SANGFOR | SANGFOR SECURITY

SANGFOR
Cyber Command

Intelligent Threat Detection and Response Platform

www.sangfor.com

Network Detection and Response (NDR) Is An Essential Tool In The Fight Against Emerging Cyber Threats

The ever-evolving cybersecurity threat landscape is a cause for concern for organizations worldwide, particularly due to the continued rise of highly sophisticated and AI-enabled malware and cyber-attacks. These advanced threats are designed to bypass traditional defenses undetected, steal sensitive data, and cause significant damage to critical infrastructure. As a result, it is imperative for organizations to adopt new, more robust security solutions that incorporate advanced technologies such as machine learning and artificial intelligence to combat these evolving threats.

One such security technology is Network Detection and Response (NDR), which takes a proactive approach to threat detection and threat hunting by assuming that threats have already breached the network instead of trying to keep them out. NDR solutions use advanced AI algorithms and machine learning to monitor and analyze network-wide traffic in real-time, identifying and alerting security teams to any anomalies in network activity. These anomalies can otherwise appear as benign network traffic that has been manipulated or disguised by intelligent malware or sophisticated adversary techniques. By providing enhanced visibility into network traffic, NDR is an essential tool in organizations' security arsenal to defend against today's advanced and AI-enabled malware and cyber-attacks.

Why Do Security Teams Struggle

- Difficult to keep up with a rapidly evolving threat landscape
- Lack of resources to detect & prevent advanced threats
- Lack of visibility into the overall security posture and cyber-attack lifecycle
- Complex management of multiple, unintegrated security tools
- Alert fatigue and inefficiency from tons of alerts & false positives
- Insufficient forensic investigations, lack of IOCs & BIOCs

Stay Ahead Of Sophisticated Threats with Sangfor Cyber Command

AI-Powered, Intelligent Threat Detection and Response Platform

Sangfor Cyber Command is a best-in-class Network Detection and Response (NDR) solution that offers organizations unprecedented visibility into their network environment, encompassing hidden threats, attacks in progress, assets including shadow IT, vulnerabilities, and risks.

Harnessing the power of artificial intelligence and machine learning technology, Cyber Command offers a comprehensive solution for detecting and responding to sophisticated security incidents, complete with advanced security analytics and real-time threat intelligence. This enables businesses to take decisive action against potential attacks before they escalate into costly breaches.

With its real-time monitoring, analysis, and alerting capabilities, Cyber Command can detect anomalies in network traffic as soon as they occur, empowering organizations to be proactive about their cybersecurity instead of relying on reactive measures.

With Sangfor Cyber Command, organizations can transform from passive bystanders to active participants in the battle against cyber threats. Equipped with this advanced security solution, they can effectively stay ahead of increasingly sophisticated cyber threats of both today and tomorrow.

Unmatched Threat Detection

Cyber Command leverages multiple threat detection technologies, including AI- and ML-driven User and Entity Behavior Analysis (UEBA) and rule-based analytics to deliver unmatched detection of advanced threats like ransomware, APTs, zero-day attacks, and fileless attacks. Cyber Command is also continuously enriched with real-time threat intelligence feeds from Sangfor Neural-X to ensure the detection of the latest and emerging threats.

Unprecedented Network Visibility

Cyber Command continuously monitors network-wide traffic and leverages advanced techniques to provide security teams with unprecedented visibility of the network environment. In addition to hidden threats, security teams also gain real-time insight into network assets, including risky shadow IT, and vulnerabilities such as uninstalled patches, weak passwords, and missing encryption to enable prompt remediation.

Automated & Integrated Incident Response

Cyber Command comes equipped with a built-in Security Orchestration, Automation, and Response (SOAR) module that enables automatic response to identified security threats. Security teams can use pre-defined or custom playbooks to address some of common threats scenario or organization-specific scenarios. Cyber Command also integrates seamlessly with Sangfor and third-party security tools to initiate coordinated response actions.

In-Depth Threat Hunting & Investigation

Cyber Command leverages advanced techniques such as attack chain visualization, MITRE ATT&CK mapping framework, and the unique Golden Eye feature to provide detailed insight into security incidents. Security teams can intuitively discover the entry point of attacks, the attack path, and the scope of impact to completely eradicate threats from the environment and remediate the vulnerabilities and weaknesses exploited by attackers.

> *Cyber Command provides comprehensive threat detection and automated response capabilities, yet is simple and intuitive to manage and operate.*

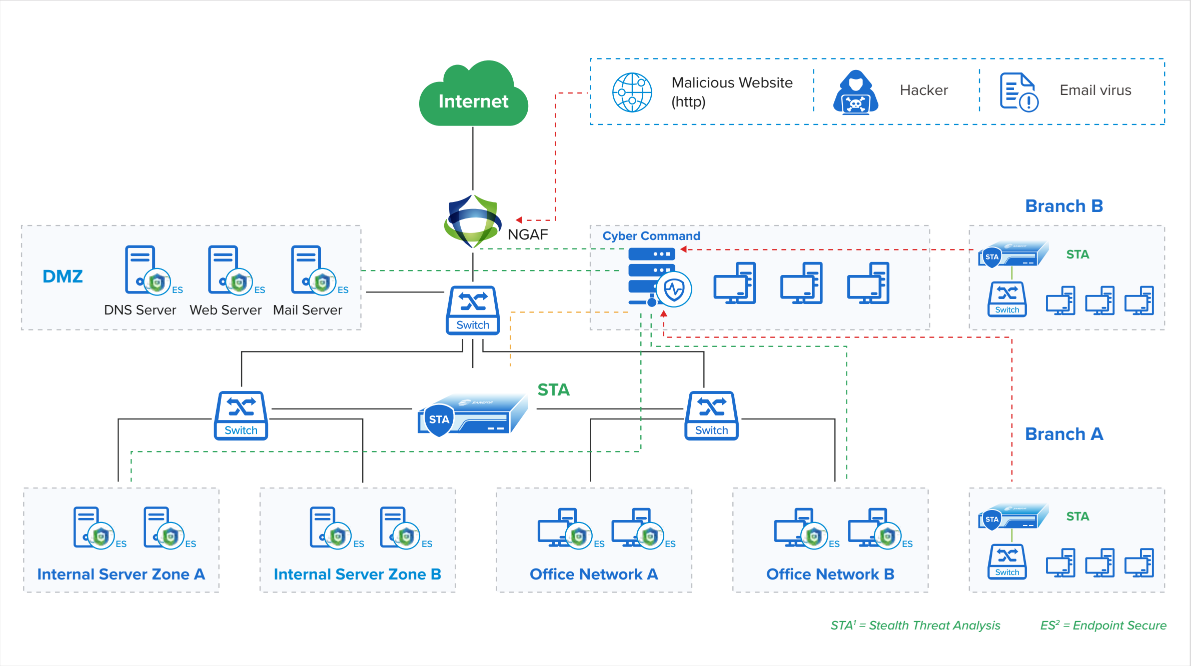
» Integrate Cyber Command Seamlessly Into Your Security Ecosystem

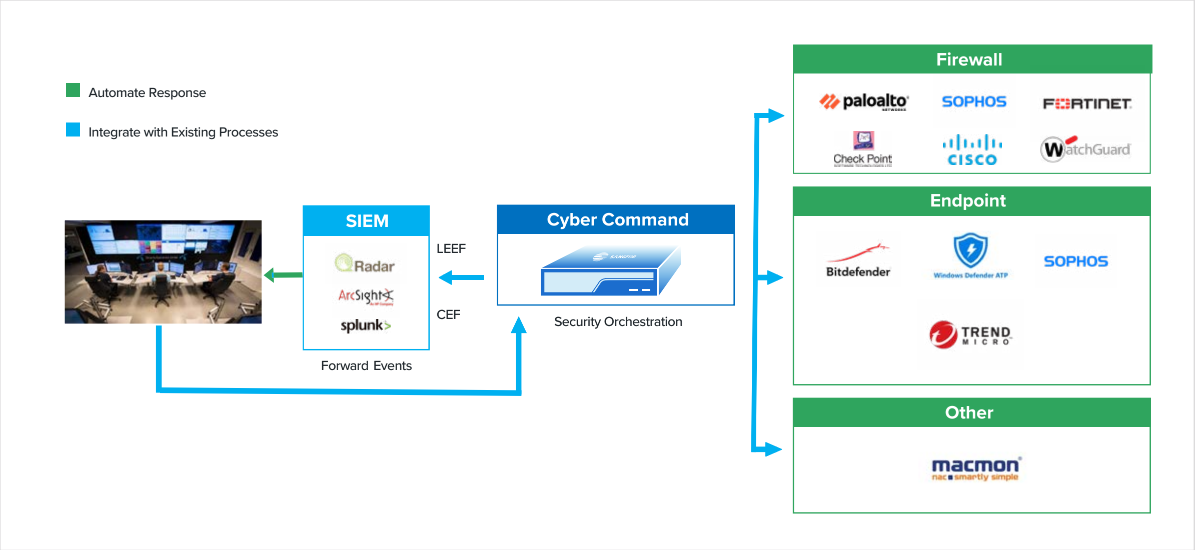
For a long time, organizations have been building complex security stacks comprising multiple security tools layered on top of each other. This approach has resulted in a range of issues, such as poor integration leading to security gaps, overlapping features, and complex management.

As such, organizations are starting to rethink their approach by adopting what is known as a security ecosystem - a comprehensive network security architecture where multiple security technologies, tools, and services are integrated to provide a unified defense against cyber threats. An integrated security ecosystem provides many advantages over a security stack, not least improved threat detection and response by having security tools operating in sync and simplified operations and maintenance through a unified management platform.

Cyber Command is designed to integrate seamlessly with other Sangfor products and services, including NGAF, Endpoint Secure, and Neural-X, as part of Sangfor's Extended Detection, Defense, and Response (XDDR) framework. Using its built-in SOAR module, Cyber Command is at the heart of this integrated system, issuing effective response actions to the other components. For example, NGAF can be instructed to block communication to and from a specific IP address or port. Endpoint Secure can provide Cyber Command with data from compromised hosts for it to extract IOCs as well as execute instructions from the NDR platform to isolate compromised hosts and scan all endpoints for the same malware.

Cyber Command also integrates with third-party firewall, endpoint protection, and SIEM products from an array of vendors, including Palo Alto, Fortinet, Sophos, Cisco, Bitdefender, Trend Micro, WatchGuard, Splunk, IBM QRadar, and more.





» Components

Cyber Command

Cyber Command is the core component of Sangfor's integrated security ecosystem, applying algorithms and machine learning to correlate and analyze data to proactively hunt for hidden threats in the form of network anomalies. It also assumes the role of the commander during incident response, issuing instructions to other security components to execute response actions aimed at containing and remediating detected threats.

Stealth Threat Analysis (STA)

Sangfor STA is the sensor used in the Cyber Command solution. It is a device that collects raw network traffic mirrored from switches and extracts traffic metadata, such as the source and destination IP addresses, protocol, port, packet size, timestamp, and other network-level data. It correlates the data into contextualized event logs and then forwards them to Cyber Command for more in-depth analysis.

Neural-X Threat Intelligence

Sangfor Neural-X is an advanced cloud-based threat intelligence and analytics platform powered by AI. It is continuously enriched with real-time threat intelligence of malicious patterns and behaviors from extensive well-established sources including VirusTotal, IBM X-Force, AlienVault OTX, EmergingThreats.net, Abuse.ch and more. Additional components like deep learning, botnet detection, sandboxing, and file reputation ensure that all Sangfor security products remain effective against advanced and emerging threats.

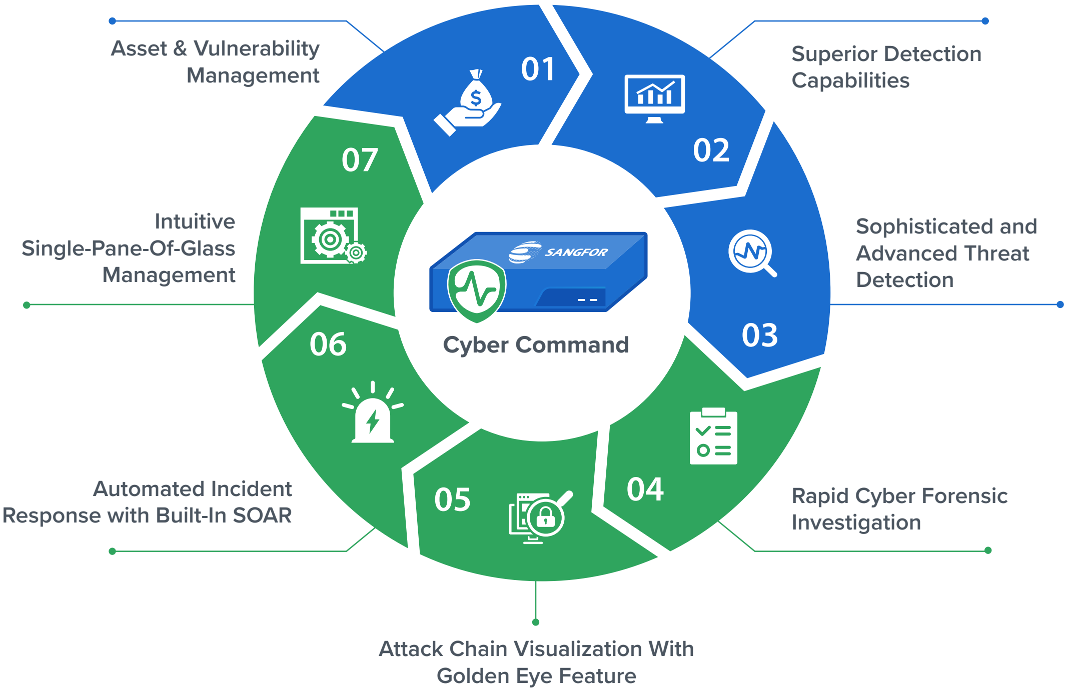
Next-Generation Application Firewall (NGAF)

Sangfor NGAF is a next-generation firewall that delivers comprehensive L2-L7 security protection to network perimeters, data centers, and web applications. When integrated with Cyber Command, NGAF provides crucial network security event information for analysis and takes instructions from Cyber Command to block Indicators of Compromise (IOCs) and isolate infected network segments.

Endpoint Secure

Sangfor Endpoint Secure is an advanced endpoint security solution that is powered by Sangfor AI malware detection engine, Engine Zero, to identify and respond to malware on PCs and servers. Endpoint Secure helps Cyber Command collect rich digital evidence to support forensic investigation while Cyber Command coordinates with Endpoint Secure to remediate endpoint threats.

» Key Features


01
Asset & Vulnerability Management
02
Superior Detection Capabilities
03
Sophisticated and Advanced Threat Detection
04
Rapid Cyber Forensic Investigation
05
Attack Chain Visualization With Golden Eye Feature
06
Automated Incident Response with Built-In SOAR
07
Intuitive Single-Pane-Of-Glass Management
SANGFOR
Cyber Command

1. Asset & Vulnerability Management

Cyber Command automatically discovers and inventories all assets in the environment, including previously unknown shadow IT assets that pose a risk to the network environment. Cyber Command also detects a range of vulnerabilities, such as uninstalled system patches, weak passwords, misconfigurations, and unencrypted traffic, empowering security teams to take prompt remedial measures before they can be exploited by threat actors.

2. Superior Detection Capabilities

Cyber Command offers unparalleled real-time detection by utilizing AI and ML algorithms, as well as the extensive MITRE ATT&CK mapping framework, which details tactics, techniques, and procedures used by adversaries. This framework enables a granular understanding of threat patterns and attack vectors. In conjunction with UEBA technology, Cyber Command monitors user and entity behavior, establishing baselines and employing machine learning for real-time anomaly detection.

3. Sophisticated and Advanced Threat Detection

Cyber Command excels at detecting advanced and sophisticated threats, including ransomware and cryptomining, by utilizing state-of-the-art AI and machine learning methodologies. These advanced algorithms persistently scrutinize network traffic, system conduct, and user interactions to recognize potential threats with real-time precision. To identify and mitigate threats effectively, Cyber Command employs a multifaceted approach that includes behavioral analysis, signature-based detection, and dynamic sandbox analysis.

4. Rapid Cyber Forensic Investigation

Elevate response efficacy with security automation by merging similar security logs into a unified event, highlighting affected assets, and conducting comprehensive forensic analysis. This methodology involves the collection of indicators of compromise (IOCs) and behavioral indicators of compromise (BIOCs) and ensuring post-incident assessment. Efficiently investigate and authenticate an extensive range of IOCs and BIOCs, which can be seamlessly downloaded and exported as needed, all from our innovative Cyber Command platform.

5. Attack Chain Visualization With Golden Eye Feature

Sangfor Cyber Command's unique Golden Eye feature provides security teams with a highly intuitive graphical representation of the attack chain displaying every stage of cyber-attacks by simply inputting the IP addresses, domains, ports, or URLs. It helps security teams with in-depth root cause analysis including tracking the entry point, source of the attack, etc, and understanding the impact and severity of attacks so that they can take the most appropriate and effective action. Users can further drill down to each step for detailed insights and remediation suggestions for remediation.

6. Automated Incident Response with Built-In SOAR

Cyber Command provides automated response with its unique built-in SOAR module. Pre-defined playbook templates allow security teams to effortlessly orchestrate incident response actions to some common threat scenarios. They can also customize responses tailored to their specific needs. With Cyber Command SOAR, organizations significantly minimize the impact caused by security incidents and liberate security teams from basic and repetitive tasks.

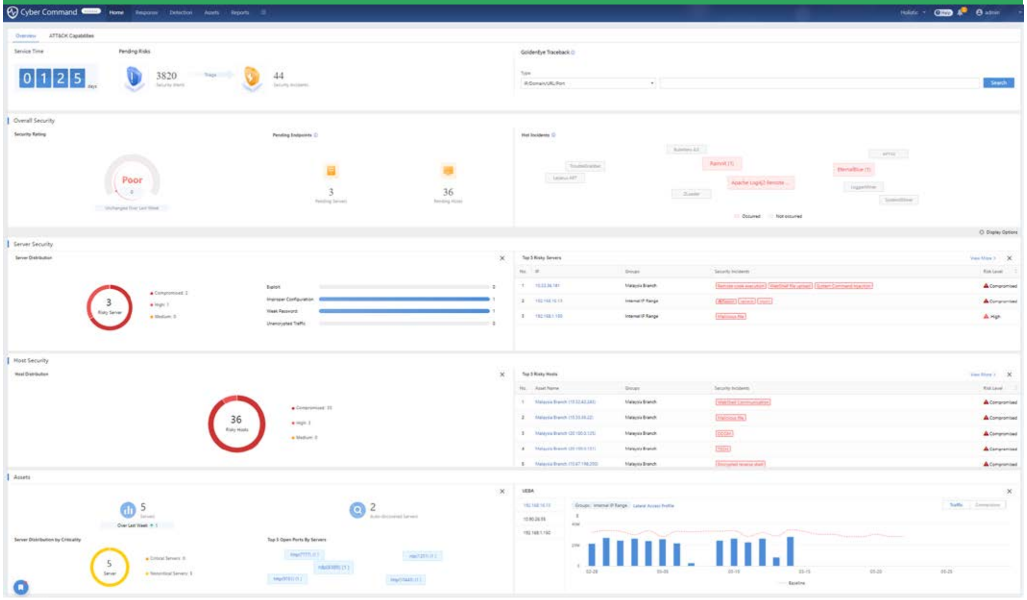
7. Intuitive Single-Pane-of-Glass Management

The Cyber Command platform offers a highly intuitive and user-friendly management console. With just a few clicks, you can manage your security operations on a single-pane-of-glass dashboard that provides a comprehensive overview of your security posture, cyber attack posture, asset posture, and vulnerability posture. This centralized view allows you to easily monitor and analyze your system's performance, identify potential threats, and take proactive measures to mitigate risk.

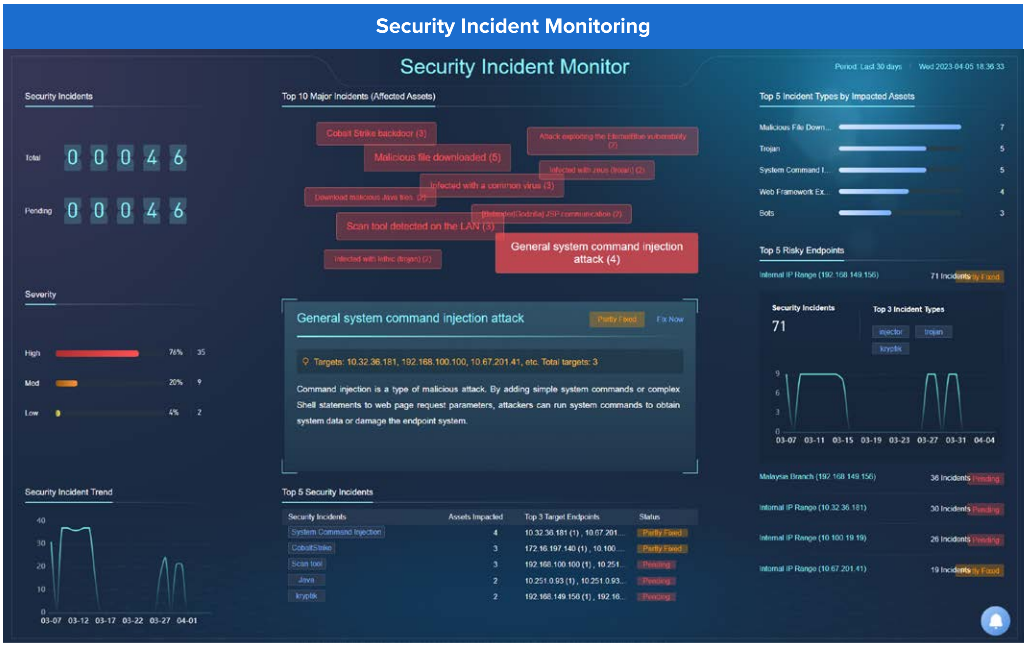
» Keep Threats at Bay with Unprecedented Visibility And Advanced Detection & Response

Cyber Command provides unprecedented real-time visibility of the entire network environment, including a graphical display of the overall security posture, security incident monitoring, outbound threat monitoring and global attack monitoring.

Security Posture Overview



Security Incident Monitoring


Security Incident Monitor
Period: Last 30 days
Wed 2023-04-05 18:36:33
Security Incidents
Total 0 0 0 4 6
Pending 0 0 0 4 6
Top 10 Major Incidents (Affected Assets)
Cobalt Strike backdoor (3)
Malicious file downloaded (5)
Attack exploiting the EternalBlue vulnerability (2)
Infected with zeus (trojan) (2)
Infected with a common virus (3)
Download malicious Java files. (2)
[Behinder]Godzilla] JSP communication (2)
Scan tool detected on the LAN (3)
General system command injection attack (4)
Infected with lethic (trojan) (2)
Severity
High 76% 35
Mod 20% 9
Low 4% 2
Top 5 Incident Types by Impacted Assets
Malicious File Down... 7
Trojan 5
System Command I... 5
Web Framework Ex... 4
Bots 3
Top 5 Risky Endpoints
Internal IP Range (192.168.149.156) 71 Incidents Partly Fixed
Security Incidents
71
Top 3 Incident Types
injector
trojan
kryptik
9
6
3
0
03-07 03-11 03-15 03-19 03-23 03-27 03-31 04-04
Malaysia Branch (192.168.149.156) 36 Incidents Pending
Internal IP Range (10.32.36.181) 30 Incidents Pending
Internal IP Range (10.100.19.19) 26 Incidents Pending
Internal IP Range (10.67.201.41) 19 Incidents Partly Fixed
Security Incident Trend
40
30
20
10
0
03-07 03-12 03-17 03-22 03-27 04-01

General system command injection attack

Partly Fixed Fix Now

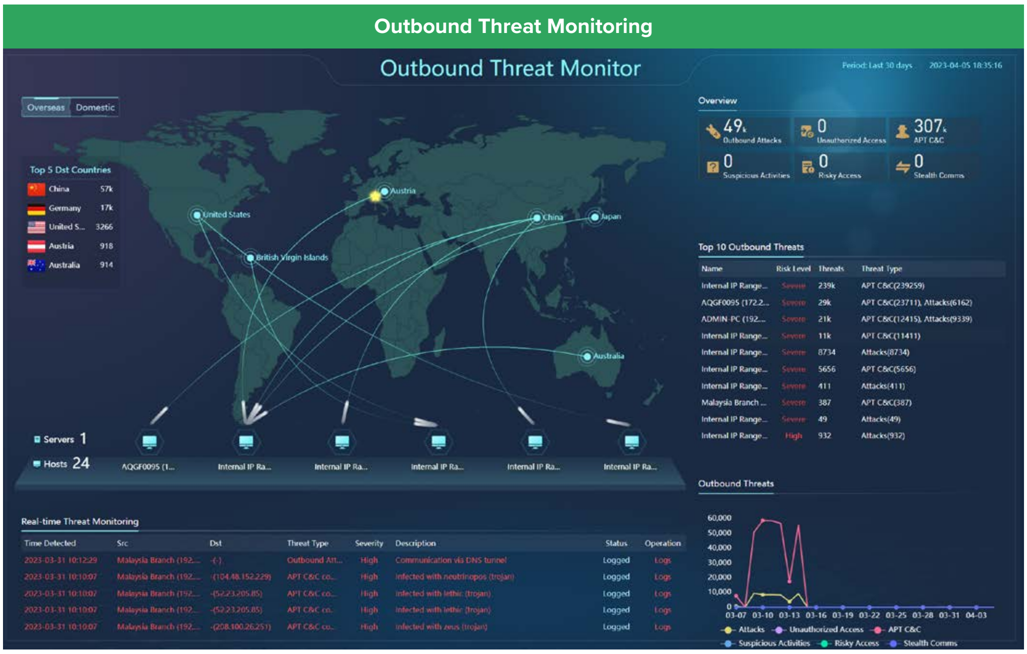
Targets: 10.32.36.181, 192.168.100.100, 10.67.201.41, etc. Total targets: 3

Command injection is a type of malicious attack. By adding simple system commands or complex Shell statements to web page request parameters, attackers can run system commands to obtain system data or damage the endpoint system.

Top 5 Security Incidents

Security Incidents	Assets Impacted	Top 3 Target Endpoints	Status
System Command Injection	4	10.32.36.181 (1) , 10.67.201...	Partly Fixed
CobaltStrike	3	172.16.197.140 (1) , 10.100...	Partly Fixed
Scan tool	3	192.168.100.100 (1) , 10.251...	Pending
Java	2	10.251.0.93 (1) , 10.251.0.93...	Pending
kryptik	2	192.168.149.156 (1) , 192.16...	Pending

Outbound Threat Monitoring



Outbound Threat Monitor

Period: Last 30 days 2023-04-05 18:35:16

Overseas | Domestic

Top 5 Dst Countries

China	57k
Germany	17k
United S...	3266
Austria	918
Australia	914

Servers 1

Hosts 24

AQGF0095 (1... | Internal IP Ra... | Internal IP Ra... | Internal IP Ra... | Internal IP Ra... | Internal IP Ra...

Overview

49k Outbound Attacks | 0 Unauthorized Access | 307k APT C&C

0 Suspicious Activities | 0 Risky Access | 0 Stealth Comms

Top 10 Outbound Threats

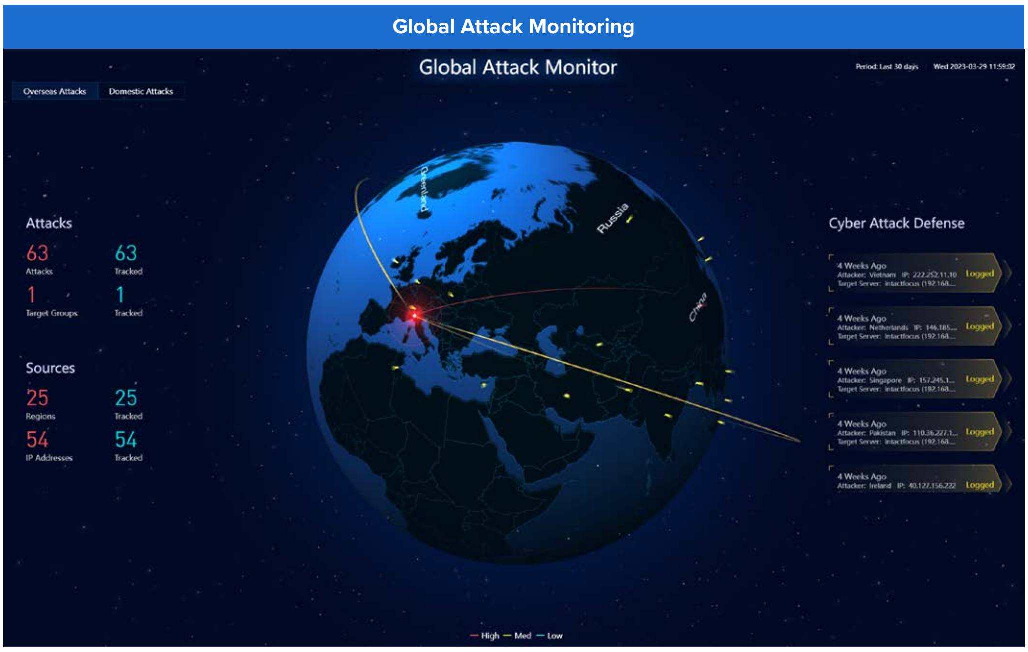
Name	Risk Level	Threats	Threat Type
Internal IP Range...	Severe	239k	APT C&C(239259)
AQGF0095 (172.2...	Severe	29k	APT C&C(23711), Attacks(6162)
ADMIN-PC (192....	Severe	21k	APT C&C(12415), Attacks(9339)
Internal IP Range...	Severe	11k	APT C&C(11411)
Internal IP Range...	Severe	8734	Attacks(8734)
Internal IP Range...	Severe	5656	APT C&C(5656)
Internal IP Range...	Severe	411	Attacks(411)
Malaysia Branch ...	Severe	387	APT C&C(387)
Internal IP Range...	Severe	49	Attacks(49)
Internal IP Range...	High	932	Attacks(932)

Real-time Threat Monitoring

Time Detected	Src	Dst	Threat Type	Severity	Description	Status	Operation
2023-03-31 10:12:29	Malaysia Branch (192....	-(-)	Outbound Att...	High	Communication via DNS tunnel	Logged	Logs
2023-03-31 10:10:07	Malaysia Branch (192....	-(104.48.152.229)	APT C&C co...	High	Infected with neutrinopos (trojan)	Logged	Logs
2023-03-31 10:10:07	Malaysia Branch (192....	-(52.23.205.85)	APT C&C co...	High	Infected with lethic (trojan)	Logged	Logs
2023-03-31 10:10:07	Malaysia Branch (192....	-(52.23.205.85)	APT C&C co...	High	Infected with lethic (trojan)	Logged	Logs
2023-03-31 10:10:07	Malaysia Branch (192....	-(208.100.26.251)	APT C&C co...	High	Infected with zeus (trojan)	Logged	Logs

Outbound Threats

Global Attack Monitoring



Global Attack Monitor

Period: Last 30 days Wed 2023-03-29 11:59:02

Overseas Attacks | Domestic Attacks

Attacks

63 Attacks | 63 Tracked

1 Target Groups | 1 Tracked

Sources

25 Regions | 25 Tracked

54 IP Addresses | 54 Tracked

Cyber Attack Defense

4 Weeks Ago
Attacker: Vietnam IP: 222.252.11.10
Target Server: intactfocus (192.168....
Logged

4 Weeks Ago
Attacker: Netherlands IP: 146.185....
Target Server: intactfocus (192.168....
Logged

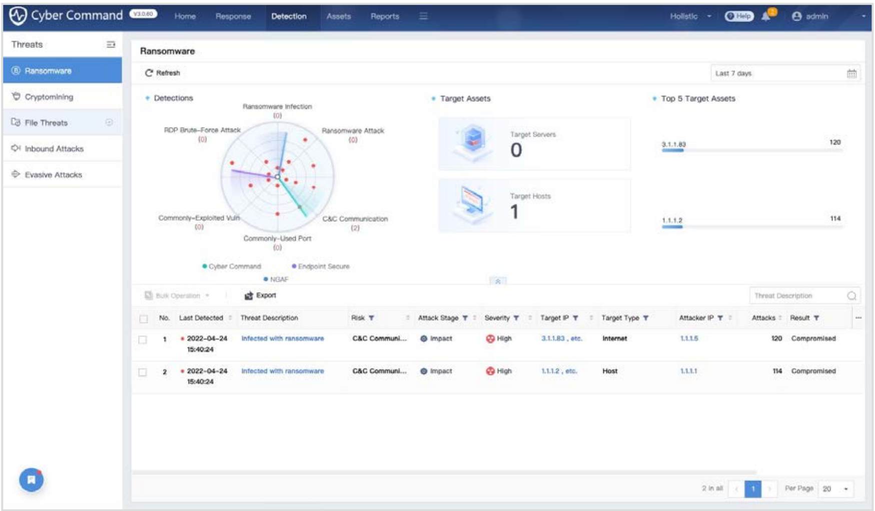
4 Weeks Ago
Attacker: Singapore IP: 157.245.1...
Target Server: intactfocus (192.168....
Logged

4 Weeks Ago
Attacker: Pakistan IP: 110.36.227.1...
Target Server: intactfocus (192.168....
Logged

4 Weeks Ago
Attacker: Ireland IP: 40.127.156.222
Logged

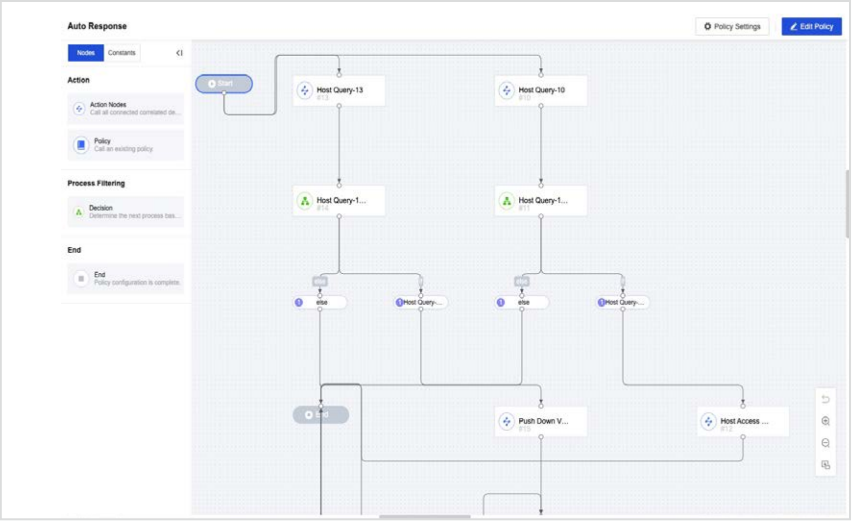
Cyber Command protects organizations from sophisticated cyber threats with multiple detection engines and advanced threat detection techniques, while built-in SOAR ensures immediate incident response to detected threats. Full MITRE ATT&CK mapping further provides detailed insights for informed decision-making.

Advanced Threat Detection

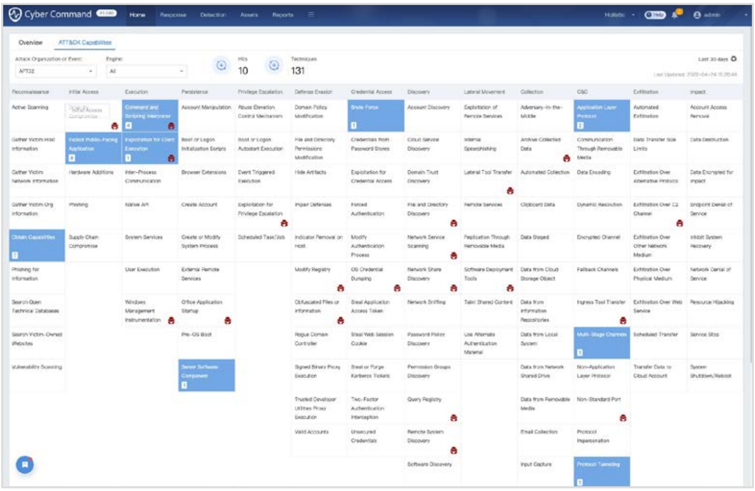


No.	Last Detected	Threat Description	Risk	Attack Stage	Severity	Target IP	Target Type	Attacker IP	Attacks	Result
1	2022-04-24 15:40:24	Infected with ransomware	C&C Communi...	Impact	High	3.1.1.83 , etc.	Internet	1.1.1.5	120	Compromised
2	2022-04-24 15:40:24	Infected with ransomware	C&C Communi...	Impact	High	1.1.1.2 , etc.	Host	1.1.1.1	114	Compromised

Auto Response with SOAR

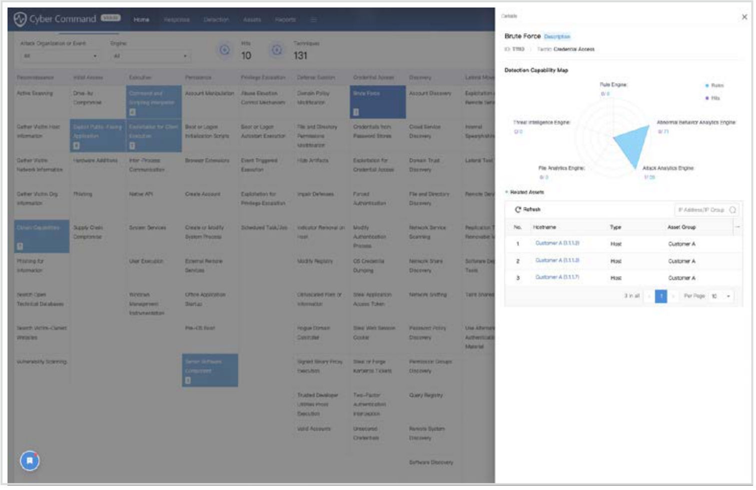


MITRE ATT&CK Mapping



Attack Organization or Event: APT32
Engine: All
Hits 10
Techniques 131
Last 30 days
Last Updated: 2022-04-24 11:20:48

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	C&C	Exfiltration	Impact
Active Scanning	Drive-by Compromise	Command and Scripting Interpreter 4	Account Manipulation	Abuse Elevation Control Mechanism	Domain Policy Modification	Brute Force 1	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol 2	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Exploit Public-Facing Application 8	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	File and Directory Permissions Modification	Credentials from Password Stores	Cloud Service Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Network Information	Hardware Additions	Inter-Process Communication	Browser Extensions	Event Triggered Execution	Hide Artifacts	Exploitation for Credential Access	Domain Trust Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Org Information	Phishing	Native API	Create Account	Exploitation for Privilege Escalation	Impair Defenses	Forced Authentication	File and Directory Discovery	Remote Services	Clipboard Data	Dynamic Resolution	Exfiltration Over C2 Channel	Endpoint Denial of Service
Obtain Capabilities 1	Supply Chain Compromise	System Services	Create or Modify System Process	Scheduled Task/Job	Indicator Removal on Host	Modify Authentication Process	Network Service Scanning	Replication Through Removable Media	Data Staged	Encrypted Channel	Exfiltration Over Other Network Medium	Inhibit System Recovery
Phishing for Information		User Execution	External Remote Services		Modify Registry	OS Credential Dumping	Network Share Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium	Network Denial of Service
Search Open Technical Databases		Windows Management Instrumentation	Office Application Startup		Obfuscated Files or Information	Steal Application Access Token	Network Sniffing	Taint Shared Content	Data from Information Repositories	Ingress Tool Transfer	Exfiltration Over Web Service	Resource Hijacking
Search Victim-Owned Websites			Pre-OS Boot		Rogue Domain Controller	Steal Web Session Cookie	Password Policy Discovery	Use Alternate Authentication Material	Data from Local System	Multi-Stage Channels 1	Scheduled Transfer	Service Stop
Vulnerability Scanning			Server Software Component 1		Signed Binary Proxy Execution	Steal or Forge Kerberos Tickets	Permission Groups Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Transfer Data to Cloud Account	System Shutdown/Reboot
					Trusted Developer Utilities Proxy Execution	Two-Factor Authentication Interception	Query Registry		Data from Removable Media	Non-Standard Port		
					Valid Accounts	Unsecured Credentials	Remote System Discovery		Email Collection	Protocol Impersonation		
							Software Discovery		Input Capture	Protocol Tunneling 1		


Details
×
Description
Rule Engine: 0/0
Threat Intelligence Engine: 0/0
Abnormal Behavior Analytics Engine: 0/71
File Analytics Engine: 0/0
Attack Analytics Engine: 1/26
Rules
Hits
Refresh
IP Address/IP Group

Brute Force

ID: T1110 | Tactic: Credential Access

Detection Capability Map

Related Assets

No.	Hostname	Type	Asset Group
1	Customer A (1.1.1.2)	Host	Customer A
2	Customer A (1.1.1.3)	Host	Customer A
3	Customer A (1.1.1.7)	Host	Customer A

3 in all 1 Per Page 10

» How is Cyber Command Different?

Superior Threat Detection and Analysis	
AI-Driven Threat Detection and Analysis	Cyber Command leverages advanced AI algorithms and machine learning techniques to continuously learn and adapt to your threat landscape, enabling you to accurately identify and analyze a wide range of threats like ransomware, zero-day attacks, APTs, and cyptomining. Cyber Command is equipped with Sangfor's Neural-X threat intelligence and analytics platform, which ensures that it is continuously enriched with real-time threat intelligence, patterns, and behaviors from extensive sources to remain effective against advanced and emerging threats.
User and Entity Behavior Analytics (UEBA)	Cyber Command integrates UEBA technology to quickly identify any irregularities or network anomalies and detect anomalous behavior patterns from both users and network entities such as devices, applications, and services at no additional cost. This enables the platform to establish dynamic baselines of normal behavior and accurately identify anomalies that may indicate potential threats.
Full MITRE ATT&CK Coverage	Cyber Command provides a comprehensive mapping of its detection and response capabilities to the MITRE ATT&CK framework, providing organizations with extensive coverage of adversary techniques across all stages of the attack lifecycle, from initial reconnaissance to data exfiltration, giving security teams the visibility and insight to prioritize response actions and allocate resources more effectively.

More In-Depth Threat Hunting and Forensic Investigation	
Business Impact Analysis	Cyber Command offers a built-in threat-hunting model that includes Business Impact Analysis (BIA) that outperforms other NDR solutions. BIA helps you understand asset prioritization and the business impact should assets be compromised. This gives you a clear picture of the potential impact on the organization's network and assets, enabling you to prepare in advance with recovery strategies.
Revolutionary Golden Eye Feature	Cyber Command leverages Sangfor's unique "Golden Eye" feature, designed to empower security teams with the ability to delve into the entire attack lifecycle with ease. By simply inputting the IP, Domain, URL, or Port, you gain access to a comprehensive, real-time timeline view that reveals the attacker's entry point and attack path. It offers in-depth root-cause analysis that goes beyond the basic security incident reporting typically provided by other vendors.
Cyber Forensic Investigation	Elevate the investigation process with streamlined workflows that take you from detection to context and evidential insights with just a few clicks. Rapidly research and validate a wide variety of indicators of compromise (IOCs) and behavior indicators of compromise (BIOCs) that are easily downloadable and exportable whenever and wherever you need from our innovative Cyber Command platform.

Truly Automated and Integrated Incident Response	
Built-In SOAR Module	Cyber Command revolutionizes NDR solutions with its built-in SOAR module at no additional cost, providing automated incident response to help organizations minimize the potential impact of detected threats and significantly reduce the workload of the security team by automatically generating and executing targeted response actions. Cyber Command's SOAR module comes with incident response playbooks tailored for some common threat scenarios. To give you greater flexibility and control over your incident response strategies, our playbooks can be easily customized by security teams to align with your organization's unique requirements and policies, and we enable you to clone or copy our built-in templates and execute them in your existing security tools.
Fully Integrated Security Platform	Sangfor is one of the few security vendors that truly integrate security products into a holistic security platform. Sangfor XDDR (Extended Detection, Defense, and Response) seamlessly integrates Cyber Command, NGAF, IAG, and Endpoint Secure to break down security silos and provide end-to-end protection across your entire network infrastructure. Cyber Command can also be integrated with prestigious 3rd party security solutions from industry giants like Cisco, Trend Micro, Sophos, Bitdefender, Microsoft, Fortinet, Palo Alto, and more to deliver rapid automated incident response without disrupting your established security framework and complicating your configurations.

» The Business Values of Cyber Command

1

Prevent Damaging Impact

The devastating impacts of cyber-attacks can have significant repercussions for businesses, ranging from data loss, financial loss, and reputation damage to compliance violations. To mitigate these risks, Cyber Command provides an advanced defense system that proactively detects and prevents cyber threats before they can inflict harm.

2

Streamline Security Operations

Cyber Command correlates data from across the network to produce high-fidelity alerts, significantly reducing the number of false positives that lead to alert fatigue and inefficiency. Security teams can further automate routine tasks to reduce operations and maintenance workload, enabling them to focus on critical tasks that create value.

3

Optimize Security Spending

Cyber Command is a cost-effective NDR solution that includes many features that other vendors typically require additional subscriptions for, such as User and Entity Behavior Analytics (UEBA), threat intelligence, and SOAR, providing organizations with a comprehensive solution that enhances their cybersecurity posture without breaking the bank.

4

Embrace Digital Transformation

Security concerns are one of the biggest showstoppers for organizations when it comes to adopting new technologies and rolling out new digital business. Backed by Cyber Command, organizations rest assured that any security threats will be promptly detected and dealt with, giving them the confidence to go big in their digital transformation.

» Experience The Gold Standard of Cyber Security

Top 3 APAC Security Vendor

by revenue based on 2021 Gartner Market Share: Security Software

Visionary Vendor

in 2022 Gartner Magic Quadrant for Network Firewalls for Sangfor NGAF

World's 4th Largest NDR Vendor

by revenue based on 2021 Gartner Market Share: Enterprise Network Equipment

Representative Vendor for NDR

in 2022 Gartner Market Guide for Network Detection and Response

ICSA Labs Firewall Certification

Sangfor NGAF meets all of ICSA Labs' corporate and baseline firewall requirements

AV-Test Certification

Sangfor Endpoint Secure receives Top Award for Windows antivirus software for business users

AAA Rating from CyberRatings

Sangfor NGAF achieves the highest security effectiveness at 99.7%

Recognized by VirusTotal

Sangfor Engine Zero AI Malware Detection Engine included in list of VirusTotal vendors

Cybersecurity Excellence Awards

Gold Winner for the Most Innovative Cybersecurity Company & Best Cybersecurity Company 2022

InfoSec Awards

Winner of Hot Company Security Company of the Year 2022

Call Us

With our comprehensive suite of offerings, you'll find the perfect one to take your organization to the next level.

Global Hotline: +60 12 711 7511 (or +60 12 711 7129) **Email:** marketing@sangfor.com

Contact us today through our website to get more information!

Free POC

Ensure your organization's resilience with a FREE Cyber Command POC.
Take this opportunity to evaluate and improve your security posture!

SANGFOR CYBER COMMAND

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