail content and attachment (Gmail, etc), BBS posts (Facebook, Twitter, etc)
Customizable Risk Report	Employee turnover trend, disclosure, work efficiency, security risks and other risk reports.
CIO Report	Tailored reports of overall network analysis and risk management for CIO.
Web-Access Connection Quality Report	Used for clear evaluation of the overall network quality. Users with poor web access quality can be listed down.
Report Format	CSV, PDF.
Report Center Storage	Built-in internal report center and optional external report center.
External Reports Storage Security	- Option to protect the report center by using external authentication key for additional security. - "Google Like" search engine GUI for external report center. - Email subscription.

Control Tools for Manageability	
Notification (Reminder)	Notify end user for online time of specific application and the flow speed of specific application.
Flow/Duration Control	Daily/Monthly flow quota per user. Daily online duration quota per user with exception case based on specific application. Concurrent session quota per user.
Endpoint Security Compliance	- Ingress Client Based (Agent) Login domain, operating system, process, file, registry, task, patch, access check, access control, external device control, windows account, anti-defacement and anti-virus software related to update and database version - Traffic Based (Agentless) Check personal software and enterprise software for anti-virus destination server IP heartbeat
Audit-Free Key	Prevents access audits and control for users that assigned with audit-free keys.
Hierarchical Administration	Functionality of different modules can be assigned to different administrators as needed, via a hierarchical management paradigm. Administration of different functions and modules can be delegated to different administrative groups.
Network & Deployment	
Centralized Management	Unified the configuration and policy for multiple devices, remote control and monitor running status.
LAN+WLAN Management	Set special control policy for mobile user based on user & location. Suitable for BYOD office environment.
Security Modules	- Built-in IPsec VPN. - IPSec Protocol: AH, ESP. - D-H Group: MODP768 Group (1), MODP1024 Group (2), MODP1536 Group (5). - IPSec Authentication Algorithm: MD5, SHA-1, SM3. - IPSec Encryption Algorithm: DES, 3DES, AES-128, AES-256, SANGFOR-DES, SCB2, SM4.
Proxy Functions	Support explicit Proxy, including HTTP/HTTPS two-level Proxy, Sock4/Sock5 Proxy, Forwarding Proxy function and support ICAP protocol.
Deployment	Route, Bridge, Double Bridge, Bypass, Single-arm.
Stability	Hardware bypass, A/A,A/P.
IPv6	Support deployment in IPv6 environment & monitoring of IPv6 traffic.
Log Monitoring	Support Syslog, SNMP V1/V2/V3
Proxy	
Proxy Service	HTTP Proxy / SOCKS4 / SOCKS5 / PAC SCRIPT.
Policies	Enables customers controller proxy data security.
Prevent Data Disclosure	- Send web content to content analysis - Support response and request modification with inspection mode of ICAP server grouping. - Support inspection type including round robin and concurrent options. - Visualization representation and statistics from forwarding log of ICAP server.
Business Intelligence	
Self-Customized Application	Be aware of trends and incidents using keyword related searches to monitor traffic in real-time.
Bandwidth Analysis	Monitor bandwidth status, availability and top bandwidth consuming applications to provide better user experience.
Overall Status Display	Identify threats quickly and easily through combined IAG and NGAF logs.
Leased Line Quality Analytics	Understand the load and real-time status of traffic by collectivly analysing user trends and application use.
Off Hours PC Scan	Monitor PC usage outside business hours.

COMPANY PROFILE

Make Your Digital Transformation Simpler and Secure. This is Sangfor Technologies' commitment to our customers. Since forming in 2000, Sangfor has been a global leader of IT infrastructure, security solutions and cloud computing. Five business groups deliver industry leading products for Hyper-Converged Infrastructure, Virtual Desktop Infrastructure, Next Generation Firewall, Secure Web Gateway, Endpoint Protection, Ransomware Protection, Incident Response, WAN Optimization, and SD-WAN. Constant innovation and dedication to creating value for our customers are the heart of our corporate strategy.

Sangfor's 9500+ employees take customer's business needs and user experience seriously by servicing and supporting them at over 60 branch offices globally in exciting locations like Hong Kong, Malaysia, Thailand, Indonesia, Singapore, Philippines, Vietnam, Myanmar, Pakistan, UAE, Italy, Türkiye and the USA.

CONTINUOUS INNOVATION & EXCELLENT SERVICE

Sangfor invests at least 20% of annual revenue in R&D to improve products and develop new solutions at our five R&D centers located. With over 2,200+ patents, Sangfor has more patent applications submitted in 2022. This dedication to innovation enables us to release product updates every quarter and launch new products annually.

We pride ourselves on our excellent service. Customers enjoy fast 24x7 online support 365 days a year and personalized on-site service support from over 10,000 certified engineers at our three Customer Service Centers in Malaysia & China.

Sangfor has more than 100,000 satisfied customers worldwide, including Fortune Global 500 companies. Governments, universities & schools, financial institutions, manufacturing, and other industries trust us to protect them from the next generation of cyberthreats and help them on their journey to digital transformation with a future-proof IT infrastructure.

SANGFOR INTERNET ACCESS GATEWAY

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
8 Burn Road # 04-09, Trivex,
Singapore (369977)
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
MD Place 3rd Floor, Jl Setiabudi No.7, Jakarta Selatan 12910, Indonesia
Tel: (+62) 21-2966-9283

SANGFOR MALAYSIA
No.45-10 The Boulevard Offices, Mid Valley City, Lingkaran Syed Putra, 59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3644

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

SANGFOR PHILIPPINES
7A, OPL Building, 100 Don Carlos Palanca, Legazpi, Makati, 122 Metro, Manila, Philippines.
Tel: (+63) 0916-267-7322

SANGFOR VIETNAM
4th Floor, M Building, Street C, Phu My Hung, Tan Phu Ward, District 7, HCMC, Vietnam
Tel: (+84) 287-1005018

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
D-81 (D-Wing), Dubai Silicon Oasis HQ Building, Dubai, UAE.
Tel: (+971) 52855-2520

SANGFOR PAKISTAN
D44, Navy Housing Scheme, ZamZamma, Karachi, Pakistan
Tel: (+92) 333-3365967

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-648773

SANGFOR TURKEY
Turgut Ozal Street, Zentra Istanbul, First Floor, Office. 20 Çekmeköy / İstanbul, Postal Code: 34788
Tel:(+90) 546-1615678

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

NGAF - Next Generation Firewall
Smarter AI-Powered Perimeter Defence

Endpoint Secure - Endpoint Security
The Future of Endpoint Security

Cyber Command - Network Detection and Response
Smart Efficient Detection and Response

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

Cyber Guardian - Managed Threat Detection & Response Service
Faster Response Through Human/AI Collaboration

HCI - Hyper-Converged Infrastructure
Fully Converge Your Data Center

MCS - Managed Cloud Services
Your Exclusive Digital Infrastructure

VDI - aDesk Virtual Desktop Infrastructure
The Ultimate User Experience that Beats a PC

Access - Secure Access Service Edge
Simple Security for Branches & Remote Users

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

SD-WAN
Boost Your Branch with Sangfor

SANGFOR

https://twitter.com/SANGFOR

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

https://www.facebook.com/Sangfor

https://www.instagram.com/sangfortechnologies/

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

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

Global Service Center: +60 12711 7129 (or 7511)

www.sangfor.com

IAG_BR_P_IAG-Brochure_20221114