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

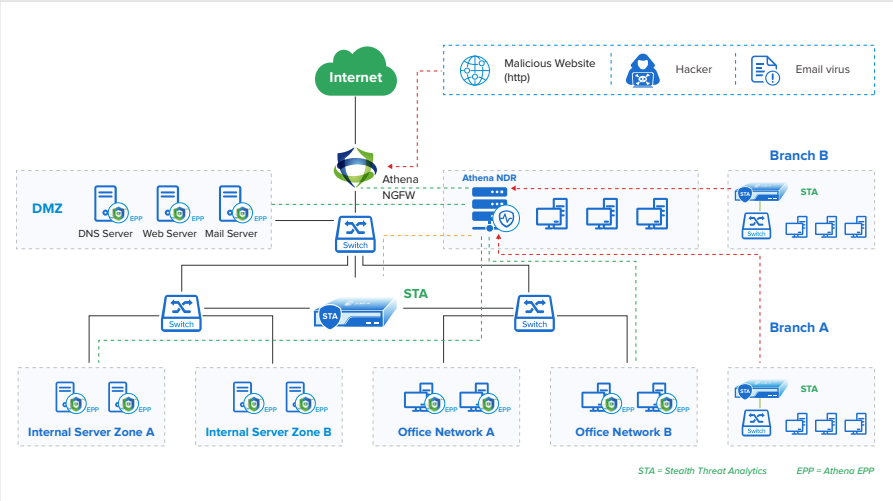
For a long time, organizations have been building complex security stacks comprising multiple security tools layered on top of each other. This approach has resulted in a range of issues, such as poor integration leading to security gaps, overlapping features, and complex management.

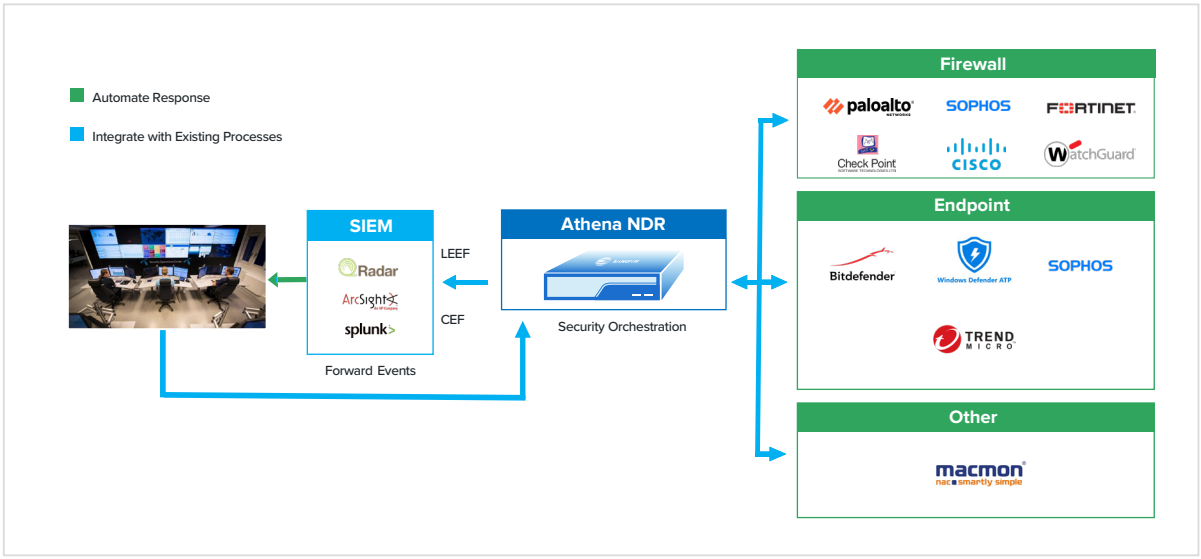
As such, organizations are starting to rethink their approach by adopting what is known as a security ecosystem - a comprehensive network security architecture where multiple security technologies, tools, and services are integrated to provide a unified defense against cyber threats. An integrated security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

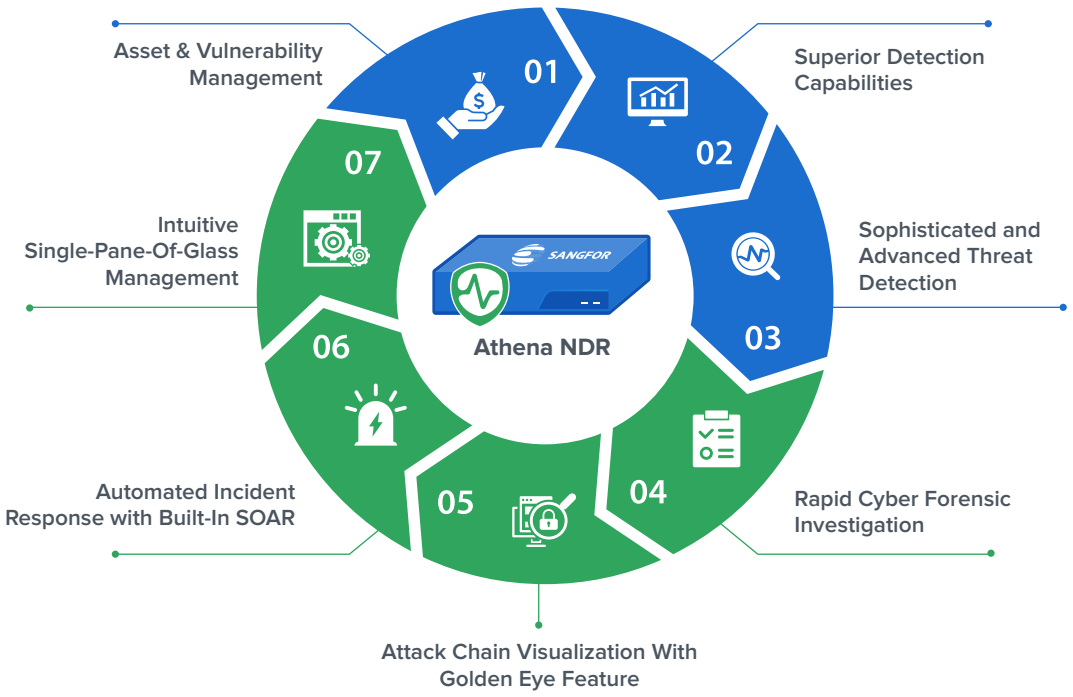
Athena NGFW

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

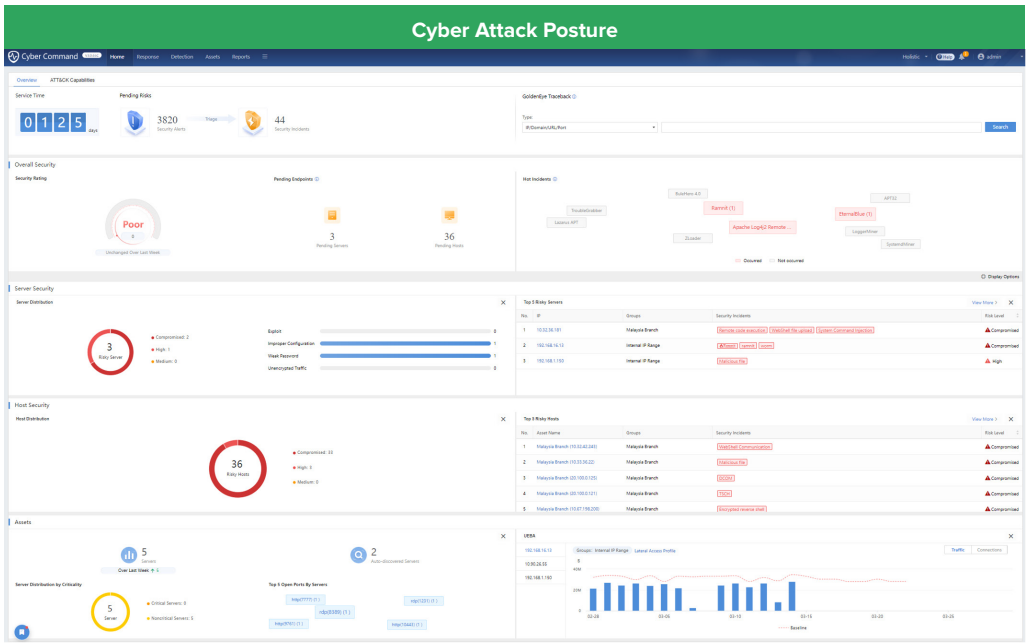
Athena NDR provides automated response with its unique built-in SOAR module. Pre-defined playbook templates allow security teams to effortlessly orchestrate incident response actions to some common threat scenarios. They can also customize responses tailored to their specific needs. With Athena NDR SOAR,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

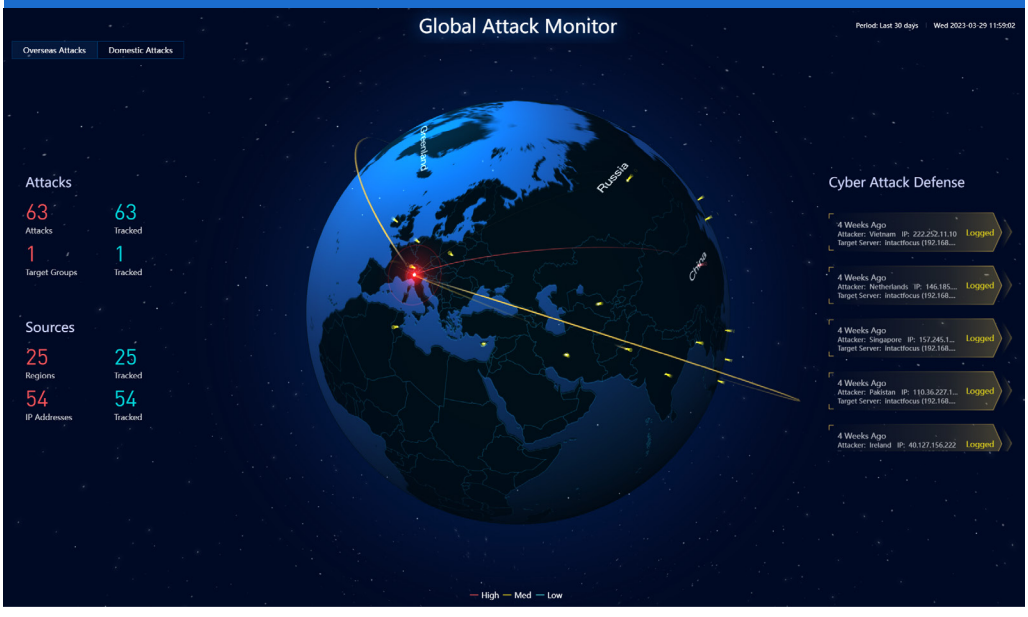
» Keep Threats at Bay with Unprecedented Visibility And Advanced Detection & Response

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.



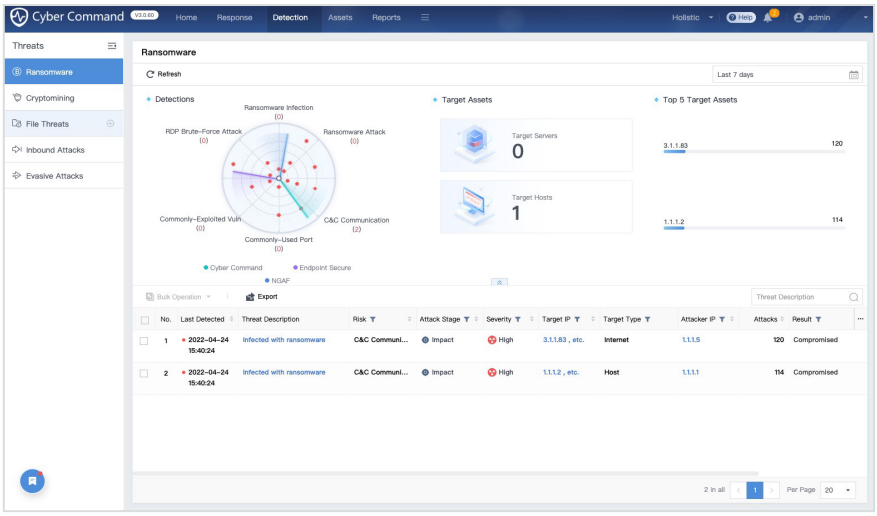
Outbound Threat Monitoring

Global Attack Monitoring

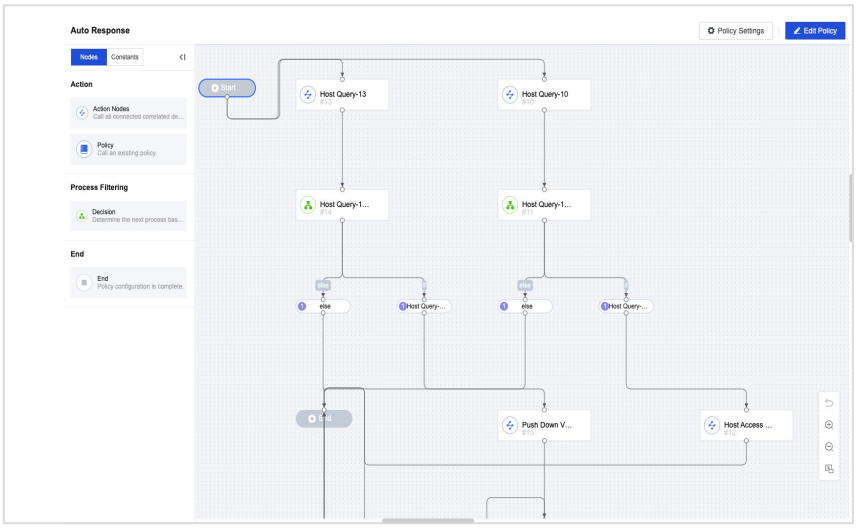


Athena NDR protects organizations from sophisticated cyber threats with multiple detection engines and advanced threat detection techniques, while built-in SOAR ensures immediate incident response to detected threats. Full MITRE ATT&CK mapping further provides detailed insights for informed decision-making.

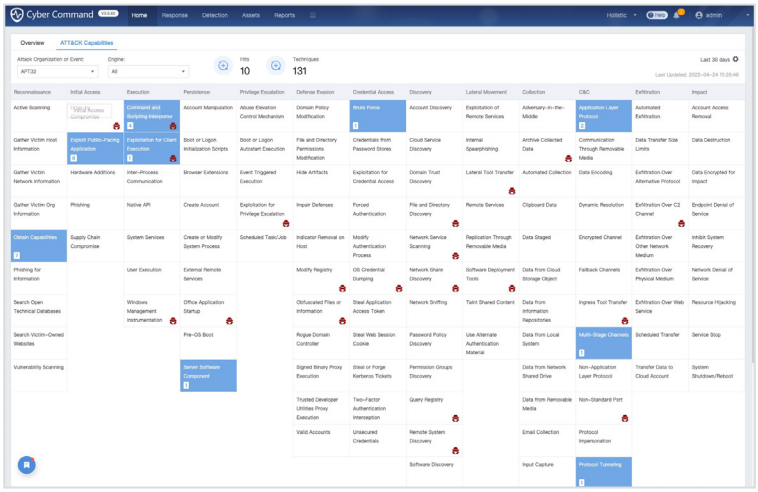
Advanced Threat Detection

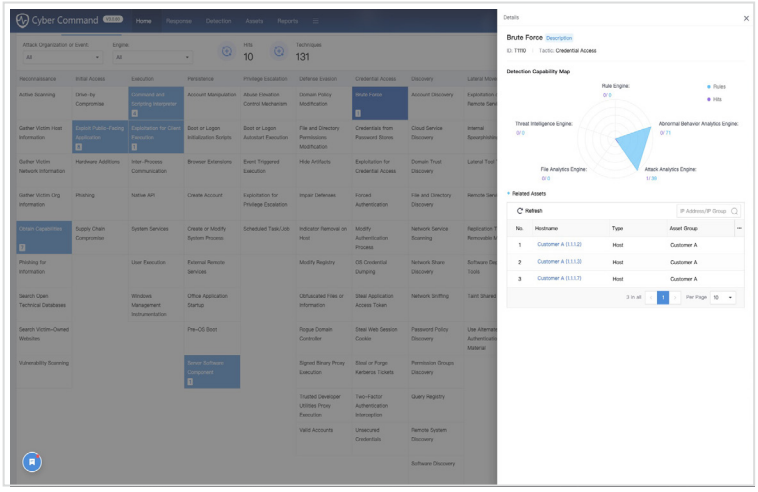


Auto Response with SOAR



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 Athena NDR

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

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

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

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

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

AVAILABLE SOLUTIONS

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

Omni-Command - Extended Detection and Response
Revolutionize Your Cyber Defense with Intelligent XDR

TIARA - Threat Identification, Analysis and Risk Assessment
Smart Threat Analysis and Assessment

IR - Incident Response
Sangfor Incident Response – One Call Away

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
Simple Security for Branches & Remote Users

EDS - Enterprise Distributed Storage
The Only Secured Data Storage You Need

SD-WAN
Boost Your Branch with Sangfor

Sales: sales@sangfor.com

Marketing: marketing@sangfor.com

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

www.sangfor.com

Copyright © 2025 Sangfor Technologies. All Rights Reserved.