



SANGFOR



Endpoint  
Secure



# SANGFOR ENDPOINT SECURE

Endpoint Security

— —  
The Future of Endpoint Security

**Gartner**

Strong Performer in Gartner® Voice of the Customer for Endpoint Protection Platforms with a 95% “Willingness to Recommend”

**AVTEST**  
The Independent IT Security Institute  
Munich, Germany

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

 Microsoft

Certificated Windows Protection by Microsoft

**OPSWAT.**

Gold OPSWAT Endpoint Security Certification for Anti-Malware

## Modern Enterprise Endpoint Security Challenges

Enterprise data holds high value for cybercriminals, making endpoints—such as PCs, servers, and the software they run—primary targets for cyberattacks, including ransomware encryption, data exfiltration, and credential theft. As the threat landscape evolves, endpoints often serve as initial access points for attackers who use sophisticated tactics like AI-generated phishing emails, zero-day exploit chains, and supply chain attacks to infiltrate systems undetected. This rising threat landscape contributes to the complexity of managing and securing these endpoints. Additionally, enterprises face strict regulatory requirements, including GDPR, PDPA, and HIPAA, which add pressure to ensure comprehensive data protection and endpoint security. Consequently, proactive endpoint protection with advanced threat detection and response is essential.

## Why Traditional Endpoint Security Falls Short

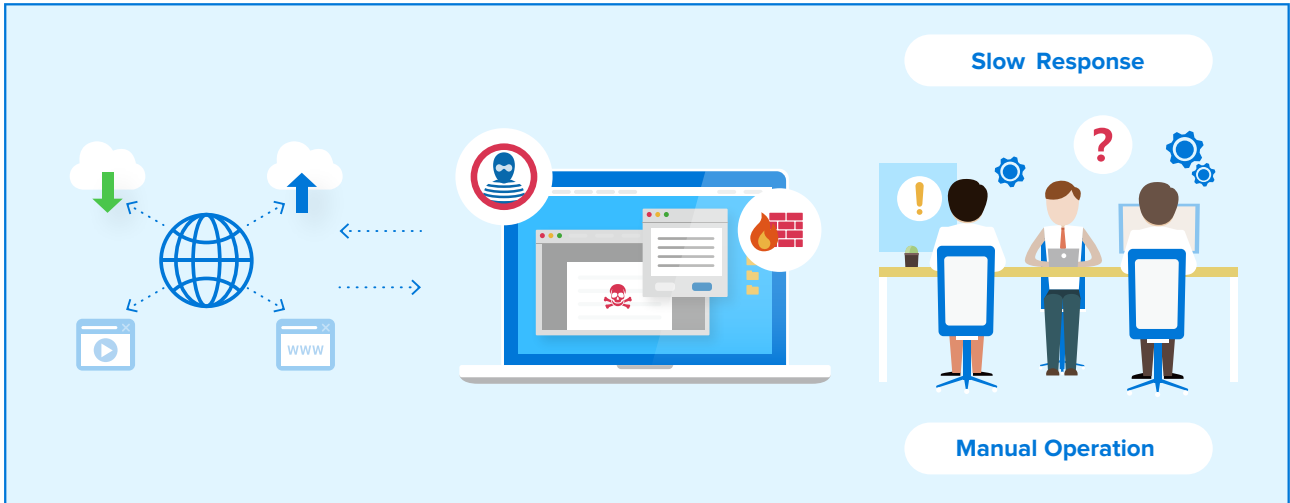
### 1. Outdated Signature-based Detection

In environments facing cyber threats, traditional endpoint security products based on signature-based detection are often bypassed by unknown malware and sophisticated attacks. Relying on a database of known signatures, this approach has limited capacity to defend against ransomware attacks and Advanced Persistent Threats (APTs), which frequently evade detection through obfuscation and fileless execution.



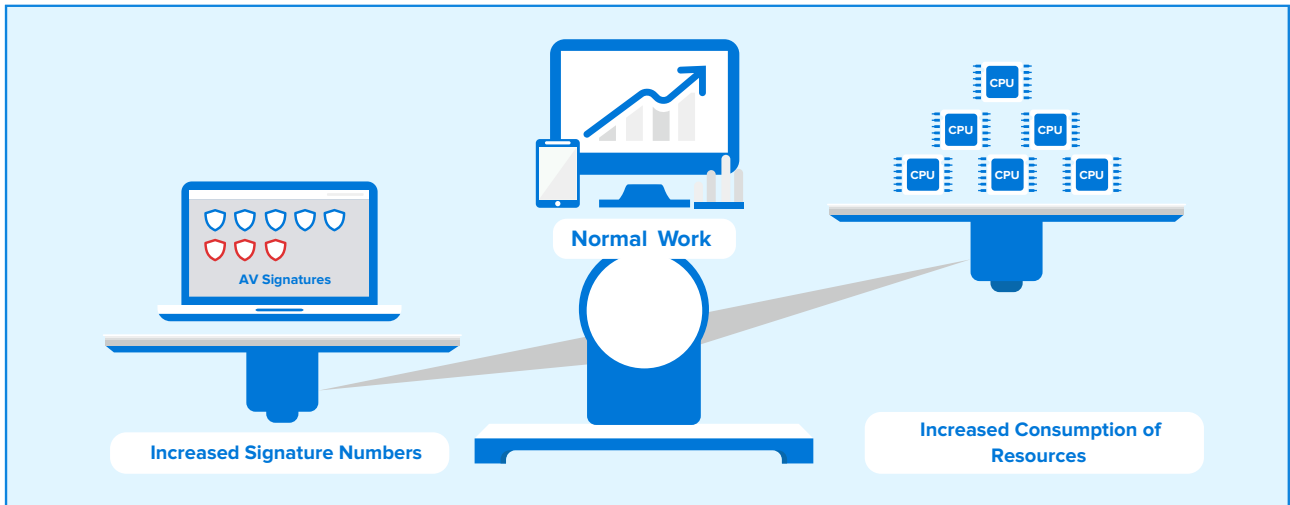
### 2. Inefficient and Costly Manual Operations and Maintenance

In traditional endpoint security, manual operation is often necessary due to limited detection and investigation capabilities. Security teams must manually review alerts, investigate incidents, and adjust policies to keep up with evolving threats. Reliance on manual processes often results in delayed response times, higher operational costs, and an increased risk of overlooking critical threats. Additionally, the lack of centralized management hinders consistent protection across endpoints, adding to operational burdens.



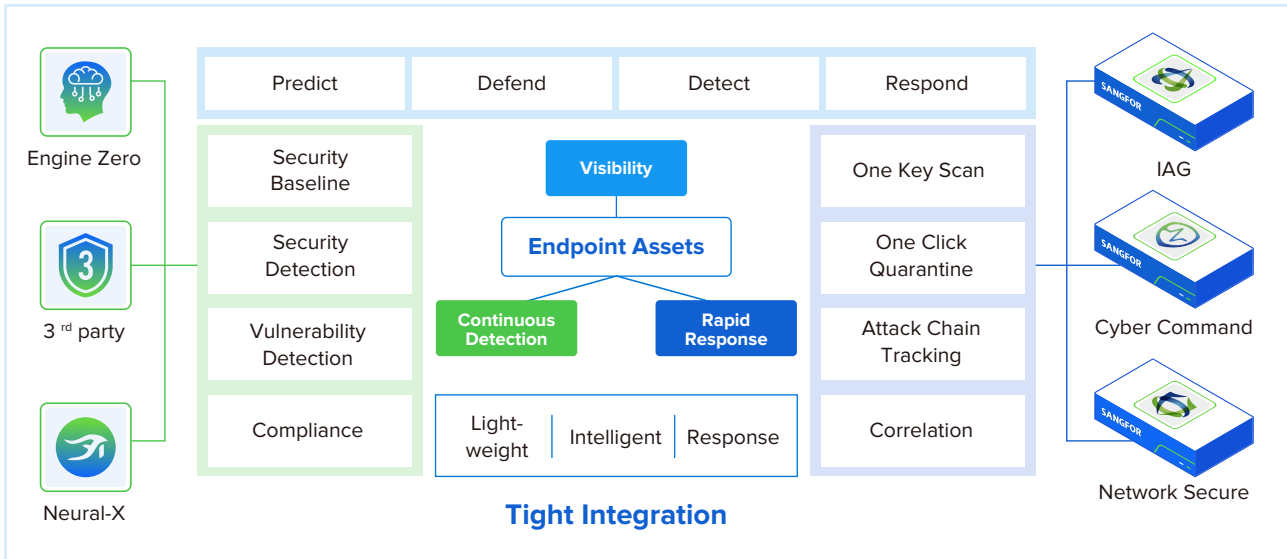
### 3. High Resource Consumption

As the number of malware signatures grows, maintaining extensive antivirus databases raises storage and computing demands on endpoint devices. This increased resource utilization can seriously impact user efficiency by slowing endpoint performance and increasing server load, resulting in significant operational costs to the organization.



## Sangfor Endpoint Secure : The Future of Endpoint Security

Sangfor Endpoint Secure is a Modern Endpoint Protection Platform (EPP) that combines Next-Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), and Endpoint Management into a single, unified solution. This all-in-one approach provides comprehensive protection to address today's complex endpoint security challenges.

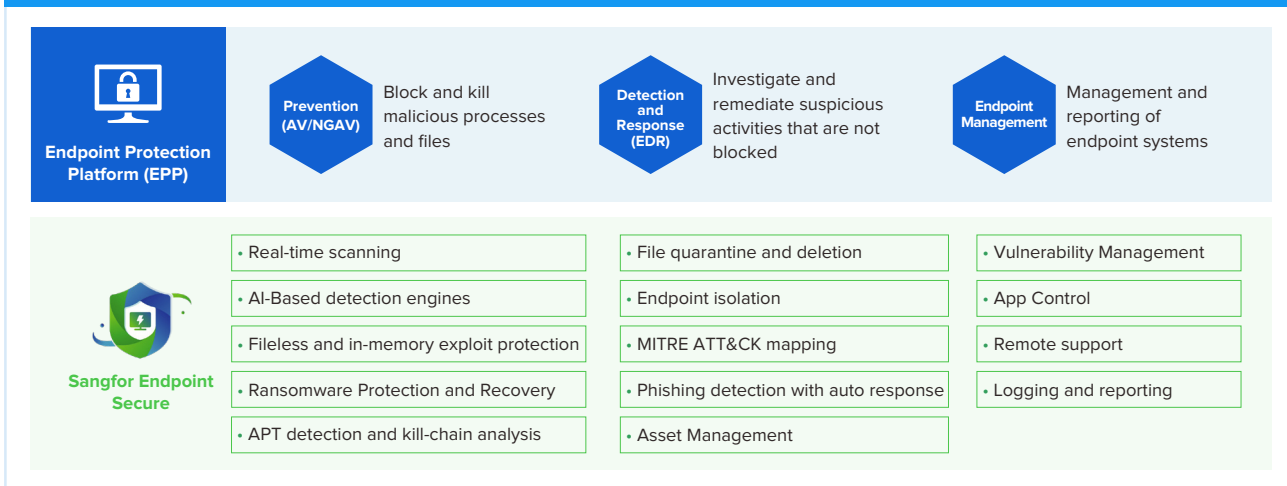


## How Endpoint Secure Addresses Modern Endpoint Security Challenges

### Advanced Threat Detection and Response

Sangfor Endpoint Secure uses advanced technologies like AI, ransomware honeypots, and behavioral analysis to detect unknown and sophisticated threats accurately. It is equipped with dedicated defenses to target specific threats such as ransomware, RDP brute-force attacks, and phishing, ensuring precise threat identification and rapid mitigation. Through its EDR capabilities, Endpoint Secure leverages anomaly-based detection to identify suspicious activities associated with advanced attacks that evade signature-based antivirus.

### Sangfor Endpoint Secure – a Modern EPP Solution



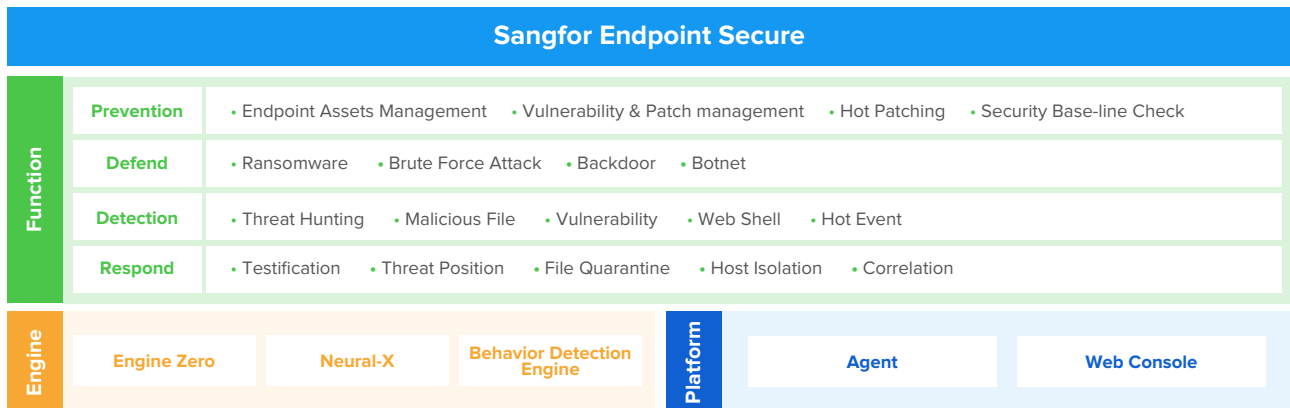
To stay ahead of the latest threats, Endpoint Secure integrates with the Sangfor Neural-X threat intelligence and analytics platform, which collects threat intelligence feeds from extensive sources. This constant stream of updated intelligence ensures that Endpoint Secure remains prepared to handle any emerging threats.

Additionally, its response capabilities are fast and automatic—blocking ransomware within as little as three seconds to minimize damage. Endpoint Secure also enhances investigation by uncovering the root cause of incidents and identifying other affected assets, facilitating comprehensive eradication and strengthening the system’s defense. By integrating with Sangfor’s network security solutions, Endpoint Secure enables threat correlation to enhance detection accuracy and enables a coordinated response across both endpoints and the network.

### Simplified Operations and Maintenance

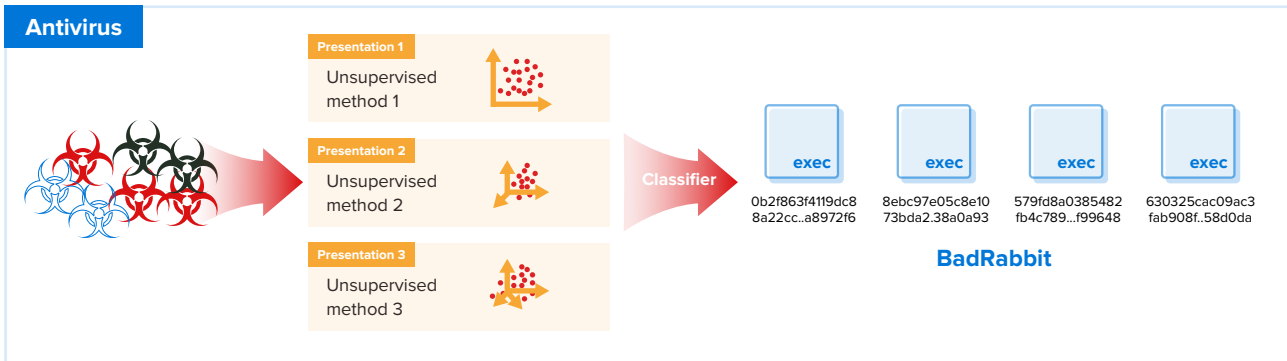
Beyond threat detection and response, Sangfor Endpoint Secure streamlines operations and maintenance (O&M) through comprehensive endpoint management capabilities. Organizations can proactively scan endpoints for misconfigurations and vulnerabilities—gaps that attackers could exploit. Addressing these risks early helps prevent potential breaches, reinforcing overall endpoint security and supporting regulatory compliance.

### Architecture of Endpoint Secure



Centralized policy management ensures consistent protection across all endpoints, while remote troubleshooting capabilities enable security teams to resolve issues without physical access to devices. These features help reduce operational complexity, enhance security efficiency, and ensure that endpoint security remains resilient and adaptable.

## Application Scenarios



### Risk Scenario:

Enterprise endpoints are widely deployed across multiple office networks. Attacks from unknown malware and ransomware can significantly impact business-critical applications, compromising the security of the organization's data and business operations. The risks are high due to:



Insufficient capabilities and resources to detect and respond to advanced and unknown threats, thus unable to provide a proactive defense.

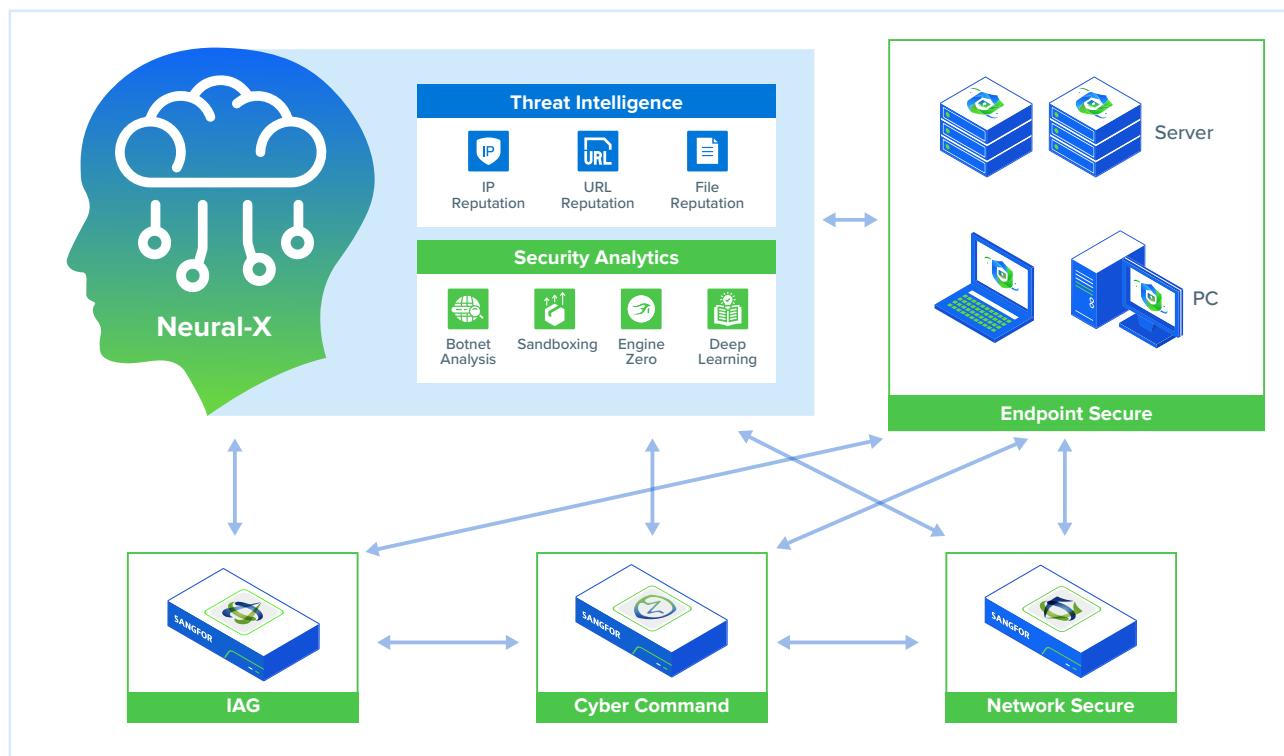


Reliance on manual security operations processes is inadequate for addressing fast-moving and complex threats, thereby exposing organizations to a wider attack surface.

### Why Endpoint Secure is Effective:

1. With AI and Neural-X threat intelligence, our static and behavior analysis detection capabilities provide comprehensive threat defense capable of detecting and preventing known and unknown malware, including APTs and ransomware.
2. Attack surface reduction capabilities complement malware detection and prevention. Endpoint Secure offers vulnerability detection and patch management to help organizations strengthen their security posture and avoid security breaches on vulnerable operating systems and applications.

## Synergy with Network Security



### Risk Scenario:

While most organizations have deployed network security solutions like firewalls, intrusion prevention systems, and other border gateway devices, their lack of integration with endpoint security results in ineffective detection and response.



Due to the lack of data correlation across devices, advanced threats may go undetected. Without shared threat intelligence, these devices cannot provide a cohesive defense, potentially allowing sophisticated attacks to evade detection.



Even if a network device detects a threat, the lack of integration between the network and endpoint solutions results in incomplete visibility to fully assess the impact and eradicate the threat. This allows threats to re-enter through other network points or endpoints, remaining unaddressed.



### Why Endpoint Secure is Effective:

1. Endpoint Secure integrates seamlessly with Sangfor Neural-X, Network Secure, Cyber Command, XDR, and IAG, creating a comprehensive defense across the cloud, network, and endpoint. Threat information is shared across the integrated solutions in real time.
2. Response is fast and efficient through integration synergy. Threats detected on Network Secure or Cyber Command can be responded to directly through Endpoint Secure without the need to operate multiple consoles.
3. No dependencies on third-party solutions. Integrating Sangfor's network and endpoint solutions does not involve complicated configurations and eliminates compatibility issues due to third-party reliance.

## 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.

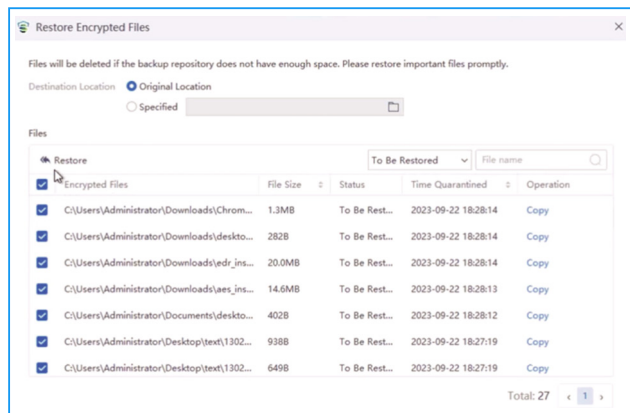
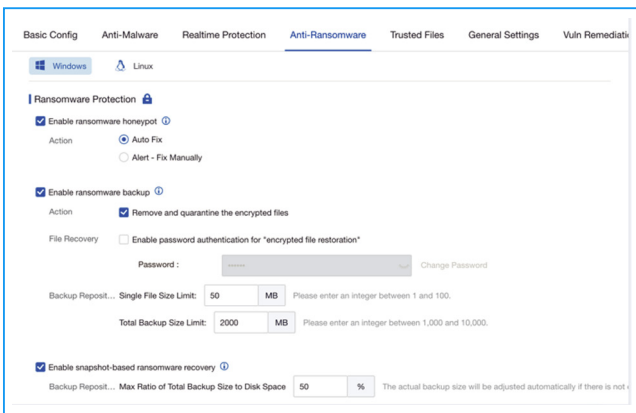
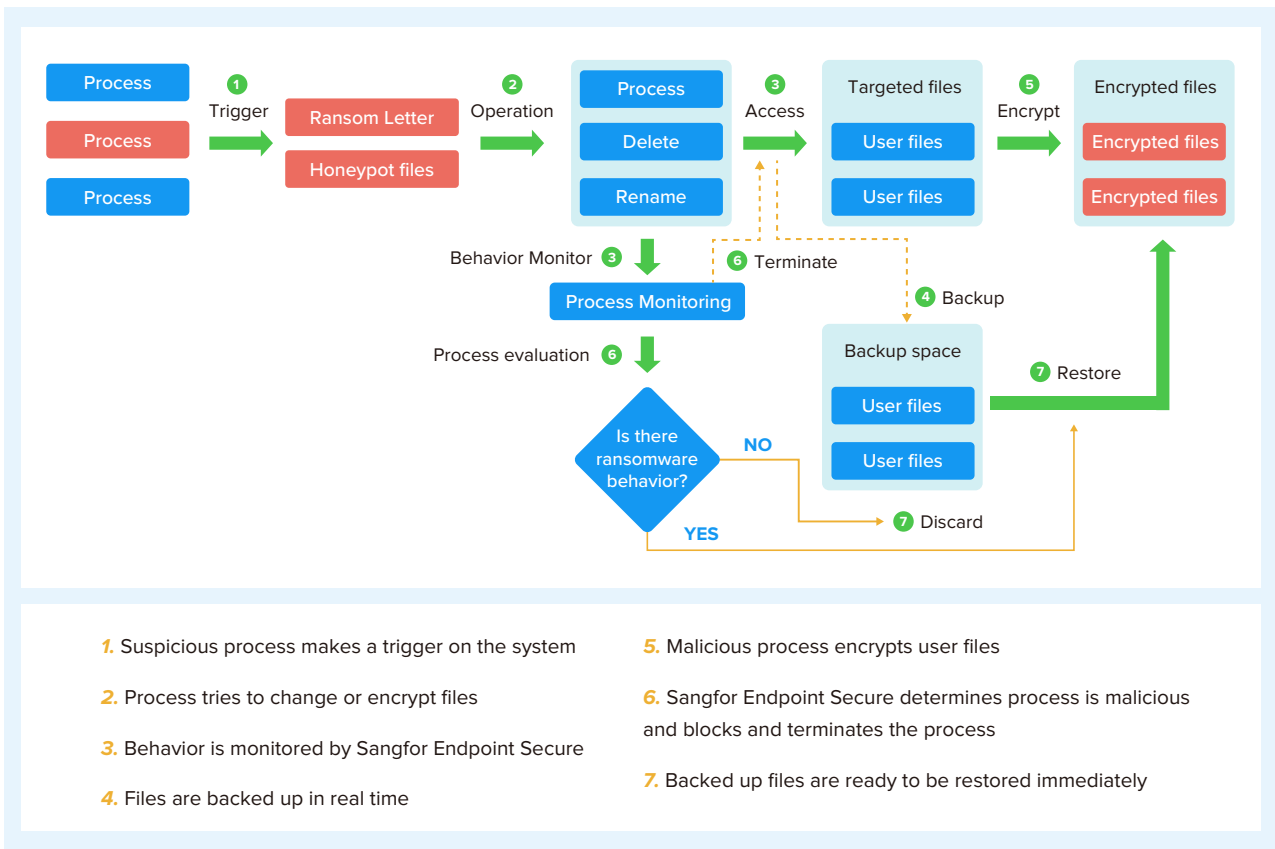


Ransomware indicators of compromise are collected from over 12 million devices deployed with Sangfor Endpoint Secure, allowing it to *achieve a detection accuracy rate of 99.83%*.




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.







## 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.



SANGFOR

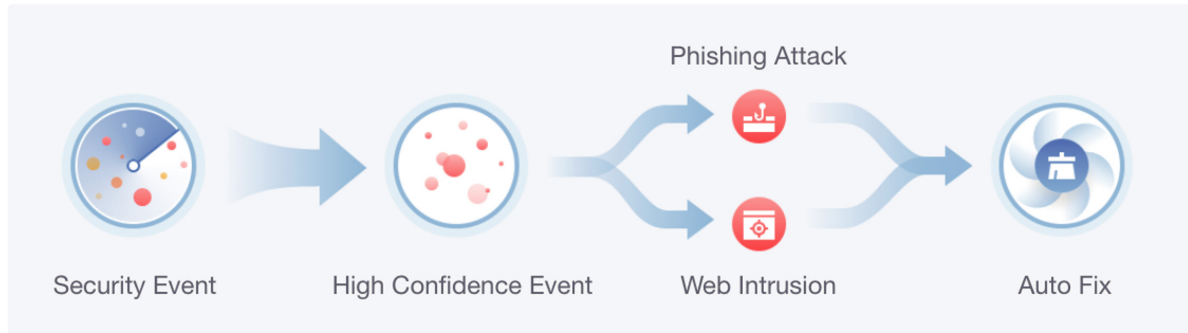


Sangfor  
Endpoint Secure

### High Confidence Event Detection and Remediation

## High Confidence Event Detection and Block [Settings](#)

High Confidence Events: **37** , Auto-Blocked: **5** Assets Protected: **1**



Endpoint Secure Trial Edition 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 Remediation

Q Severity: Critical, High, Medium x Status: Pending x Event Tag: Phishing Attack, Web Intrusion, Malicious Virus, Other x Time: Last 30 days x Excluded Alerts: Hide [Search](#)

Mark As IOA Exclusions Refresh  Show high confidence events only

Severity	Event Tag	Last Detected	Description	ATT&CK	Endpoint	Detection Sou...	Status	Time Fixed	Realtime Protec...	Threat Intelligenci...
Critical	High Phishing Attack	2023-09-27 11:10:04	Hackers launched phishing attacks via...	6 hits	Win10_1909(192...	IOA Engine	Pending	-	Pending	<a href="#">View Details</a>   <a href="#">In-D...</a>

Endpoint Secure Trial Edition 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... Pending Isolate

Legend

**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

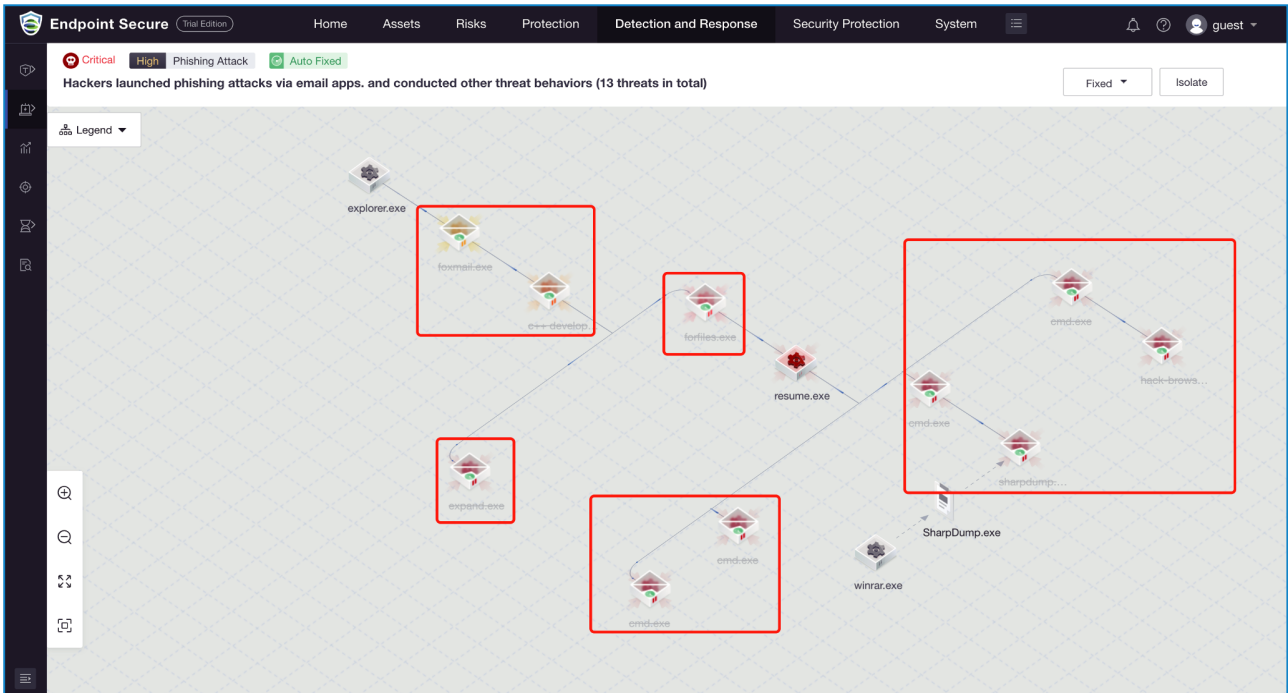
**Network Connections(1)**

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 << < 1 > >> 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
<b>Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing)</b> 306 samples used	99.7%	100%	99.4%
<b>Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set)</b> 18,589 samples used	100%	100%	100%
<b>Protection Score</b>	<b>6.0/6.0</b>		

Figure 1. Sangfor Endpoint Secure Protect test results for Protection

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

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
<ul style="list-style-type: none"> <li>Windows XP SP3 <sup>1,3</sup></li> <li>Windows 7 <sup>1</sup></li> <li>Windows 8 <sup>1</sup></li> <li>Windows 8.1 <sup>1</sup></li> <li>Windows 10</li> <li>Windows 11</li> <li>Windows Server 2003 SP2 <sup>1,2</sup></li> <li>Windows Server 2008<sup>1</sup></li> <li>Windows Server 2008R2<sup>1</sup></li> <li>Windows Server 2012</li> <li>Windows Server 2016</li> <li>Windows Server 2019</li> <li>Windows Server 2022</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> <li>macOs 13.x</li> </ul>	<ul style="list-style-type: none"> <li>Ubuntu 10 <sup>2</sup></li> <li>Ubuntu 11 <sup>2</sup></li> <li>Ubuntu 12 <sup>2</sup></li> <li>Ubuntu 13 <sup>2</sup></li> <li>Ubuntu 14 <sup>2</sup></li> <li>Ubuntu 16 <sup>2</sup></li> <li>Ubuntu 18</li> <li>Ubuntu 20</li> <li>Ubuntu 22</li> </ul>	<ul style="list-style-type: none"> <li>RHEL5 <sup>2</sup></li> <li>RHEL 6 <sup>2</sup></li> <li>RHEL7</li> <li>RHEL 8</li> </ul>	<ul style="list-style-type: none"> <li>CentOs 5 <sup>2</sup></li> <li>CentOs 6 <sup>2</sup></li> <li>CentOs 7</li> <li>CentOs 8</li> </ul>	<ul style="list-style-type: none"> <li>Debian 6 <sup>2</sup></li> <li>Debian 7 <sup>2</sup></li> <li>Debian 8 <sup>2</sup></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>OracleLinux 5 <sup>2</sup></li> <li>Oracle Linux 6 <sup>2</sup></li> <li>Oracle Linux 7</li> <li>Oracle Linux 8</li> <li>Oracle Linux 9</li> </ul>

<sup>1</sup> The following Windows versions are no longer supported or receiving security updates from Microsoft.

<sup>2</sup> End-of-support for Sangfor Endpoint Secure in Q1 2025

<sup>3</sup> End-of-support for Sangfor Endpoint Secure in Q3 2025

## Advanced Threat Analysis & Respond with MITRE ATT&CK®

ATT&CK™ Matrix

HR Tactics: 5 HR Techniques: 11

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	Command and Scri... 1	Scheduled Task/Job 3 Valid Accounts 1 Event Triggered Ee... 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.

## Endpoint Secure Certifications and International Awards

Endpoint Secure achieved a 95% “Willingness to Recommend” rating in Gartner Voice of the Customer (VoC) for Endpoint Protection Platforms (June 2024). This is higher than the average across 17 other vendors highlighted in the report. This rating reflects the robust performance of Endpoint Secure and the excellent user experience we deliver.



Endpoint Secure was also awarded Top Product by AV-Test (December 2023). In the Windows antivirus software evaluation, we achieved a perfect score of 6 across the three categories of Protection, Performance, and Usability.



Sangfor Endpoint Secure has achieved the Gold OPSWAT Endpoint Security Certification for Anti-Malware (for Windows). The Gold certification badge is awarded to security solutions that achieve access control compatibility, ensuring seamless integration with over 100 leading endpoint security products that leverage the OPSWAT Endpoint Security Framework. Sangfor Endpoint Secure’s achievement of this certification demonstrates its compliance with OPSWAT’s rigorous standards and its commitment to delivering an effective endpoint security solution.



## Edition and Features

	Feature/Module	Essential Edition	Ultimate Edition
Prevention	Vulnerability Scan	✓	✓
	Remediation	✓	✓
	Security Compliance Check	✓	✓
	Asset Inventory	✓	✓
	Asset Discovery	✓	✓
	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	✓	✓
	Botnet 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.

## 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

Unit 11.01 MB Sunny Tower, 259 Tran Hung  
Dao Street, Co Giang Ward, District 1,  
Ho Chi Minh City, Vietnam  
Tel: (+84) 903-631-488

### SANGFOR SOUTH KOREA

Floor 15, Room 1503, Yuwon bldg. 116,  
Seosomun-ro, Jung-gu, Seoul,  
Republic of Korea  
Tel: (+82) 2-6261-0999

### SANGFOR UAE

Office #718, Publishing Pavilion,  
Production City, Dubai, UAE  
Tel: (+971) 52855-2520

### SANGFOR ITALY

Sede Principale: Via Marsala 36B,  
21013, Gallarate (VA)  
Sede a Roma: Via del Serafico,  
89-91, 00142 Roma RM  
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: +92 304 5170714  
Central Region: +92 314 519 8386

### SANGFOR TÜRKIYE

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

### SANGFOR LATAM

Torre Onyx Segundo Piso, Av. Río San Joaquin 406,  
Amp Granada, Miguel Hidalgo, C.P. 11529,  
Ciudad de México, CDMX

### SANGFOR SAUDI ARABIA

Office No. 3103A, Tower 2, 2nd Floor,  
Al Akaria Al Sittin, Salahuddin Street,  
Al Malaz, Riyadh

### GLOBAL SERVICE CENTER

Tel: +60 12711 7129  
tech.support@sangfor.com

## 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

### Omni-Command - Extended Detection and Response

Revolutionize Your Cyber Defense with Intelligent XDR

### 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

Secure, Agile, and Everywhere

### EDS - Enterprise Distributed Storage

The Only Secured Data Storage You Need



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



<https://www.facebook.com/Sangfor>  
<https://www.linkedin.com/company/sangfor-technologies>  
<https://www.youtube.com/user/SangforTechnologies>

### Contact Us

[marketing@sangfor.com](mailto:marketing@sangfor.com)   
[sales@sangfor.com](mailto:sales@sangfor.com)   
[www.sangfor.com](http://www.sangfor.com) 