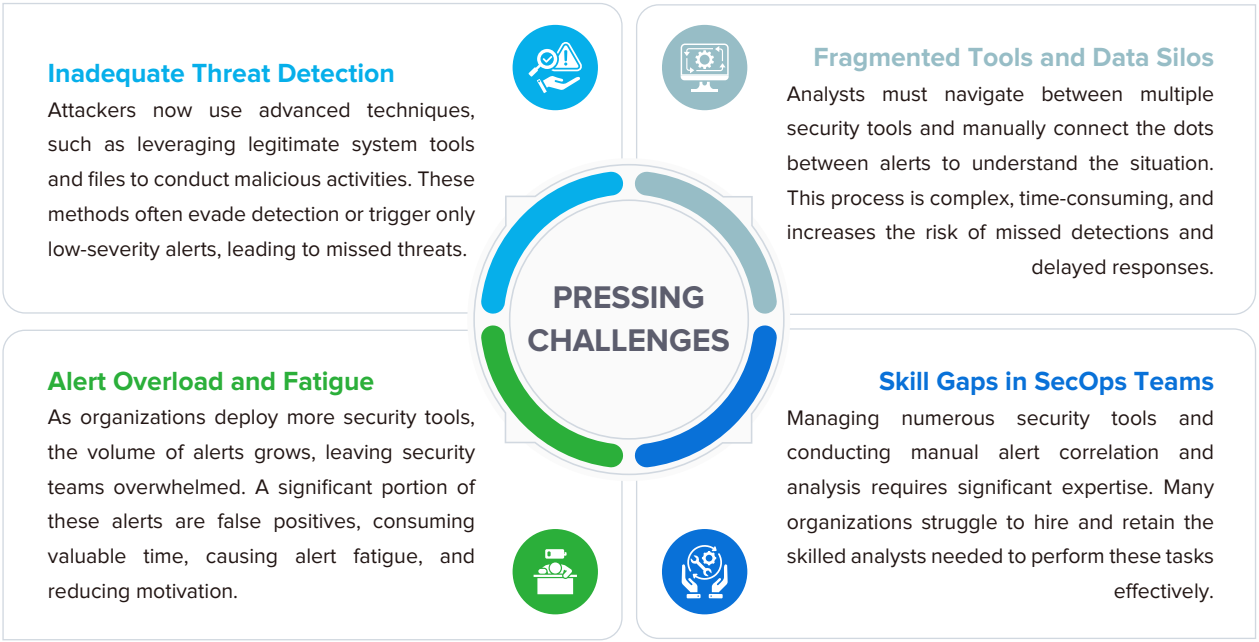
SANGFOR | SANGFOR SECURITY

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

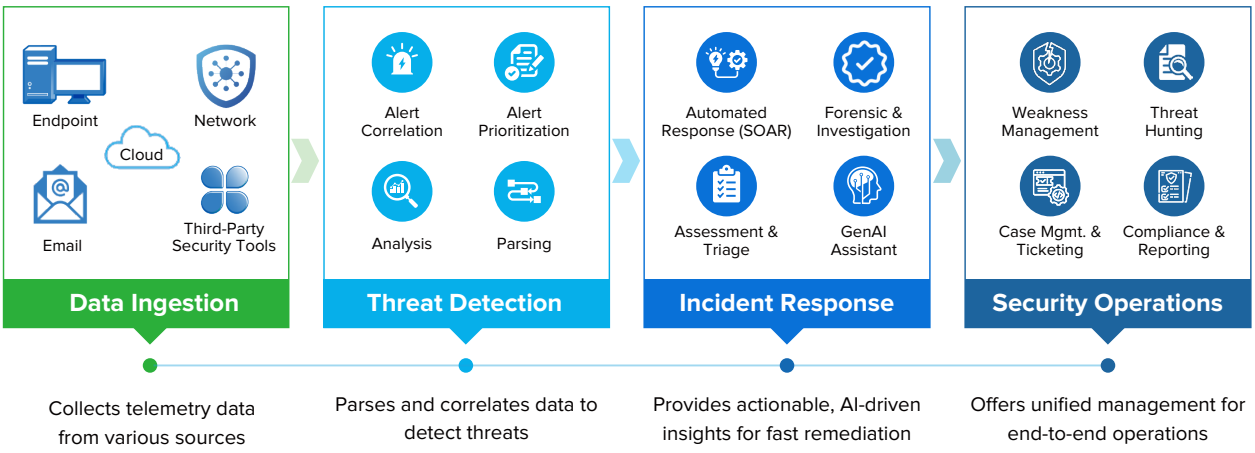
Sangfor Athena XDR (Extended Detection and Response) rises to this challenge by unifying detection and response through the consolidation of data and alerts from diverse sources. These include endpoint security tools, network security devices (firewalls and NDR), cloud environments, applications and 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

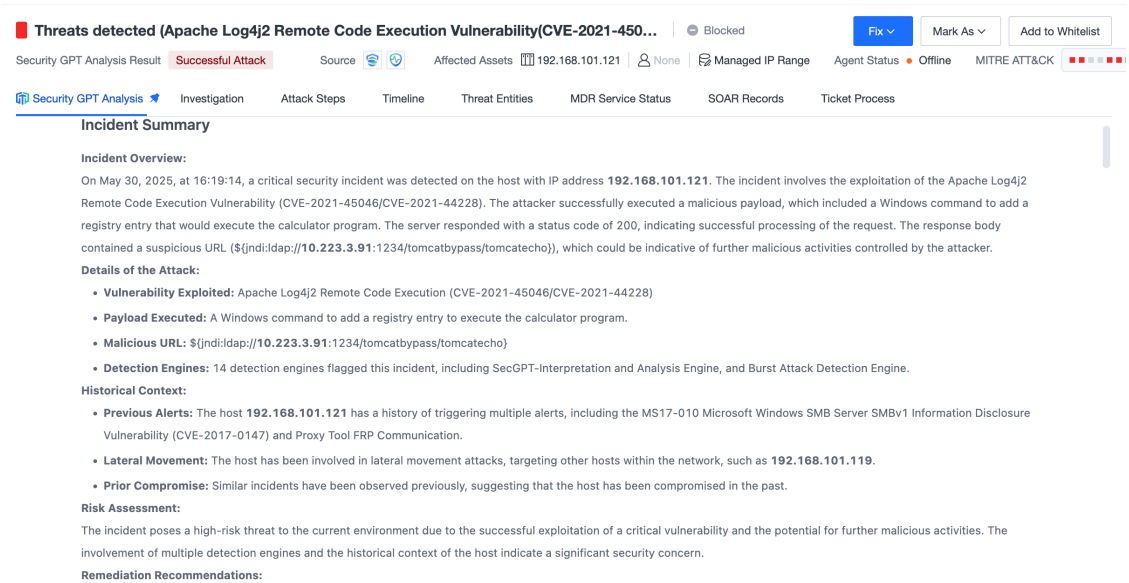
Sangfor Athena XDR redefines security operations by serving as a unified SecOps platform. It integrates critical security functions into a single solution, including workflow automation, threat intelligence, SOAR, SIEM-like data fusion, reporting, and ticketing. This integration eliminates the traditional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

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

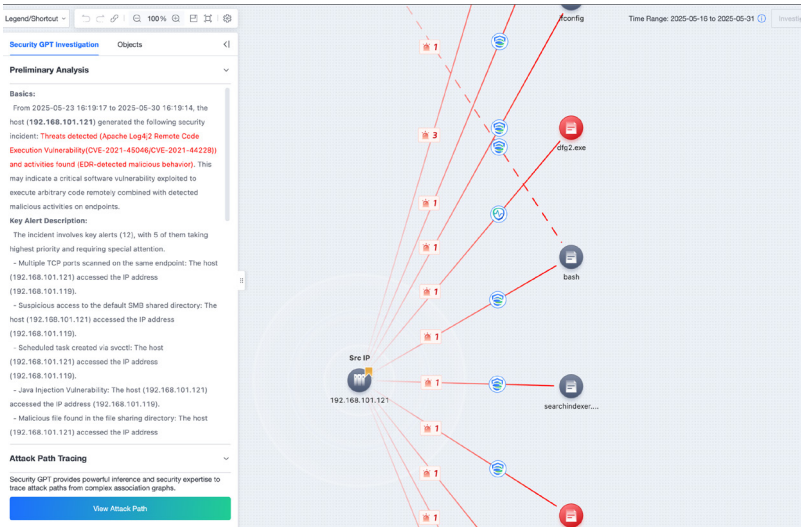
Athena XDR also supports flexible integration with third-party tools, allowing organizations to maximize existing investments while gradually transitioning to Sangfor's native solutions for optimized performance. Available in both **on-premises and SaaS-based models**, Athena XDR adapts to your organization's 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

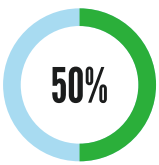
Reduce false positives by 90% through precise, AI-driven alert correlation and analysis. This lets your security team focus on the most critical incidents, alleviating alert fatigue and enabling faster response.

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.

Sangfor Athena XDR

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
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

Sangfor Athena SWG
Secure User Internet Access Behaviour

Sangfor Athena NGFW
Smarter AI-Powered Perimeter Defence

Sangfor Athena EPP
The Future of Endpoint Security

Sangfor Athena NDR
Smart Efficient Detection and Response

Sangfor Athena XDR
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

Sangfor Athena MDR
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

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

Copyright © 2025 Sangfor Technologies. All Rights Reserved.

HAFS
Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY V vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision