Rumi: Your On-Premise AI Analyst

Every WireTrace deployment includes Rumi, a built-in AI analyst that runs entirely on your hardware. Rumi answers natural language questions about your network environment, generates audience-aware security reports, and correlates data across every module - assets, threats, compliance, vulnerabilities, baselines, and file activity. No cloud connectivity. No data leaving your perimeter. No API keys. No GPU required. Intelligence from your own network data, delivered in seconds.

WireTrace AI Intelligence | Version 1.3 | 2026

100% Offline | No GPU Required | 21 Built-in Query Tools | 6 Report Personas | Sub-200ms Answers | Conversation Memory

1. Natural Language Queries

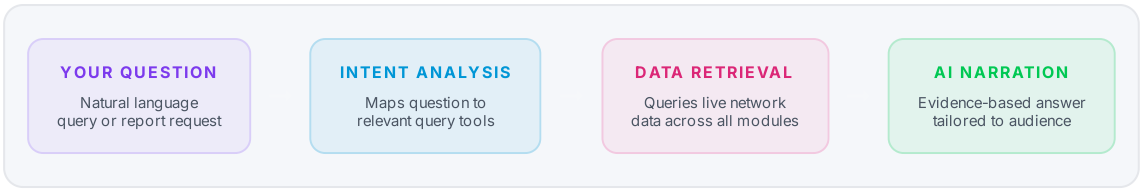
Ask Rumi about your network in plain language. Every answer is drawn from real, observed network data - asset inventories, connection records, protocol evidence, threat detections, vulnerability assessments, file activity logs, and compliance status. Rumi never fabricates information. If the data does not exist in your environment, Rumi says so.

EXAMPLE QUERIES

- **"How many OT assets are on my network?"** - Returns a count of industrial assets by device type, with Purdue level distribution and classification confidence.
- **"Show me all cleartext protocols in use."** - Lists every unencrypted protocol observed, the assets using them, and which connections are most exposed.
- **"What changed on my network this week?"** - Summarizes new devices discovered, classification updates, firmware changes, and new threat detections since last Monday.
- **"Which assets have critical vulnerabilities?"** - Returns assets with high-severity CVEs, prioritized by exploit prediction scores and known-exploited status.
- **"Show file activity on the DICOM server."** - Lists every file operation (read, write, upload, download) observed on medical imaging systems.
- **"What is the Purdue level distribution?"** - Breaks down assets by Purdue model level, showing how devices are distributed across your network architecture.

2. How It Works

Rumi processes your question through a pipeline that translates natural language into structured queries against your live network data, then narrates the results into a polished, context-aware answer.



Evidence-Based Answers

Every answer cites actual network observations. When Rumi says "14 PLCs are running firmware older than 2023," it has queried your asset inventory and can show each device, its firmware version, and when it was last observed. No guessing. No hallucination. If the data is not available, Rumi tells you explicitly.

Conversation Memory

Follow-up questions reference previous answers. Ask "How many assets have critical vulnerabilities?" then follow with "Which of those are in the OT zone?" - Rumi remembers the context and narrows the results. Multi-turn conversations let you drill down into findings naturally.

Response time: Rumi answers structured queries in under 200 milliseconds. Narrative-enhanced responses that include AI-generated context and recommendations typically complete within a few seconds. All processing runs locally on your server hardware.

3. 21 Built-in Query Tools

Rumi includes 21 specialized query tools that cover every dimension of your network intelligence. Each tool retrieves structured data from the appropriate module and returns it for narration.

Asset Summary
Total assets, breakdown by domain, device type, and classification status

Asset Details
Specific asset lookup with full identity, protocols, and enrichment data

Asset Search
Find assets by IP, MAC, hostname, vendor, model, or device type

Connection Map
Communication pairs with protocol, port, direction, and volume

Connection Analysis
Cross-zone traffic, new connections, lateral movement indicators

Protocol Distribution
Protocol usage across the network with asset counts per protocol

Protocol Detail
Deep protocol analysis: cleartext exposure, authentication status, versions

Threat Summary
Active threats, IoC matches, risk scores, and detection categories

Threat Detail
Per-asset threat breakdown with affected connections and evidence

Vulnerability Overview
CVE counts by severity, exploitability scores, affected assets

Vulnerability Detail
Specific CVE lookup with affected assets, CVSS, EPSS, and KEV status

File Activity Summary
File operations across SMB, FTP, NFS, TFTP, HTTP, DICOM

File Activity Detail
Per-asset file operations with paths, types, and timestamps

Compliance Status
Framework compliance scores across IEC 62443, ISO 27001, HIPAA, NCA

Compliance Evidence
Specific control evidence with mapped network observations

Purdue Topology
Asset distribution by Purdue level with cross-level communications

Purdue Detail
Per-level device breakdown with segmentation validation

Change Summary
Recent changes: new devices, reclassifications, firmware updates

Baseline Status
Behavioral baseline coverage and recent deviations

Risk Assessment
Per-asset risk scores with contributing factors

Environment Overview
Complete network summary: assets, protocols, threats, compliance

4. Persona-Aware Report Generation

Rumi generates security reports tailored to six distinct audiences. The same underlying network data is presented differently depending on who needs to read it - executives see risk summaries and business impact; engineers see technical details and remediation steps.

EXECUTIVE

Risk posture, compliance status, key metrics, and business impact. Board-ready language with strategic recommendations.

SECURITY MANAGER

Threat landscape, vulnerability exposure, detection coverage, and incident trends. Operational priorities with resource recommendations.

TECHNICAL SPECIALIST

Protocol-level findings, asset configurations, connection analysis, and detection rule details. Deep technical context for SOC analysts.

OT ENGINEER

Industrial protocol status, PLC and RTU inventory, Purdue segmentation, and OT-specific threats. Operational technology focus.

MEDICAL SECURITY

Medical device inventory, clinical protocol exposure, HIPAA evidence, and biomedical network segmentation. Healthcare compliance focus.

COMPLIANCE OFFICER

Framework-mapped evidence, control status, audit readiness, and gap analysis. Regulatory and standards compliance focus.

5. Streaming Reports

Reports generate progressively. When you request a security assessment, Rumi begins streaming the executive summary immediately while continuing to query data for subsequent sections. You start reading while the report is still being assembled.

Progressive Delivery

Report sections appear one at a time as they are generated. The executive summary arrives first, followed by asset analysis, threat findings, compliance status, and recommendations. You do not wait for the entire report to finish before reading the first findings.

Template Fallbacks

If any section encounters an issue during generation, Rumi falls back to structured templates that present the raw data in a well-formatted layout. Reports always complete. Every section always has content. The AI enhances the narrative, but never blocks delivery.

6. Security and Privacy

Rumi is designed for environments where data sovereignty is non-negotiable.

Fully Offline

The AI engine runs entirely on your server hardware. No internet connection required. No cloud APIs called. No data transmitted externally. Rumi works identically in air-gapped environments.

No GPU Required

Rumi is optimized to run on standard server hardware. No dedicated GPU, no specialized AI accelerators. The same server that runs WireTrace's analytics engine runs Rumi at full capability.

Your Data Stays Yours

Every query, every answer, every report is processed and stored locally. No telemetry. No usage analytics sent externally. No model training on your data. Complete data sovereignty.

Air-gap compatible: Rumi requires zero external connectivity. The AI model ships with the WireTrace installer and runs locally from day one. No activation keys, no license servers, no cloud dependencies of any kind.

7. Use Cases

Daily Situational Awareness

"What changed overnight?" - Get a morning briefing on new assets discovered, new vulnerabilities detected, baseline deviations, and threat activity. Replace manual log review with a single natural language question.

Incident Investigation

"Show me all connections from this IP in the last 24 hours." - Drill into suspicious activity with follow-up questions. Rumi correlates asset identity, protocol evidence, file activity, and threat intelligence for rapid triage.

Audit Preparation

"Generate an IEC 62443 compliance report for the board." - Rumi queries live compliance evidence and generates a persona-appropriate report with framework-mapped findings, gap analysis, and recommendations.

Executive Reporting

"Create a risk summary for the CISO." - Board-ready reports that translate technical findings into business language. Risk scores, trend analysis, and prioritized recommendations tailored for executive audiences.

File Activity Forensics

"Show file activity on the shared drive server this week." - Review every file read, write, delete, and rename across SMB, FTP, NFS, and other protocols. Essential for ransomware investigation and data loss prevention.

Network Architecture Review

"What is the Purdue level distribution and are there any segmentation violations?" - Rumi maps your network architecture, identifies cross-level communications that violate policy, and highlights assets that may be miscategorized.

8. AI-Enhanced Narration

Rumi does more than return raw query results. The AI narration layer transforms structured data into polished, executive-ready prose. Numbers become context. Findings become recommendations. Raw counts become risk assessments.

Without AI Narration

```
Total assets: 847
OT domain: 312
Medical domain: 89
Critical vulnerabilities: 23
Cleartext protocols: 7
```

With AI Narration

"Your network contains 847 classified assets, with 312 in the OT domain and 89 medical devices. Of immediate concern: 23 assets carry critical vulnerabilities, and 7 unencrypted protocols remain active across sensitive zones. The OT segment shows the highest exposure, with 4 PLCs running firmware with known CVEs. Recommended priority: address cleartext SCADA protocols in the Level 2 zone."

Intelligence Built Into Every Deployment

Rumi ships with every WireTrace installation. No add-on license, no cloud subscription, no GPU hardware. Ask your network a question and get an evidence-based answer in seconds. wiretrace.io | sales@wiretrace.io