

# N-AI

# DATASHEET

---

Next Generation IT Operation Platform  
Integrate Network Management, Flow Analysis and Log Reporting



2026/05/18



N-Partner develops N-Cloud and N-Reporter log management platforms, delivering a comprehensive and efficient data analytics environment. With N-AI Server integration, the platform enables proactive data analysis and intelligent reporting to improve operational efficiency, decision-making accuracy, and overall user experience.

N-AI Server powers the built-in N-Robot with advanced analytics capabilities, supporting natural language Q&A, report analysis, and recommendations. Users can quickly gain actionable insights, monitor network conditions and anomalies through automated reports, and receive personalized threshold recommendations to enhance monitoring and alert accuracy.

## ■ Software Features

### N-AI Learn Fast. Analyze Smart. Explain Clearly. Decide Better.

N-AI Server includes the N-Robot AI engine, delivering capabilities in learning, analytics, explanation, and decision support.

Deeply integrated with N-Cloud and N-Reporter, N-Robot transforms network management, user behavior analytics, and log platforms into an intelligent operations assistant. By continuously learning from network and log data, it provides real-time insights, summary reports, and actionable recommendations to support daily operations, troubleshooting, and decision-making.

#### Overall Analysis Conclusion

##### Key Findings

The cybersecurity analysis highlights several critical issues, such as high-risk threats originating from Taiwan, with attackers using specific IP addresses (e.g., 211.23.18.242, 211.23.18.243, and 192.168.5.55) to engage in prolonged session monitoring, indicative of potential reconnaissance or data exfiltration attempts. The attackers primarily target port 22, associated with SSH, suggesting efforts to exploit SSH vulnerabilities. The geographical distribution analysis identifies Taiwan as a significant source, while many attack origins and destinations remain unknown, complicating defensive efforts. Attack trend analysis reveals peak activities at 15:00 and targeted occurrences on February 26, 2026, signaling organized attack campaigns. Scanning behavior analysis identifies horizontal and vertical scanning, especially from IP 192.168.5.55, indicating sophisticated probing activities. The attack impact analysis emphasizes the "Long Time Session Monitor" attack type, pointing to potential unauthorized access or data exfiltration. Service type analysis shows low-risk threats across observed ports, yet port 22 remains a frequent target for attacks.

##### Potential Risks

The findings suggest several potential risks, including system compromise through SSH vulnerabilities, data exfiltration, and prolonged unauthorized access. The attack patterns and scanning behaviors indicate a risk of automated and organized attacks targeting system weaknesses. The geographical concentration of threats from Taiwan and unidentified sources complicates attribution and response efforts. The extended attack durations could strain defensive resources, increasing the likelihood of successful breaches. The unknown victim locations hinder targeted defensive measures, while the observed lateral movement suggests reconnaissance activities that could precede larger attacks.

##### Risk Assessment

The risk of compromise through SSH vulnerabilities is high, given the attackers' focus on port 22 and the use of sophisticated scanning techniques. The prolonged attacks and large data transfers increase the likelihood of data breaches. The lack of specific victim information and unknown attack origins present a substantial intelligence gap, elevating the risk of misattribution and delayed response. The overall severity is high, with a significant potential impact on system, network, and data security. The likelihood of continued attacks remains high, given the organized and persistent nature of the observed activities.

##### Recommended Countermeasures

###### Short-term Strategies:

1. Enhance network monitoring, especially on SSH services, and implement geofencing against traffic from Taiwan.
2. Deploy intrusion detection systems (IDS) for real-time threat identification and mitigation.
3. Conduct thorough security audits to identify and patch vulnerabilities across critical services, especially those related to SSH.
4. Implement dynamic firewall rules to block suspicious IPs and restrict access to high-risk ports.

###### Long-term Strategies:

1. Improve data collection and threat intelligence to reduce unknowns in attack origins and destinations.
2. Implement robust anomaly detection systems and comprehensive network segmentation to limit the impact of breaches.

#### Peak Attack Hours



#### Attack Density Analysis

Statistic Item	Value
Average Hourly Attacks	5.75

Time Period	Attack Times	Percentage
15:00	13	56.52
11:00	8	34.78
08:00	1	4.35
21:00	1	4.35

#### Analysis Result

The analysis of the provided data reveals several key insights into attack trends and density. The peak attack hour is identified at 15:00, with 13 attacks and significant data transfer, indicating a concentrated threat during this time frame. The daily analysis shows the highest attack occurrence on February 26, 2026, with 12 attacks, suggesting targeted activity that day. The average hourly attacks are 5.75, with substantial session, packet, and byte counts, underscoring a consistent threat presence. Notably, the "Long Time Session Monitor" indicates prolonged session durations, which could signify persistent threats. The absence of specific target port data (represented by port 0) suggests random targeting across all ports, complicating defensive measures. Key concerns include the high volume of data packets and bytes during peak hours, indicating potential data exfiltration or Denial of Service (DoS) attempts. Recommendations include enhancing monitoring during identified peak hours, implementing robust anomaly detection systems, and ensuring comprehensive network segmentation to mitigate the impact of potential breaches. Additionally, further investigation into the root causes of these peak activities and the deployment of advanced threat intelligence measures is advised to proactively address these cyber threats.

## Natural Language & Screenshot-Based Q&A

N-Robot supports natural language queries and screenshot-based analysis, allowing users to ask questions or upload visuals to instantly gain insights and recommendations.

It quickly interprets charts and data to identify anomalies and potential root causes, significantly improving large-scale data analysis efficiency. With intuitive and flexible interaction, N-Robot acts as an intelligent operations assistant for troubleshooting and decision-making, ensuring both accuracy and responsiveness.

**N-Robot** ✕

Analyze current system and network status

Based on the comprehensive analysis of your monitoring reports, here's the current **System and Network Status Assessment**.

**🚨 CRITICAL STATUS OVERVIEW**

**Overall System Health: HIGH RISK** ⚠️

The current monitoring data reveals multiple critical issues across different system layers that require immediate attention.

**1. SECURITY POSTURE - CRITICAL** ●

**Active Threats Detected:**

- **Persistent Backdoor Connections:** 17 long-duration sessions (5+ days) from external Taiwan IPs
- **Potential Data Exfiltration:** DNS query anomalies with 670-5,117% increase rates
- **Compromised Internal Systems:** Multiple internal-to-internal suspicious communications

**Risk Assessment:**

Threat Level: CRITICAL  
 Confidence: HIGH  
 Impact: Organization-wide data breach potential

**N-Robot** ✕

Prioritize and list items requiring immediate attention

**🚨 IMMEDIATE ATTENTION REQUIRED - PRIORITY ACTION LIST**

**PRIORITY 1 - CRITICAL SECURITY THREATS** 🚨 *Action Required: NOW*

**1.1 Block Suspicious External Connections**

**Risk:** Active data breach in progress

- Block [redacted] IPs: [redacted]
- Isolate affected internal systems: [redacted]
- Duration: 5+ days continuous sessions = ACTIVE COMPROMISE

**1.2 Investigate DNS Exfiltration**

**Risk:** Data theft via DNS tunneling

- Analyze DNS queries to [redacted] (2,189% spike)
- Block [redacted] (4,211% increase)
- Review [redacted] anomalies (3,441% spike)

**1.3 Quarantine Compromised Internal Systems**

**Risk:** Lateral movement and data access

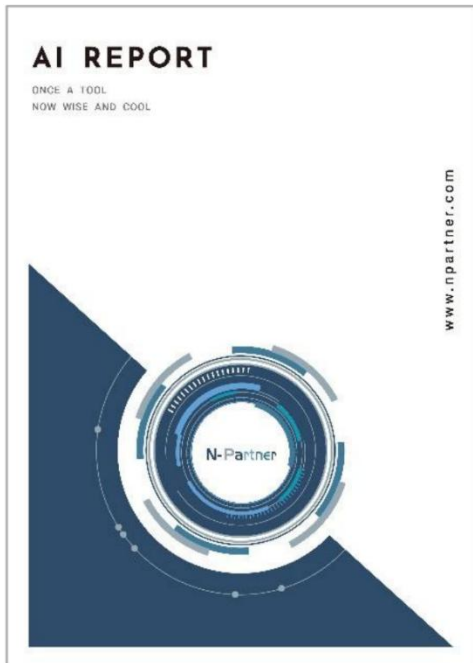
- Isolate: [redacted] (multiple long sessions)
- Monitor: [redacted]
- Preserve forensic evidence before isolation

**PRIORITY 2 - INFRASTRUCTURE FAILURES** 🚨 *Action Required: Within 1 Hour*

## AI-Driven Operational Insight Reports

N-Robot automatically generates operational performance reports, analyzing network usage trends, device health, security status, collaborative defense records, and anomaly alerts over a selected time period.

Reports are presented in natural language with key insights, enabling rapid root cause identification and effective decision-making. With continuous learning and fine-tuning, N-Robot delivers real-time analysis and intelligent recommendations, improving system stability, security, operational efficiency, and decision accuracy.



### Security Threat Analysis Report

Generated Date: 2026-03-05

Report Summary Data Time Range: 2026-02-05 14:50 - 2026-03-05 14:50

23 Total Attacks	6 Unique Attackers	9 Unique Victims	8.05 Total Traffic (GB)
------------------	--------------------	------------------	-------------------------

Average Attack Duration: 7 days 15 minutes 26 seconds

#### Analysis Result

In the analysis period from February 6 to February 27, 2026, a total of 23 attacks were recorded, involving 6 unique attackers and 9 unique victims, generating 8.05 GB of traffic. The average attack duration was approximately 605.726 seconds, indicating that the attacks were sustained over significant periods, suggesting a potential persistence strategy by the attackers. The use of random ports, as denoted by target port 0, complicates the prediction and prevention of future attacks, highlighting the need for robust intrusion detection systems capable of adaptive learning. The relatively low number of unique attackers suggests the possibility of repeated attempts by the same adversaries, potentially indicating targeted campaigns. Key concerns include the extended duration of attacks, which may strain defensive resources and increase the likelihood of successful breaches. It is recommended to enhance network monitoring capabilities, implement advanced threat intelligence, and conduct regular security audits to identify and mitigate vulnerabilities. Additionally, organizations should consider deploying more dynamic firewall rules and network segmentation to limit potential attack vectors.

#### Priority Ranking

Priority	Defense Strategy	Response	Risk Level
P1	Geo-IP Blocking	Immediate	High
P1	Internal Threat Scanning	24 Hours	High
P2	Incident Containment	3 Days	Medium-High
P2	Threat Intelligence Correlation	1 Week	Medium-High
P3	Network Segmentation	2 Weeks	Medium
P3	Zero Trust Planning	1 Month	Medium

#### Key Recommendations

##### Immediate Action Checklist

- Examine Pre-Attack Sources: Analyze threat markers on geo-maps.
- Inspect Internal IP Activity: Verify the legitimacy of listed IPs.
- Adjust Alert Thresholds: Ensure Critical events are notified instantly.
- Back Up Key Data: Prevent potential attack impacts.

##### Monitoring Focus

Type your query

## Dynamic Configuration Recommendations

N-Robot analyzes historical data to recommend optimal threshold settings for different systems and applications. Thresholds are dynamically adjusted based on peak and off-peak patterns to maintain optimal configurations, improving monitoring accuracy while reducing false alerts.

Users can maintain optimal decision-making and operational efficiency without complex manual configuration, even in rapidly changing environments.

**Device Alert Template Optimization - Select Plan**

Device:

方案

Plan Name	Monitoring Device	CPU (%)	Memory (%)
Current Plan	<input type="text"/>	Red Alert: 99 Yellow Alert: Disallowed	Red Alert: 99 Yellow Alert: Disallowed
N-Robot Suggested Plan	<input type="text"/>	Red Alert: 50 Yellow Alert: 40	Red Alert: 50 Yellow Alert: 40
Create New Template	<input type="text"/>		
Apply Template	<input type="text"/>	Red Alert: 50 Yellow Alert: 40	Red Alert: 50 Yellow Alert: 40
Apply Template	<input type="text"/>	Red Alert: 50 Yellow Alert: Disallowed	Red Alert: 50 Yellow Alert: Disallowed

Previous Submit Cancel

## Multi-Event Correlation

N-Robot provides multi-event correlation capabilities, automatically identifying relationships between multiple security events and assessing their severity in real time.

For example, if a source IP within successful login events is identified as high-risk by threat intelligence, the system correlates the events and triggers immediate alerts, enabling rapid response such as isolation. With automated analysis and real-time notifications, users can significantly reduce security risks and potential losses without additional operational overhead.

**N-Robot** ▾
✉ ✕

### Network Issue Analysis Report

Based on the system-provided analysis, I have found some abnormal network events. This report highlights a specific network issue:

**Issue 1 : MAC Table Entry Flapping (MAC Flapping)**

**Analysis:**

- This is a classic case of MAC Flapping (MAC table entry instability)
- The same MAC address (00:50:56:88:7C:32) frequently oscillates between two ports (Po25 and Po11) within a short period.
- This situation can **potentially** degrade network performance and security by incessantly updating MAC table entries.

**Possible Causes:**

01. Layer 2 Loop exists in the network
02. Misconfigured or faulty STP (Spanning Tree Protocol)
03. Unintended aggregation switches causing cable loops
04. Malfunctioning device continuously flapping MAC entries.

**Action Recommendation:**

Immediate action is recommended. Checking network topology for loops, addressing STP configurations, and testing suspect devices for malfunction is advised to mitigate the network performance and security risks associated with MAC Flapping.

This issue needs urgent attention, as unchecked MAC Flapping can degrade network performance, impact security, and increase network vulnerabilities.

This issue needs urgent attention, as unchecked MAC Flapping can degrade network performance, impact security, and increase network vulnerabilities.



## ■ Hardware

	NP-EN-AI-S	NP-EN-AI-G1	NP-EN-AI-G2
CPU	Intel Xeon 6369P (24M Cache, 3.3GHz) / Equal or superior specifications	Intel Xeon Silver 4416+ (37.5M Cache, 2.0GHz) / Equal or superior specifications	Intel Xeon Silver 4416+ (37.5M Cache, 2.0GHz) / Equal or superior specifications
Memory	32G DDR5 x2 / Equal or superior specifications	32G DDR5 x6 / Equal or superior specifications	32G DDR5 x6 / Equal or superior specifications
Ethernet Controller	Dual Port 1GbE LAN	Dual Port 1GbE LAN 、 Dual Port 10GbE LAN	Dual Port 1GbE LAN 、 Dual Port 10GbE LAN
IPMI	Integrated IPMI and KVM with Dedicated LAN	Integrated IPMI and KVM with Dedicated LAN	Integrated IPMI and KVM with Dedicated LAN
I/O Port	1 VGA, 1 COM	1 VGA, 1 COM	1 VGA, 1 COM
Power Supply	600W Redundant (1+1) / Equal or superior specifications	2000W Redundant (1+1) / Equal or superior specifications	2000W Redundant (1+1) / Equal or superior specifications
SSD	480GB / Equal or superior specifications	1TB / Equal or superior specifications	1TB / Equal or superior specifications
HDD	4TB (2x4TB with RAID1) / Equal or superior specifications	4TB (2x4TB with RAID1) / Equal or superior specifications	4TB (2x4TB with RAID1) / Equal or superior specifications
RAID	Supports RAID 0,1,5	Supports RAID 0,1,5	Supports RAID 0,1,5
GPU	N/A	RTX PRO 6000 blackwell / Equal or superior specifications	RTX PRO 6000 blackwell x2 / Equal or superior specifications
AC Power	100-127Vac ,7-5.5A, 50-60Hz / 200-240Vac, 3.3-2.7A, 50-60Hz	90–264Vac or HVDC (180–310V), 47-63Hz	90–264Vac or HVDC (180–310V), 47-63Hz
Operating Temperature	10°C to 35°C (50°F to 95°F)	0 ~ 40 °C (32 ~ 104 °F)	0 ~ 40 °C (32 ~ 104 °F)
Operating Relative Humidity	8% to 80% (Non-condensing)	10 ~ 95% @ 40 °C (Non-condensing)	10 ~ 95% @ 40 °C (Non-condensing)
Size	1U Rackmount, 19 Inch Standard Wide RackMount Industry Server	4U Rackmount, 19 Inch Standard Wide RackMount Industry Server	4U Rackmount, 19 Inch Standard Wide RackMount Industry Server
Feature	Provides AI-powered Q&A, reporting, and recommendations.		

## ■ N-AI VM Requirements & Notes

1. The VM specifications listed are minimum requirements; actual configurations should be adjusted based on deployment needs.
2. Prepare a server with VMware ESXi 6.0 or later, or Proxmox VE (PVE) 7.0 or later.
3. Recommended hardware configuration:
  - CPU: Intel Xeon 6369P (24MB cache, 3.3 GHz) or equivalent and above
  - Memory: At least 64GB RAM
  - Storage: Minimum 480GB system disk and 4TB data storage

## ■ Material

Material Code	Description
NP-EN-AI-S	N-AI Server standard version with 1 Year MA. Internet access is required.
NP-EN-AI-G1	N-AI Server build-in 1 GPU with 1 Year MA.
NP-EN-AI-G2	N-AI Server build-in 2 GPU with 1 Year MA.
NP-EN-AI-VM	N-AI Server VM version with 1 Year MA.
NP-EN-AI-S-1YRMA	1 Year MA for NP-EN-AI-S
NP-EN-AI-G1-1YRMA	1 Year MA for NP-EN-AI-G1
NP-EN-AI-G2-1YRMA	1 Year MA for NP-EN-AI-G2
NP-EN-AI-VM-1YRMA	1 Year MA for NP-EN-AI-VM



Tel : +886-4-23752865    Fax : +886-4-23757458

Sales Information : [sales@npartner.com](mailto:sales@npartner.com)

Technical Support : [support@npartner.com](mailto:support@npartner.com)

