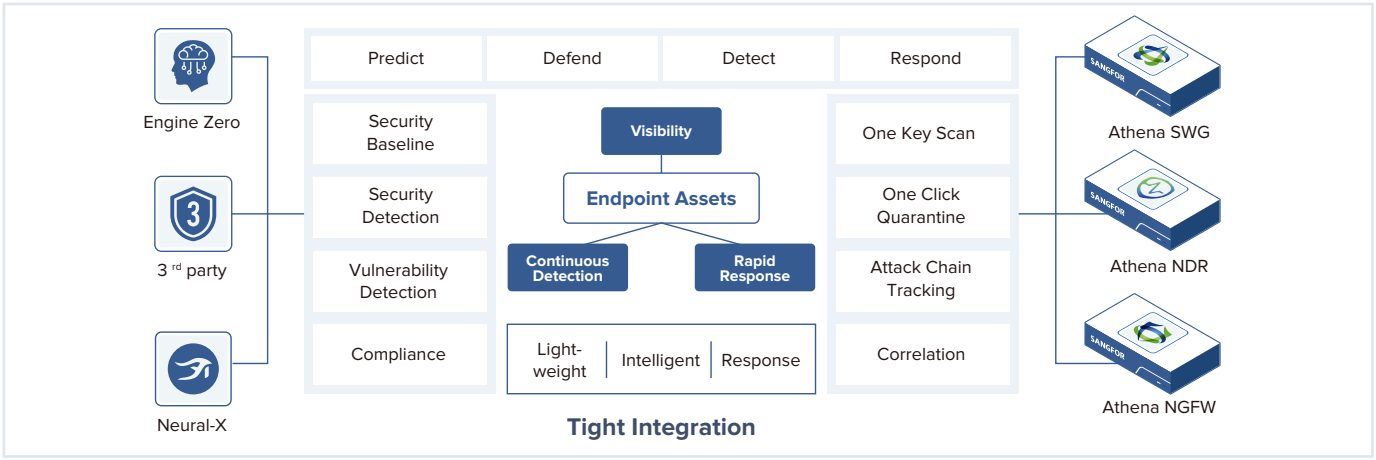
SANGFOR

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

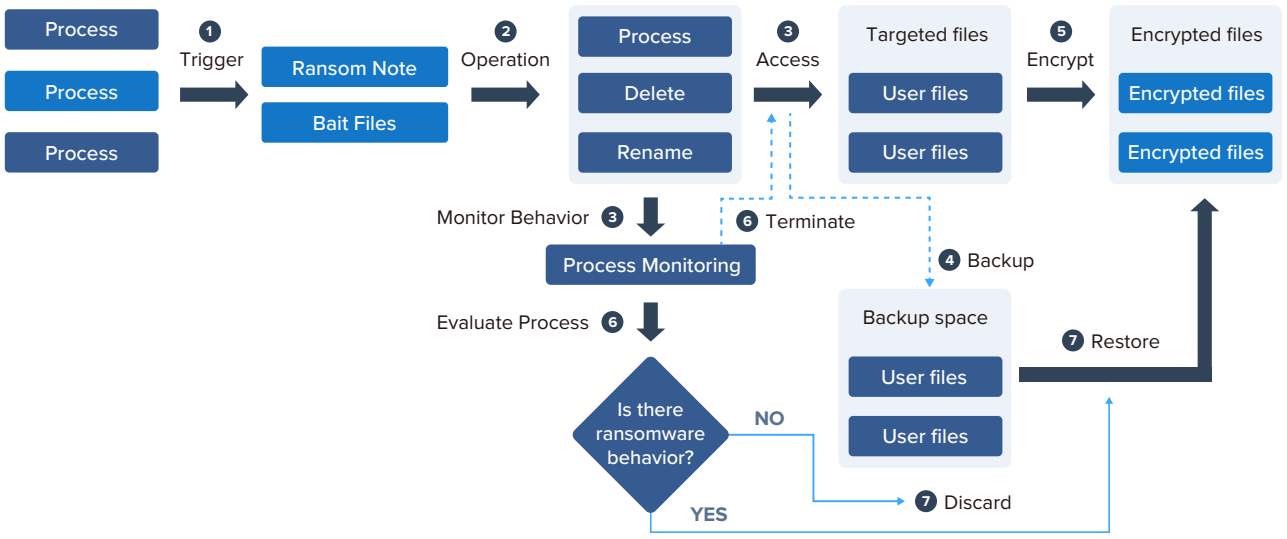
Protects against all types of ransomware through static and dynamic AI-based detection engines.

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



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

Sangfor Engine Zero
Sangfor Anti-Malware Engine
Artificial Intelligence Based Non-Signature Engine
Detect Unknown Malware Accurately

Sangfor Athena EPP Industry Recognitions and Certifications

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

Microsoft — Certified Windows Protection by Microsoft

AV-TEST The Independent IT-Security Institute — Certified Best Windows Antivirus Solution and "TOP PRODUCT" Award by AV-Test

OPSWAT. — 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.