



SANGFOR



**Sangfor
Athena EPP**



SANGFOR Athena EPP

Endpoint Protection Platform

The Future of Endpoint Security

Gartner

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



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



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

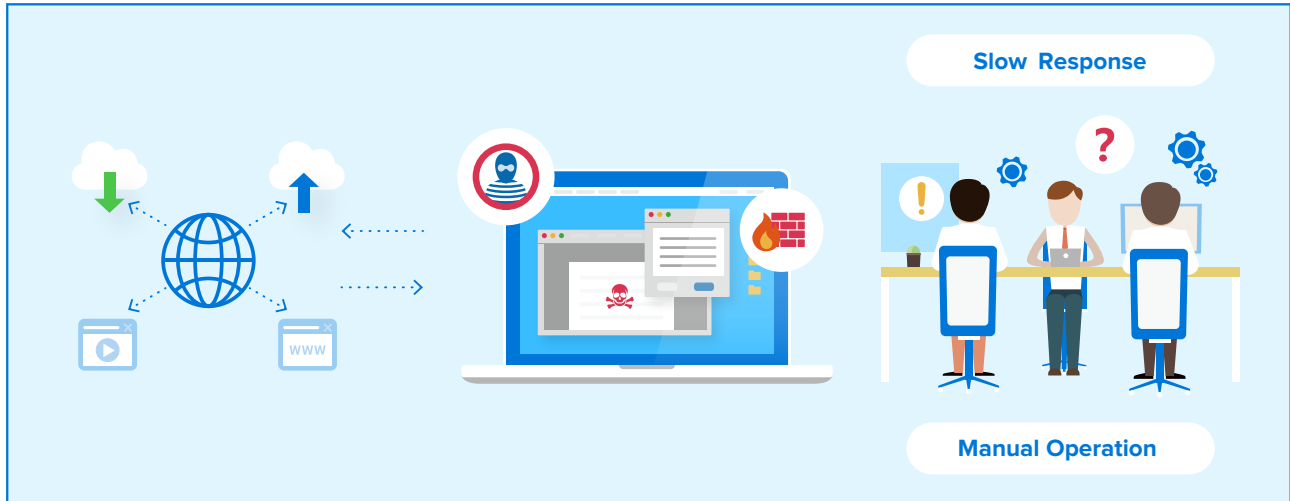
1. Outdated Signature-based Detection

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.



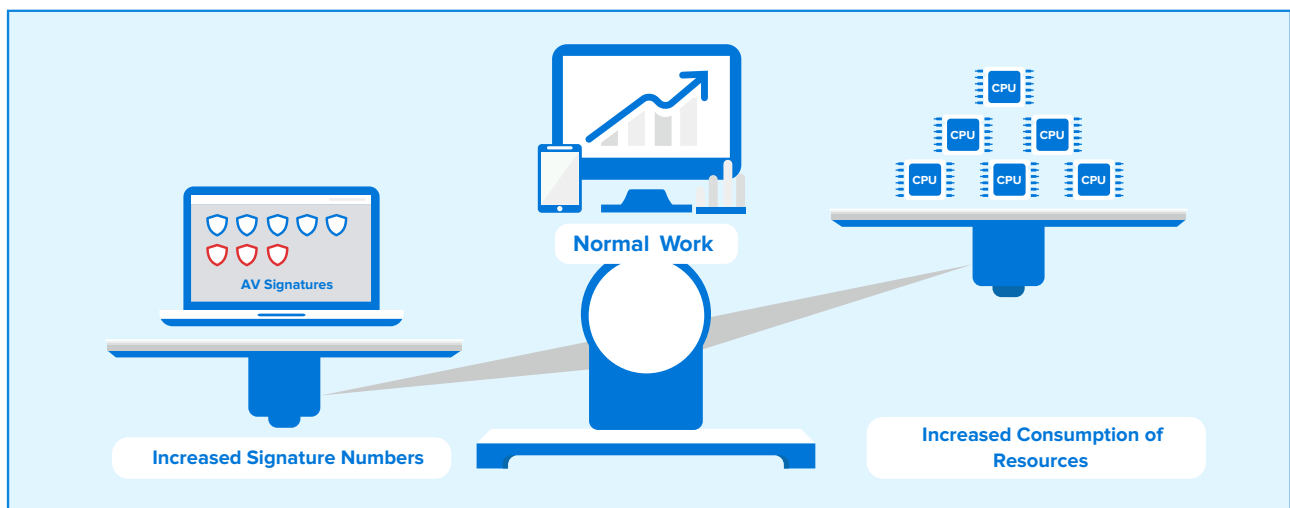
2. Inefficient and Costly Manual Operations and Maintenance

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.



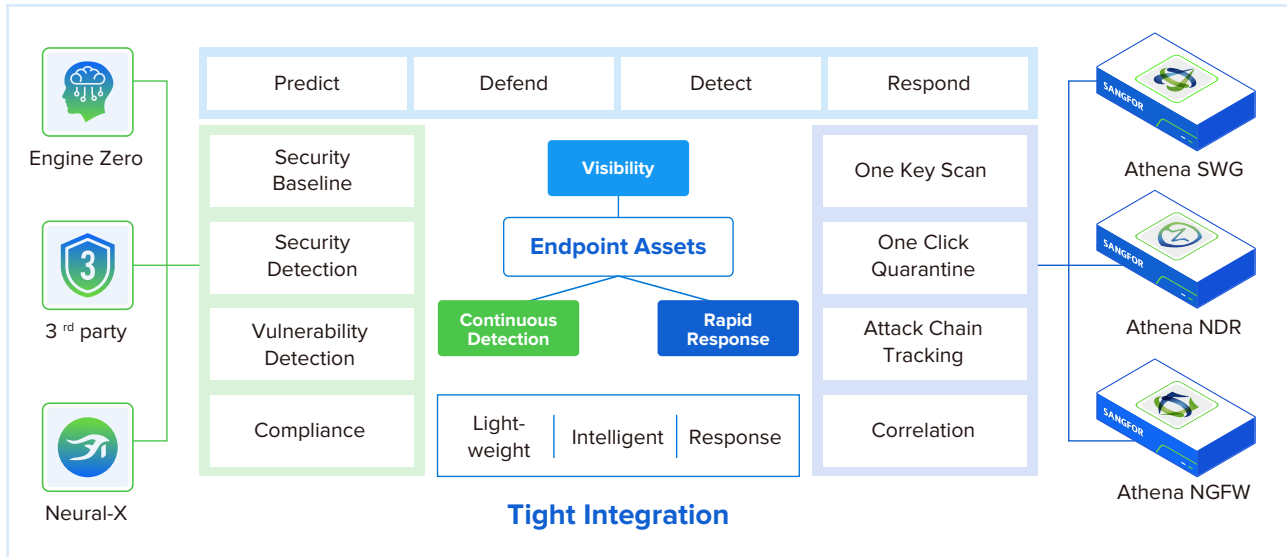
3. High Resource Consumption

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 Athena EPP: The Future of Endpoint Security

Sangfor Athena EPP (previously known as 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.

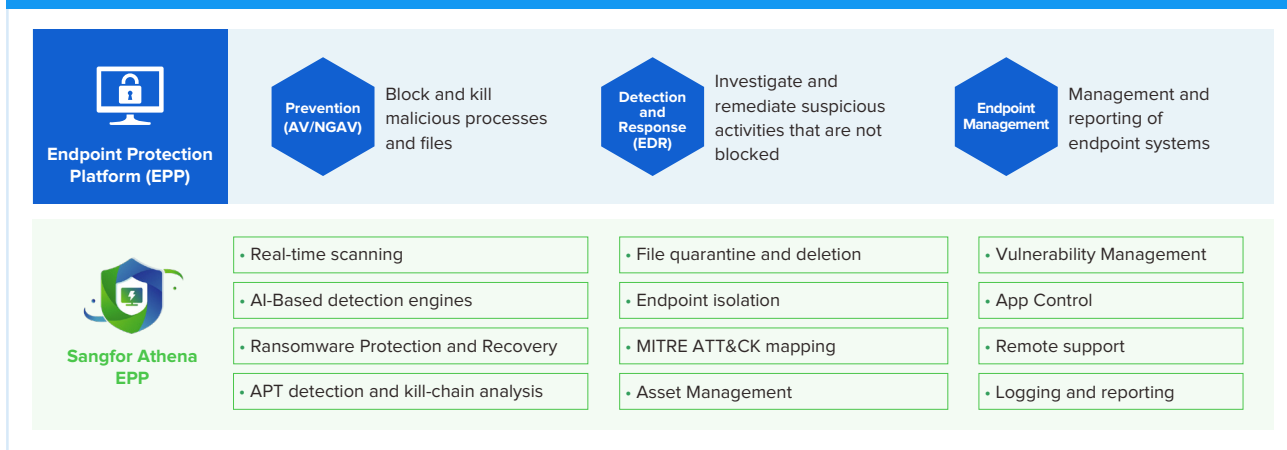


How Athena EPP Addresses Modern Endpoint Security Challenges

Advanced Threat Detection and Response

Sangfor Athena EPP 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, Athena EPP leverages anomaly-based detection to identify suspicious activities associated with advanced attacks that evade signature-based antivirus.

Sangfor Athena EPP – a Modern EPP Solution



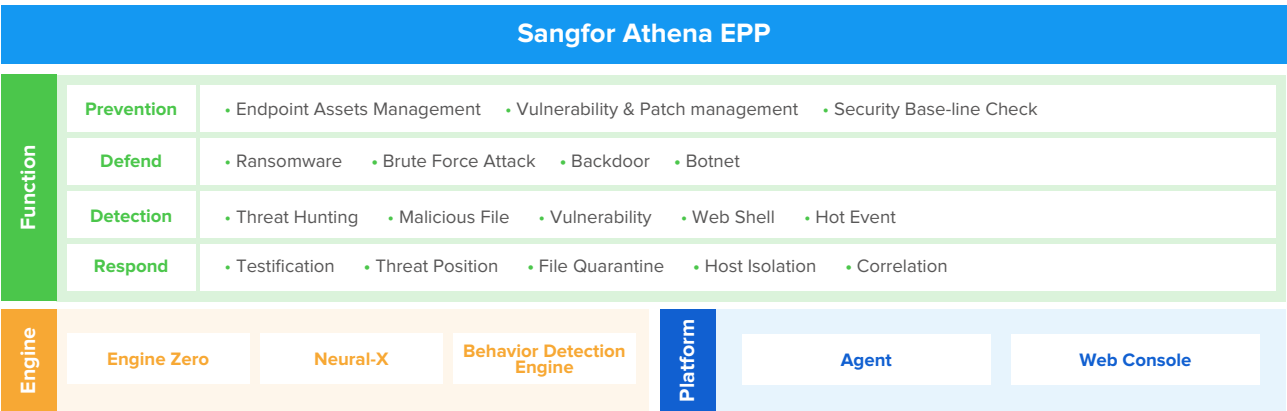
To stay ahead of the latest threats, Athena EPP integrates with the Sangfor Neural-X threat intelligence and analytics platform, which collects threat intelligence feeds from extensive sources. This constant stream of updated intelligence ensures that Athena EPP remains prepared to handle any emerging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

Additionally, its response capabilities are fast and automatic—blocking ransomware within as little as three seconds to minimize damage. Athena EPP 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, Athena EPP 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, Athena EPP 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.

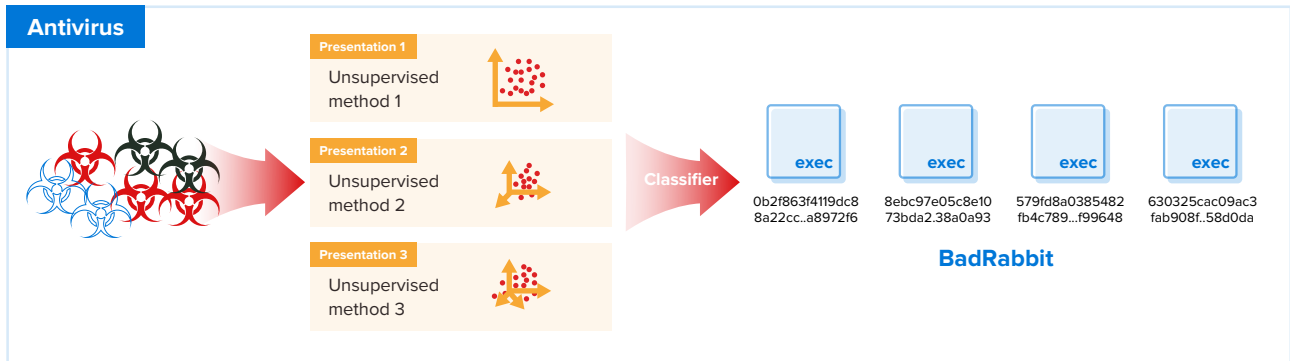
Architecture of Athena EPP



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.

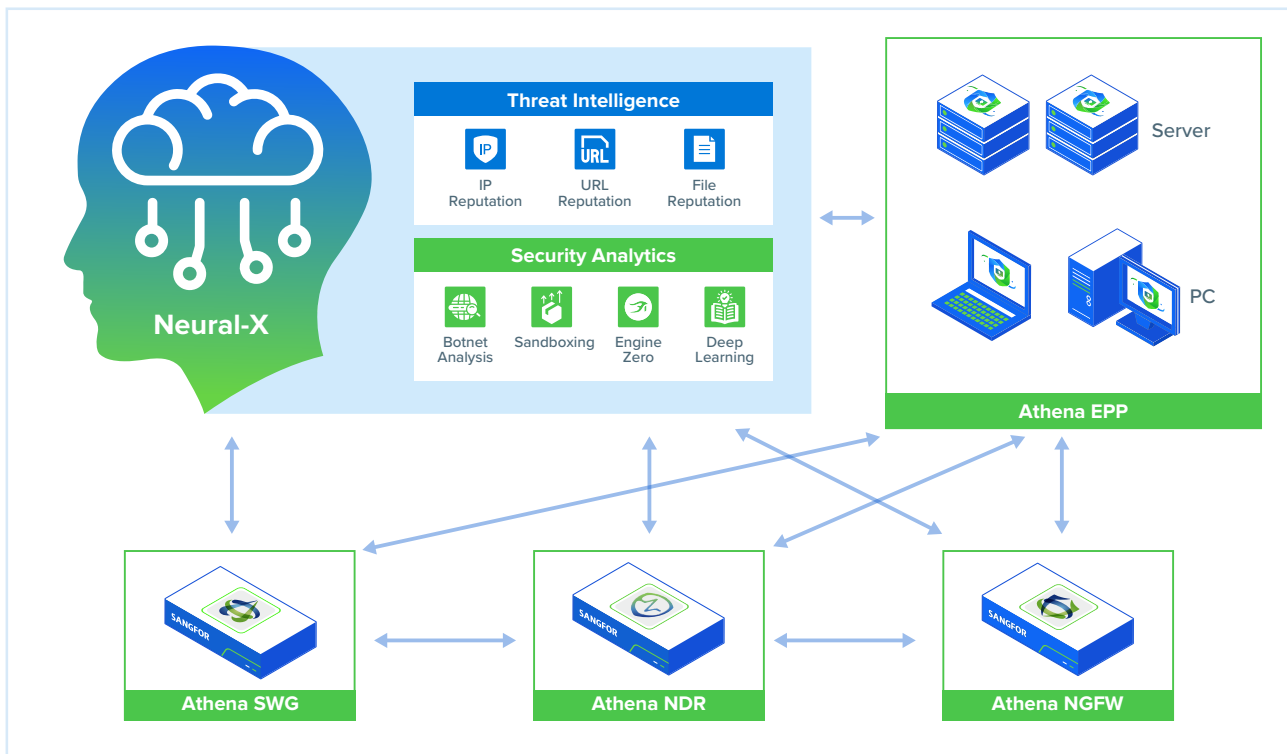


Reliance on manual security operations processes is inadequate for addressing fast-moving and complex threats, thereby exposing organizations to a wider attack surface.

Why Sangfor Athena EPP 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. Athena EPP 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 Sangfor Athena EPP is Effective:

1. Athena EPP integrates seamlessly with Sangfor Neural-X, Athena NGFW, Athena NDR, Athena XDR, and Athena SWG, 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 Athena NGFW or Athena NDR can be responded to directly through Athena EPP 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 Athena EPP Key Capabilities



Protects against all types of ransomware through static and dynamic AI-based detection engines.



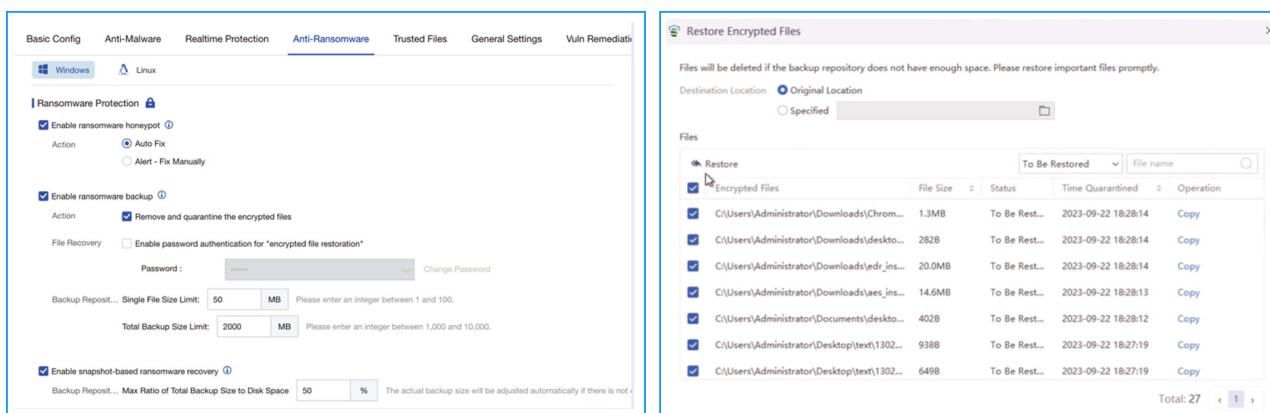
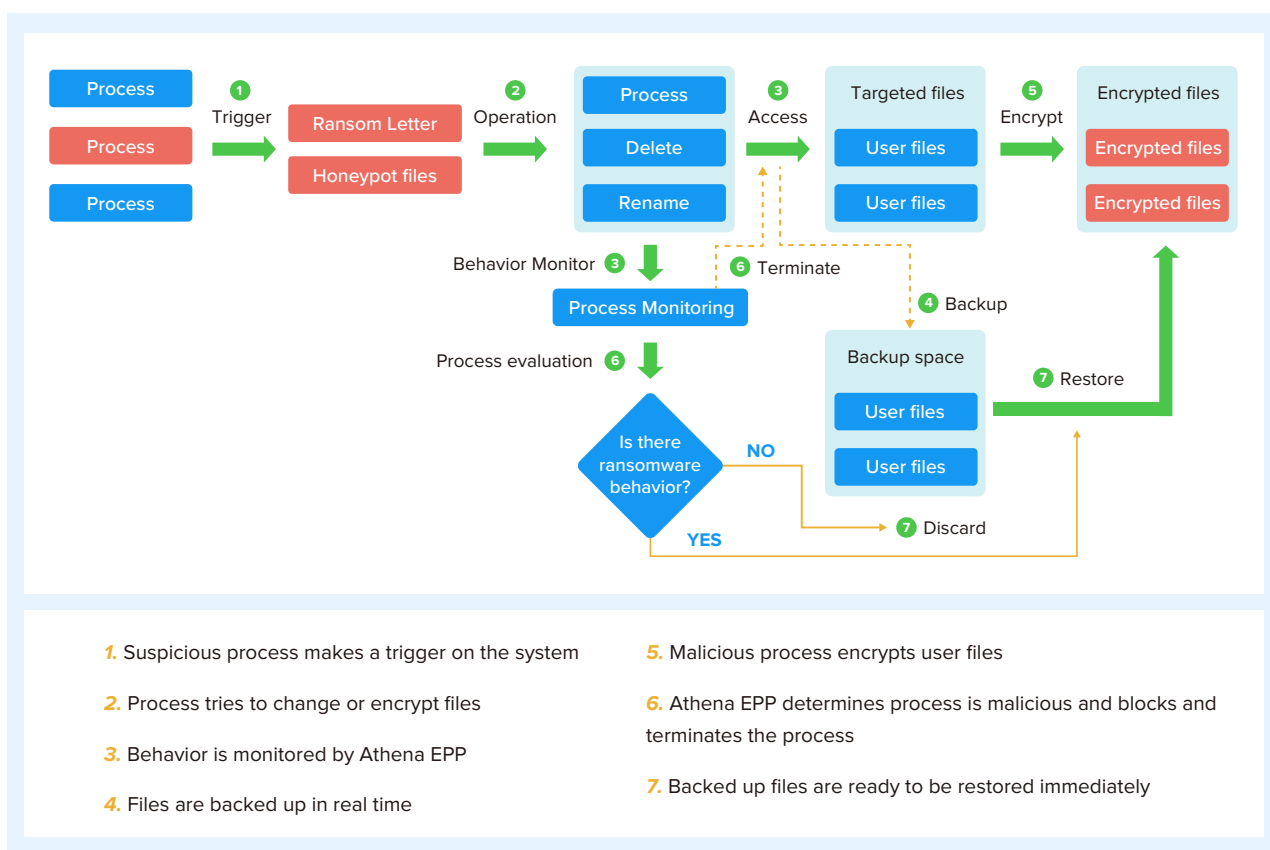
Detects suspicious ransomware-related processes and blocks them *in as little as 3 seconds* to ensure minimal impact on users' assets.



Ransomware indicators of compromise are collected from over 12 million devices deployed with Athena EPP, 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, Athena EPP 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.



AI-powered Malware Detection 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 Athena EPP a perfect 6 for Protection, Performance, and Usability, earning it the AV-TEST "TOP PRODUCT" award.



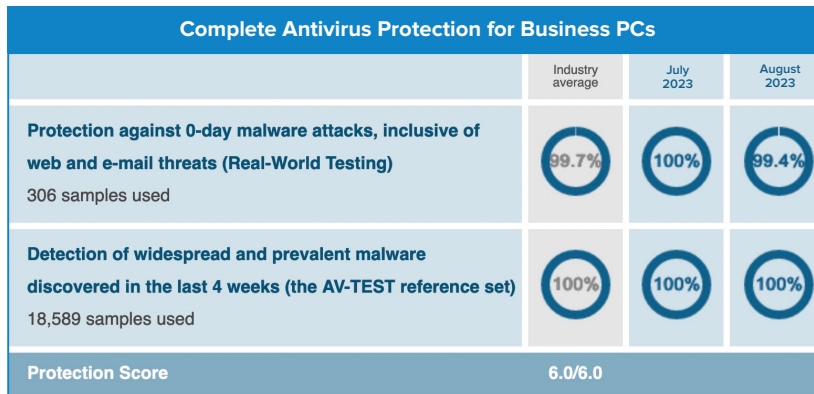


Figure 1. Sangfor Athena EPP Protect test results for Protection

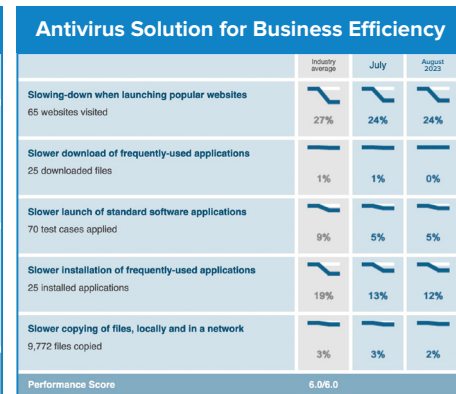













Figure 2. Sangfor Athena EPP Protect test results for Performance

High Compatibility

Covers multiple operating systems with constant updates to adapt to new systems and reinforce your defenses.

 Windows				
Windows	macOS	Ubuntu	Redhat	CentOS
<ul style="list-style-type: none"> Windows 7 SP1 (with SHA256 Patch) Windows 10 Windows 11 Windows Server 2008 R2 SP1 (with SHA256 Patch) Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 	<ul style="list-style-type: none"> macOS 10.13 macOS 10.14 macOS 10.15 macOS 11.x macOS 12.x macOS 13.x macOS 14 macOS 15 	<ul style="list-style-type: none"> Ubuntu 18 Ubuntu 20 Ubuntu 22 Ubuntu 24 	<ul style="list-style-type: none"> RHEL7 RHEL 8 RHEL 9 	<ul style="list-style-type: none"> CentOS 7 CentOS 8

					
Debian	SUSE	Oracle Linux	AlmaLinux	Rocky Linux	Alibaba Cloud Linux
<ul style="list-style-type: none"> Debian 9 Debian 11 Debian 12 	<ul style="list-style-type: none"> SUSE 12 SUSE 15.X 	<ul style="list-style-type: none"> Oracle Linux 7 Oracle Linux 8 Oracle Linux 9 	<ul style="list-style-type: none"> AlmaLinux 8.3 AlmaLinux 8.9 AlmaLinux 9.2 AlmaLinux 9.3 AlmaLinux 9.4 AlmaLinux 9.5 	<ul style="list-style-type: none"> Rocky Linux 8.4 Rocky Linux 8.7 Rocky Linux 8.8 Rocky Linux 8.10 Rocky Linux 9.2 	<ul style="list-style-type: none"> Alibaba Cloud Linux 3.2104 LTS Alibaba Cloud Linux 2.1903 LTS

Advanced Threat Analysis & Respond with MITRE ATT&CK®

ATT&CK™ Matrix											
Hit Tactics: 5					Hit 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		Masquerading 1					Ingress Tool Transfer 1		Resource Hijacking 1
		Valid Accounts 1		Obfuscated Files or ... 1					Application Layer P... 2		
		Event Triggered Exe... 1		BITS Jobs 1							
				Impair Defenses 1							

Faster and more accurately find the threats in the endpoint.

Sangfor Athena EPP Certifications and International Awards

Athena EPP 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 Athena EPP and the excellent user experience we deliver.

Gartner

Athena EPP 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.

AV-TEST
The Independent IT-Security Institute
Established 1996

Sangfor Athena EPP 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. Athena EPP’s achievement of this certification demonstrates its compliance with OPSWAT’s rigorous standards and its commitment to delivering an effective endpoint security solution.

OPSWAT.

Edition and Features

	Feature/Module	Essential Edition	Ultimate Edition
Prevention	Vulnerability Scan	✓	✓
	Remediation	✓	✓
	Security Compliance Check	✓	✓
	Asset Inventory	✓	✓
	Asset Discovery	✓	✓
	TOTP Authentication	✓	✓
	Endpoint Behavior Data & Log Collection		✓
Protection	Realtime File Monitoring	✓	✓
	Ransomware Honeypot	✓	✓
	Ransomware Protection	✓	✓
	Ransomware Backup Recovery	✓	✓
	Ransomware Defense	✓	✓
	RDP Secondary Authentication (Anti-Ransomware)		✓
	Trusted Processes (Anti-Ransomware)		✓
	Key Directory Protection (Anti-Ransomware)		✓



Edition and Features

Feature/Module		Essential Edition	Ultimate Edition
Detection	Malicious File Detection	✓	✓
	Botnet Detection	✓	✓
	Brute-Force Attack Protection	✓	✓
	Coordinated Threat Detection with Athena SecOps		✓
	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	✓	✓
	Coordinated Response with Athena NGFW	✓	✓
	Coordinated Response with Athena SecOps		✓
	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

380 Jln Besar, #08-04/05 ARC 380,
Singapore 209000
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

Suite 11.01 & 11.02, Level 11 Centrepoint North,
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) 968-899-8920

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 TÜRKİYE

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 Joaquín 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

Athena SWG - Secure Web Gateway

Secure User Internet Access Behaviour

Athena NGFW - Next Generation Firewall

Smarter AI-Powered Perimeter Defence

Athena EPP - Endpoint Protection Platform

The Future of Endpoint Security

Athena NDR - Network Detection and Response

Smart Efficient Detection and Response

Athena XDR - 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

Athena MDR - 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

Athena SASE - Secure Access Service Edge

Secure, Agile, and Everywhere

EDS - Enterprise Distributed Storage

The Only Secured Data Storage You Need





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 
sales@sangfor.com 
www.sangfor.com 