aa teknoloji

Sangfor Athena EPP

A next-generation endpoint protection platform that centrally manages endpoint security and threat management, defending endpoints with AI-powered analysis, advanced ransomware protection, and instant response capabilities.

Modern Endpoint Security Challenges

Organizations struggle to provide full visibility over endpoints due to expanding remote working models, increasing device diversity, and advanced cyber threats. Traditional antivirus software operating in isolation falls short in detecting modern and complex attacks.
Especially ransomware and zero-day attacks spread rapidly after infiltrating endpoints, causing critical corporate data to be encrypted and business continuity to grind to a halt. Manual analysis of scattered alerts by security teams delays response processes.
The lack of integration between network security and endpoint systems makes it difficult to find the root cause of a threat and block lateral movement, thereby reducing operational efficiency in cybersecurity operations.

What Problems Does It Solve?

- Inability to instantly detect and prevent advanced cyber attacks and ransomware.
- Loss of centralized control, traceability, and visibility across distributed endpoints.
- Significant time and efficiency losses during manual threat hunting and alert analysis processes.
- Disconnected operation of network and endpoint security products, and the lack of a centralized integration infrastructure.

Core Principles

Proactive Protection
Blocks threats using artificial intelligence before they damage the system.

Automation
Automates repetitive analysis and isolation processes seamlessly.

Unified Security
Merges network and endpoint solutions into a single architecture.

Visibility
Makes all endpoints trackable from a single centralized dashboard.

How Does Sangfor Athena EPP Work?

Sangfor Athena EPP operates by collecting real-time data from all endpoints across the corporate network via agents. Collected metrics are analyzed using the Engine Zero AI engine and behavioral analysis rules; when a threat is detected, the system automatically isolates the relevant endpoint and terminates the malicious process.

Technical Specifications

Threat Detection and AI
- Engine Zero AI-based malware analysis
- Behavioral analysis and anomaly detection
- File integrity monitoring and auditing
- In-memory attack prevention support

Advanced Ransomware Protection
- AI-powered ransomware mitigation
- Intelligent honeypot technology integration
- Automated file backup and restoration
- Instant containment of encryption attempts

Instant Response and Isolation
- One-click host and endpoint isolation
- Automated termination of malicious processes
- Network-level micro-segmentation support
- Network quarantine and remote response workflows

Centralized Management and Integration
- Single-panel tracking of all endpoints
- XDDR integration with Sangfor NGAF and Cyber Command
- Comprehensive asset inventory and risk scoring
- Centralized SOC logging support via Syslog

Consulting and Managed Services
- Deployment design of agent infrastructure and resource optimization consulting
- Centralized automated rolling deployment and native third-party API integration
- Advanced alert analysis and optimization support
- Administrative platform enablement and incident simulation training for internal teams

Workflow

1. Data Collection and Scanning
- Live activity logs are gathered from endpoints.
- Continuous vulnerability and risk scanning is executed.
- System asset inventory is automatically updated.
- Continuous monitoring is provided via agents.

2. AI Analysis and Detection
- Malicious software is analyzed with Engine Zero.
- Suspicious behaviors and anomalies are searched.
- Ransomware encryption steps are identified.
- Risk scores are prioritized on the central pane.

3. Response and Reporting
- The compromised endpoint is isolated from the network.
- Malicious files are deleted and processes are stopped.
- The attack chain is visually reported.
- Security findings are transmitted to the central SOC architecture.

Continuous Improvement
Thanks to continuously updated global threat intelligence feeds and AI rule sets, Sangfor Athena EPP regularly optimizes its protection capabilities against next-generation attack methods.

Advantages

Engine Zero AI Engine
Detects unknown malware and zero-day attacks missed by traditional signature-based solutions with high accuracy through its artificial intelligence architecture.

Anti-Ransomware Honeypot
Catches and blocks ransomware encryption activities before they damage real files, thanks to intelligent honeypot files deployed on endpoints.

Effective Threat Hunting
Allows security experts to rapidly locate the root cause of threats and shortens response times thanks to advanced visualized attack chain (kill chain) analysis.

XDDR Unified Defense
Works fully integrated with Sangfor network security products, ensuring that a threat starting at an endpoint is automatically blocked at the network level to form a unified defense line.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.