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

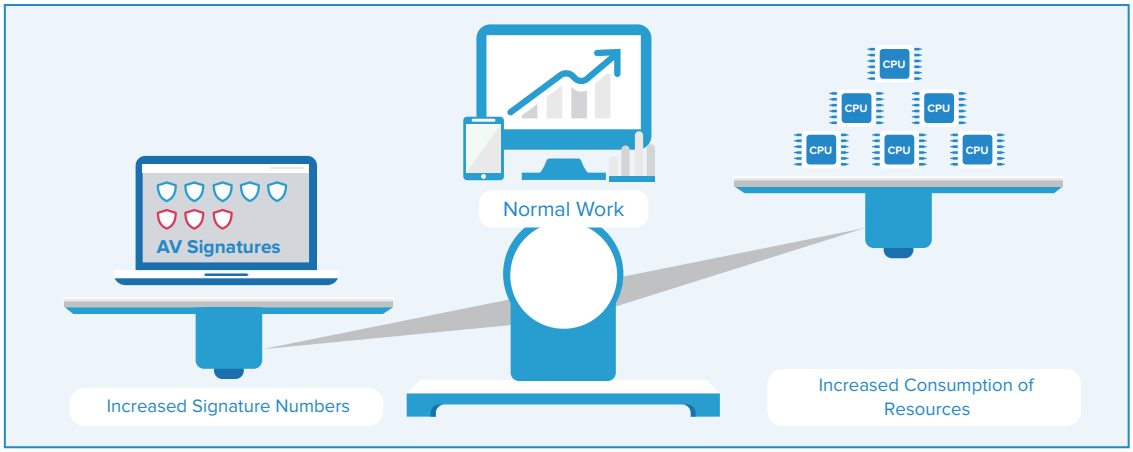
Traditional endpoint security products operate on common policies and characteristics, often based on more traditional organizational rules and operation regulations, designed to defend against threats from known sources. Organizations utilizing this more traditional approach to security, yet suffering 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.

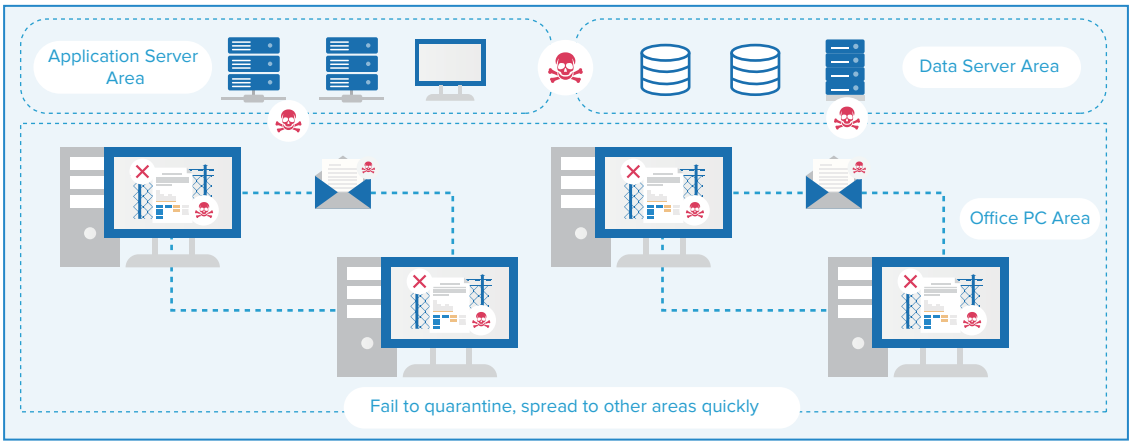
High-capacity antivirus feature databases lead to increased host computing resource costs

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



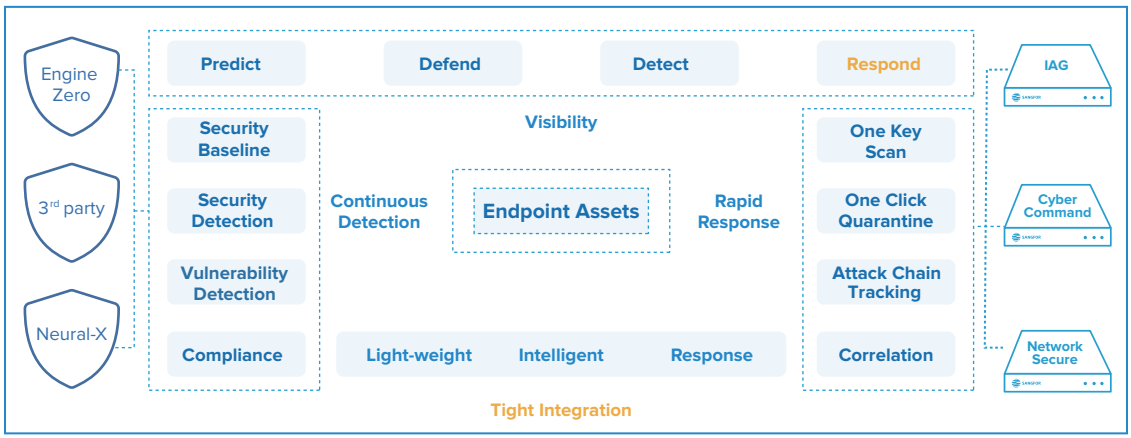
Outdated virus protection is incompatible with new propagation modes and virus environments

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.

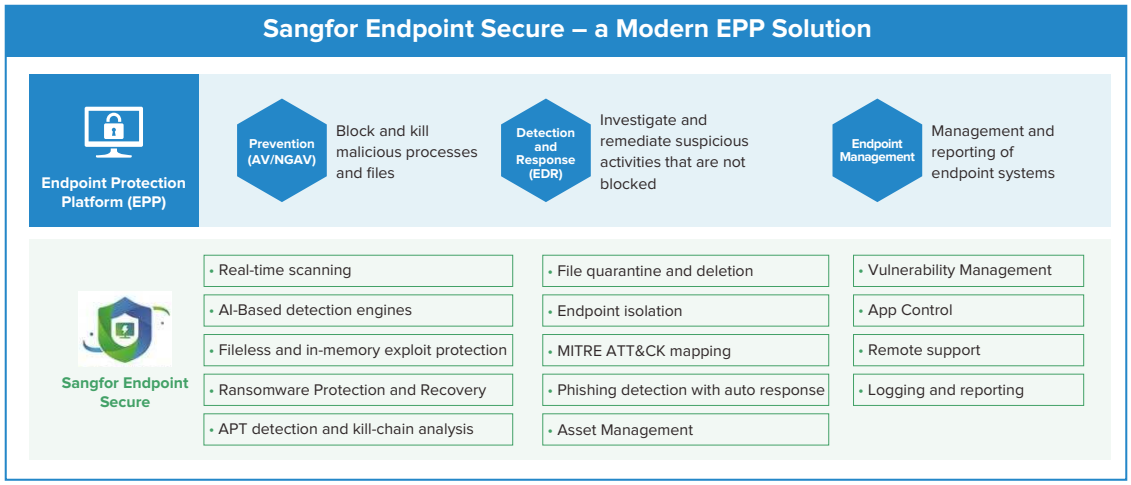


Sangfor Endpoint Secure

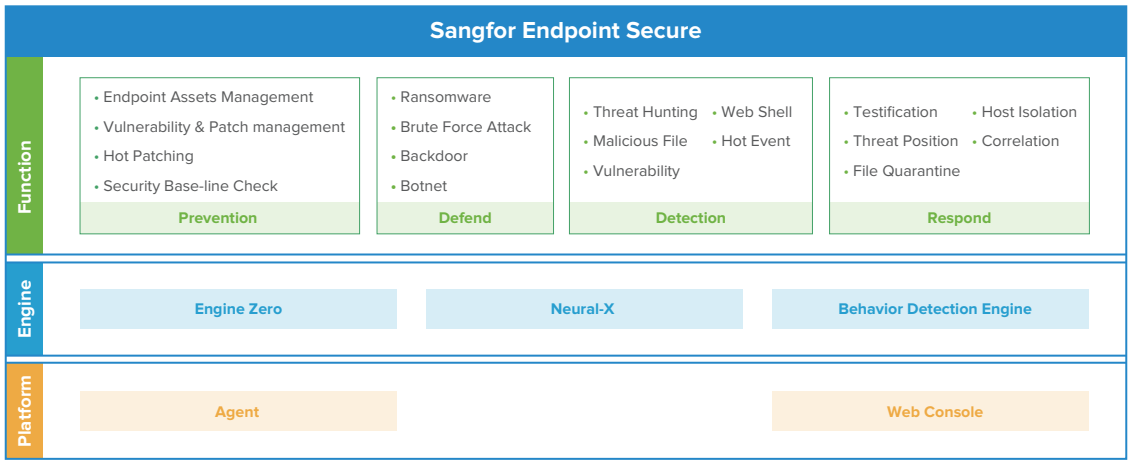
Sangfor's Endpoint Protection and Response platform (Endpoint Secure) provides the endpoint with a more detailed isolation policy, enabling more accurate search and destroy capabilities, sustainable detection capabilities and faster processing capabilities including prevention, defense, detection and 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.



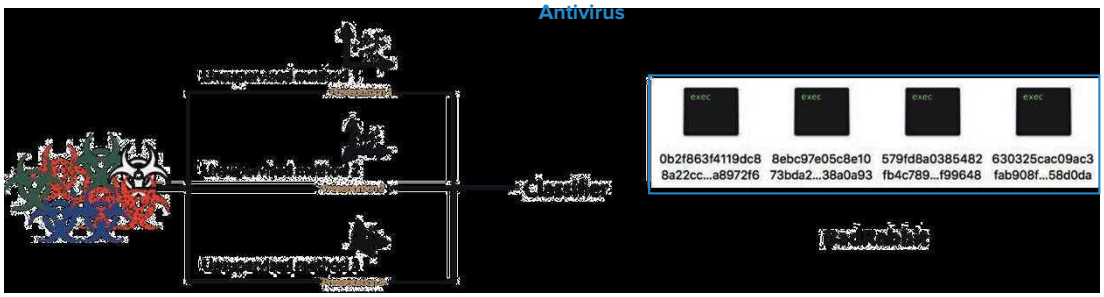
Endpoint security has evolved over the years from providing preventive capabilities, namely antivirus (AV) and next-generation AV, to a solution capable of correlating security events and performing investigation and response (EDR). Sangfor Endpoint Secure is a Modern Endpoint Protection Platform (EPP) that integrates NGAV, EDR, and endpoint management capabilities into a single solution. With Endpoint Secure, organizations can take preventive measures by scanning their endpoints for risky configurations and vulnerabilities, conduct investigations when security threats occur, and respond quickly with an easy-to-use solution. Endpoint Secure's endpoint management capabilities include vulnerability & patch management to mitigate risks and improve compliance. Centralized policy management and remote troubleshooting further help operations teams streamline and simplify O&M.



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:

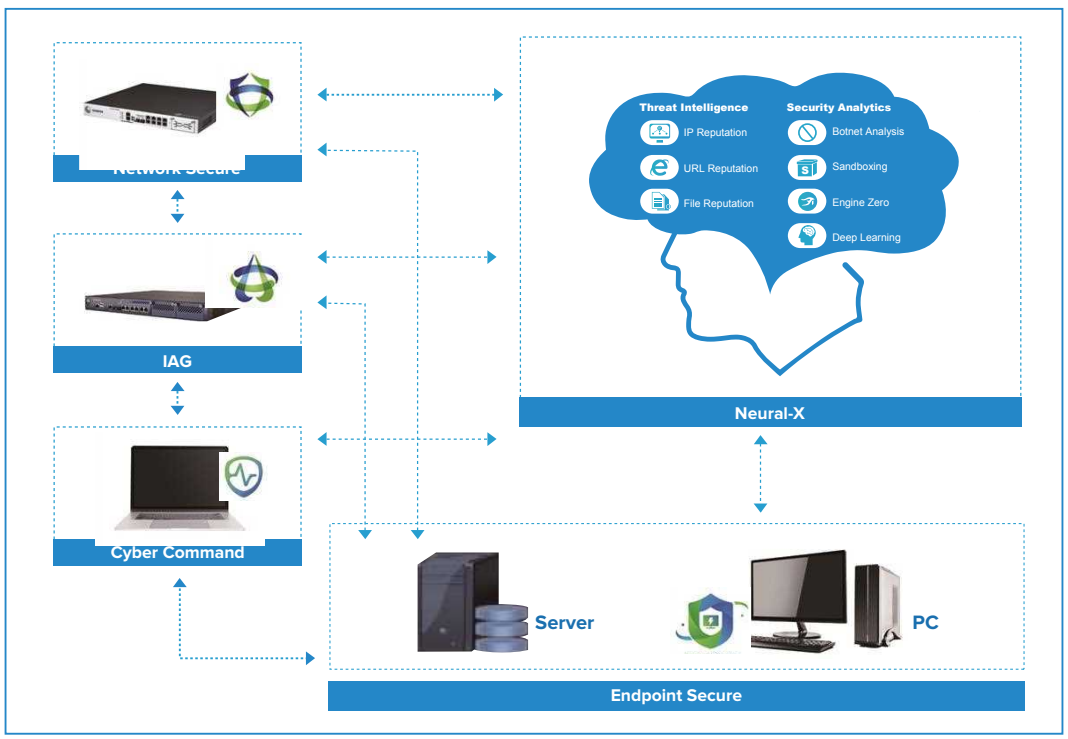
1. The lack of resources available to detect and respond to advanced and unknown threats prevent proactive defense.
2. Manual system management being inadequate when dealing with fast-moving and unknown threats - exposing the system to numerous attack surfaces.

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, Network Secure, 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.

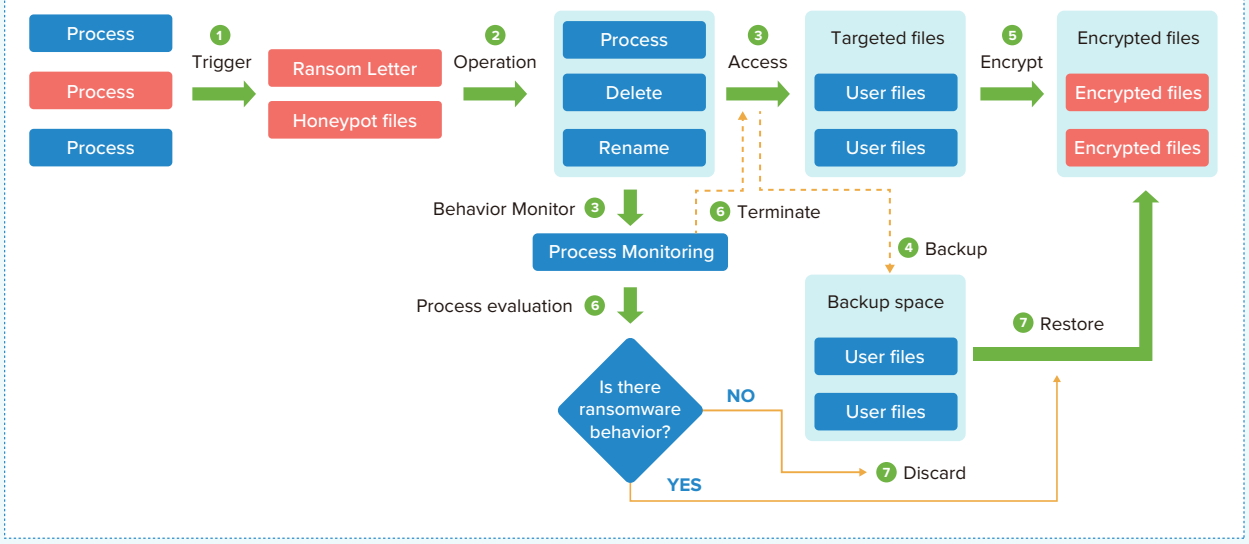
2. The Endpoint Secure intelligent linkage mechanism shares external threat information in a timely manner, allowing automatic response.

Advantages and Characteristics

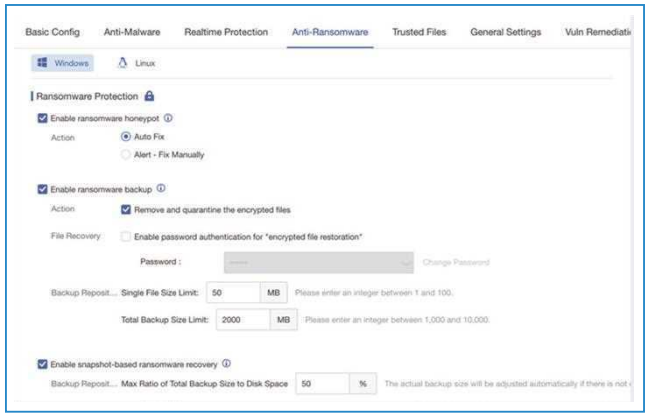
Ransomware Protection and Recovery

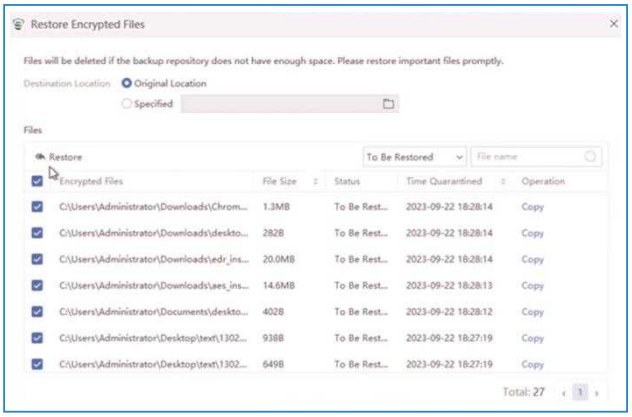
Sangfor Endpoint Secure Key Capabilities

- Protects against all types of ransomware through static and dynamic AI-based detection engines.
- Detects suspicious ransomware-related processes and blocks them ***in as little as 3 seconds*** to ensure minimal impact on users' assets.
- Ransomware indicators of compromise are collected from over 12 million devices deployed with Sangfor Endpoint Secure, allowing it to ***achieve a detection accuracy rate of 99.83%.***
- In addition to existing ransomware protections, such as honeypot and RDP two-factor authentication, Sangfor Endpoint Secure provides ransomware recovery capabilities. These include file recovery and recovery via Windows Volume Shadow Copy Service (VSS) snapshot backup to fully secure and restore your data in case of ransomware encryption.



1. Suspicious process makes a trigger on the system
2. Process tries to change or encrypt files
3. Behavior is monitored by Sangfor Endpoint Secure
4. Files are backed up in real time
5. Malicious process encrypts user files
6. Sangfor Endpoint Secure determines process is malicious and blocks and terminates the process
7. Backed up files are ready to be restored immediately



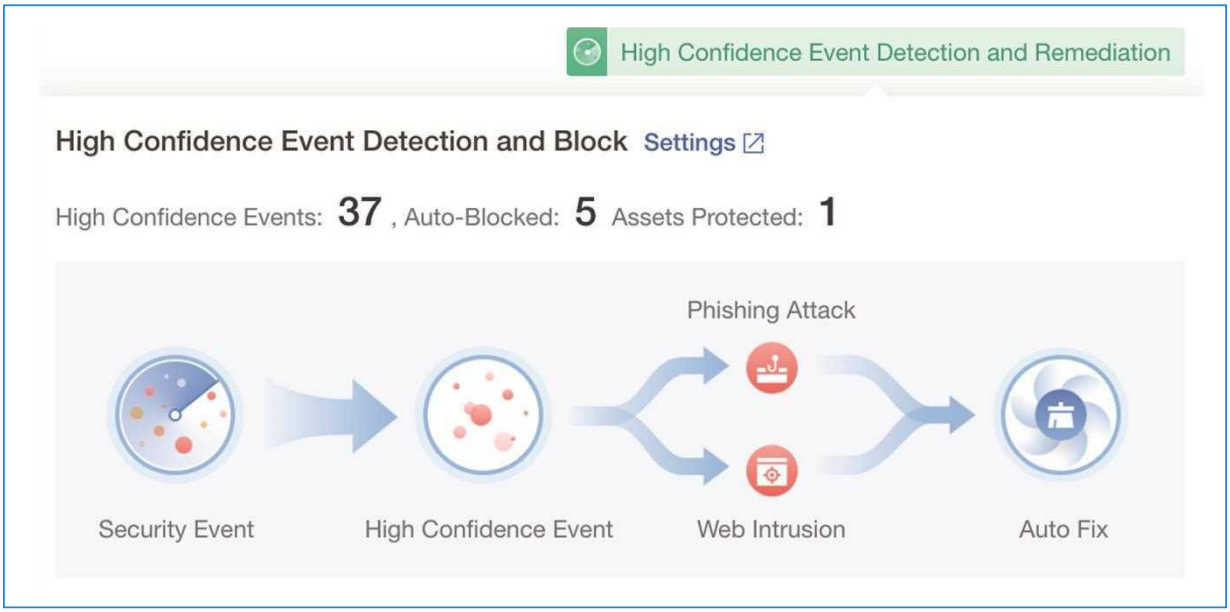


Phishing and Web Intrusion Protection with Automated Response

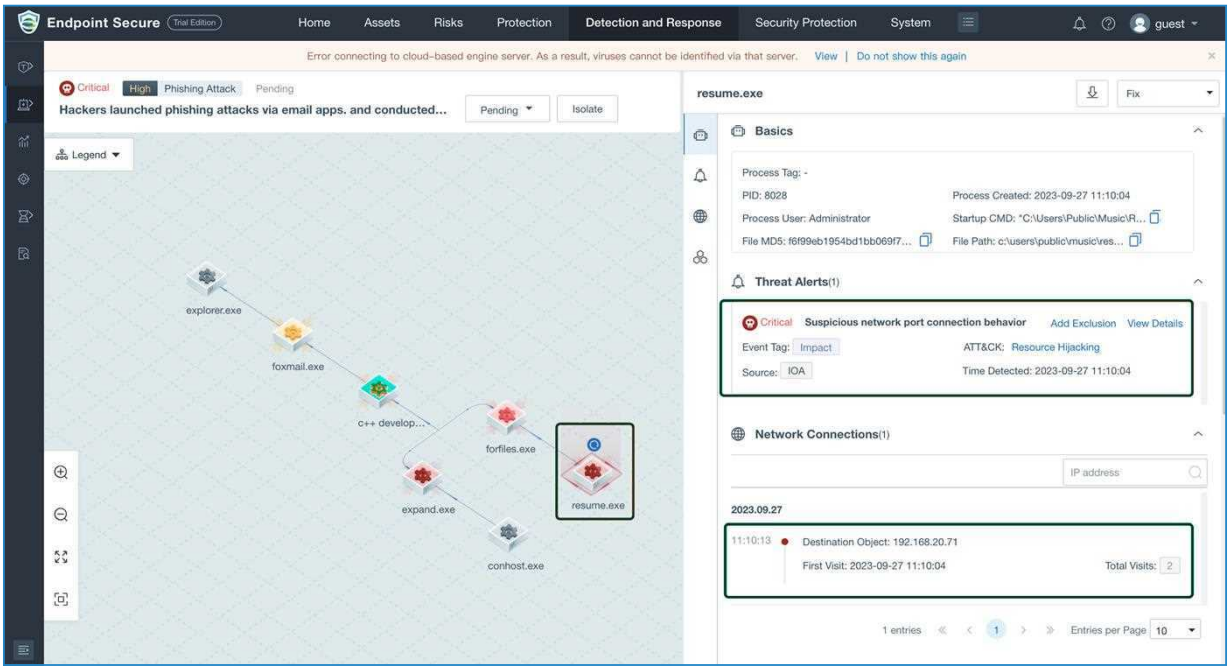
Enhanced protection against phishing and web intrusion attacks to counter the rising number of incidents worldwide.

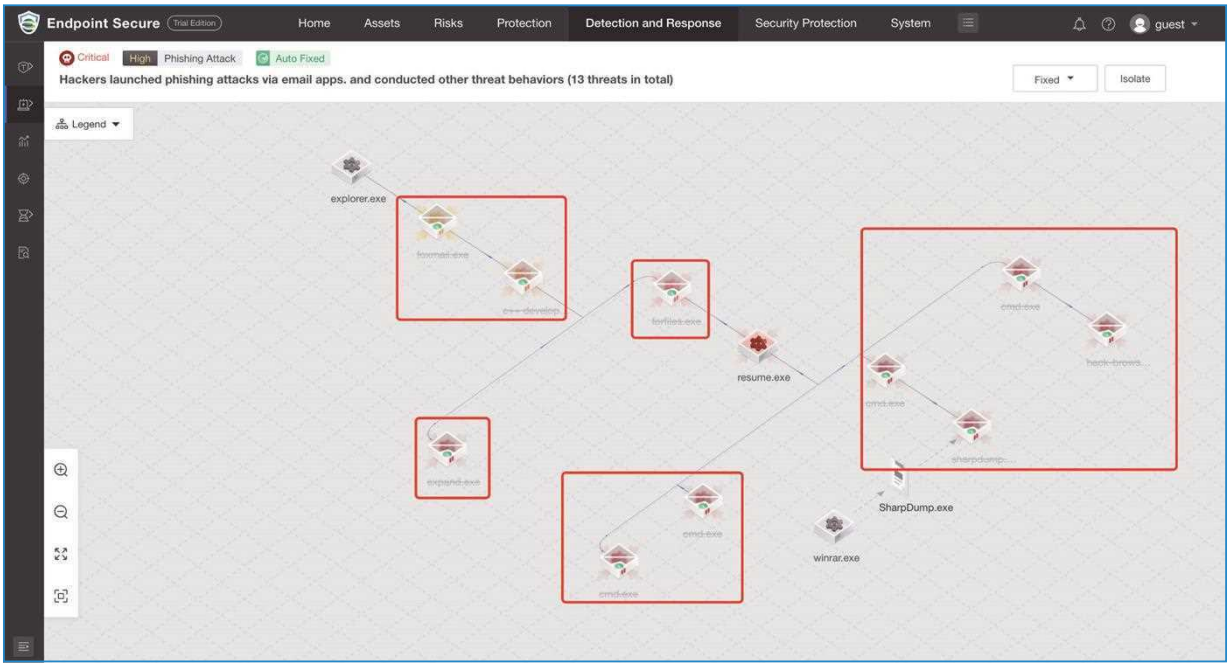
Accurate detection of phishing and web intrusion attacks, with detailed insights, including a comprehensive visual kill chain to pinpoint the origin and associated behaviors of the attack.

Users can configure Sangfor Endpoint Secure to respond automatically to such attacks, such as terminating malicious processes and deleting malicious files to prevent lateral movement.


High Confidence Event Detection and Remediation
High Confidence Event Detection and Block Settings
High Confidence Events: 37 , Auto-Blocked: 5 Assets Protected: 1
Phishing Attack
Security Event
High Confidence Event
Web Intrusion
Auto Fix


Endpoint Secure
Home
Assets
Risks
Protection
Detection and Response
Security Protection
System
guest
Error connecting to cloud-based engine server. As a result, viruses cannot be identified via that server. View | Do not show this again
Security Event
Event Mode
Alert Mode
High Confidence Event Detection and Remediatic
Search
IOA Exclusions
Refresh
Severity
Event Tag
Last Detected
Description
ATT&CK
Endpoint
Detection Sou...
Status
Time Fixed
Realtime Protec...
Threat Intelligenc
Critical
High
Phishing Attack
2023-09-27 11:10:04
Hackers launched phishing attacks via...
6 hits
IOA Engine
Pending
View Details


Endpoint Secure
Home
Assets
Risks
Protection
Detection and Response
Security Protection
System
guest
Error connecting to cloud-based engine server. As a result, viruses cannot be identified via that server. View | Do not show this again
Critical
High
Phishing Attack
Pending
Hackers launched phishing attacks via email apps, and conducted...
Isolate
Legend
explorer.exe
foxmail.exe
c++ develop...
forfiles.exe
expand.exe
resume.exe
conhost.exe
resume.exe
Fix
Basics
Process Tag: -
PID: 8028
Process Created: 2023-09-27 11:10:04
Process User: Administrator
Startup CMD: "C:\Users\Public\Music\R...
File MD5: f6f99eb1954bd1bb069f7...
File Path: c:\users\public\music\res...
Threat Alerts(1)
Critical
Suspicious network port connection behavior
Add Exclusion
View Details
Event Tag: Impact
ATT&CK: Resource Hijacking
Source: IOA
Time Detected: 2023-09-27 11:10:04
Network Connections(1)
IP address
2023.09.27
11:10:13
Destination Object: 192.168.20.71
First Visit: 2023-09-27 11:10:04
Total Visits: 2
1 entries
Entries per Page 10



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	July 2023	August 2023
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 306 samples used	99.7%	100%	99.4%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 18,589 samples used	100%	100%	100%
Protection Score	6.0/6.0		

Figure 1. Sangfor Endpoint Secure Protect test results for Protection

Antivirus Solution for Business Efficiency

	Industry average	July	August 2023
Slowing-down when launching popular websites 65 websites visited	27%	24%	24%
Slower download of frequently-used applications 25 downloaded files	1%	1%	0%
Slower launch of standard software applications 70 test cases applied	9%	5%	5%
Slower installation of frequently-used applications 25 installed applications	19%	13%	12%
Slower copying of files, locally and in a network 9,772 files copied	3%	3%	2%
Performance Score	6.0/6.0		

Figure 2. Sangfor Endpoint Secure Protect test results for Performance

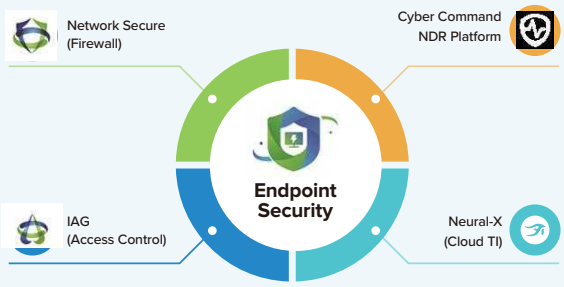
High Compatibility

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
• Windows XP SP3 * • Windows 7 * • Windows 8 * • Windows 8.1 * • Windows 10 • Windows 11 • Windows Server 2003 SP2 * • Windows Server 2008 * • Windows Server 2008R2 * • Windows Server 2012 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.13 • macOS 10.14 • macOS 10.15 • macOS 11.x • macOS 12.x • macOS 13.x	• Ubuntu 10 • Ubuntu 11 • Ubuntu 12 • Ubuntu 13 • Ubuntu 14 • Ubuntu 16 • Ubuntu 18 • Ubuntu 20 • Ubuntu 22	• RHEL 5 • RHEL 6 • RHEL 7 • RHEL 8	• CentOS 5 • CentOS 6 • CentOS 7 • CentOS 8	• Debian 6 • Debian 7 • Debian 8 • Debian 9	• SUSE 12 • SUSE 11.X • SUSE 15.X	• Oracle Linux 5 • Oracle Linux 6 • Oracle Linux 7 • Oracle Linux 8 • Oracle Linux 9	• Red Flag Asianux Server 4 • NeoKylin 5 • NeoKylin 6 • NeoKylin 7 • KylinOS 4 • Ubuntu Kylin 18

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

Multi-dimensional Linkage



Endpoint Security coordinated with Network Secure, IAG and Cyber Command to provide faster response and more integrated chain of evidence.

Advanced threat analysis & respond with MITRE ATT&CK®

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		✓
Protection	Realtime File Monitoring	✓	✓
	Ransomware Honeypot	✓	✓
	Ransomware Protection	✓	✓
	Ransomware Backup Recovery	✓	✓
	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	✓	✓
	Improved Phishing and Web Intrusion Detection	✓	✓
	Coordinated Malware Response with XDDR		✓
	WebShell Detection		✓
	Advanced Threat Detection		✓
	Suspicious Login Detection	✓	✓
	Memory Backdoor Detection		✓
	Reverse Shell Detection		✓
	Local Privilege Escalation Detection		✓
	Remote Command Execution Detection		✓
Response	File Quarantine	✓	✓
	Endpoint Isolation	✓	✓
	File Remediation	✓	✓
	Virus Mitigation	✓	✓
	Automated Response to Phishing and Web Intrusion events	✓	✓
	Extended Detection, Defense and Response (XDDR)		✓
	Threat Hunting		✓
	Domain Isolation	✓	✓
	Process Blocking	✓	✓
Maintenance	Script File Upload	✓	✓
	USB Control	✓	✓
	Unauthorized Outbound Access Detection	✓	✓
	Remote Support	✓	✓
IT Governance	Application Blacklist		✓
	Software Metering		✓
	Software Uninstallation		✓

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

SANGFOR ENDPOINT SECURE

INTERNATIONAL OFFICES

SANGFOR SINGAPORE
10 Ubi Crescent, #04-26 Ubi
Techpark (Lobby B), Singapore 408564
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
Atrium Mulia 3rd Floor, Jl. H.R. Rasuna Said Kav.
B 10-11 Kuningan, Setia Budi, Kecamatan
Setiabudi, Kota Jakarta Selatan, Daerah Khusus
Ibukota Jakarta 12910, Indonesia
Tel: (+62) 21-2168-4132

SANGFOR MALAYSIA
No. 45-10 The Boulevard Offices,
Mid Valley City, Lingkaran Syed Putra,
59200 Kuala Lumpur, Malaysia
Tel: (+60) 3-2702-3645

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

SANGFOR PHILIPPINES
Unit 14B 14th Floor, Rufino Pacific Tower,
6784 Ayala Avenue, Makati City, Metro Manila,
Philippines
Tel: (+63) 916-267-7322

SANGFOR VIETNAM
210 Bùi Văn Ba, Tân Thuận Đông, Quận 7,
Thành phố Hồ Chí Minh 700000, Vietnam
Tel: (+84) 903-631-488

SANGFOR SOUTH KOREA
Floor 17, Room 1703, Yuwon bldg. 116,
Seosomunro, Jung-gu, Seoul, Republic of Korea
Tel: (+82) 2-6261-0999

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

SANGFOR ITALY
Floor 8, Via Marsala, 36B, 21013 Gallarate VA, Italia
Tel: (+39) 0331-6487-73

SANGFOR PAKISTAN
Office No.210, 2nd Floor, "The Forum",
Plot No. G-20, Block 9, Khayaban-e-Jami, Clifton,
Karachi, Pakistan
South Region: +92 321 2373991
North Region: +92 345 2869434
Central Region: +92 321 4654743

SANGFOR TÜRKIYE
A Blok. Kat 51. D 643, Atatürk Mh, Ertuğrul Gazi Sk,
Metropol İstanbul Sitesi. 34758 Ataşehir/İstanbul
Tel: (+90) 216-5156969

AVAILABLE SOLUTIONS

IAG - Internet Access Gateway
Secure User Internet Access Behaviour

Network Secure - 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
Seamless Experience, Secure and Efficient

Access Secure - 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

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

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

www.sangfor.com