HAFS
Distributeur à valeur ajoutée

Distributeur à valeur ajoutée de solutions IT

Cybersécurité | Réseaux | Wi-Fi | Stockage

Une solution pour chaque environnement

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”

AV-TEST
The Independent IT-Security Institute

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.

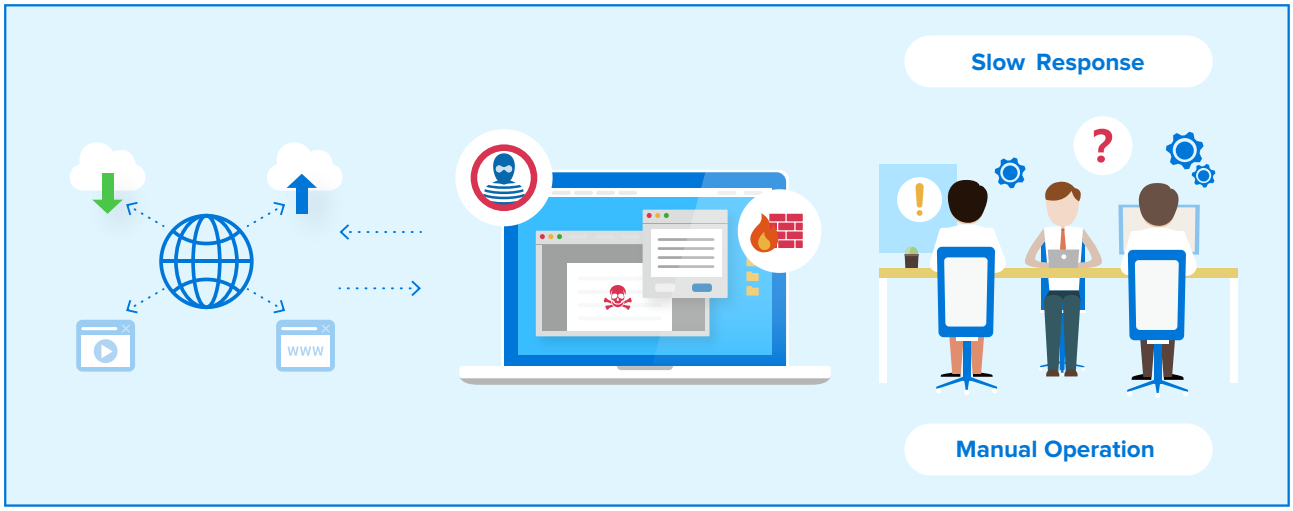
Why Traditional Endpoint Security Falls Short

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 Outdated Signature-based Detection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.

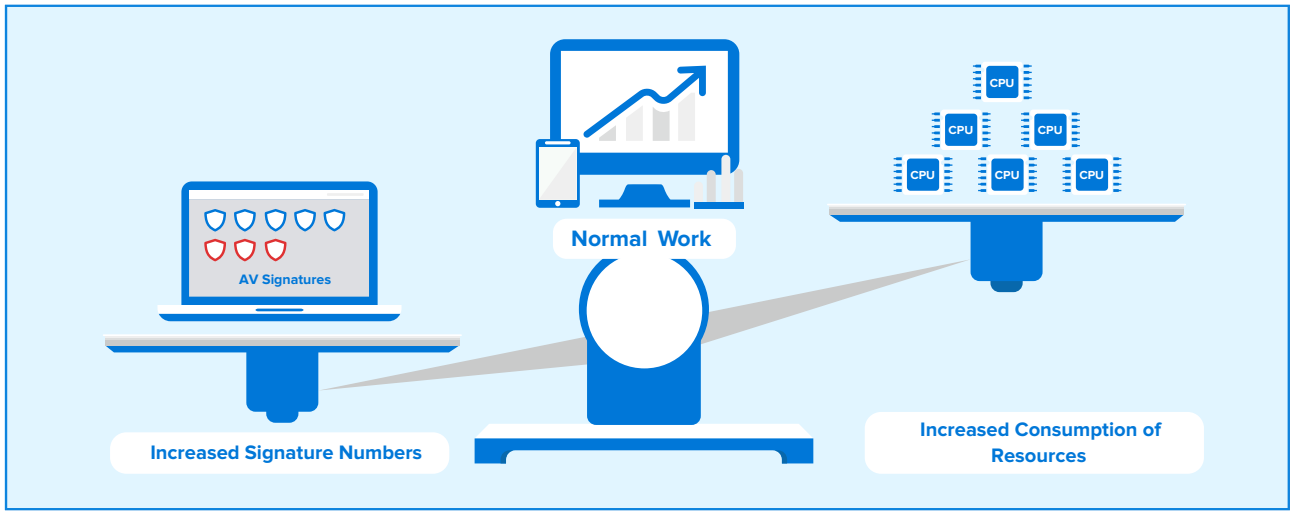
2. Inefficient and Costly Manual Operations and Maintenance

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.



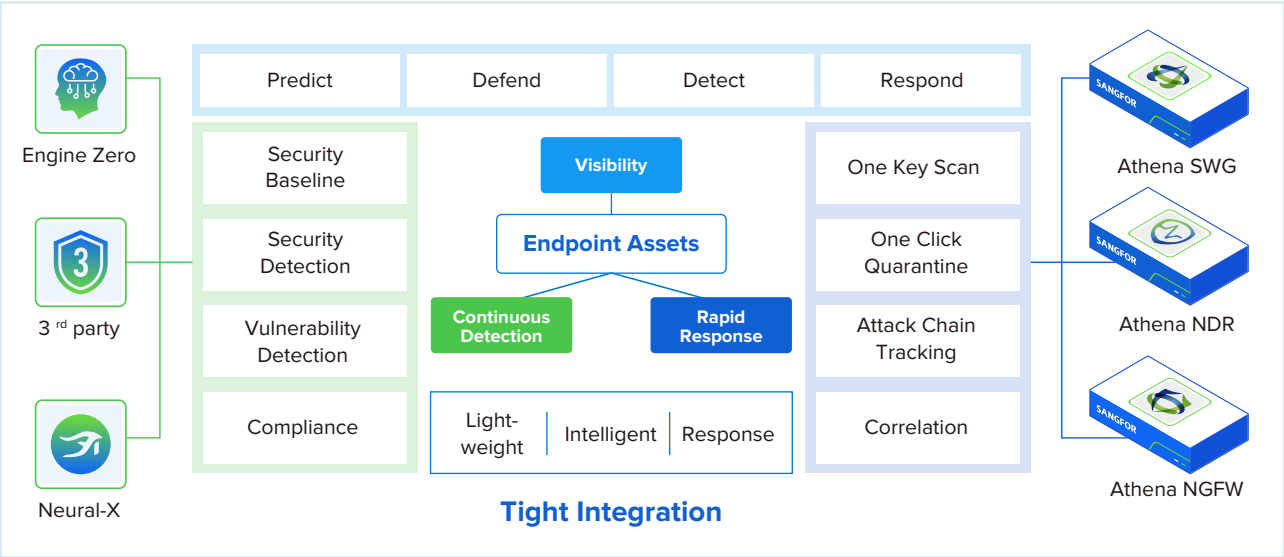
3. High Resource Consumption

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 Athena EPP: The Future of Endpoint Security

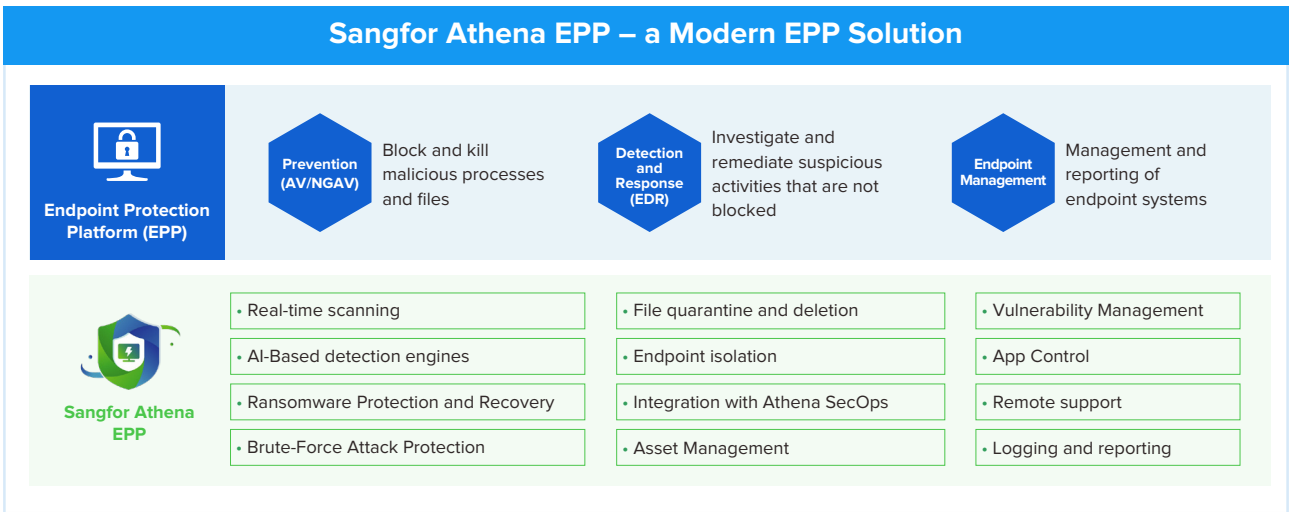
Sangfor Athena EPP (previously known as Sangfor Endpoint Secure) is a Modern Endpoint Protection Platform (EPP) that combines Next-Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), and Endpoint Management into a single, unified solution. This all-in-one approach provides comprehensive 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.



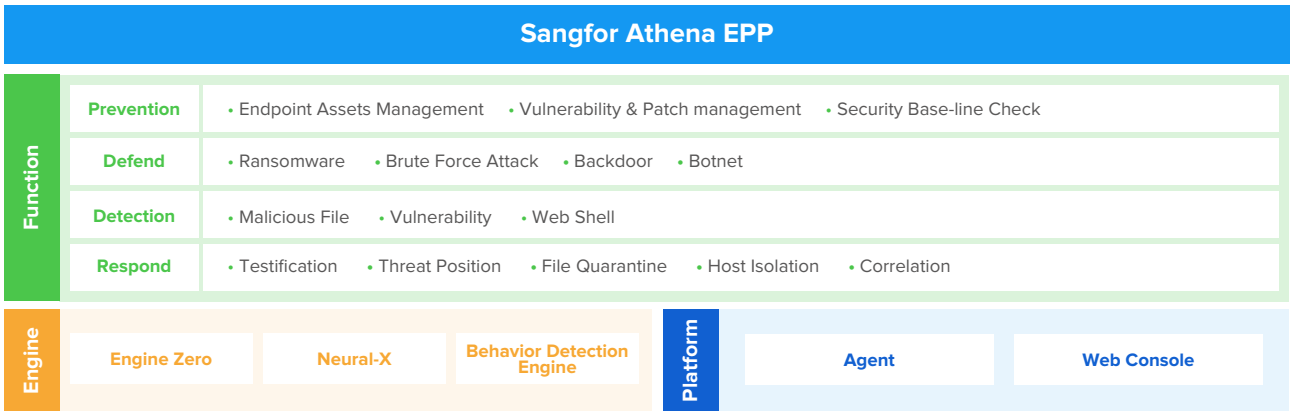
To stay ahead of the latest threats, Athena EPP integrates with the Sangfor Neural-X threat intelligence and analytics platform, which collects threat intelligence feeds from extensive sources. This constant stream of updated intelligence ensures that Athena EPP remains prepared to handle any emerging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

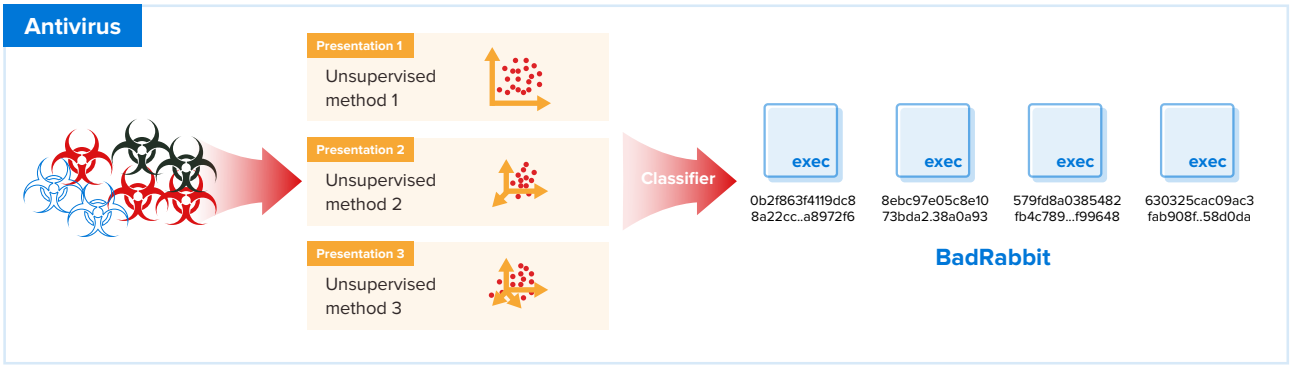
Beyond threat detection and response, Athena EPP streamlines operations and maintenance (O&M) through comprehensive endpoint management capabilities. Organizations can proactively scan endpoints for misconfigurations and vulnerabilities—gaps that attackers could exploit. Addressing these risks early 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:

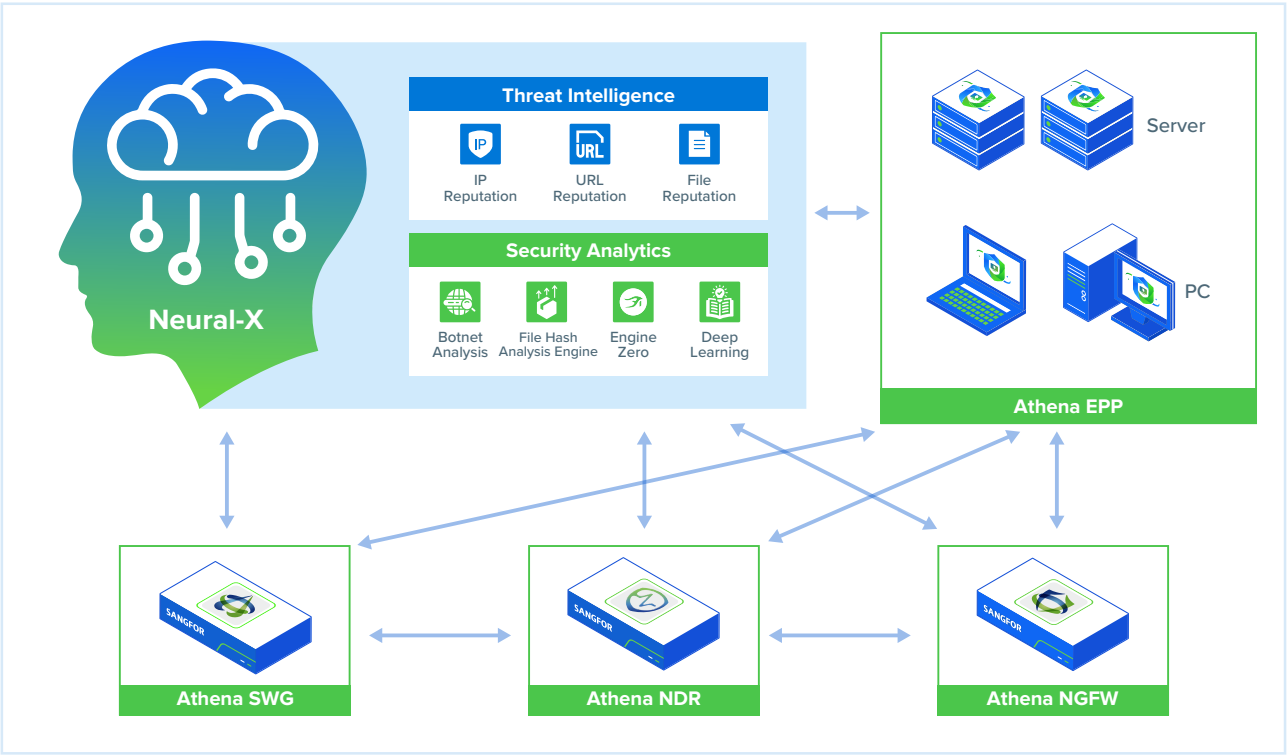
- Insufficient capabilities and resources to detect and respond to advanced and unknown threats, thus unable to provide a proactive defense.
- Reliance on manual security operations processes is inadequate for addressing fast-moving and complex threats, thereby exposing organizations to a wider attack 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.

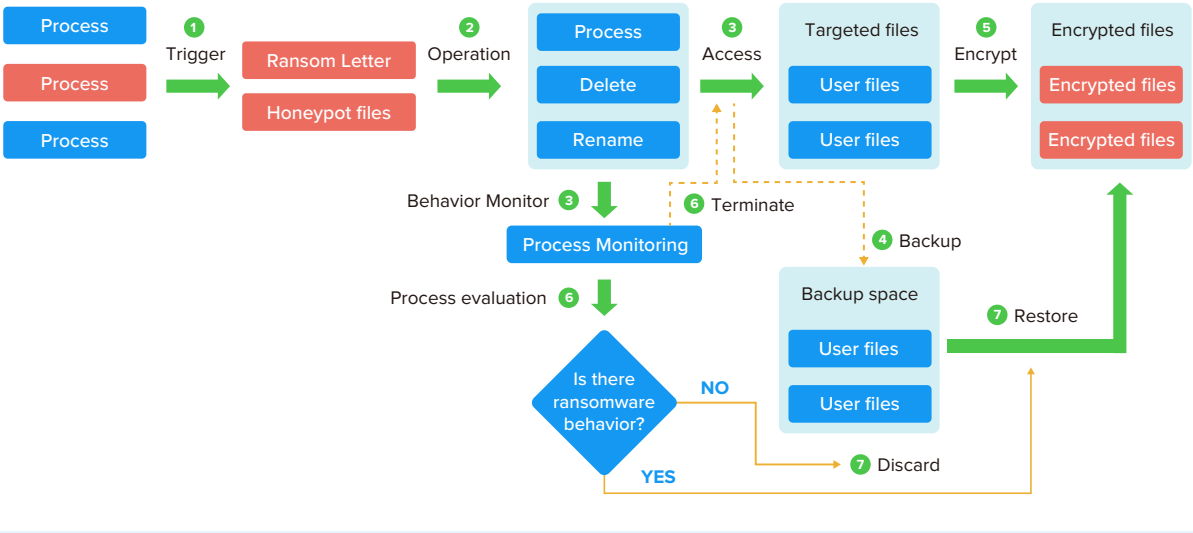
2. Response is fast and efficient through integration synergy. Threats detected on Athena NGFW or Athena NDR can be responded to directly through Athena EPP without the need to operate multiple consoles.

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.

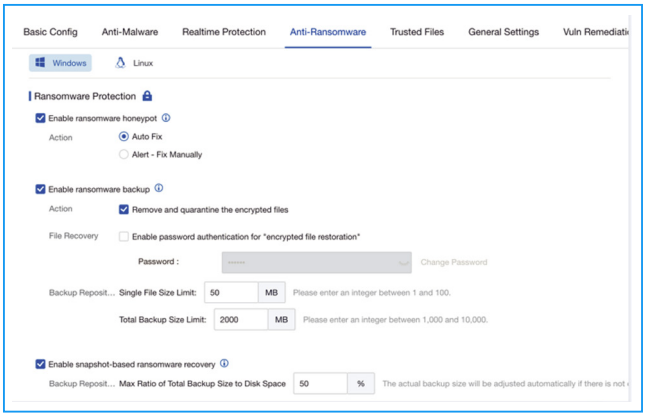
Advantages and Characteristics

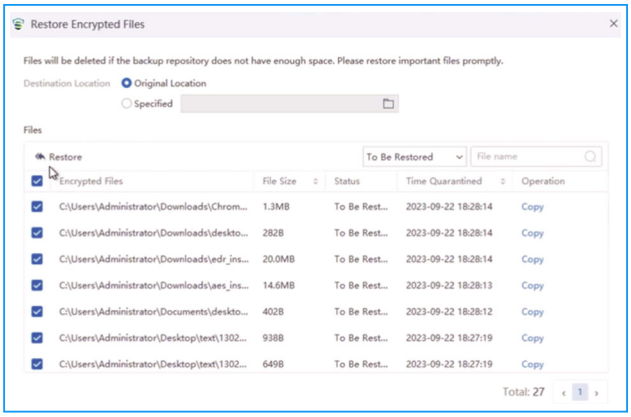
Ransomware Protection and Recovery

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.



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





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.

Sangfor Engine Zero

Sangfor Anti-Malware Engine

Artificial Intelligence Based Non-Signature Engine
Detect Unknown Malware Accurately

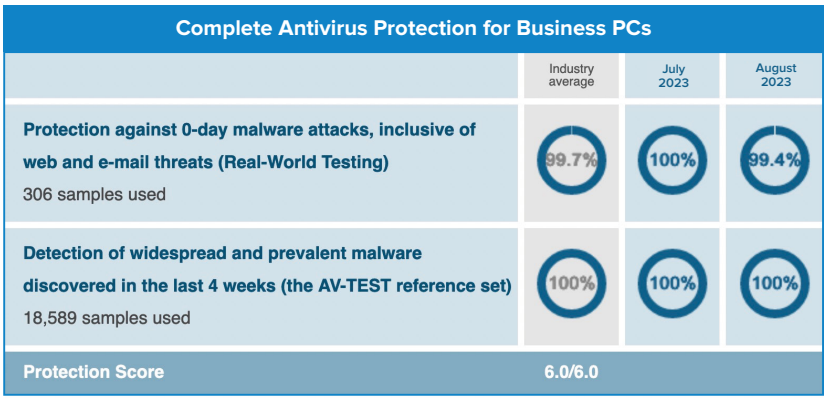


Figure 1. Sangfor Athena EPP Protect test results for Protection

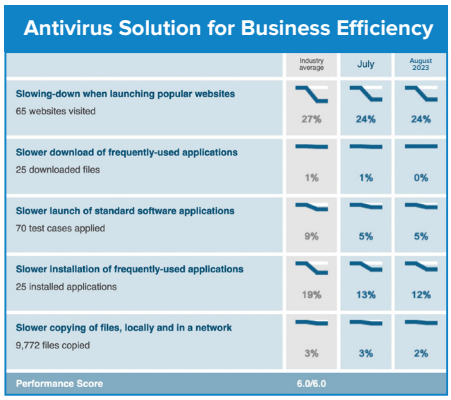


Figure 2. Sangfor Athena EPP Protect test results for Performance

High Compatibility

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

Windows	macOS	Ubuntu	Redhat	CentOS
• 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	• macOS 10.13 • macOS 10.14 • macOS 10.15 • macOS 11.x • macOS 12.x • macOS 13.x • macOS 14 • macOS 15	• Ubuntu 18 • Ubuntu 20 • Ubuntu 22 • Ubuntu 24	• RHEL7 • RHEL 8 • RHEL 9	• CentOS 7 • CentOS 8

Debian	SUSE	Oracle Linux	AlmaLinux	Rocky Linux	Alibaba Cloud Linux
• Debian 9 • Debian 11 • Debian 12	• SUSE 12 • SUSE 15.X	• Oracle Linux 7 • Oracle Linux 8 • Oracle Linux 9	• AlmaLinux 8.3 • AlmaLinux 8.9 • AlmaLinux 9.2 • AlmaLinux 9.3 • AlmaLinux 9.4 • AlmaLinux 9.5	• Rocky Linux 8.4 • Rocky Linux 8.7 • Rocky Linux 8.8 • Rocky Linux 8.10 • Rocky Linux 9.2	• Alibaba Cloud Linux 3.2104 LTS • Alibaba Cloud Linux 2.1903 LTS

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.

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.

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.

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 Bait Files	✓	✓
	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.

SANGFOR | SANGFOR SECURITY

SANGFOR
ATHENA NDR

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 Athena NDR

AI-Powered, Intelligent Threat Detection and Response Platform

Sangfor Athena NDR (previously known as 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, Athena NDR 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, Athena NDR 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 Athena NDR, 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

Athena NDR 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. Athena NDR 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

Athena NDR persistently monitor network-wide traffic, employing advanced techniques to furnish the security team with unparalleled visibility of the network environment. This not only uncovers hidden threats but also provides real-time insights into network assets, exposing risky shadow IT and vulnerabilities like unpatched software, weak passwords, and missing encryption, thereby enabling immediate remediation. Additionally, we have extended our integration capabilities with third-party tools, facilitating the ingestion of data from a variety of firewalls and endpoints from distinguished vendors such as Sophos, Symantec, PaloAlto, Kaspersky, and others. This expanded capacity enhances your operational visibility, offering a more holistic understanding of potential threats within your network, and empowering you with the tools to effectively detect and counter them.

In-Depth Threat Hunting & Investigation

Athena NDR 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.

Automated & Integrated Incident Response

Athena NDR 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. Athena NDR also integrates seamlessly with Sangfor and third-party security tools to initiate coordinated response actions.

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

Integrate Athena NDR Seamlessly Into Your Security Ecosystem

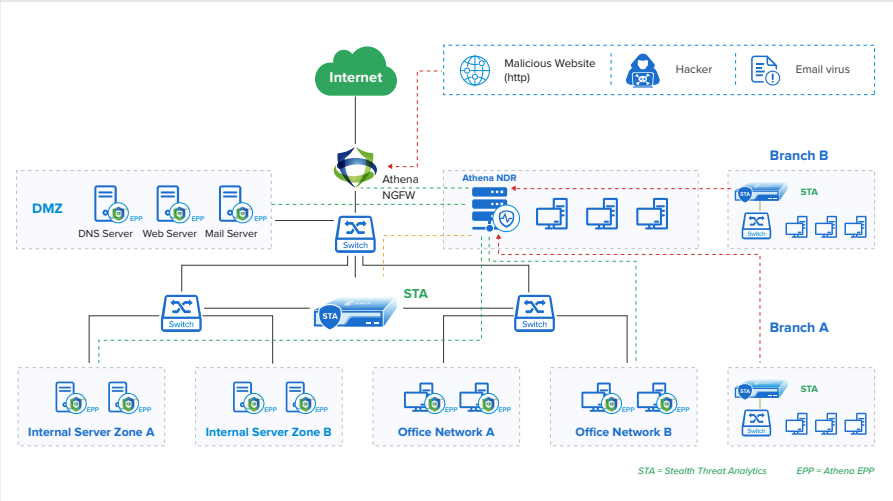
For a long time, organizations have been building complex security stacks comprising multiple security tools layered on top of each other. This approach has resulted in a range of issues, such as poor integration leading to security gaps, overlapping features, and complex management.

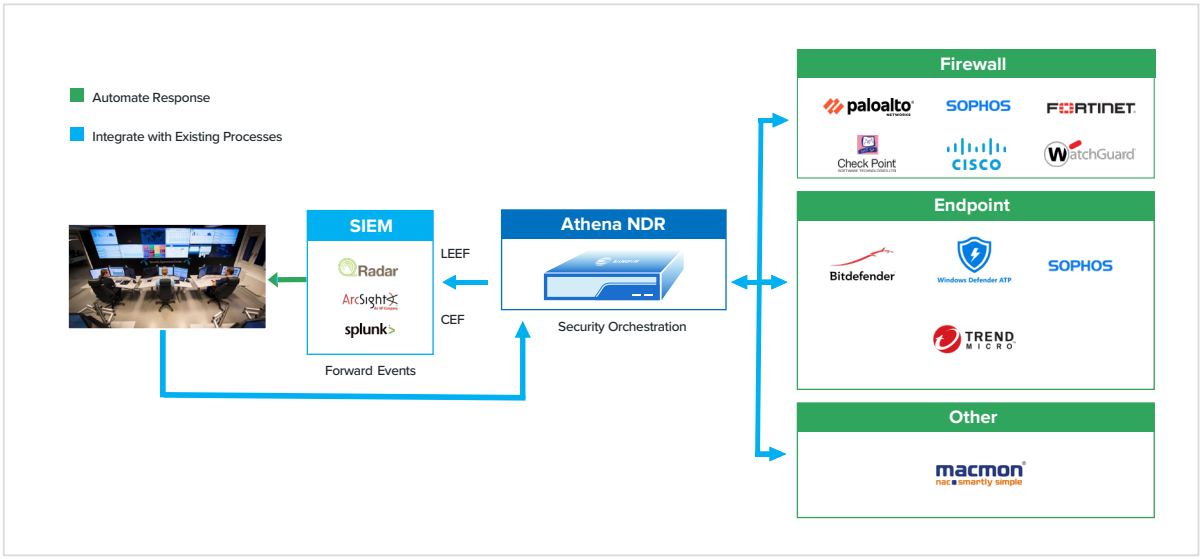
As such, organizations are starting to rethink their approach by adopting what is known as a security ecosystem - a comprehensive network security architecture where multiple security technologies, tools, and services are integrated to provide a unified defense against cyber threats. An integrated security 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.

Athena NDR is designed to integrate seamlessly with other Sangfor products and services, including Athena NGFW, Athena EPP, and Neural-X, as part of Sangfor's Extended Detection, Defense, and Response (XDDR) framework. Using its built-in SOAR module, Athena NDR is at the heart of this integrated system, issuing effective response actions to the other components. For example, Athena NGFW can be instructed to block communication to and from a specific IP address or port. Athena EPP can provide Athena NDR 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.

Athena NDR also extends its capabilities by incorporating third-party firewalls and endpoint protection systems from a wide range of industry-leading vendors such as Palo Alto, Fortinet, Sophos, Cisco, Bitdefender, Trend Micro, WatchGuard, and others. This collaborative approach enhances our capacity to provide incident response capabilities.

Moreover, we now offer enhanced support for ingesting data from third-party devices for a more profound analysis and detection process. We've broadened our integration capabilities, with the capability to ingest data from an array of firewalls and endpoints, from highly esteemed vendors such as Sophos, Symantec, PaloAlto, Microsoft, Kaspersky, McAfee, Cisco, Fortinet, and more. This feature augments your operational visibility by providing a more comprehensive understanding of potential endpoint threats within your network and equips you with the capacity to effectively detect and respond to them.





Components

Athena NDR

Athena NDR 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 Analytics (STA)

Sangfor STA is the sensor used in the Athena NDR 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 Athena NDR 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.

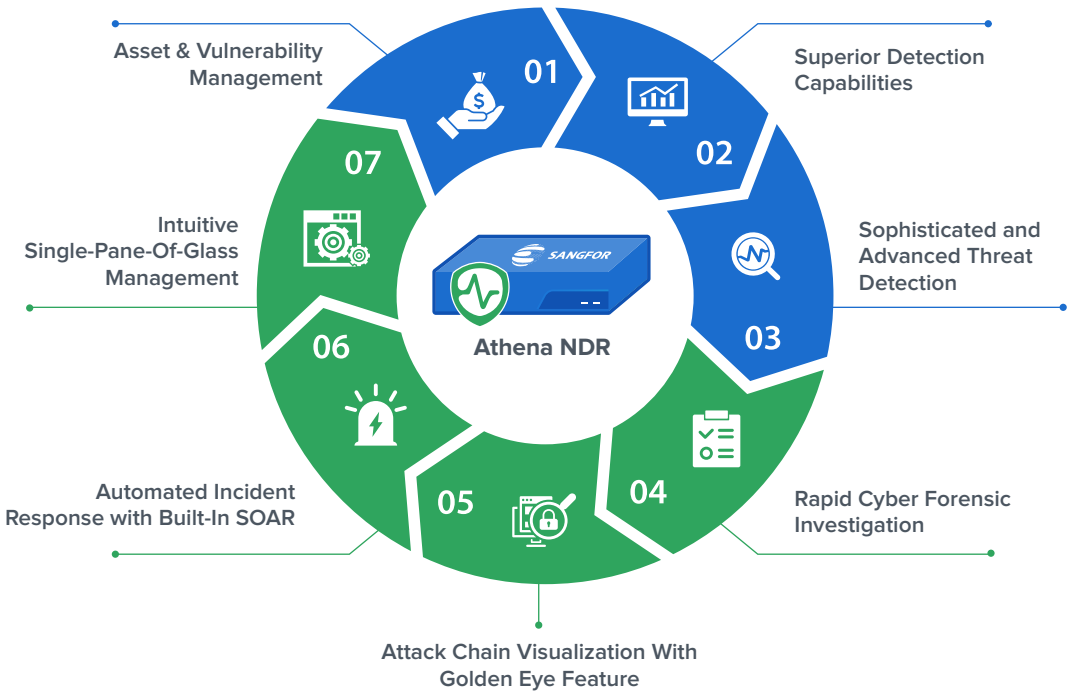
Athena NGFW

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

Athena EPP

Sangfor Athena EPP 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. Athena EPP helps Athena NDR collect rich digital evidence to support forensic investigation while Athena NDR coordinates with Athena EPP to remediate endpoint threats.

Key Features



1. Asset & Vulnerability Management

Athena NDR automatically discovers and inventories all assets in the environment, including previously unknown shadow IT assets that pose a risk to the network environment. Athena NDR 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

Athena NDR 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, Athena NDR monitors user and entity behavior, establishing baselines and employing machine learning for real-time anomaly detection.

3. Sophisticated and Advanced Threat Detection

Athena NDR 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, Athena NDR 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 Athena NDR platform.

5. Attack Chain Visualization With Golden Eye Feature

Athena NDR'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

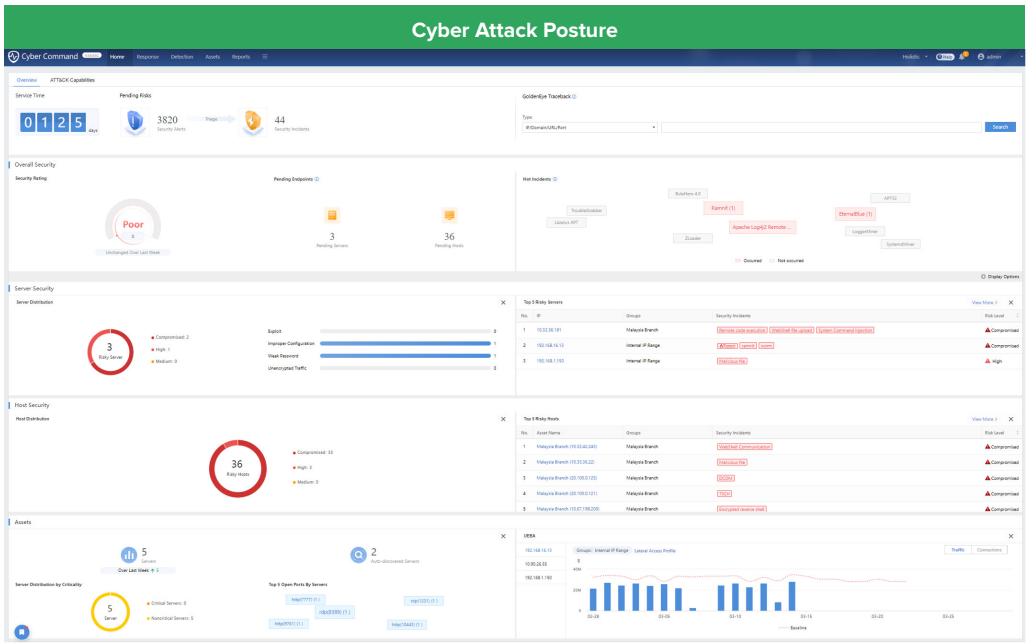
Athena NDR provides automated response with its unique built-in SOAR module. Pre-defined playbook templates allow security teams to effortlessly orchestrate incident response actions to some common threat scenarios. They can also customize responses tailored to their specific needs. With Athena NDR SOAR, 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 Athena NDR 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.

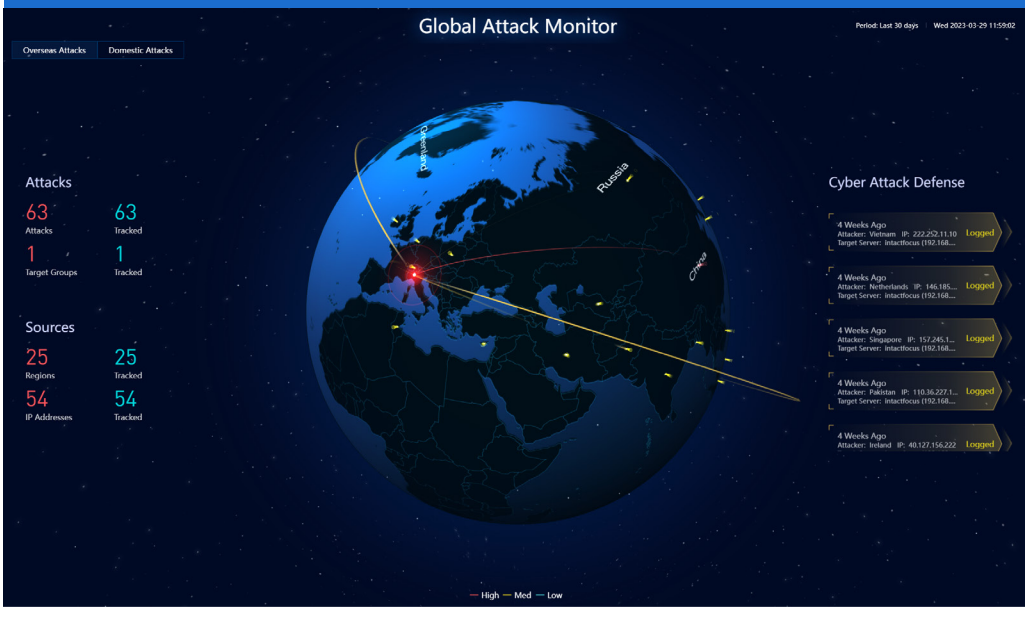
» Keep Threats at Bay with Unprecedented Visibility And Advanced Detection & Response

Athena NDR 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.



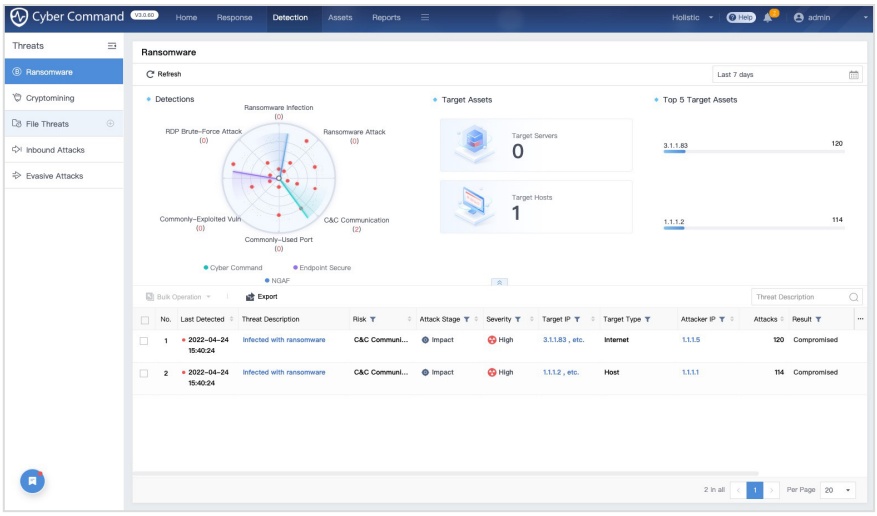
Outbound Threat Monitoring

Global Attack Monitoring

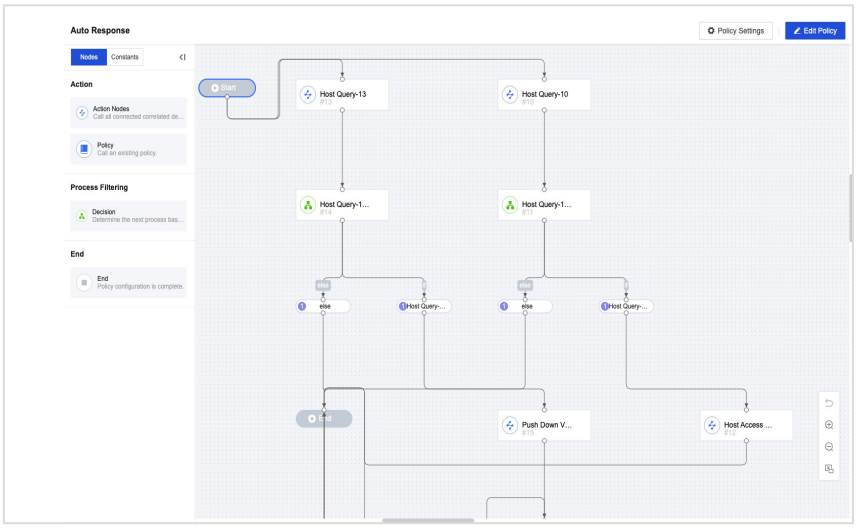


Athena NDR protects organizations from sophisticated cyber threats with multiple detection engines and advanced threat detection techniques, while built-in SOAR ensures immediate incident response to detected threats. Full MITRE ATT&CK mapping further provides detailed insights for informed decision-making.

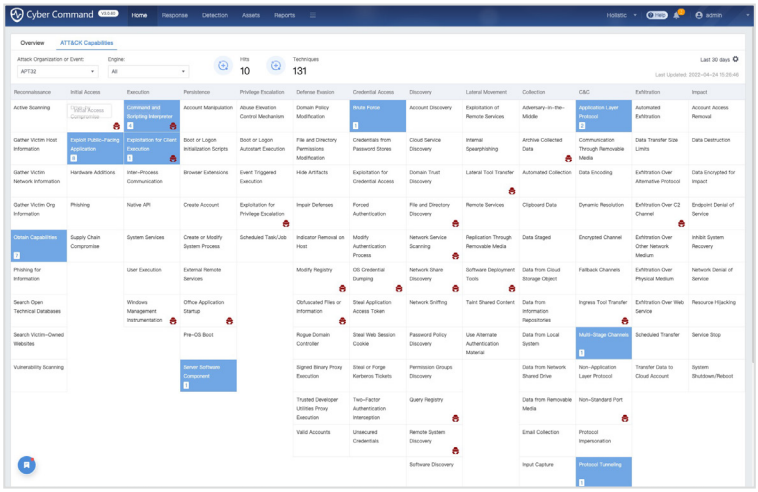
Advanced Threat Detection

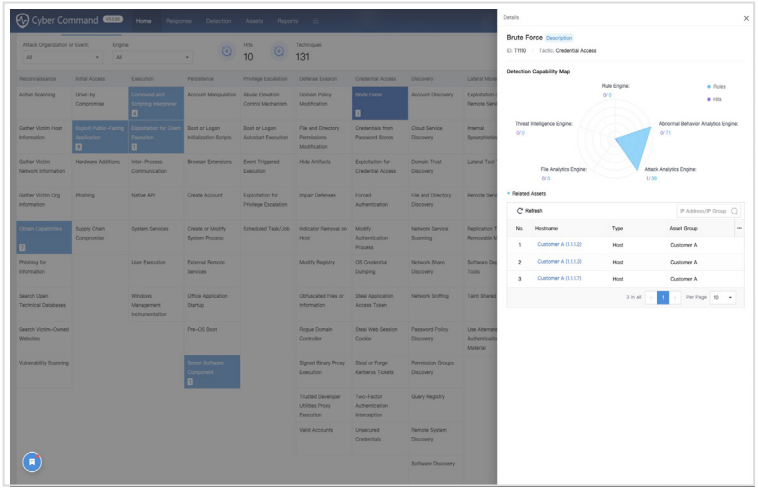


Auto Response with SOAR



MITRE ATT&CK Mapping





How is Athena NDR Different?

Superior Threat Detection and Analysis	
AI-Driven Threat Detection and Analysis	Athena NDR 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. Athena NDR 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)	Athena NDR 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	Athena NDR 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	Athena NDR 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	Athena NDR 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 Athena NDR platform.

Truly Automated and Integrated Incident Response	
Built-In SOAR Module	Athena NDR 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. Athena NDR'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 Athena NDR, Athena NGFW, Athena SWG, and Athena EPP to break down security silos and provide end-to-end protection across your entire network infrastructure. Athena NDR 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 Athena NDR

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, Athena NDR provides an advanced defense system that proactively detects and prevents cyber threats before they can inflict harm.

2 Streamline Security Operations

Athena NDR 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

Athena NDR 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 Athena NDR, 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 Athena NGFW

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
Athena NGFW meets all of ICSA Labs' corporate and baseline firewall requirements

AV-Test Certification
Sangfor Athena EPP receives Top Award for Windows antivirus software for business users

AAA Rating from CyberRatings
Athena NGFW 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 Athena NDR POC.
Take this opportunity to evaluate and improve your security posture!

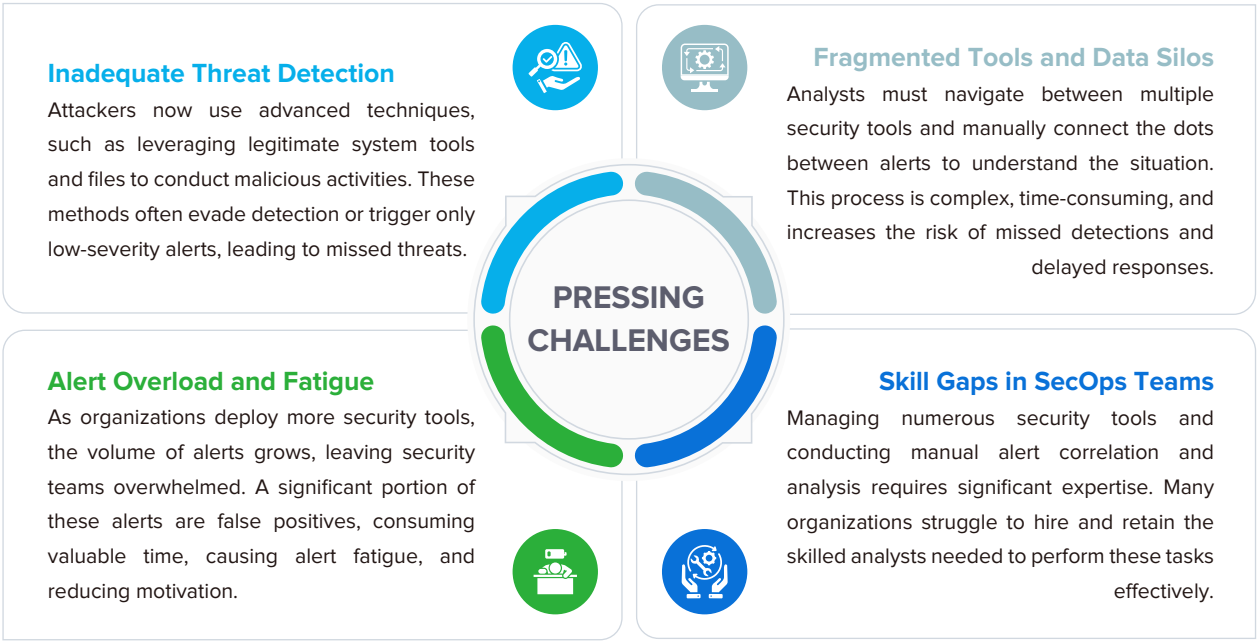
SANGFOR | SANGFOR SECURITY

SANGFOR ATHENA XDR

Extended Detection and Response

The Challenge: The Mismatch Between Traditional Security Solutions and Modern Cyber Threats

Today's cyber threat landscape is marked by adversaries deploying AI-powered malware, sophisticated phishing campaigns, and stealthy lateral movements to exploit organizational vulnerabilities. While traditional security tools still play an important role, they often lack the integration and context needed to counter these advanced tactics. Security teams face several pressing challenges:



The Solution: Sangfor Athena XDR SecOps Platform

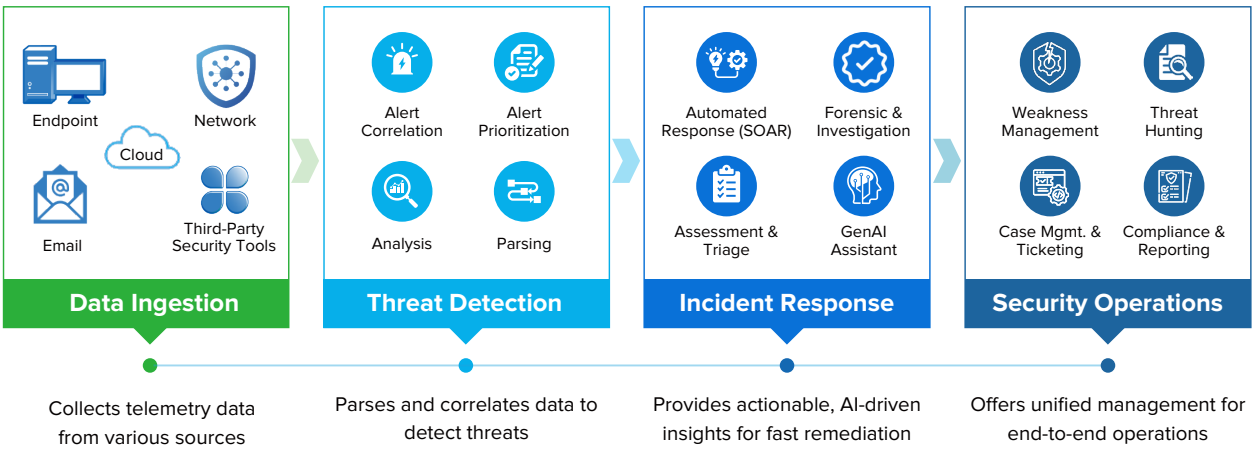
Sangfor Athena XDR (Extended Detection and Response) rises to this challenge by unifying detection and response through the consolidation of data and alerts from diverse sources. These include endpoint security tools, network security devices (firewalls and NDR), cloud environments, applications and email (Microsoft 365), and third-party solutions. By analyzing and correlating this data with advanced AI-driven analytics, Athena XDR provides critical context, enabling the detection of complex, multi-stage attacks that individual point solutions might overlook or flag as false positives.

The platform connects events across the technology landscape to offer a holistic view of threats. This helps security analysts assess the entire attack chain—from the initial entry point to the overall impact. This enhanced visibility enables teams to verify threats effectively and make informed response decisions.

Through this seamless integration of security tools, Athena XDR also enables automated, coordinated responses. It can instruct firewalls to block malicious domains or IP addresses, command endpoint tools to isolate compromised devices and initiate scans, and more. This ensures a swift and comprehensive defense against identified threats.

How Sangfor Athena XDR Works

Athena XDR provides a unified approach to threat detection, investigation, and response through these key steps:



Comprehensive Data Collection

- Aggregates data from endpoints security tools, network security devices, cloud, applications and email (Microsoft 365), and third-party tools.
- Ensures no blind spots across the security landscape.

AI-driven Incident Correlation & Analysis

- Correlates related alerts into unified incidents with actionable insights.
- Utilizes three powerful layers of detection engines to accurately uncover hidden threats and attacks.

Simplified Threat Investigation & Response

- Enriches incident alerts with full context for threat hunting and investigation.
- Features SOAR capabilities with customizable playbooks for automated response actions.
- Powered by Security GPT, ensuring every security alert and incident are summarized in natural language dialogue to allow faster and more accurate visualization and determination of attack patterns.

Beyond XDR: Revolutionize Your Security Operations

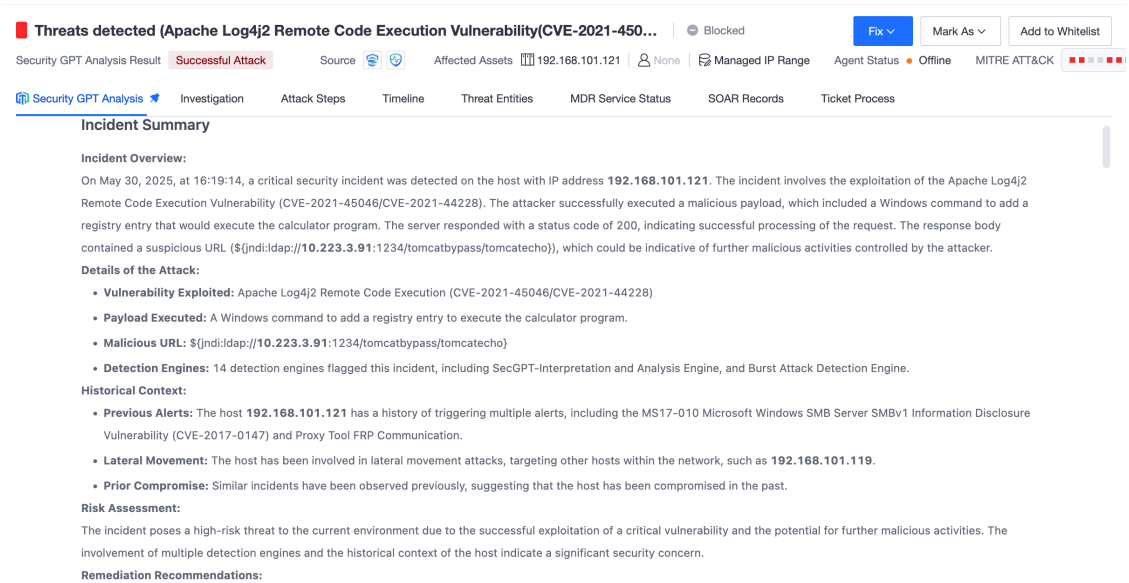
Sangfor Athena XDR redefines security operations by serving as a unified SecOps platform. It integrates critical security functions into a single solution, including workflow automation, threat intelligence, SOAR, SIEM-like data fusion, reporting, and ticketing. This integration eliminates the traditional challenges of managing separate toolsets, saving costs and reducing operational complexity.

Security Operations	Data Fusion	Threat Intelligence	AI Engines	Threat Triage	SOAR	Ticketing	Reporting

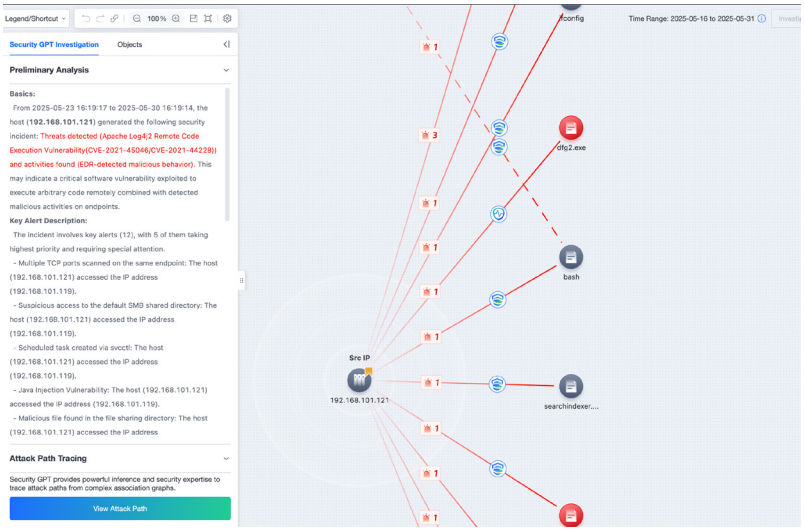
Athena XDR also supports flexible integration with third-party tools, allowing organizations to maximize existing investments while gradually transitioning to Sangfor's native solutions for optimized performance. Available in both **on-premises and SaaS-based models**, Athena XDR adapts to your organization's unique deployment needs. Whether you're looking for the control of an on-premises setup or the scalability of a cloud solution, Athena XDR provides a flexible, future-ready approach to cybersecurity.

Intelligent & Autonomous Operations with Security GPT

A standout feature of Athena XDR is the integration of **Security GPT**, a GenAI tool powered by a Large Language Model (LLM). Security GPT enhances Athena XDR's threat detection and response capabilities with cutting-edge AI-driven functionality. Its operations module, **Operation GPT**, analyzes all alerts with the precision of a human analyst, accurately identifying security incidents and filtering out false positives. This not only saves significant time for security teams but also ensures that no threats remain hidden in uninvestigated alerts.



Security GPT not only detects incidents but investigates them, presenting findings in clear, plain language. It provides detailed insights, including the type of threat, the chain of events, the affected assets, and more. This actionable information enables security teams to quickly grasp the “why” behind each incident and accelerate remediation. Even less experienced analysts can confidently handle complex incidents with the support of these detailed insights.



Through self-learning, Security GPT can autonomously execute response actions, such as isolating endpoints, blocking malicious domains, and removing malicious files. This further reduces the need for manual intervention, cutting response times and minimizing impact. Moreover, Security GPT supports dialogue-based operations, enabling analysts to ask questions and visualize data patterns interactively. This functionality makes threat analysis more intuitive and actionable.

Together, Athena XDR and Security GPT streamline security operations, empowering security teams to act faster and more effectively in a constantly evolving threat landscape.

Essential Components of Sangfor Athena XDR

Sangfor Athena EPP

A modern Endpoint Protection Platform (EPP) used for collecting endpoint data and enforcing response actions. Rated a “Top Product” by AV-TEST, consistently achieving maximum scores for Protection, Performance, and Usability.

and/or

Sangfor Athena STA

Athena STA is a network sensor used for aggregating network traffic and performing initial analysis before sending results to the XDR platform. Customers who have purchased Athena NDR with Athena STA can also integrate it with Athena XDR to forward alerts for unified analysis and management.

Optional Components of Sangfor Athena XDR

Sangfor Security GPT (for on-premises XDR)

A powerful generative AI that significantly enhances threat detection accuracy (Detection GPT) and autonomously handles alert analysis, incident investigation, and incident response (Operation GPT).

Sangfor Athena NGFW

A Next-Generation Firewall (NGFW) used for collecting network data and enforcing response actions. Recognized as a “Visionary” in the Gartner Magic Quadrant and rated “Recommended” by CyberRatings.org for its comprehensive security capabilities.

Sangfor Athena SWG

A Secure Web Gateway (SWG) used for synchronizing user authentication information, helping security operations teams pinpoint at-risk users and hosts.

Third-Party Security Tools – EDR/EPP and Firewall

Used for data ingestion and executing response actions. Other customized integrations can be supported upon evaluation by the Sangfor team.

Sangfor Athena MDR

A Managed Detection and Response service that connects to the customer's Athena XDR platform for expert-led 24/7 monitoring, threat detection, and response.

Key Features & Capabilities of Sangfor Athena XDR

Threat Detection in Real Time

- Detection technologies: Purpose-built AI threat detection models, machine learning, indicators of attack (IOA) engine, behavioral baseline, network anomaly detection, custom IOCs & IOAs
- End-to-end visibility across endpoints, networks, and third-party security tools, enabling proactive defense against hidden threats like shadow IT, vulnerabilities and eliminating blind spots
- Detection mapped to the MITRE ATT&CK framework of tactics, techniques, and procedures (TTPs)

Noise Reduction with Correlation Analysis

- Uses machine learning to build a reliable baseline of normal business operations
- Correlates related attack data across multiple data sources to detect anomalies
- Endpoint + Network (E+N) correlation analysis, stitching all related events into a unified incident
- Intelligently groups alerts from different times, stages, methods of the same attack

Proactive Threat Hunting

- Security GPT: Enables dialogue-based threat investigations and delivers insights in graphical formats for easy interpretation
- Reconstructs the entire attack chain to understand the root cause and scope of impact
- See the entire chain of incidents with full contextual insights in an elegant visualization

AI-Driven Incident Response

- Built-in Security Orchestration, Automation, and Response (SOAR) module with predefined and customizable playbook policies, enabling coordinated responses across both Sangfor's native security tools and third-party tools
- Security GPT: Automates threat containment after a few days of self-learning from users' historical actions, such as isolating compromised endpoints, blocking malicious domains, or revoking compromised credentials
- Speed up incident response with Sangfor's in-house threat intelligence, providing direct context on adversaries

SecOps Task-Driven Platform

- Integrates essential SecOps functionalities, including SIEM-like data fusion, SOAR, reporting, and ticketing, into a single platform
- AI-driven platform transforming the SOC with XStream technology for automated data parsing, workflow automation to streamline operations, early threat detection, and rapid incident response
- Supports integration with GenAI - Security GPT: a 24/7 virtual security analyst

Key Business Benefits of Sangfor Athena XDR

99% Threat Detection Accuracy

Detect and neutralize 99% of threats within 5 minutes. This swift and accurate action is crucial for protecting your organization against advanced cyber threats and preventing associated losses and disruptions.

90% Reduction in Alert Volume

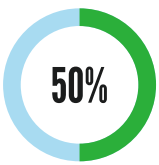
Reduce false positives by 90% through precise, AI-driven alert correlation and analysis. This lets your security team focus on the most critical incidents, alleviating alert fatigue and enabling faster response.

90% Faster Incident Investigation

Slash investigation time by 90% with our platform's integration of Security GPT. Security analysts of varying skill levels can navigate complex incidents through natural language dialogue, cutting investigation time from hours to minutes.

70% Increase in Security Robustness

Boosts overall system security by 70% by breaking down silos in security tools and reducing the complexity to manage and juggle multiple security tools.



50% Reduction in Operational Costs

Cut security operation costs by at least 50%, minimizing infrastructure investment and maintenance costs while consolidating multiple security functions into a unified platform.

The Competitive Edge: Why Sangfor Athena XDR

1) Leading-Edge Technology

Athena XDR leverages the best of Sangfor's security technologies, including the groundbreaking Security GPT. Sangfor is one of the few vendors integrating generative AI, setting us apart from vendors using traditional AI models. Trained on over 110 billion security data points and continuous learning from new threats, Security GPT empowers Athena XDR to achieve detection rates unmatched by most security vendors. Security GPT further revolutionizes security operations with dialogue-based interactions, alleviating the security skills gap and enhancing operational efficiency.

2) Simplified Security Operations

Sangfor provides a complete security portfolio, including next-generation firewall, endpoint security, network detection and response, secure web gateway, and managed detection and response services. With Athena XDR, these components integrate seamlessly, enabling unified management, streamlined operations, and improved functionality.

3) Cost-Effective

Athena XDR offers scalable, cost-effective options with flexible modules, allowing businesses to customize the solution based on actual needs. This approach reduced unnecessary expenses often associated with bundled solutions from other vendors.

4) Flexible Deployment

Athena XDR provides a flexible deployment model designed to meet diverse organizational requirements. For on-premises deployments, data remains within your native country, ensuring compliance with data sovereignty regulations. For SaaS-based deployments, Athena XDR offers scalable flexibility, allowing your security infrastructure to grow effortlessly alongside your business. This adaptable approach ensures you have the right deployment strategy to support your cybersecurity and compliance goals.

5) Local Support

Sangfor boasts a strong presence in Southeast Asia with local branch offices across the region and the Middle East. We are expanding in Europe and Latin America. This extensive presence ensures fast and reliable support services, even in local languages, providing smooth service delivery and rapid issue resolution.

Distributeur à valeur ajoutée de solutions IT

Cybersécurité | Réseaux | Wi-Fi | Stockage

HAFS NETWOKS,
Représente et accompagne les éditeurs et les constructeurs pour créer de la proximité auprès des partenaires et des clients finaux.

Notre objectif :
Proposer des solutions qui repondent aux besoins. Accompagner, former et développer pour accroître le rayonnement sur le marché français et en Afrique sub-sahérienne.

Solutions **Formations** **Services**

Portfolio Solutions

Portfolio Solutions

HAFS
Distributeur à valeur ajoutée

Site web : www.hafs-networks.com

France
sales@hafs-networks.com
+33 (0)6 51 10 87 49 / (0)9 74 98 52 96

Côte d'Ivoire
sales-ci@hafs-networks.com
+225 07 89 82 56 49 / +225 07 59 05 85 82