T-INNOWARE TECHNOLOGY (SINGAPORE) PTE. LTD.

Contact us :

Email: sales@t-innoware.com
Web: www.t-innoware.com
Address: 6 Raffles Quay, #14-02, Singapore 048580

T-INNOWARE

AI-POWERED SECURITY OPERATION

About T-INNOWARE

COMPANY PROFILE

T-INNOWARE is a global provider of IT security products and solutions, leveraging AI technology to address the increasingly complex security challenges faced by government institutions and enterprises. Our AI-driven solutions offer automated network security operations, helping clients build intelligent, efficient, and cost-effective security systems.

The founding team is made up of data science and cybersecurity experts, experienced IT product developers, and international business veterans with over 20 years of experience in sectors such as government, finance, education, healthcare, and enterprises.

KEYWORDS

- AI-Powered Threat Detection
- Multi-Source Threat Intelligence
- DeepSeek Powered
- Incident Disposal Recommendation
- AI-driven Automated Pentesting
- AI-Guided Compliance Assurance
- Significantly Reduce Opex
- Improving the efficiency of SOC
- Automated Attack Analysis
- Self-Evolving Security Model
- Human-Like Reasoning
- Security Incidents Investigation
- Smart Code Auditing
- Custom AI Agent
- Security Tools Integration
- More Reliable and Efficient

SAI (Security AI): Your Evolving Expert in Cybersecurity Operation and Maintenance

SOLUTION BACKGROUND

As the digital economy grows, cybersecurity threats are becoming more complex, with a rising gap between attackers and defenders and a shortage of skilled professionals. Meanwhile, stricter data privacy and security regulations are putting more pressure on organizations to comply. In this context, generative AI, driven by large language models (LLMs), has quickly emerged, bringing fresh momentum to the cybersecurity industry.

Current Challenges

The need for AI to fight AI

Cyber attackers have greatly improved their attack efficiency and accuracy through AI . In order to solve the imbalance between offense and defense, using AI to fight AI has become the best solution.

Insufficient Skills and Over-reliance on Personnel

Security operations heavily depend on personnel, but with the increasing frequency of cyberattacks, many security staff lack the specialized expertise needed to respond effectively.

Tightened Budgets and Limited Security Investment

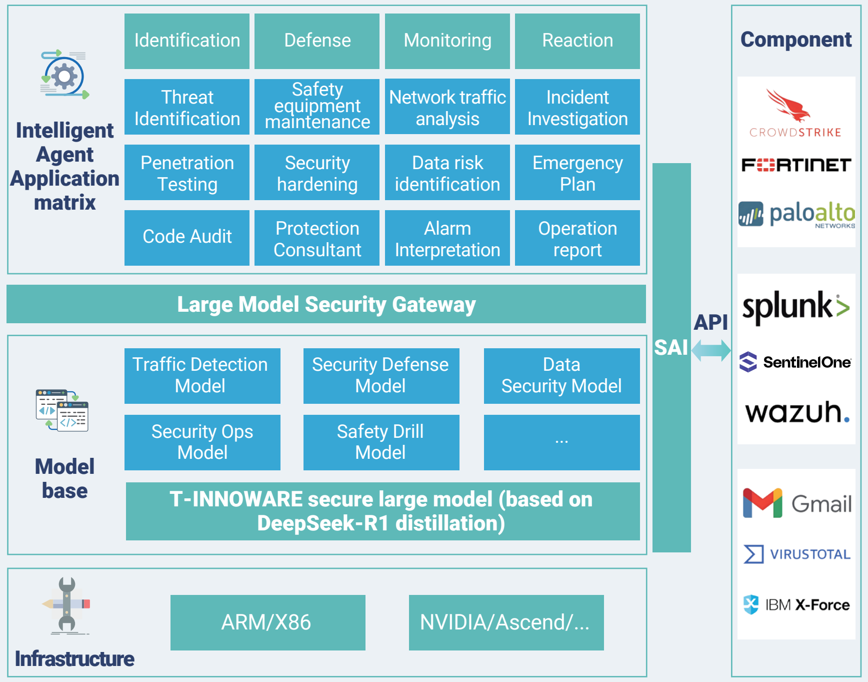
Organizations face reduced security budgets and are moving away from simply acquiring more tools. Instead, they seek to maximize security effectiveness through technological innovation.

Challenges in Measuring Security Outcomes

There is a lack of standardized metrics to evaluate the effectiveness of security operations. Without clear indicators, it is difficult to validate security results and demonstrate the value of security investments.

SOLUTION OVERVIEW

Security AI (SAI) is a network security automated operation and maintenance product created by T-INNOWARE based on GenAI technology. As the " general commander of security operation and maintenance work ", SAI provides a ready-to-use intelligent matrix covering identification, protection, monitoring and response , realizing the efficient and intelligent upgrade of security operation and maintenance work.

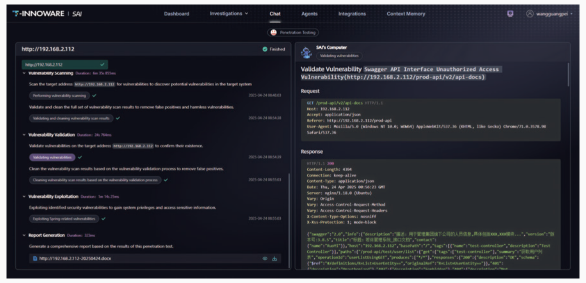


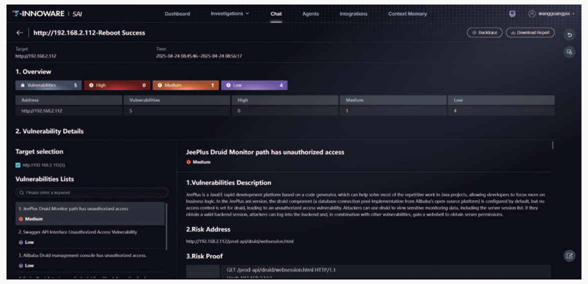
SOLUTION FEATURE

SAI assigns and executes security scanning or penetration testing tasks around the clock, continuously assessing the vulnerability of business systems. It promptly identifies security issues, generates penetration testing reports, and helps proactively address risks, ensuring early remediation and prevention.

01

A 24/7 Experienced Penetration Testing Expert (Offense)

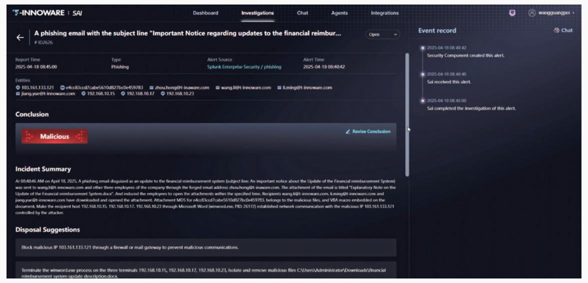




Through API integration, SAI connects both proprietary and third-party security devices, enabling alert management, data queries, analysis, and incident investigation. Unlike other large models, which primarily enhance their own security products, SAI acts as a "neutral third-party referee," assisting customers with security incident investigations and evidence collection, supporting informed decision-making.

02

An Always-Awake Security Analyst (Defense)



SOLUTION FEATURE

SAI features a variety of intelligent tools, each tailored to meet basic security operation needs. It continually evolves, gathering real-world user feedback to release more tools, perfectly suited for various operational scenarios.

03

Integration of a Range of Security Operations Tools

Security Operations Agents	Network Threat Detection Code Auditing	Penetration Testing Intelligent Decoding	Threat Intelligence Incident Investigation
Security Advisor Agent	Security Q&A	Compliance Consulting	Security Hardening Q&A
Data Security Agent	Sensitive Data Identification	API Risk Identification	Classification & Ranking
Custom Agent	Knowledge Base Upload	Role Configuration	Scenario-based Customization

SAI ALREADY CONNECTED TO DEEPSEEK BIG MODEL

Recently, SAI has completed the comprehensive docking with DeepSeek R1, aiming to further enhance its capabilities in security incident investigation, automated penetration testing, etc. , and help customers achieve efficient and intelligent upgrades in security operation and maintenance.

DeepSeek

Improve event detection efficiency and accuracy

Further enhancing the ability to deeply understand and analyze log data can more keenly capture abnormal behaviors and discover potential security risks in a timely manner.

Accelerate incident response with automation

In complex attack scenarios (such as lateral movement of ransomware), the impact of different response measures is simulated in real time to assist manual decision-making and automatically output event analysis reports that meet regulatory requirements .

Improve operation and maintenance management capabilities

Based on DeepSeek 's advantages in deep reasoning, SAI can understand operation and maintenance goals more clearly, and its intelligence level is further improved!

USER VALUE

With **the transformation, cost reduction, and measurement** enabled by SAI, **security operations capabilities** are truly enhanced.

Transformation

By leveraging SAI, security operations processes are redefined through AI, making them smarter and more efficient.

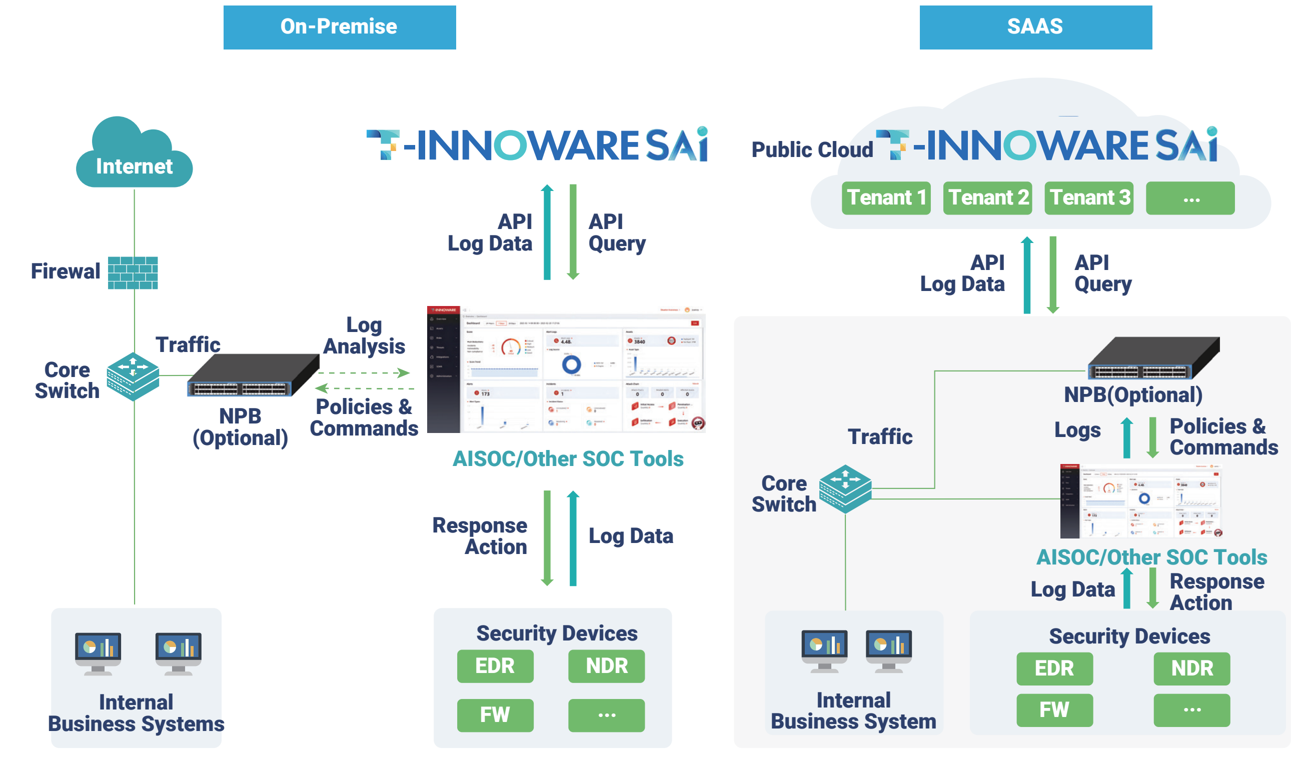
Cost Reduction

Utilizing various intelligent agents, orchestration becomes smarter, driving large-scale automation and enhancing the completeness of security operations.

Measurement

All security operations can be measured, with quantifiable data driving the continuous improvement of personnel and product capabilities.

Typical Deployment



Next Generation Security Operation Center (AISOC)

SOLUTION BACKGROUND

During digital transformation, enterprises often face slow response times in security operations, along with inadequate policies and regulations, leaving vulnerabilities for attackers to exploit.

Pain Points for Security Operation

Asset Status Uncertainties

Difficulty in incident localization and troubleshooting.

Massive False Alarms

Difficulty in analyzing security alarms accurately and efficiently.

Unknown New Threats

Traditional static defense technologies struggle to keep up with emerging threats.

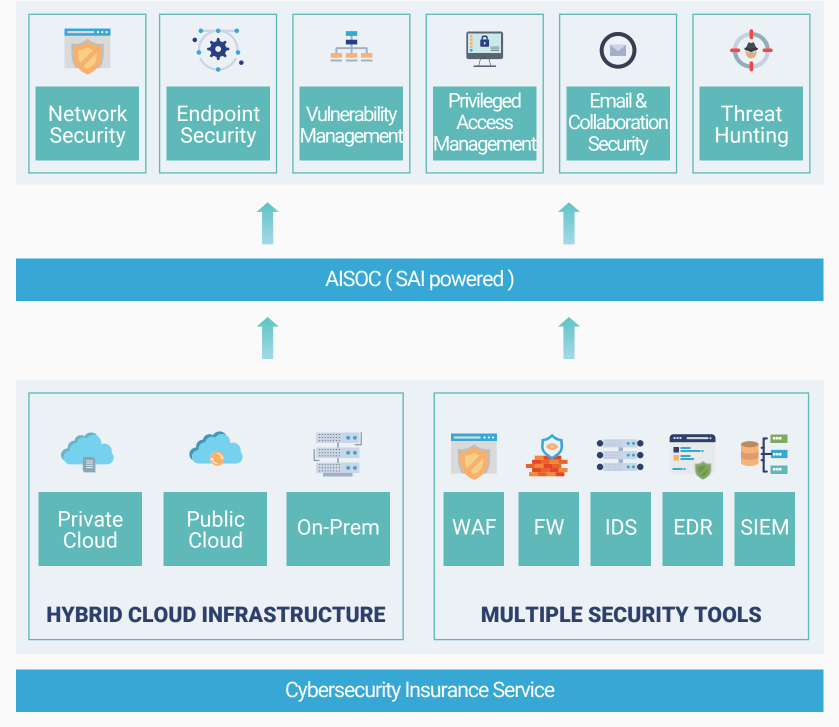
Fragmented Security Tools

Fragmented Security Tools resulting in slow response and poor results.

SOLUTION INTRODUCTION

In order to break the network security dilemma, T-INNOWARE launched the AI-enabled next generation security operation center (AISOC). By integrating the T-INNO AI security operation engine, it can achieve unified analysis of massive security alarms and unified scheduling of security tools, accurately identify security incidents and deal with threats in time, and comprehensively improve security operation efficiency for enterprise and organization.

In addition, T-INNOWARE incorporated network security insurance into the overall security strategy, forming a closed loop of risk management.



SOLUTION CAPABILITIES

01 Comprehensive Data Integration
It covers asset management and log access across cloud networks, terminals, emails, applications, data, and other security dimensions, achieving unified correlation and management of multi-source security data.

02 Intelligent Alarm Analysis and False Alarm Reduction
Use AI algorithms to analyze massive security logs, accurately identify real threats and filter irrelevant alarms, reduce the false alarms and missed alarms of traditional security tools.

03 Powerful Threat Intelligence Integration
Integrate multi-source threat intelligence, update and correlate the latest threat intelligence data in real time, quickly identify potential security threats, and improve threat detection rate and response speed.

04 SOAR Automated Response Orchestration
Preset a variety of templates to automatically trigger corresponding response measures according to the threat type, ensure rapid response in the face of complex and changing threats, reducing security risks and losses.

05 AI Empowers Security Operations
Integrating AI capabilities, enables topics such as detection analysis, alarm interpretation, vulnerability analysis, disposal suggestions and intelligent operation reports, improves the efficiency of threat detection.

GUARANTEED SECURITY FOUNDATION

Cybersecurity Insurance Services

Our cybersecurity insurance covers a wide range of potential losses, including business interruption, data recovery costs, cyber extortion, security testing expenses, and more.

Pre-Insurance Services

Risk Assessment

- ·Conduct a nine-dimensional risk evaluation and provide detailed risk reports.
- ·Deliver a comprehensive cybersecurity maturity assessment report to help you understand your current security posture.

Insuring

Continuous Protection

- ·Regular risk inspections.
- ·24/7 monitoring and early warning systems.
- ·Real-time blocking of advanced threats.
- ·Reinforced endpoint security.

Post-Insurance Support

Technical Assistance

- ·Emergency incident response.
- ·Data recovery services.
- ·Security incident analysis.
- ·Incident impact assessment.

“ 1 Insurance = 1 Protection + 365 Days of Service ”

Comprehensive Prevention
Continuous Monitoring
Rapid Response
Risk Mitigation

SOLUTION VALUE

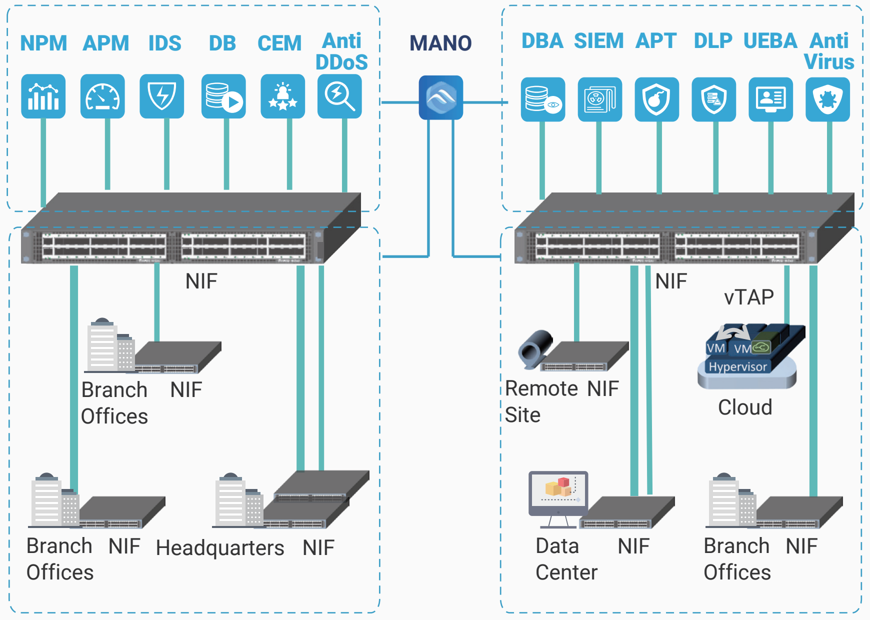
Lower Cost, Higher Value

40% ↓	200% ↑	90% ↓	99% ↓
Lower Operational Cost	ROI in Ownership Study	Mass Alarm Reduction	Risk Exposure Reduction

Network Packet Broker (NPB)

OUT-OF-BAND PRODUCT - NIF SERIES

T-INNOWARE' s Network Insight Fabric (NIF) simplifies network visibility by providing a unified platform for traffic aggregation, supporting both performance and security monitoring. It enables seamless deployment of monitoring tools, mirrors network traffic as required, eliminates bandwidth competition among tools, and offers comprehensive traffic optimization.



Hybrid IT Infrastructure

NIF FEATURES

01 **Deployment Mode**

The NIF device supports bypass mode, connecting to splitter or switch mirror ports.

02 **Product Functions**

Basic: Flow mapping, VLAN tagging, traffic filtering, traffic aggregation and replication, configuration logging, role-based access control (RBAC), port access control, and REST API.
Advanced: Advanced header stripping, de-duplication, packet slicing, flow slicing, masking, load balancing, tunneling, NetFlow generation, application filtering, application metadata, and application visualization.

03 **Device Type**

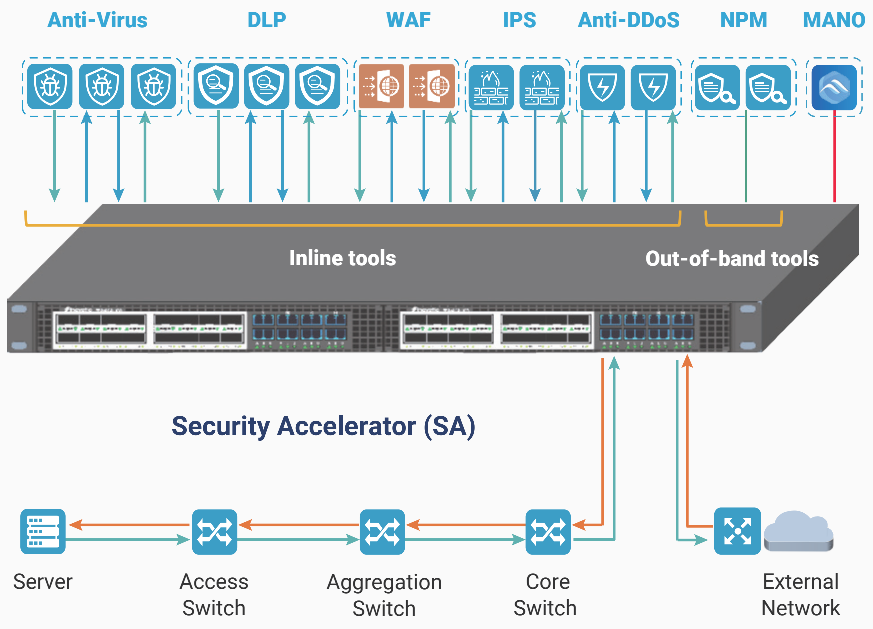
NIF-S11A/ NIF-S15A/NIF-S20A/ NIF-X10A/ NIF-X15A/NIF-X20A.

04 **Interface Type**

RJ45/ GE/ 10GE/ 25GE/ 40GE/ 100GE.

IN-LINE PRODUCT - SA SERIES

T-INNOWARE' s Security Accelerator (SA) simplifies the architecture and deployment of border security. It is primarily deployed at key network borders, such as the Internet and data centers, to provide unified management of security tools. The SA enables the flexible orchestration of security toolchains in critical areas, while addressing common network challenges like multiple points of failure and performance bottlenecks. By optimizing the efficiency of network maintenance and increasing the throughput of security tools, the SA significantly enhances overall network performance.



SA FEATURES

01 **Deployment Mode**

SA device supports deployment in the network in inline mode, connected to the core switch.

02 **Product Functions**

Basic: Link bypass, heartbeat packets, Inline Bypass, L2-L4 service-chain, Traffic Distribution (load-balancing), Traffic Aggregation & Replication, Configuration Log, Role-Based Access Control (RBAC), REST API.
Advanced: L7 service-chain, NetFlow Generation, Application Intelligence, Application Filtering, Application Metadata, Application Visualization, TLS/SSL Decryption.

03 **Device Type**

SA-S10A/ SA-S20A/ SA-X10A/ SA-X20A.

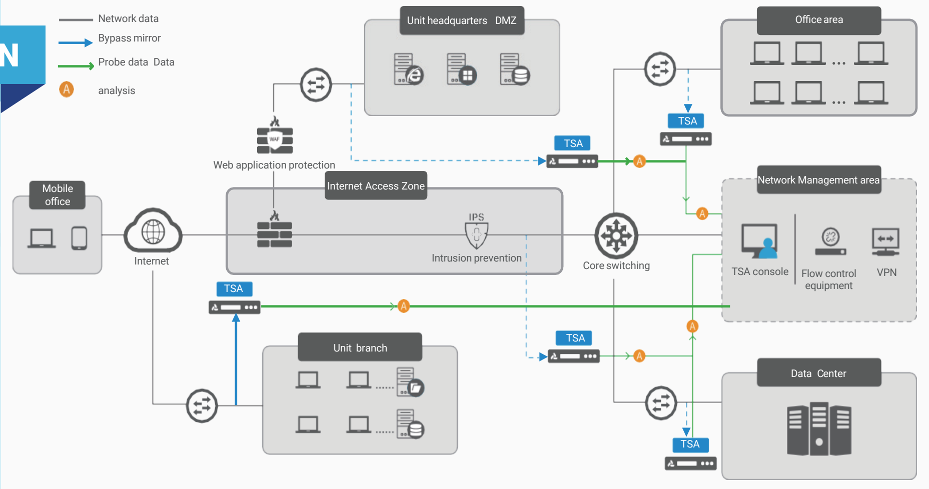
04 **Interface Type**

RJ45/ GE/ 10GE/ 25GE/ 40GE/ 100GE.

Traffic Security Analysis System

PRODUCT INTRODUCTION

The Network Full Traffic Security Analysis System (TSA) is a full traffic analysis product combines hardware and software seamlessly to meet the needs of diverse network environments, including cloud, industrial control systems, and multi-source, heterogeneous network scenarios.



PRODUCT FEATURE

01	Visibility into Network Activities	Gaining comprehensive insights into network behaviors.
02	Evidence Collection for Incidents	Providing irrefutable evidence for incident response.
03	Data Breach Traceability	Identifying the root cause of data leaks.
04	Detection of Advanced Threats	Identifying sophisticated, previously unknown cyber threats.
05	Asset Attack Surface Management	Minimizing exposure and risk for critical assets.
06	Impact Assessment	Evaluating the potential consequences of cyber incidents.

Product Value

Network Traffic Forensics and Liability Determination

Provide complete retention of full-traffic network communication data, enabling second-level extraction of massive historical traffic records and packet-level forensic analysis, facilitating precise reconstruction of all network communication content.

Proactive Risk Mitigation and Swift Incident Response

Conduct comprehensive mapping of event data to accurately assess the validity, severity, and potential outcomes of security alerts. evaluating the scope of potential impacts, identifying vulnerabilities and blind spots in their security infrastructure.

Comprehensive Cyber Threat Detection

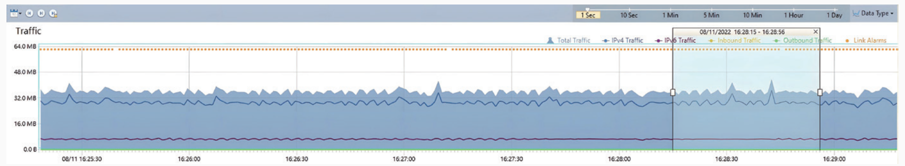
Provide 24/7, all-aspect real-time identification and analysis of network traffic data. With our advanced traffic visualization capabilities, we help you identify assets, pinpoint security vulnerabilities, and uncover potential risks.

Network Performance Analysis System

PRODUCT INTRODUCTION

Network Performance Analysis System(NPM) is an enterprise-class network monitoring and performance analysis system. Designed for 24x7 network packet capture, analysis and storage, dedicated to the sustainable, efficient and safe running of networks, NPM provides a reliable data basis for determining constructive suggestions for enterprise profit growth.

Excellent in data drilldown, data tracing and locating, and security forensics, NPM makes it possible to troubleshoot historical network issues by rewinding and zooming in to any previously recorded time period. This feature saves a tremendous amount of time and effort that would be required to reconstruct network scenarios. Besides troubleshooting network issues, NPM can be also used to evaluate and benchmark long-term network performance along with auditing user activity.



Benefits for Network Engineers

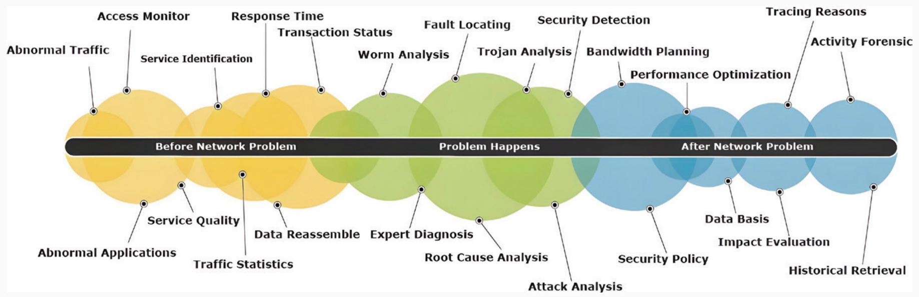
01 Identifying - Intelligently analyze critical network traffic in real-time, identify network performance and application anomalies, and abnormal network activities.

02 Tracing - Rapid data mining and traffic analysis, accurately analyze and locate the root causes of network faults and security events.

03 Troubleshooting - Replay the original network communication data, reproduce how the faults, anomalies and events happen, provide direct proofs for network troubleshooting.

PRODUCT VALUE

With an analysis performance of up to 100 Gbps, NPM is able to capture large traffic of backbone links in line speed, and to analyze and store the traffic in real-time, and able to monitor several network adapters simultaneously to aggregate the traffic from multiple links. Together with a storage filter and splicing storage technology, NPM is able to store only the interested and useful information, which makes the storage space utilized effectively.



API Security Solution

SOLUTION BACKGROUND

As digital transformation accelerates, APIs have become essential for data sharing and business operations in industries like finance, healthcare, and government. However, the growing reliance on APIs also introduces heightened data security risks.

To ensure API security, many Southeast Asian countries have implemented data protection laws and standards to guide the development of API security measures, enhance risk monitoring, and protect business data.

- Increased Internet exposure of APIs
- Abnormal API interface access
- API security vulnerabilities
- Insufficient API authentication mechanisms
- Unauthorized API access
- ...

API SECURITY SOLUTIONS

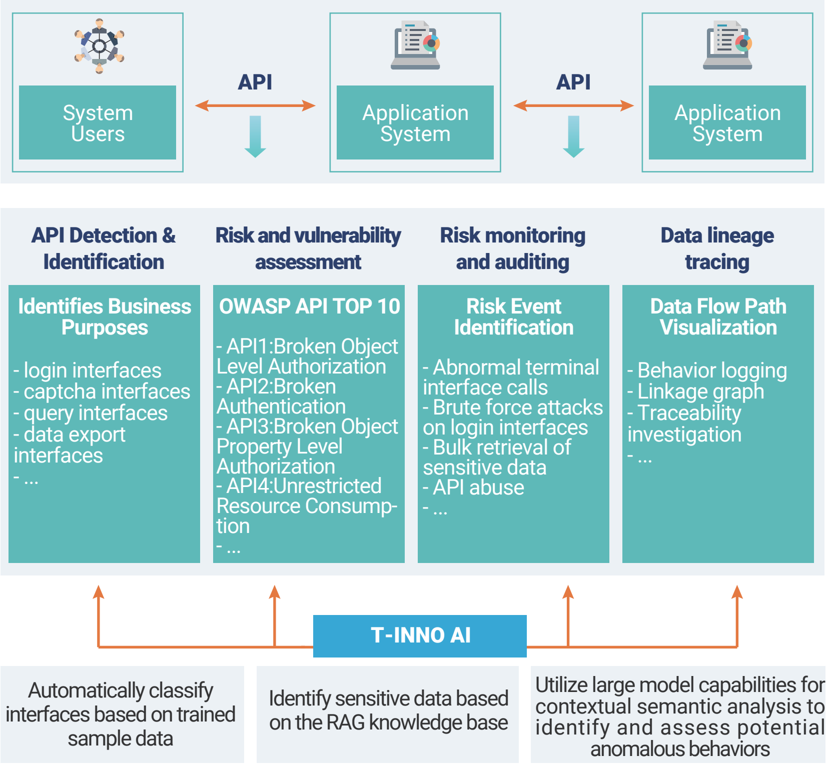
To tackle challenges in API asset management, risk detection, and sensitive data breaches, we've developed an API security solution powered by T-INNO AI technology. This solution enhances risk monitoring and traceability with the following key features:

API Asset Discovery: Automatically identifies APIs and their exposure points.

Vulnerability Assessment: Detects vulnerabilities, pinpoints security flaws, and recommends remediation actions.

Risk Monitoring: Provides 24/7 real-time monitoring to minimize security incidents.

Data Traceability: Tracks access to sensitive data, enabling investigations in the event of breaches.



System Users ⟷ API ⟷ Application System ⟷ API ⟷ Application System

API Detection & Identification

Identifies Business Purposes

- login interfaces
- captcha interfaces
- query interfaces
- data export interfaces
- ...

Risk and vulnerability assessment

OWASP API TOP 10

- API1:Broken Object Level Authorization
- API2:Broken Authentication
- API3:Broken Object Property Level Authorization
- API4:Unrestricted Resource Consumption
- ...

Risk monitoring and auditing

Risk Event Identification

- Abnormal terminal interface calls
- Brute force attacks on login interfaces
- Bulk retrieval of sensitive data
- API abuse
- ...

Data lineage tracing

Data Flow Path Visualization

- Behavior logging
- Linkage graph
- Traceability investigation
- ...

T-INNO AI

Automatically classify interfaces based on trained sample data

Identify sensitive data based on the RAG knowledge base

Utilize large model capabilities for contextual semantic analysis to identify and assess potential anomalous behaviors

SOLUTION HIGHLIGHTS

01 Independent Bypass Deployment

Using deep traffic analysis technology, the solution audits applications/API interfaces independently, offering a plug-and-play approach that doesn't interfere with business operations.

02 Abundant Types

Four API formats, 25 data formats, 66 data tags, 23 API types, over 20 risk models, and fully addresses all OWASP vulnerabilities.

03 Workflow Visualization

Automatically organizes data flow paths and conducts heat analysis and statistical analysis of data transfers, saving 75% of the time required for leak analysis and localization.

04 Intelligent Analyzing

Leveraging T-INNO AI's intelligent API security vulnerability detection capabilities, the system improves discovery rates by 30% and interprets vulnerability characteristics to accurately identify potential risks.

SOLUTION VALUE

Promote Data Development and Utilization

By enhancing API risk monitoring and auditing, the openness of APIs is significantly safeguarded, effectively promoting data sharing and circulation.

Ensure Users Data Security

By comprehensively monitoring application access behaviors, the system identifies and flags abnormal activities to prevent data breaches, leaks, or unauthorized use.

Data Privacy Compliance

Conducts regular monitoring of data security risks to ensure the lawful and compliant use of business data.