WHITE PAPER

AIStorm

ThreatTrace Evolution

Your 24/7 AI Chief Security Analyst

From alert overload to actionable security outcomes — combining AI-assisted threat assessment, full-traffic traceability, file-threat visibility, centralized multi-node operations, and value-focused reporting.

Data-Driven • AI-Native • Enterprise-Ready

Table of Contents

Executive Overview

As cyberattacks become more sophisticated, security teams are increasingly challenged by alert fatigue and traceability gaps. ThreatTrace addresses these operational pressures by combining network threat detection with AI-assisted analysis, full-traffic retention, network-wide file threat monitoring, hierarchical deployment, and intelligent reporting.

The upgraded ThreatTrace integrates with the large-model ecosystem and is designed to act as a 24/7 "Virtual Chief Security Analyst" for enterprise security teams. It is built on AIStorm's self-developed XinCube security model and supports integration with mainstream third-party large-model platforms, including DeepSeek and Tongyi Qianwen.

What The Upgrade Delivers

- AI-assisted alert assessment and standardized remediation guidance
- Correlated host-risk analysis across internal networks
- Full-traffic retention and forensic traceability
- Network-wide file visibility with static and dynamic sandbox analysis
- Centralized visibility and policy distribution across branches
- Dashboards and scheduled reporting focused on measurable security value

AI-Powered Threat Assessment

ThreatTrace is designed to reduce investigative burden by helping security teams distinguish genuine threats from high volumes of daily alerts. AI-assisted analysis turns raw detections into structured security assessments that can accelerate triage and response.

Automated Alert Analysis

Automatically extracts attack signatures, assesses severity, and generates standardized remediation playbooks.

Intelligent Host Risk Analysis

Correlates and summarizes host-level risks across internal networks to surface hidden risk patterns.

Flexible Operational Modes

Supports background automated batch processing and on-demand manual triggering, balancing efficiency with analyst control.

Unified Full-Traffic Retention & Traceability

Traditional deployments often separate detection from traceability. ThreatTrace brings threat analysis, full-traffic log retention, and forensic investigation into a unified workflow, helping security teams move from detection to evidence and investigation more efficiently.

Full-Scenario Protocol Support

Deep metadata extraction and storage for 15 commonly used threat-tracing protocols.

High-Performance Hardware Assurance

Purpose-built data-retention models using RAID + SSD architecture to support high-speed writing and storage stability in high-traffic environments.

Tiered Storage Strategy

Supports full-packet retention for 1G-10G traffic volumes. Malicious files are retained by default, with full-file retention supported through external storage expansion.

Why it matters

By retaining the evidence needed for investigation, ThreatTrace helps reduce the operational gap between detecting suspicious activity and reconstructing what actually happened.

Network-Wide File Threat Awareness

ThreatTrace extends network visibility to file movement, helping organizations identify malicious or suspicious files and understand how they propagate across the environment.

Global Situational Monitoring

Tracks total file volume, threat counts, and distribution in real time to improve transparency of internal file movement.

Storage Efficiency Optimization

Uses intelligent hash-based deduplication so identical files are stored only once, reducing storage consumption without changing detection logic.

Full-Link Visualized Tracking

Graphically presents transmission nodes and timelines for specific files to help identify propagation paths.

Integrated Static & Dynamic Detection

Automatically submits suspicious files to the sandbox for combined static and dynamic analysis.

Hierarchical Deployment for Global Operations

For large enterprises and government environments with multiple sites, ThreatTrace introduces hierarchical cascaded deployment to support the goal of "One Platform, One Network-Wide View."

Unified Global Visibility

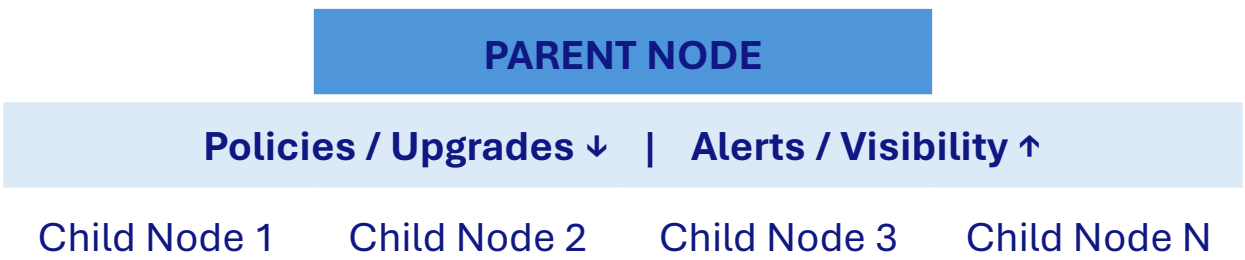
Aggregates asset risks and threat alerts from multiple nodes in real time, enabling centralized correlation analysis and security-posture reporting.

Centralized Intelligence & Policy Distribution

Allows the master platform to distribute detection policies and custom intelligence to subordinate nodes.

Cross-Tier Collaborative Investigation

Supports drill-down investigation from the central platform into raw data on subordinate nodes.



Intelligent Dashboard & Reporting

The upgraded reporting experience shifts the emphasis from "data piling" to value visualization, helping security teams communicate risk, activity, and outcomes more clearly.

Next-Generation Dashboard

Uses a modular design centered on asset risk, external attacks, file monitoring, and real-time alerts so analysts can identify important activity faster.

3D Operations Reporting

Covers Comprehensive Threats, Asset Risks, and File Threats, with automated generation and scheduled delivery through Email, Feishu, WeChat, DingTalk, and other supported channels.

From Data Overload to Actionable Value

ThreatTrace connects assets, threats, alerts, investigation evidence, and remediation guidance into a more operationally useful security workflow. By automating repetitive analysis and reporting tasks, the platform is designed to help security teams focus their time on higher-value investigation and response.

Operational Challenge	ThreatTrace Response
High alert volume	AI-assisted alert analysis and severity assessment
Slow investigation	Full-traffic retention and forensic traceability
File-transfer blind spots	Network-wide file monitoring and propagation tracking
Distributed environments	Hierarchical centralized visibility and policy control
Difficult security reporting	Value-focused dashboards and scheduled reports

Conclusion

The ThreatTrace evolution represents AIStorm's move toward a more intelligent, evidence-driven model for network security operations. By combining AI-assisted threat assessment with traffic traceability, file-threat awareness, multi-node management, and outcome-oriented reporting, ThreatTrace is positioned to help enterprises build more resilient and efficient defense operations in increasingly complex threat environments.

Turn ThreatTrace Into Action

AIStorm helps enterprises move beyond fragmented security alerts to AI-driven, unified defence across cloud, network and endpoint environments.

With deep cybersecurity expertise and an expanding global presence, AIStorm combines advanced threat intelligence, AI-native analytics and integrated security operations to help organisations detect threats earlier, respond faster and strengthen cyber resilience.

Request a Demo

Discover how ThreatTrace can help your security team cut through alert overload, reconstruct complex attack chains and turn security data into actionable outcomes.

Contact your representative or submit your form at www.aistorm.com today!