

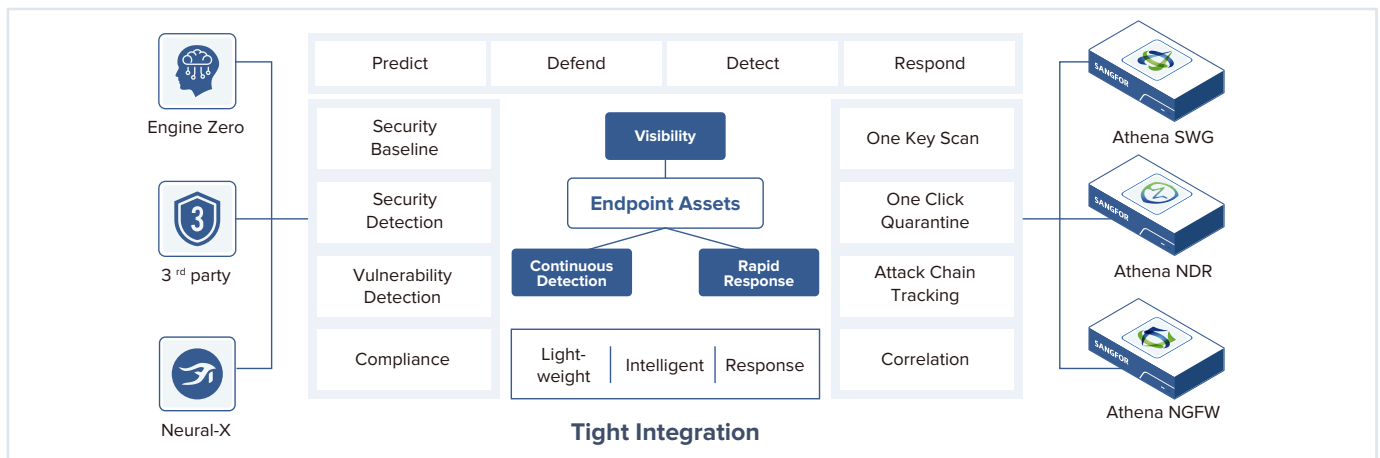
Une solution pour chaque environnement

# Sangfor Athena EPP Datasheet

The Future of Endpoint Security

Sangfor\_BR\_P\_Athena EPP-Datasheet\_20251216

Sangfor Athena EPP (formerly 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.



## 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.

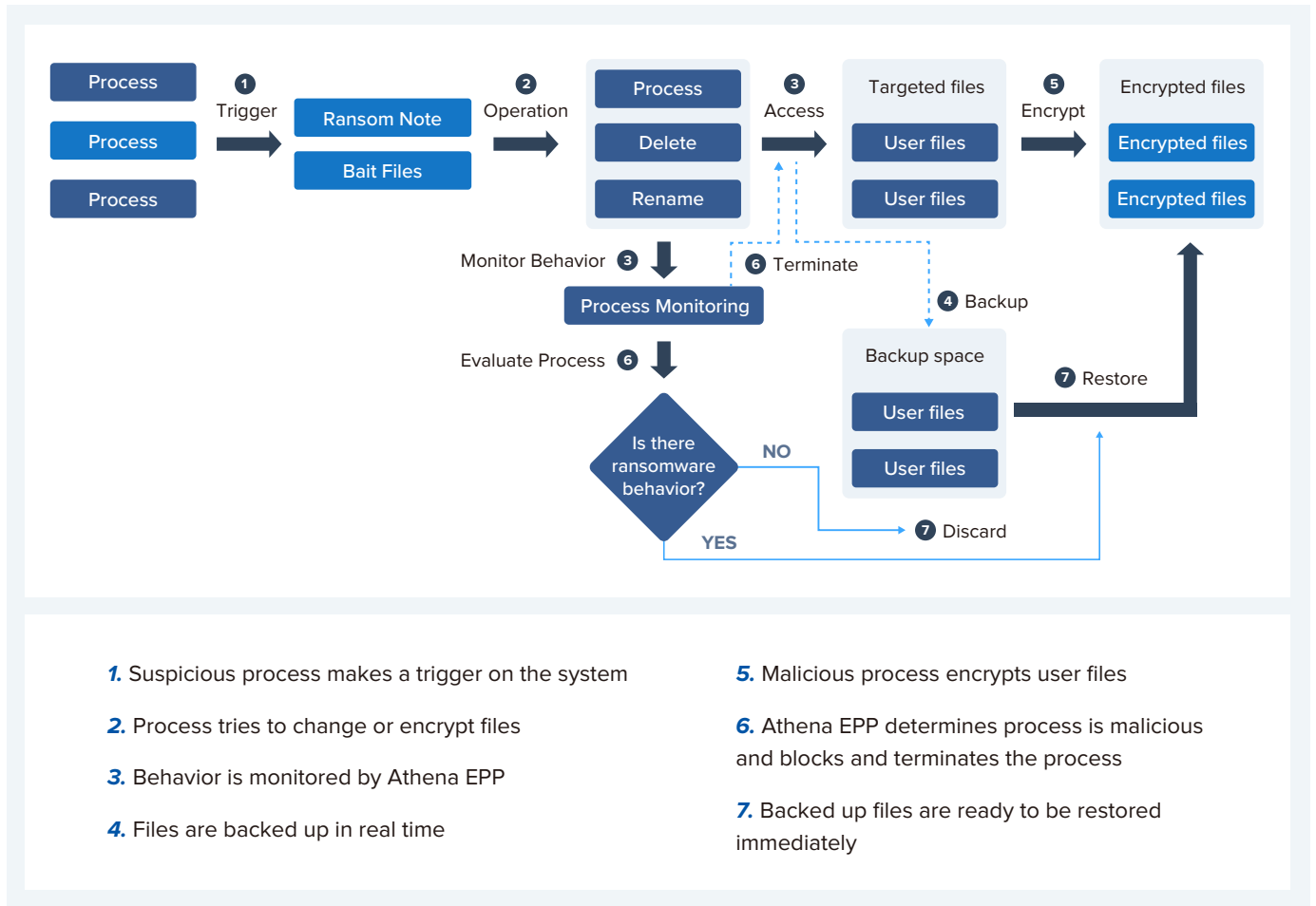


Ransomware indicators of compromise are collected from over 12 million devices deployed with Athena EPP, allowing it to *achieve a detection accuracy rate of 99.83%*.



In addition to existing ransomware protections, such as bait files and RDP two-factor authentication, Athena EPP provides dynamic file backup and recovery capabilities to fully secure and restore your data in case of ransomware encryption.

## Ransomware Protection and Recovery



## AI-powered Malware Detection Engine

Unlike traditional antivirus engines, Engine Zero uses AI-driven, signature-less detection to identify unknown viruses and variants, including those not recorded in antivirus databases.



## Sangfor Athena EPP Industry Recognitions and Certifications

	Strong Performer in Gartner® Voice of the Customer for Endpoint Protection Platforms with a 95% "Willingness to Recommend"		Certified Windows Protection by Microsoft
	Certified Best Windows Antivirus Solution and "TOP PRODUCT" Award by AV-Test		Gold OPSWAT Endpoint Security Certification for Anti-Malware

## Editions 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)		✓	
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 Athena NDR Datasheet

## Intelligent Threat Detection and Response Platform

Sangfor\_BR\_P\_Athena NDR-Datasheet\_20250616

### Stay Ahead Of Emerging Threats With Sangfor Athena NDR

Sangfor Athena NDR is a best-in-class Network Detection and Response (NDR) solution that is designed to help organizations detect and respond to advanced and unknown security threats residing in their network.

Athena NDR harnesses the power of advanced artificial intelligence (AI) and machine learning (ML) technologies 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 unprecedented visibility of their network environment, Athena NDR empowers security teams to take rapid action to remediate hidden threats, attacks in progress, as well as risks and vulnerabilities. Athena NDR's built-in SOAR module further enables security teams to automate response actions to detected threats, significantly minimizing the impact caused by security incidents.

Sangfor Athena STA (Stealth Threat Analytics) is the sensor used in the Athena NDR solution. It is a hardware 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.



Athena STA Front & Rear view



Athena NDR Front & Rear view

Athena NDR collects data from the STA sensor and applies AI and machine learning techniques to correlate and analyze the data. It then compares the real-time analysis results with established baselines of normal network behaviors to detect anomalies concealing malicious activities, such as stealthy command and control (C2) communication, lateral movement disguised as business traffic and irregular user behavior indicating insider threats.

## Sangfor Athena NDR – Physical Appliance

Model		CC-1000a	CC-2000a	CC-3000a
<b>Performance</b>				
Based on Athena STA	Athena STA	5STA-100	8STA-100	12STA-100
	Throughput (Gbps)	5	8	12
Based on Logs	Daily access log number (Million/Day)	200	250	350
	Average EPS (Per log/Sec)	3,130	4,380	6,255
	Peak EPS (Per log/Sec)	12,000	15,000	18,000
	Disk consumption (GB/Day)	112	140	196
	Estimated storage days/1Gbps (Assumed throughput)	1,200	1,500	1,800
<b>Technical Specifications</b>				
Memory (GB)		128	128	256
CPU (Cores)		12	16	48
System Disk		240GB SSD	240GB SSD	240GB SSD
Data Hard Drive Capacity		SATA 4TB*8 (Total: SATA 32TB)	SATA 4TB*10 (Total: SATA 40TB)	SATA 4TB*12 (Total: SATA 48TB)
LSI Raid		9460-8i	9460-8i	9361-8i or 9460-8i
<b>Hardware Specifications</b>				
Dimension (L x W X H) (mm)		790*447*86.1	790*447*86.1	790*447*86.1
Rack Height		2U	2U	2U
Gross Weight (kg)		28	28	37.5
Power Supply		Redundant	Redundant	Redundant
Rated Power (W)		345	380	900/648 [200-240VAC]
Maximum Power (W)		900	900	1300/900 [200-240VAC]
Bypass		N/A	N/A	N/A
Copper Ports		10/100 /1000BASE-T*4	10/100 /1000BASE-T*4	10/100 /1000BASE-T*4
SFP/SFP + Ports		N/A	10GbE SFP+*2	10GbE SFP+*2
USB		4**USB2.0 or above	4**USB2.0 or above	4**USB2.0 or above
Conversion Relation for Athena STA		STA-300 = STA-100*3 , STA-500 = STA-100*10		

## Sangfor Athena STA – Physical Appliance

Model	STA-50	STA-100	STA-300	STA-500	STA-1000
<b>Performance</b>					
Peak Sustained Throughput (Network Layer)	Up to 500Mb	Up to 1Gb	Up to 3Gb	Up to 10Gb	Up to 40Gb
Peak Sustained Throughput (Application Layer)	Up to 160Mb	Up to 350Mb	Up to 1Gb	Up to 5Gb	Up to 20Gb
Maximum Unique Internal Devices Analyzed	1,000	3,000	10,000	35,000	150,000
<b>Technical Specifications</b>					
Memory (GB)	4	8	8	48	256
Hard Drive	128GB SSD	128GB SSD	480GB SSD	960GB SSD	8 TB SSD
<b>Hardware Specifications</b>					
Dimension (L x W X H) (mm)	175 x 275 x45	300 x 430 x 44.5	600 x 440 x 89	600 x 440 x 89	600 x 440 x 89
Rack Height	1U	1U	2U	2U	2U
Gross Weight (kg)	2.3	6	15.4	21	21.6
Power Supply	Single	Single	Dual	Dual	Dual
Rated Power (W)	22	30	48	250	560
Maximum Power (W)	24	40	60	300	800
Bypass	N/A	N/A	N/A	N/A	N/A
Copper Ports	10/100/1000 Base-T*4	10/100/1000 BASE-T*8	10/100/1000 BASE-T*8	10/100/1000 BASE-T*4	10/100/1000 BASE-T*4
SFP/SFP + Ports	N/A	10GbE SFP+*2	10GbE SFP+*2	1GbE SFP*4 10GbE SFP+*8	1GbE SFP*4 10GbE SFP+*4 40GbE SFP+ *4
Serial Ports	RJ45*1	RJ45*1	RJ45*1	RJ45*1	RJ45*1
USB	USB2.0*2	USB2.0*2	USB2.0*2	USB2.0*2	USB2.0*2

## Sangfor Athena NDR - Virtual

Model	vCC-10	vCC-50	vCC-100	vCC-500	vCC-1000	vCC-2000	vCC-3000
<b>Performance</b>							
Traffic Handling Capacity (Gbps)	0.5	1	2	3	5	8	12
Blog Handing Capacity (EPS/s, Peak)	5,000	5,000	5,000	5,000	10,000	12,000	15,000
<b>Technical Specifications</b>							
CPU (Main Frequency, Number of Cores)	2.10GHz*1*8	2.10GHz*1*8	2.10GHz*1*8	2.10GHz*1*8	2.10GHz*2*12	2.40GHz*2*16	2.10GHz*2*24
Memory (GB)	32	32	64	64	96	128	256
System Disk	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD	128GB SSD
Minimum Hard Disk Requirement	1TB	1TB	2TB	2TB	4TB	8TB	8TB
Recommended Hard Disk Requirement	6TB	6TB	12TB	12TB	24TB	48TB	48TB

Notes: With larger hard disk capacities, the duration for retaining data is extended, enabling more prolonged storage

## Sangfor Athena STA - Virtual

Model	vSTA-10	vSTA-30	vSTA-50	vSTA-100	vSTA-200	vSTA-500	vSTA-1000
<b>Performance</b>							
Traffic Handling Capacity (Network Layer)	100Mb	300Mb	500Mb	1Gb	2Gb	5Gb	10Gb
Traffic Handling Capacity (Application Layer)	50Mb	150Mb	250Mb	500Mb	1Gb	1.5Gb	3.3Gb
<b>Technical Specifications</b>							
CPU (Main Frequency, Number of Cores)	2.4GHz*4	2.4GHz*4	2.4GHz*4	2.4GHz*4	2.4GHz*8	2.4GHz*16	2.4GHz*28
Memory (GB)	4	4	4	8	16	32	48
System Disk	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB	> 64GB
Recommended Minimum Data Disk	> 128GB	> 128GB	> 128GB	> 128GB	> 480GB	> 480GB	> 480GB



# Sangfor Athena XDR (On-Premises) Datasheet



Making Your Security Simple, Reliable and Effortless

Sangfor Athena XDR goes beyond traditional security measures by correlating and analyzing telemetry data from a wide range of sources through a unified platform. Leveraging AI, machine learning, user behavior analytics, and big data, it proactively identifies hidden threats to deliver a comprehensive and preventive cybersecurity posture that safeguards digital environments. Athena XDR is available in both a versatile SaaS version and one of the industry’s first on-premises XDR solutions, supporting a broad range of cybersecurity strategies.



Athena XDR (On-Premises) is ideal for organizations with strict data privacy and data residency requirements, delivering advanced security while meeting compliance needs. It provides the option to integrate with SaaS Security GPT—Sangfor’s flagship GenAI-powered security toolset—transforming security operations by enhancing efficiency across alert analysis, threat hunting, incident investigation, and response.



In today’s threat landscape, Sangfor Athena XDR delivers more than just a platform—it provides a complete ecosystem that accelerates detection and response, minimizes breach impact, and ensures seamless integration across security infrastructures for comprehensive protection and operational efficiency.



Contact Us  
To Know More >>

Sangfor Technologies [sales@sangfor.com](mailto:sales@sangfor.com) [marketing@sangfor.com](mailto:marketing@sangfor.com)



## Datasheet

### Sangfor Athena XDR (On-Premises) – Physical Appliance

<b>Model</b>	aServer-XDR-C-3500 <sup>1</sup>
<b>Performance</b>	
Log Volume/Day	200 million logs per day
Average EPS (Per log/Sec)	Up to 6,666 <sup>2</sup>
<b>Technical Specifications</b>	
Memory (GB)	8*32
CPU (Main Frequency, Number of Cores)	2.4GHz, 16 cores
System Disk	240 GB SSD
Data Hard Drive Capacity	3 Options (Please select the size according to your needs): 4TB*12, 8TB*12 or 12TB*12
LSI Raid	Raid 50
<b>Hardware Specifications</b>	
Dimension (L x W x H) (mm)	790 x 447 x 86.1
Rack Height	2U
Gross Weight (kg)	28
Power Supply	Redundant
Rated Power (W)	380
Maximum Power (W)	900 or 800
Bypass	N/A
Copper Ports	10/100/1000BASE-T*4
SFP/SFP+ Ports	10 GbE SFP+*2
Serial Ports	N/A
USB	USB 3.0 *4

1. At least three (3) hardware appliance nodes are required to deploy Athena XDR (On-Premises)
2. The EPS above refers only to the maximum capacity supported by the hardware appliance. The actual log processing rate is also subject to limitations imposed by the software license. Therefore, to accurately determine the achievable EPS, both hardware specifications and software license configurations must be considered together.



# Distributeur à valeur ajoutée de solutions IT

Cybersécurité | Réseaux | Wi-Fi | Stockage

## **HAFS NETWORKS,**

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 répondent aux besoins. Accompagner, former et développer pour accroître le rayonnement sur le marché français et en Afrique sub-saharienne.

**Solutions**

**Formations**

**Services**



# Portfolio Solutions

**NEXT GEN  
FIREWALL**

**HSM / HSA**

**ZTNA**  
Zero-Trust Network Access

**SD-WAN**

**EDR**  
Endpoint Detection and Response

**NIPS**  
Network Intrusion Prevention  
System

**NDR**  
Network detection and response

**WAF**  
Web application firewall

**ADC**  
Load balancer application

**XDR**  
Extended Detection et Response

**DLP/NEXT GEN.DLP**  
Data loss prevention

**NAS/SAN**

**HCI/VDI**

**SWITCH**

**Wifi/Wireless**

**Wifi Penetration  
Testing**

**Vulnerability  
scanner**

**Web Vulnerability  
Scanner**

**STRONG  
AUTHENTICATION**  
Hardware Token Authentication

**IAM / MFA**  
Identity et Access Management

**NETWORK  
VISIBILITY**  
Network Performance Monitoring

# Portfolio Solutions



Site web : [www.hafs-networks.com](http://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