



**SANGFOR**



**Endpoint  
Secure**

# Endpoint Secure

## Endpoint Security

### The Future of Endpoint Security

Certification of the Best Windows Antivirus Solution  
and "TOP PRODUCT" Award by AV-Test



Recommended Windows Protection by



**Microsoft**





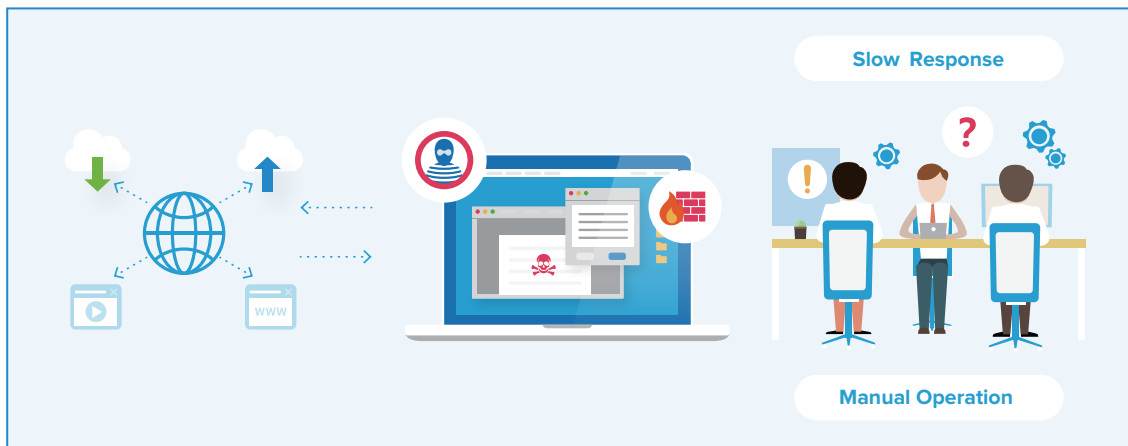
## Enterprise-level endpoints face serious security challenges in a new era

Enterprise LAN endpoints and data have significant value to cyber criminals, putting endpoints, servers, software and hardware at serious risk of attack from complex and sophisticated viruses, ransomware and various other propagation modes. These serious endpoint security challenges as well as increasingly strict regulations on protection, management and applications make proactive endpoint protection critical.



## Manual operation and maintenance increases the cost of defense

Traditional endpoint security products operate on common policies and characteristics, often based on more traditional organizational rules and operation regulations, designed to defend against threats from known sources. Organizations utilizing this more traditional approach to security, yet suffering attack from more complex and advanced threats, often experience an exponential increase in labor costs, while specialized enterprise O&M personnel have inadequate experience to effectively respond to the threat.



## Feature matching response to viruses is inadequate protection to new attack methods

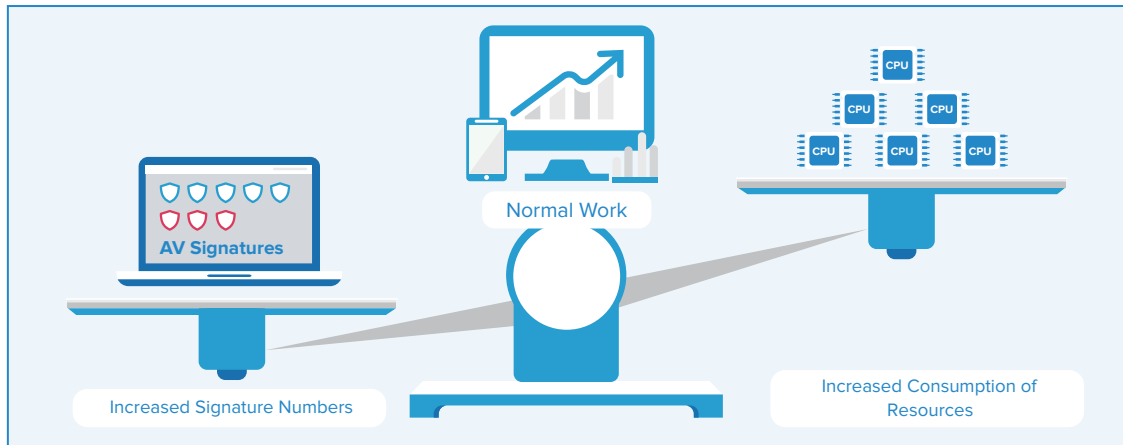
In environments where there is constant risk from advanced threat, virus prevention methods utilizing the more passive antivirus database identification and response methods are often penetrated by newer viruses and ransomware. In addition, the limited capacity of local feature databases often fails to meet basic protection requirements against unknown and even some known viruses.





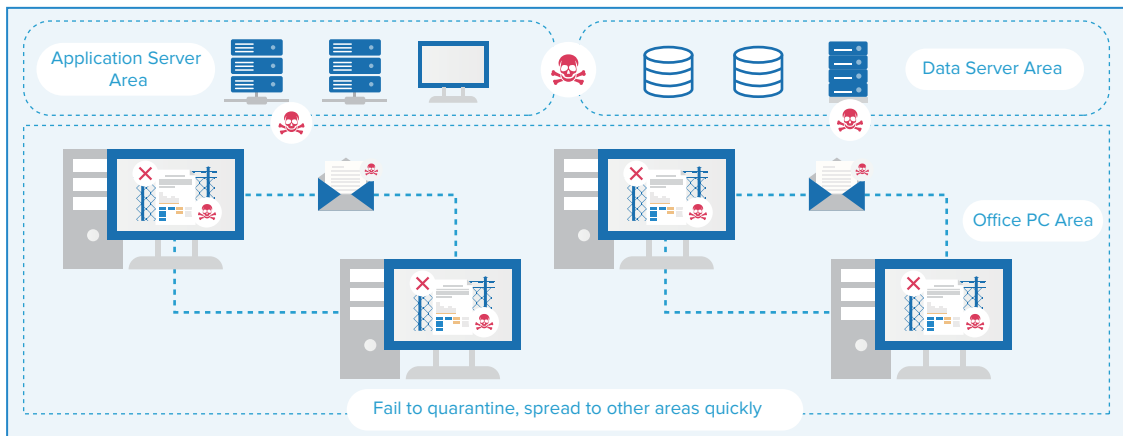
## High-capacity antivirus feature databases lead to increased host computing resource costs

The gradual increase in quantity of antivirus feature databases increases the cost of endpoint storage and computing resources. When threat defense monopolizes a significant amount of work hours and employee effort, users are unable to focus on optimization scenarios such as shifting to the cloud.



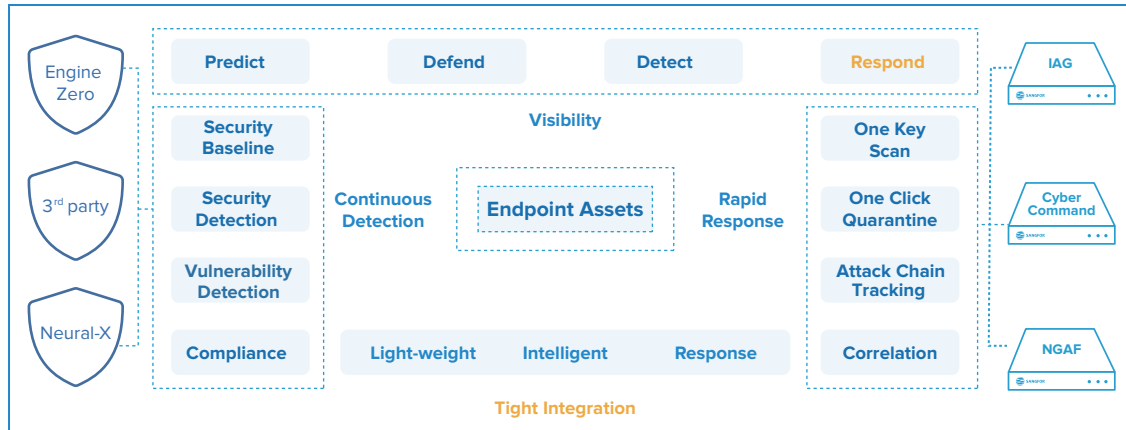
## Outdated virus protection is incompatible with new propagation modes and virus environments

Virus killing based on the file isolation method is outdated, with failure allowing a single-point threat to spread quickly. New viruses and propagation modes are often able to bypass traditional antivirus products, which are not designed to adapt to new threats and environments.

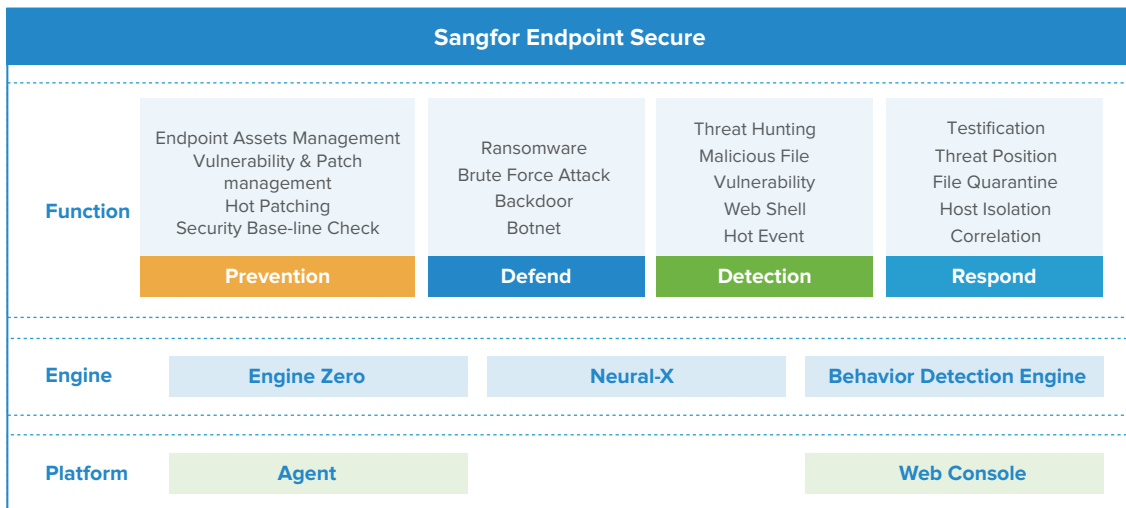


## Sangfor Endpoint Secure

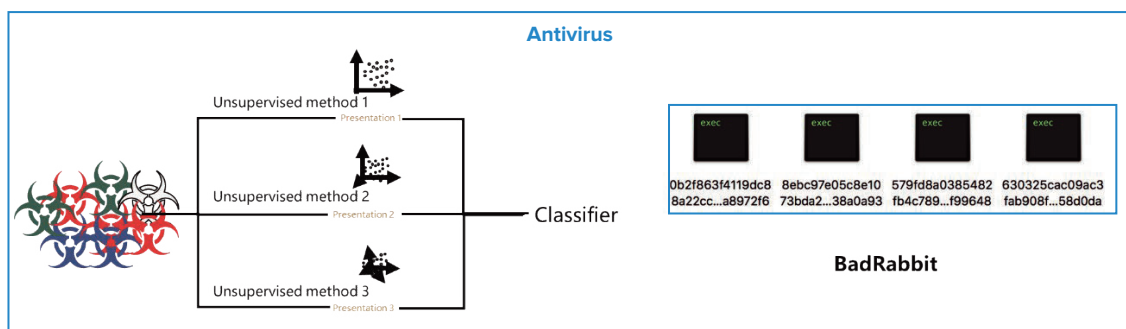
Sangfor's Endpoint Protection and Response platform (Endpoint Secure) provides the endpoint with a more detailed isolation policy, enabling more accurate search and destroy capabilities, sustainable detection capabilities and faster processing capabilities including prevention, defense, detection and response. Endpoint Secure is constructed through cloud linkage and coordination, threat information sharing and multi-level response mechanisms. Advanced threat response is immediate, with Endpoint Secure providing users with assistance dealing with any endpoint security problems by way of its new, light-weight, intelligent and instantaneous endpoint security system.



## ● Architecture of Endpoint Secure ●



## Application Scenarios



### Risk Scenario:

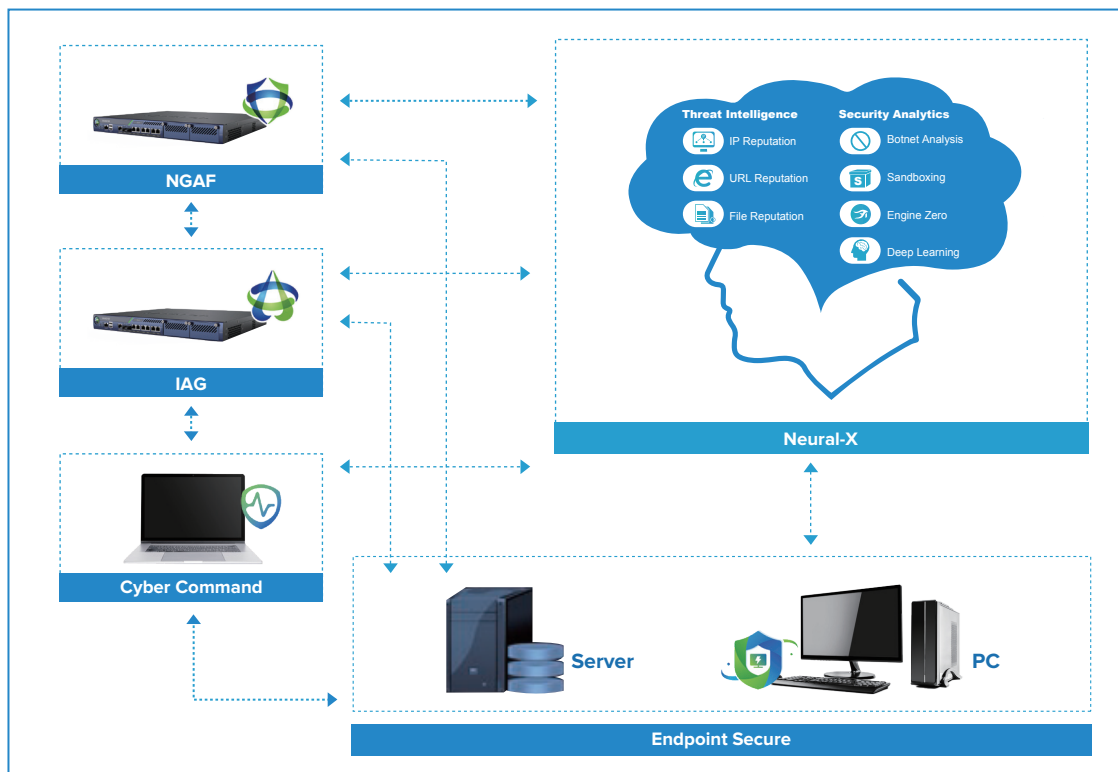
Internal endpoints are widely deployed across multiple office networks. Attacks from unknown malware or ransomware significantly affect business critical applications, compromising the security of core organization data. Risk increases due to:

1. The lack of resources available to detect and respond to advanced and unknown threats prevent proactive defense.
2. Manual system management being inadequate when dealing with fast-moving and unknown threats - exposing the system to numerous attack surfaces.

### Endpoint Secure Application Effects:

1. An AI core and the supplementation of the reputation database, gene and behavior analysis functions provides a 100% threat defense system capable of immediate and comprehensive detection and prevention.
2. Multi-dimensional innovative micro-segmentation technology and intelligent coordination of cloud-pipe-device functions provide immediate identification and response and comprehensive threat neutralization.

### ● Device Linkage ●



### Risk Scenario:

While most internal infrastructure utilizes firewall, intrusion prevention and other various border gateway devices, many gateway devices perform their own independent functions, preventing cohesive and effective security defense.

1. Gateway devices acting independently to prevent malicious attack means that once the boundary is breached, the malicious attacker propagates rapidly and can't be controlled.
2. Even if the external threat is known, effective shared linkage with the endpoint cannot be formed and endpoint control cannot be achieved.

### Application Effects:

1. Endpoint Secure can be coordinated and linked with Sangfor Neural-X, NGAF, IAG and Cyber Command to form a defense structure covering the cloud, boundary and endpoint, sharing the internal and external threat information in real time.
2. The Endpoint Secure intelligent linkage mechanism shares external threat information in a timely manner, allowing automatic response.



## Advantages and Characteristics

### ● New Artificial Intelligent Antivirus Engine ●

Unlike traditional antivirus engines, Engine Zero has adopted artificial intelligence (AI) featureless technology, enabling effective identification of unknown viruses and variants, including those unlisted in the antivirus database.

Official performance testing conducted by AV-TEST awarded Sangfor Endpoint Secure a perfect 6 for Protection, Performance, and Usability, earning it the AV-TEST "TOP PRODUCT" award.



**Sangfor  
Engine Zero**  
Sangfor Anti-Malware Engine

Artificial Intelligence Based Non-Signature Engine  
Detect Unknown Malware Accurately

### Complete Antivirus Protection for Business PCs:

	Industry average	March	April
<b>Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing)</b> 408 samples used	99.8%	100%	100%
<b>Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set)</b> 21,784 samples used	100%	100%	100%
<b>Protection Score</b>	6.0/6.0		

Figure 1. Sangfor Endpoint Secure Protect test results for Protection










### Antivirus Solution for Business Efficiency:

	Industry average	Standard PC	Industry average	High end PC
<b>Slowing-down when launching popular websites</b> 60 websites visited	13%	7%	12%	10%
<b>Slower download of frequently-used applications</b> 25 downloaded files	3%	0%	2%	2%
<b>Slower launch of standard software applications</b> 63 test cases applied	12%	6%	12%	7%
<b>Slower installation of frequently-used applications</b> 25 installed applications	22%	16%	20%	12%
<b>Slower copying of files (locally and in a network)</b> 9,850 files copied	5%	1%	4%	0%
<b>Performance Score</b>	6.0/6.0			

Figure 2. Sangfor Endpoint Secure Protect test results for Performance

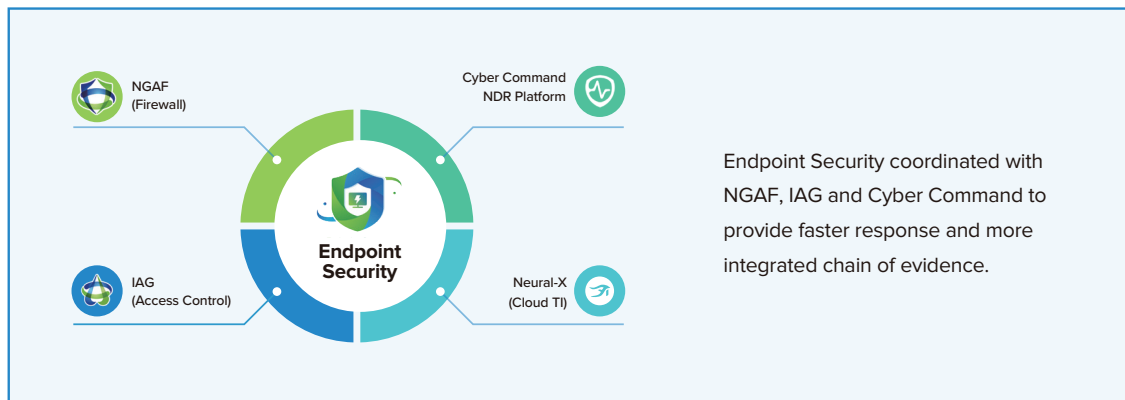
## • High Compatibility •

Continuously protect the End of Support (EOS) OS system and provide hot patching function to protect None-Restart server.


 Windows	 macOS	 Ubuntu	 Redhat	 CentOS	 Debian	 SuSE	 Oracle Linux	 Other
<ul style="list-style-type: none"> <li>• Windows XP SP3 *</li> <li>• Windows 7 *</li> <li>• Windows 8 *</li> <li>• Windows 8.1 *</li> <li>• Windows 10</li> <li>• Windows 11</li> <li>• Windows Server 2003 SP2 *</li> <li>• Windows Server 2008 *</li> <li>• Windows Server 2008R2 *</li> <li>• Windows Server 2012</li> <li>• Windows Server 2016</li> <li>• Windows Server 2019</li> </ul>	<ul style="list-style-type: none"> <li>• macOS 10.13</li> <li>• macOS 10.14</li> <li>• macOS 10.15</li> <li>• macOS 11.x</li> <li>• macOS 12.x</li> </ul>	<ul style="list-style-type: none"> <li>• Ubuntu 10</li> <li>• Ubuntu 11</li> <li>• Ubuntu 12</li> <li>• Ubuntu 13</li> <li>• Ubuntu 14</li> <li>• Ubuntu 16</li> <li>• Ubuntu 18</li> <li>• Ubuntu 20</li> </ul>	<ul style="list-style-type: none"> <li>• RHEL 5</li> <li>• RHEL 6</li> <li>• RHEL 7</li> <li>• RHEL 8</li> </ul>	<ul style="list-style-type: none"> <li>• CentOS 5</li> <li>• CentOS 6</li> <li>• CentOS 7</li> <li>• CentOS 8</li> </ul>	<ul style="list-style-type: none"> <li>• Debian 6</li> <li>• Debian 7</li> <li>• Debian 8</li> <li>• Debian 9</li> </ul>	<ul style="list-style-type: none"> <li>• SUSE 12</li> <li>• SUSE 11.X</li> <li>• SUSE 15.X</li> </ul>	<ul style="list-style-type: none"> <li>• Oracle Linux 5</li> <li>• Oracle Linux 6</li> <li>• Oracle Linux 7</li> <li>• Oracle Linux 8</li> </ul>	<ul style="list-style-type: none"> <li>• Red Flag Asianux Server 4</li> <li>• NeoKylin 5</li> <li>• NeoKylin 6</li> <li>• NeoKylin 7</li> <li>• KylinOS 4</li> <li>• Ubuntu Kylin 18</li> </ul>

\* The following Windows versions are no longer supported or receiving security updates from Microsoft.

## • Multi-dimensional Linkage •



## • Advanced threat analysis & respond with MITRE ATT&CK® •

ATT&CK™ Matrix 										
MITRE Tactic: 5    MITRE Technique: 11										
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
	Command and Scri... 1	Scheduled Task/Job 3 Valid Accounts 1 Event Triggered Exe... 1		Masquerading 1 Obfuscated Files or ... 1 BITS Jobs 1 Impair Defenses 1					Ingress Tool Transfer 1 Application Layer P... 2	Resource Hijacking 1

Faster and more accurately find the threats in the endpoint.



## Edition and Features

	Feature/Module	Essential Edition	Ultimate Edition
Prevention	Vulnerability Scan	✓	✓
	Remediation	✓	✓
	Security Compliance Check	✓	✓
	Asset Inventory	✓	✓
	Asset Discovery	✓	✓
	Micro-Segmentation		✓
	Hot Patching		✓
	TOTP Authentication	✓	✓
	Endpoint Behavior Data & Log Collection		✓
Prevention	Realtime File Monitoring	✓	✓
	Ransomware Honeypot	✓	✓
	Ransomware Protection	✓	✓
	Ransomware Defense	✓	✓
	Fileless Attack Protection		✓
	End-of-Support Windows System Protection	✓	✓
	RDP Secondary Authentication (Anti-Ransomware)		✓
	Trusted Processes (Anti-Ransomware)		✓
	Key Directory Protection (Anti-Ransomware)		✓
Detection	Malicious File Detection	✓	✓
	APT Detection	✓	✓
	Brute-Force Attack Protection	✓	✓
	Coordinated Malware Response with XDDR		✓
	WebShell Detection		✓
Response	File Quarantine	✓	✓
	Endpoint Isolation	✓	✓
	File Remediation	✓	✓
	Virus Mitigation	✓	✓
	Extended Detection, Defense and Response (XDDR)		✓
	Threat Investigation		✓
Maintenance	Script File Upload	✓	✓
	USB Control	✓	✓
	Unauthorized Outbound Access Detection	✓	✓
	Remote Support	✓	✓

Ultimate Edition is recommended for device linkage scenario and advanced protection.

# SANGFOR ENDPOINT SECURE

## 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



<https://twitter.com/SANGFOR>



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



<https://www.facebook.com/Sangfor>



<https://www.instagram.com/sangfortechologies/>



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



[www.sangfor.com](http://www.sangfor.com)

**Sales:** [sales@sangfor.com](mailto:sales@sangfor.com)

**Marketing:** [marketing@sangfor.com](mailto:marketing@sangfor.com)

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