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

AI-POWERED SECURITY OPERATION

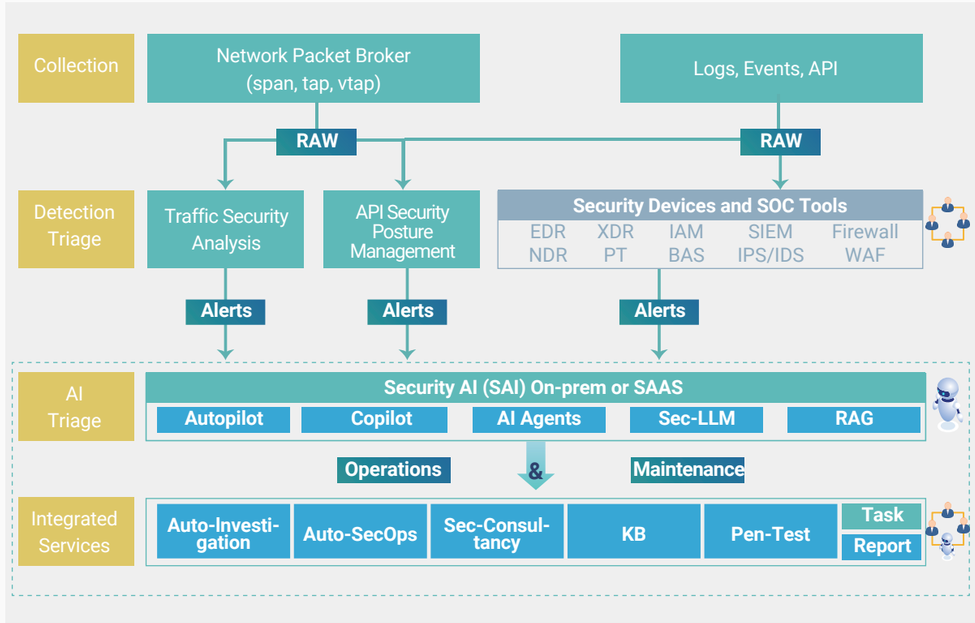
About T-INNOWARE

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.

OVERALL ARCHITECTURE



SAI (Security AI): Your AI Orchestrator in Cybersecurity Operations and Maintenance

INDUSTRY BACKGROUND

- Cybersecurity threats have been escalated in complexity.
- Widening capability gap between attackers and defenders and a critical talent shortage.
- Stricter data privacy and security regulations create tremendous compliance pressure.
- **Large Language Models (LLMs)** bring fresh momentum to the cybersecurity industry.

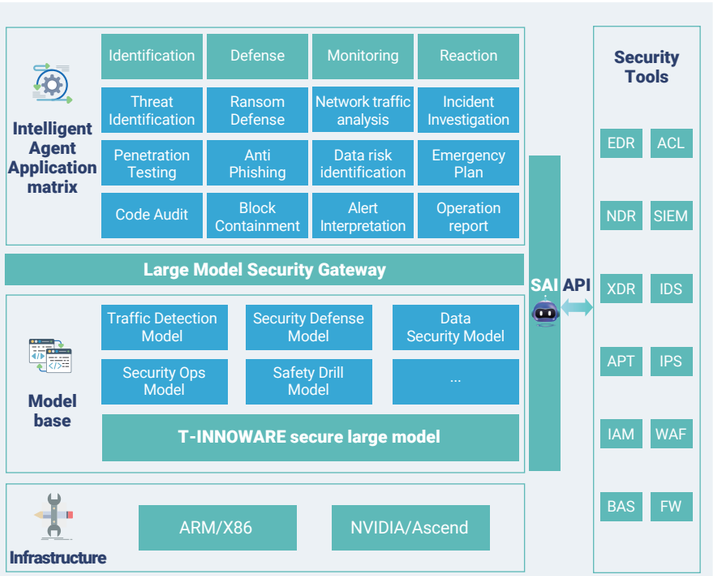
Current Challenges

Massive security alerts that generate false alarms overwhelm SOC teams, causing delays, burnout, and missed threats. This inefficiency increases operational costs and reduces overall security effectiveness, impacting both business and technical resilience.

Leveraging LLM's capability, SAI turns the impossible trinity into intuitive, intelligent and actionable reality.

SOLUTION OVERVIEW

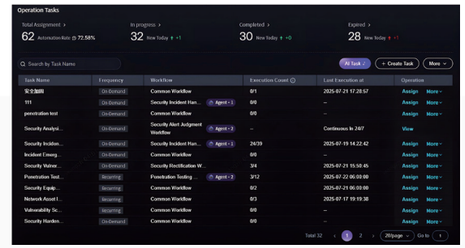
Based on GenAI technology, SAI works as the "**orchestrator of security operations**". It provides a ready-to-use intelligent matrix covering **identification, protection, monitoring and response**, realizing the efficient and intelligent upgrade of security operation and maintenance.



SOLUTION FEATURES

01 AI Cybersecurity O&M Tasks and Tickets Management

- **O&M Solution Plan & Management**
- **O&M Tasks Implementation**
- **O&M Performance Assessment**



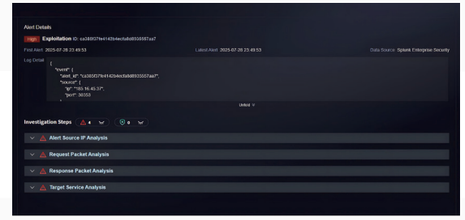
Automatically make annual work schedules, dispatch tasks, and establish an automated O&M task creation process.

Automatically create tickets to complete pen-test, assets inspection, incidents investigation, and other O&M tasks.

Automatically generates O&M reports, including number of alerts, key performance metrics and staff efficiency.

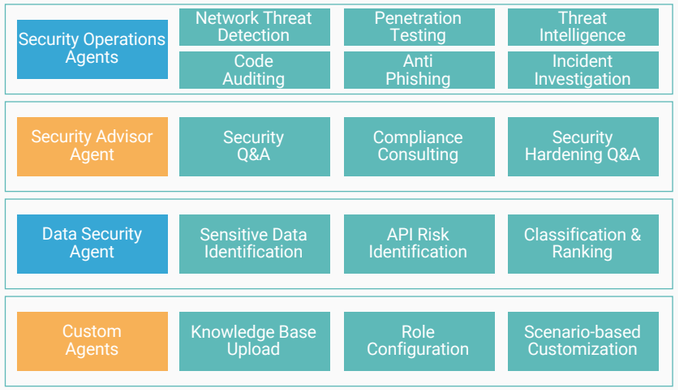
02 AI Auto-pilot: Automatic Incident Investigation

- **Intergrate all SOC tools through API or syslog**
- **True automatic implementation of Incident investigation**
- **AI's capability used for alert analysis and incident identification**
- **Conclusion and disposal suggestions are provided for incident response**



03 AI Co-pilot: 24/7 Cybersecurity O&M Experts Team

As a virtual security experts team, SAI assists security analysts with **continuous consultation**, pen-testing, and sensitive data identification. By automating complex tasks and providing expert guidance, it strengthens security posture, enhances operational resilience, and enables proactive threat management without increasing headcount.



BUSINESS VALUES

Industry Revolution

SAI autopilot and copilot automates investigation, guides analysts for unmatched security resilience, minimizing financial and reputable damage.

Cost Reduction

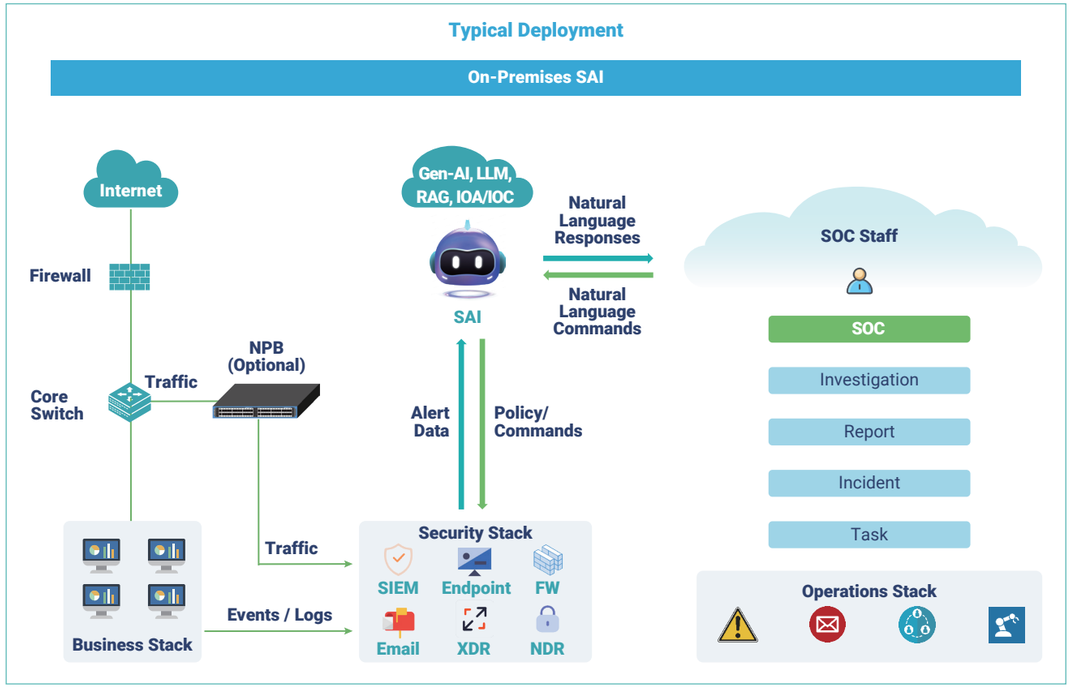
SAI is security O&M runs nonstop 24x7x365. It can scale and expand without operational headcount increases.

Stronger Competition

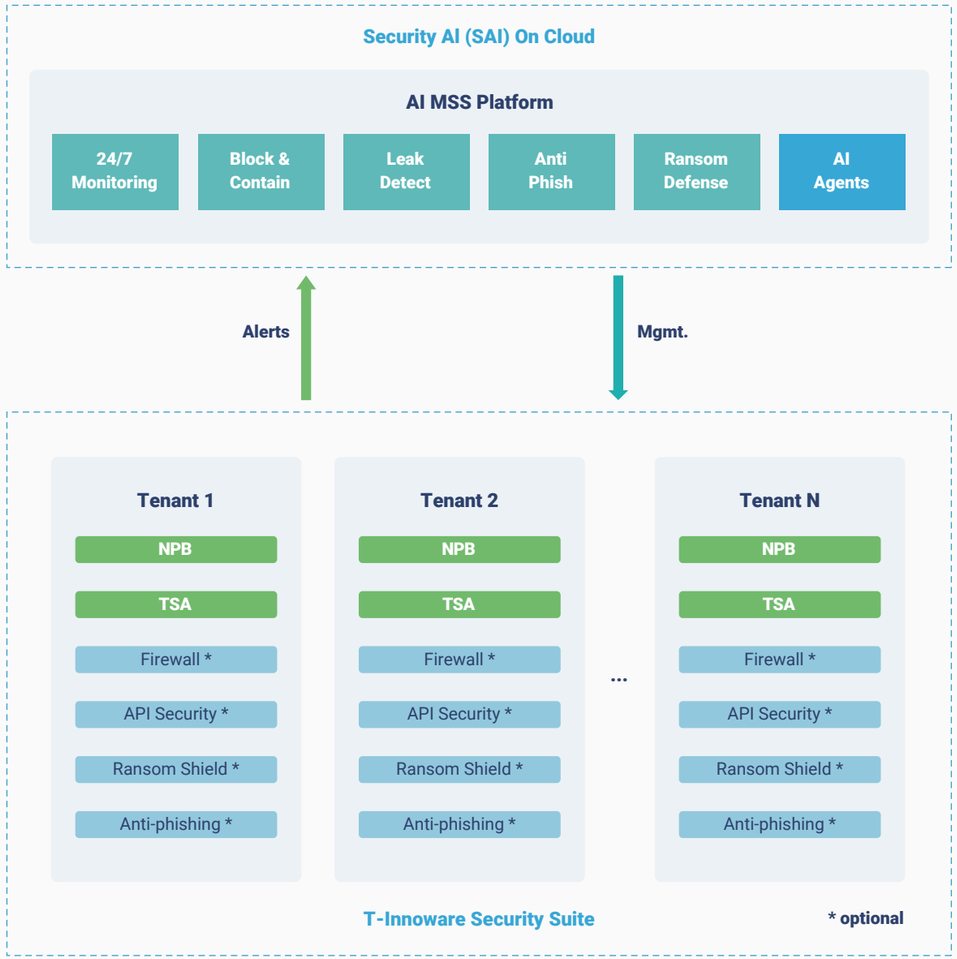
SAI delivers faster and adaptive defence, ensuring resilience and keeping businesses ahead of all competitive security challenges.

EXISTING DEPLOYMENT

- Government Agencies
- Telecom Operators
- Financial Services / Banking
- Energy and Manufacturing



SAAS SAI



API Security Posture Management

BACKGROUND

As crucial channels for transmitting data, APIs have garnered significant attention from attackers in the dark and gray industries, becoming a hotspot for data breaches. Meanwhile, regulations and compliance requirements are becoming increasingly stringent, further highlighting the urgency of API security issues. Therefore, organizations urgently need to attach great importance to API data security and actively explore effective risk mitigation strategies.

API assets are agnostic

- What is the total amount of API?
- What is the status of the API?
- Is there any correlation between APIs?
- Is the API sensitive?

API risk is unobservable

- Does the API have any security flaws?
- Does the API have any security vulnerabilities?
- Is there any risk associated with the access behavior?
- Is there any risk in data flow?

API access is not traceable

- Who accessed the sensitive API?
- When to access sensitive APIs?
- Data flow is not traceable?
- Violation call is not traceable?

PRODUCT INTRODUCTION

01 An intelligent security solution designed to address the complex API security threats.

02 Making API assets visible, assessing hidden risks, detecting risks, and tracing access behaviors.

03 Monitoring the API data exposure and attack status in real time, ensuring timely detection and response to security incidents, and safeguarding data security and the steady development of business.

Data-centric

Detection

- Automated API identification
- Data exposure analysis
- Generate an API asset inventory

Monitoring

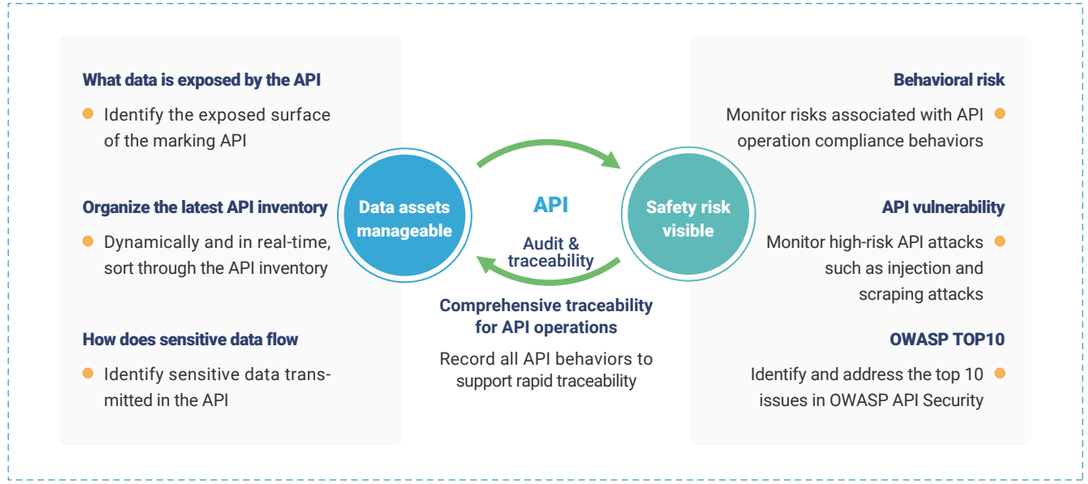
- Monitor API behavior in real time
- Find security issues such as data leaks

Assessment

- Evaluate the OWASP API Security TOP 10
- Rectification suggestions

Traceback

- Record the entire process of accessing sensitive data.
- Track and trace the source of data leaking.



Wide coverage

Multi-dimensional API asset management

- It covers multiple API formats, data formats, various data tags, API types, and risk models, and supports intelligent API asset sorting and identification.

Flow visualization

Visual data flow management

- Automatically organize data flow paths, conduct data flow heat analysis and statistical analysis, and assist in monitoring data flow risks.

AI-powered

Intelligent security analysis and protection

- Intelligent API security risk discovery capabilities based on LLM, interpreting risk characteristics to accurately identify potential risks.

VALUES

The API Security Posture Management provides enterprises with comprehensive value ranging from compliance management to data security and business innovation. It assists enterprises in effectively addressing API security challenges, promoting stable business development, and truly achieving a win-win situation for both business and security.

Compliance worry free
Easily handle regulatory audits

Data Protection
Prevent data leakage and illegal utilization

Open Data
Promote secure data sharing and innovation

Network Packet Broker

PRODUCT INTRODUCTION

A Network Packet Broker (NPB) is a **hardware** and **software** system that sits between network infrastructure with probes and network monitoring or security tools. The probes run inlined (SA) or mirrored (NIF) mode to capture, filter, and distribute network traffic to the appropriate tools for building up use cases.

Business Value

Full Traffic Visibility

Centralized monitoring network and application traffic North-South / East-West for performance optimization and distribution to downstream tools.

Cost Efficiency

Single tool for distributing traffic to existing tools. Reducing overhead for improving network and security ops efficiency.

High Scalability

Highly scalable solution with stackable platform for more than 100+ Gbps throughput. Extend visibility for virtual, containerized and cloud workloads.

Use Case Flexibility

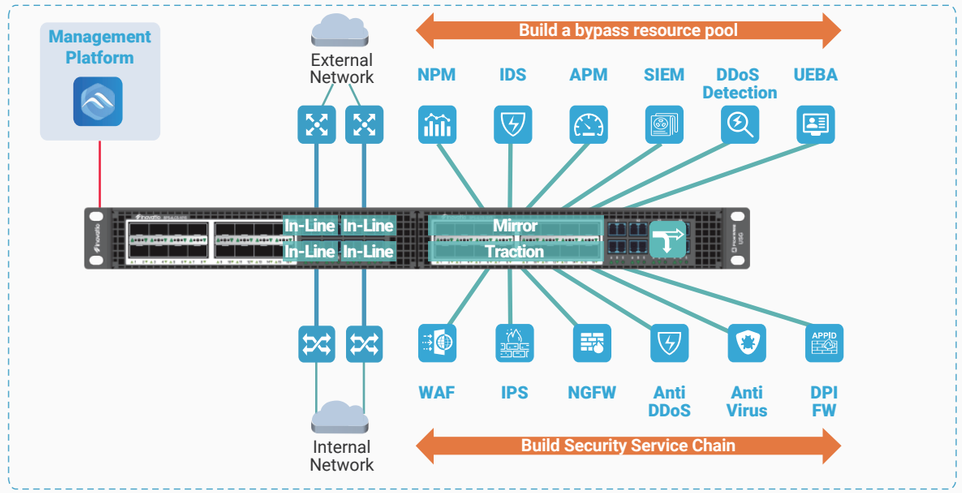
Flexible use case deployment for network, security and application traffic management with downstream integration to NPMD, APMD and SIEM.

TECHNICAL VALUE

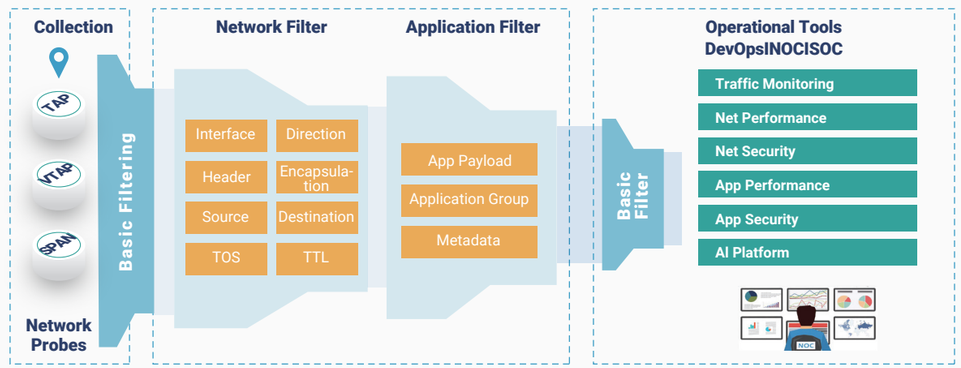
Network Insight Fabric (NIF)	Security Accelerator (SA)
Out-of-band deployment.	In-line deployment.
Supports aggregating and replicating traffic from switch mirroring or link splitting.	Enable transparent mode deployment for redirecting link traffic to in-line tools within the service chain.
Support VTAP on virtualization and microservices (K8S, Docker).	Support bypass protection：logical and physical bypass.
Support L2-L7 traffic filtering.	Support L2-L7 traffic orchestration.
Support timestamps and VLAN tagging.	Support TLS/SSL Offloading.
Support traffic optimization such as tunnel stripping, tunnel termination, and traffic deduplication.	Support tool health detection.

01. Application-aware, which enables identifying thousands of applications and Layer 7 protocol metadata.
02. Netflow generation for further monitoring and troubleshooting.
03. Multiple load balancing strategies to ensure balanced traffic distribution across tools.
04. Support RBAC and Rest API integration.

TYPICAL NETWORK INFRASTRUCTURE



TYPICAL USE CASES



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.

01 24x7x365 real-time collection with single device high-capacity storage.

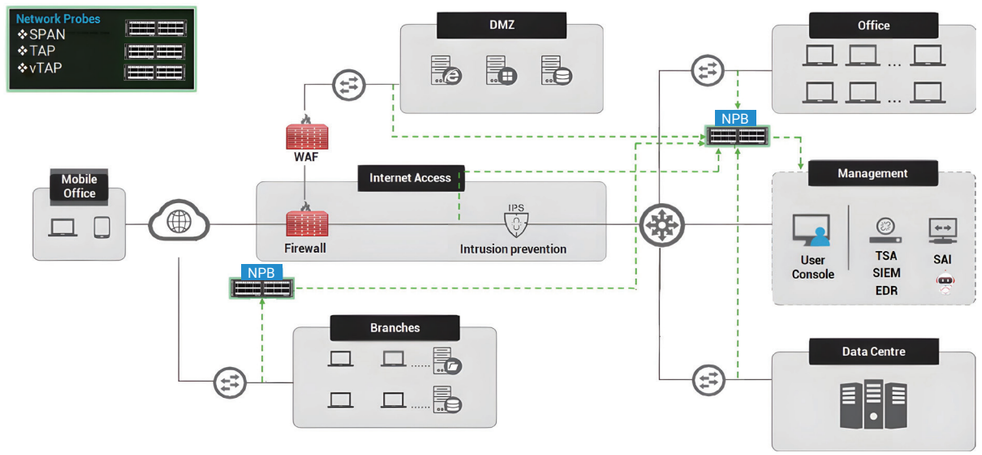
02 Traffic analyzer for raw packets (PCAPS).

03 Advanced Security Detection, Forensics and Investigations.

04 Flexible behavior rules with optimization capabilities.

05 Ability to discover unknown threats (zero-day).

Typical Diagram with TSA



Business Values

Threat Detection and Tracing

Ability to detect and trace of threats and breaches will highly protect against downtime, financial losses and reputable damage.

Asset Impact Assessment

Ability to minimize exposure of critical assets, support risk prioritization and prevent potential business disruption while maintaining, governing and securing business goals.

Evidence Collection for Incident

Ensures legally defensible proof for regulators, law enforcement, and stakeholders post-breach will reduce liability in lawsuit and strengthen in recovery.

TECHNICAL VALUES

Traffic Visibility and Forensic

Capture and retain all network traffic, enabling instant access to historical data and precise forensic analysis for complete communication reconstruction.

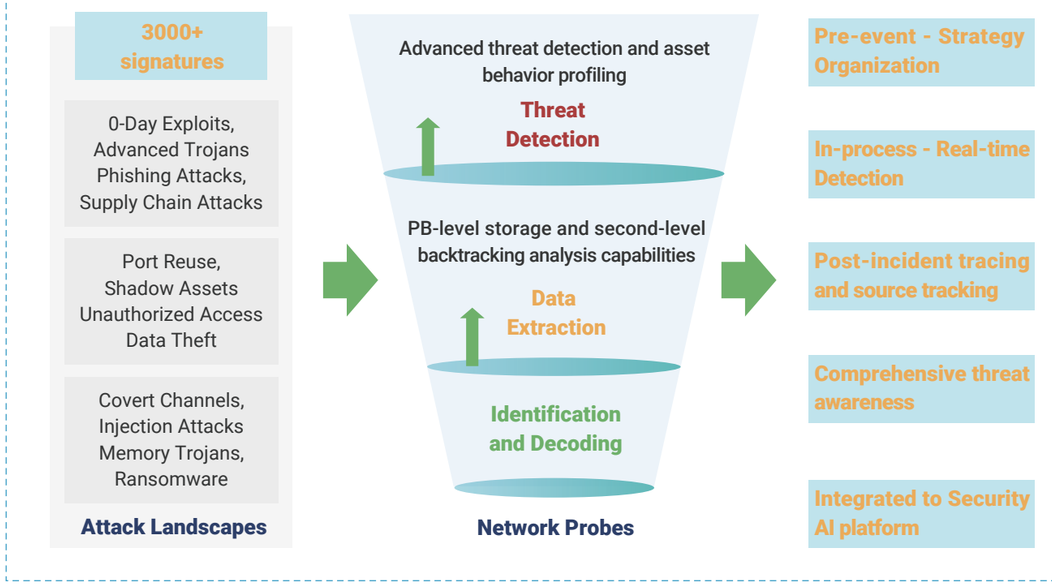
Risk Mitigation and Incident Response

Map and analyse event data to validate alerts, measure impacts, and expose hidden vulnerabilities for a stronger, smarter security postures.

Comprehensive Threat Detection

Deliver 24/7 real-time detection and analysis of network traffic. Our advanced visualization tools reveal assets, expose vulnerabilities, and uncover potential risks with precision.

Use Cases

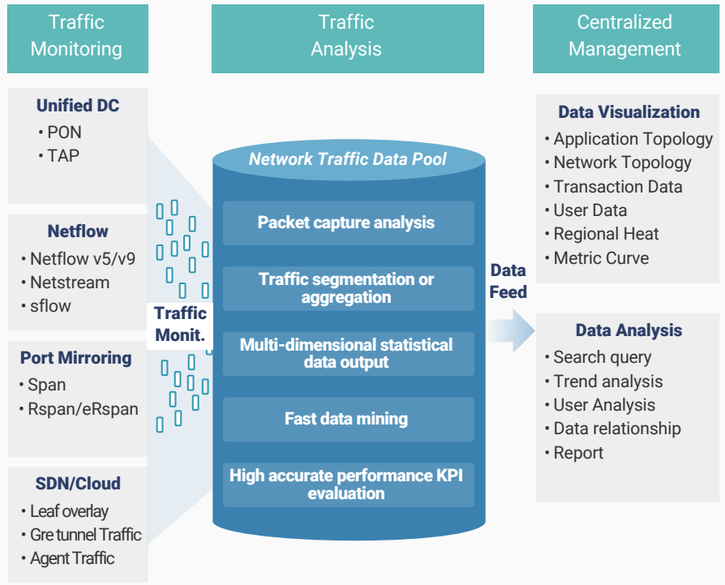


Network Performance Monitoring and Diagnostics

PRODUCT INTRODUCTION

With NPMD, you don’ t just troubleshoot—you rewind, zoom in, and dissect every packet, user action, and performance glitch.

- **Data Drilldown with Surgical Precision – Isolate root causes in minutes, not days.**
- **Replay & Audit Any Moment – No guessing. See what happened, when, and by whom.**
- **Benchmark Performance Over Time – Prove ROI on upgrades and stop recurring issues.**



PRODUCT HIGHLIGHTS

With 100 Gbps analysis performance, NPMD monitors multiple network adapters simultaneously, aggregating traffic across links while smart storage filters retain only critical data, realizing Real-time visibility, no blind spots, and actionable network insights.

Before network problems

- Abnormal traffic & service monitoring & identification
- Service quality & traffic statistics

Problem happens

- Security detection, attack analysis
- Expert diagnosis
- Fault locating, root cause analysis

After network problems

- Bandwidth planning, perf. optimization
- Activity forensic, impact evaluation
- Tracing reasons, security policy

TECHNICAL VALUES

High Performance Analysis

analyse 100 Gbps+ network traffic in real-time, identify network performance and application anomalies, and abnormal network activities.

Tracing

Rapid data mining and traffic analysis, accurately analyze and locate the root causes of network faults and security events via payload inspection.

Granular Troubleshooting

Replay the original L2-L7 network protocols, reproduce how the faults, anomalies and events happen, provide direct proofs for network troubleshooting.

Optimized Storage

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

TYPICAL USE CASES