



NetEye Conference 2026

**Network Intelligence for the AI Era:
Unifying Security, Performance
and Observability**

Luca Deri | ntop | ntopng + NetEye

22 Ottobre 2026, Crowne Plaza Verona Fiera



Today: ntop Inside NetEye

Collect

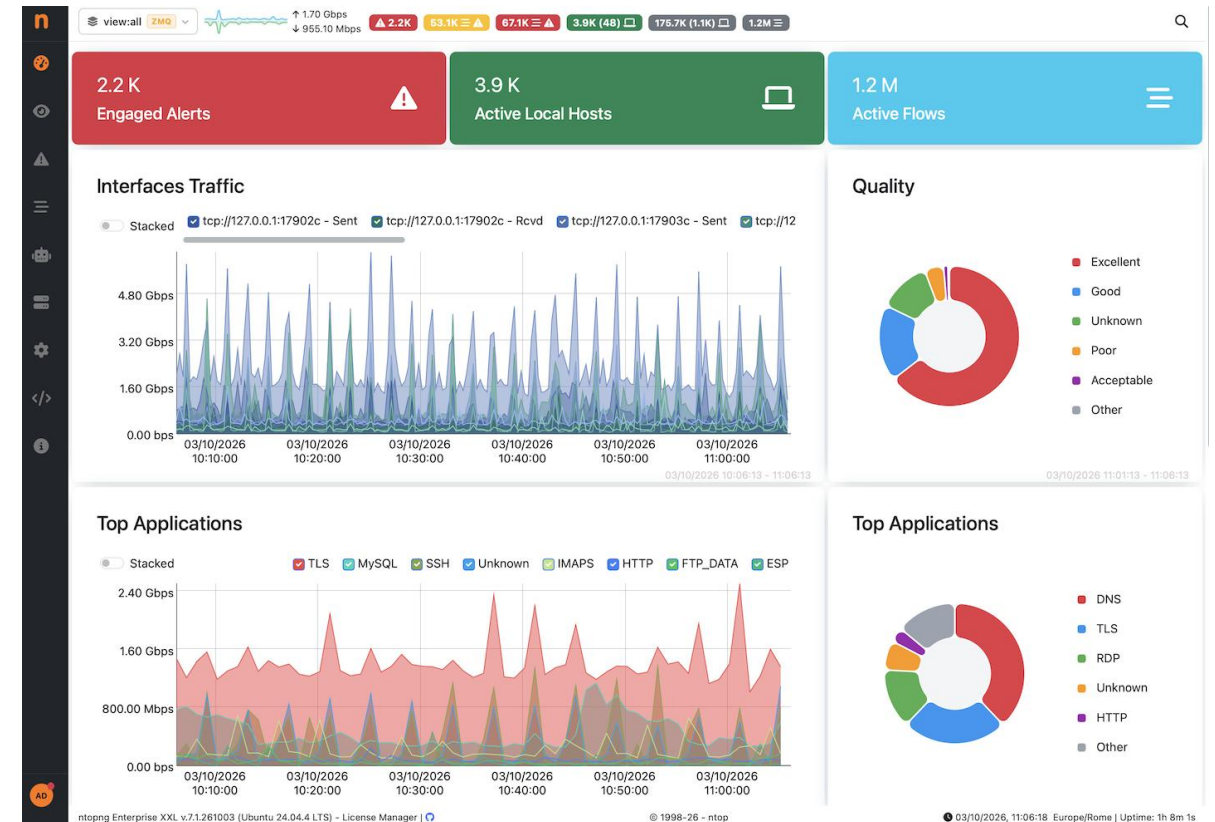
NetFlow/IPFIX collection from routers and switches, plus packet-based probes.

Monitor

Live traffic visibility: hosts, applications, interfaces and Layer 7.

Alert and Protect

Alerts and a network-traffic cybersecurity component feeding NetEye.



Solid foundation. Now: what else can the same data tell a NOC?

Why Go Beyond Detection?

- Alerts tell you something happened (past), not what the network is becoming (forecast).
- New risks (quantum, AI, drift) are invisible to threshold alerts.
- NOCs need answers, not only security events.
- The same telemetry can serve NOC, SOC and application teams.

Shift

Move from event-driven alerting to *continuous* network intelligence.



Encryption Hides Payload, Not Behaviour

- TLS 1.3, QUIC and ECH (Encrypted Client Hello) remove payload and SNI (target hostname) visibility.
- Decrypting at scale is costly and often not permitted.
- Metadata, fingerprints and behaviour become the signals.
- Encrypted traffic is both the problem and the data source (user and application hints).

Challenge

Intelligence on encrypted traffic without breaking privacy.



A Typical Bad Day: One Slow Service, Four Partial Views

09:02 Alert

NetEye flags the ERP service as slow. Response time is high, the cause is unknown.

NOC

Interfaces look healthy. Is it the network? No per-application proof, no history.

SOC

Logs show nothing odd. Encrypted traffic: backup, transfer or scan?

Application Team

Server metrics are normal. They blame the network. Escalation ping-pong starts.

Shared flow and application evidence replaces four opinions with one answer.



Challenge: PQC readiness

- Post-quantum migration needs a cryptographic inventory
- Which hosts and apps negotiate which TLS versions, ciphers, key exchange?
- Harvest-now, decrypt-later makes long-lived data urgent
- Scanners see servers; the network sees real usage, including clients

Question

- Who is already quantum-safe and who is not?
- What is your network PQC posture?



Challenge: AI Traffic and Shadow AI

- GenAI and LLM services: long-lived streaming sessions over TLS.
- Employees adopt unsanctioned AI tools (shadow AI).
- Data may leave the organisation: prompts, documents, code.
- Internal AI workloads and agents add API and east-west traffic.
- CDNs and cloud hide the service behind shared IP addresses.

Questions a NOC Gets Asked

- Which AI services are in use?
- Which hosts send most data to them?
- AI traffic is sanctioned and growing ?



Challenge: How The Network Changes Over Time

- Networks drift: new hosts, services, ports, dependencies.
- Point-in-time views miss slow change and shadow IT.
- Change often precedes incidents: a new port, a moved server.
- After a migration, nobody proves traffic moved as planned.
- Few tools answer: what is different from last week?

Questions a NOC Asks

- Which hosts and services are new?
- What disappeared without notice?
- Did traffic shifted as planned after migration?



Challenge: Misuse and Compromised Hosts

- Compromise often shows as *behaviour change*, not a signature.
- Misuse: policy violations, unauthorised services, abnormal usage.
- Typical signals: scans, beaconing, odd destinations, data bursts.
- Unmanaged devices and IoT cannot run agents.
- The NOC sees symptoms first but lacks security context.

Questions a NOC Asks

- Which hosts changed behaviour?
- What is taking to?
- Is it expected ?
- Misuse, misconfiguration or compromise ?



Vision: Continuous, Contextual, Correlated

Continuous

Always-on observation with historical depth, edge to cloud.

Contextual

Every flow enriched: application, crypto, risk, role.

Correlated

Linked to hosts, services and business processes in NetEye.

Intelligence is the right context at the right time.



Three Pillars, One Operational Picture

Security

Behaviour, fingerprints and risk flags to find threats and compromised hosts.

Performance

Latency, retransmissions and experience per application.

Observability

Dependencies, change over time, PQC and AI posture.

Same data, three audiences: NOC, SOC, application owners.



From Monitoring to Acting

● Monitor

Flows, metrics, events. Example:
ERP traffic is up 40% since 10:00.

● Understand

Enrich and correlate.
Example: it is one backup
job from a new host.

● Predict

Baselines and trends.
Example: the WAN link
saturates by Friday.

● Act

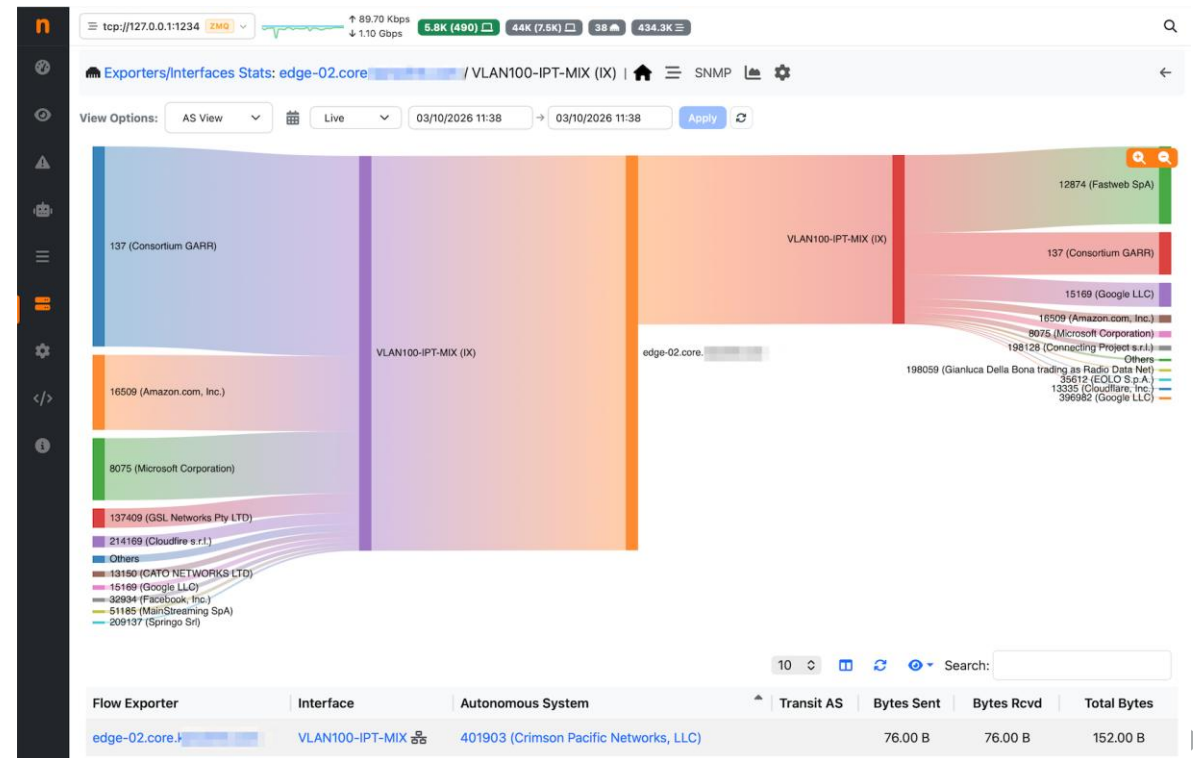
Governed response. Example:
new policy, alert or ticket, human
approves.

nAnalyst makes steps 2 to 4 conversational and auditable.



ntopng: Real-time and Historical Network Analytics

- Sources: packets, NetFlow, IPFIX, sFlow, cloud flows.
- Hosts, flows, applications, ASNs, VLANs, interfaces.
- Live view plus historical flow storage.
- Alerts, APIs and exports for integration.



At a Glance

From raw packets or flows to explained conversations.

nDPI: Layer 7 and Encrypted Traffic Metadata

- Open-source DPI library, hundreds of protocols.
- TLS handshake metadata and fingerprints.
- Behavioural classification of encrypted flows.
- Flow risk flags for suspicious or weak traffic.

Why it Matters

nDPI is the enrichment engine behind PQC, AI and misuse use cases.

 TLS Certificate	Client Requested:  raw.githubusercontent.com +
TLS ALPN	h2,http/1.1
Client Supported TLS Protocols	TLSv1.3,TLSv1.2,TLSv1.1,TLSv1

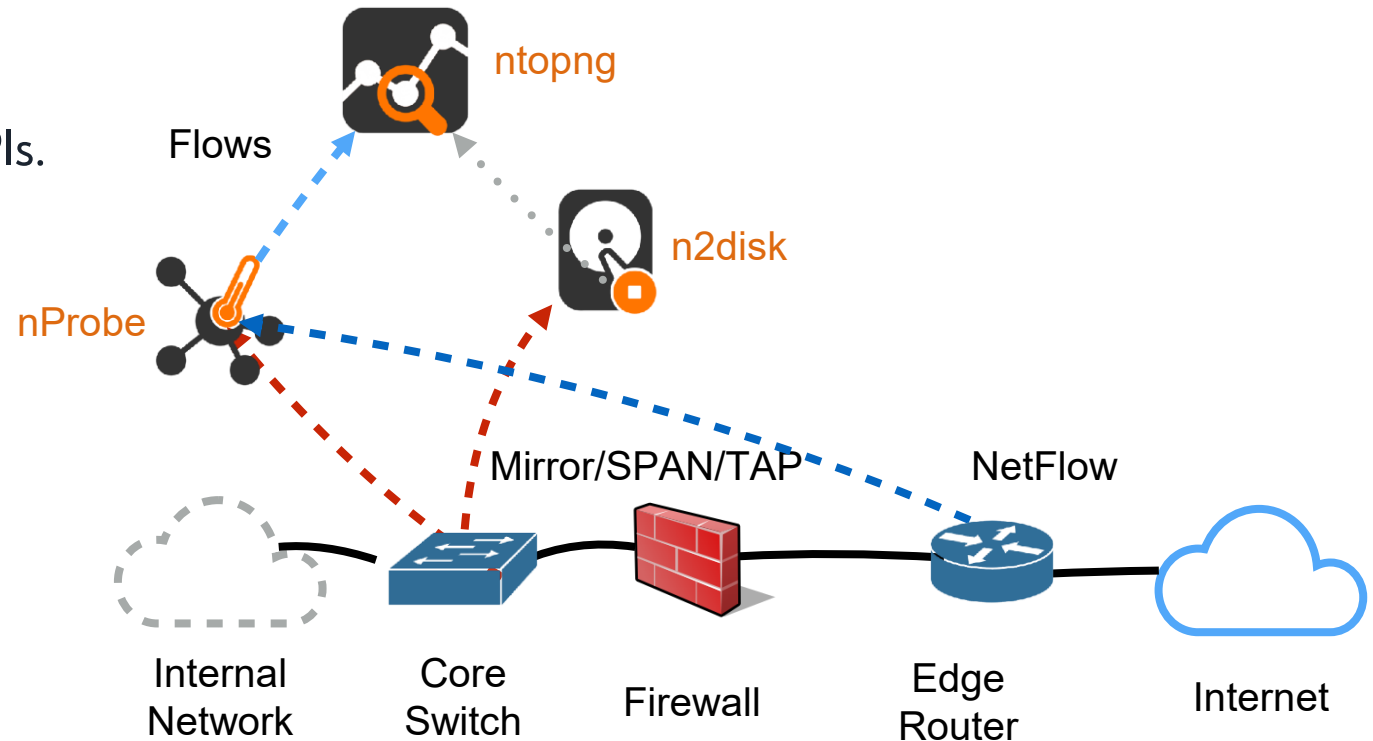


A Scalable Pipeline: Capture, Classify, Analyse

- PF_RING / ZC: high-speed capture.
- nProbe: flow export and collection.
- nDPI: classification and risk.
- ntopng: analytics, alerting, dashboards, APIs.

Deployment

Probes at the edge, collection in the core, one data model.



Performance: The User Experience on The Wire

- Latency (RTT), application delay and jitter.
- TCP retransmissions, out-of-order, zero windows.
- Throughput and top talkers per application.
- Separate network from application problems.

Outcome

Answer "is it the network?" in seconds, with proof.

Network Quality (QoE) [Client->Server / Server ->Client]	Excellent (100 %)	Excellent (100 %)
RTT Breakdown	server 100%	
Client/Server Estimated Distance	2,567 Km	1,593 Miles
Application Latency	14.65 ms	
Packet Inter-Arrival Time [Min / Avg / Max]	Client → Server: < 1 ms / < 1 ms / 14 ms	Server → Client: < 1 ms / < 1 ms / 14 ms



PQC Readiness with ntopng

- Observe TLS versions, ciphers and key-exchange offers per host.
- Classical-only vs post-quantum-capable clients and servers.
- Track migration progress over time per network or application.
- Find legacy and weak crypto before attackers or auditors do.

Outcome

A live cryptographic asset inventory built from real traffic.

Description	Score	Info	Mitre Att&ck
Obsolete non-PQC Flow 	50	Obsolete non-PQC client 	T1027 Defense Evasion



Network Change Over Time

- Historical flow analytics (e.g. ClickHouse-backed).
- Baselines per host, network and service.
- Report new hosts, services, ports and dependencies.
- Compare periods: this week vs last week, before vs after a change.



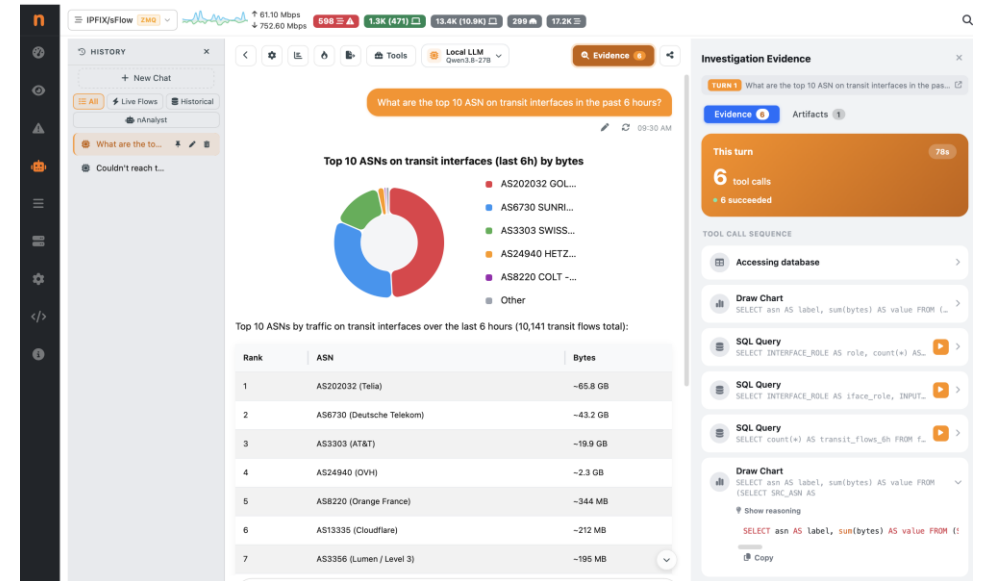
Outcome

Change becomes visible, explainable and auditable.



nAnalyst: From Visibility to Interpretation

- The problem is not visibility but interpretation.
- Ask in natural language, in any language your LLM supports.
- The agent runs SQL on ntopng data, gathering flows, hosts, assets, SNMP, alerts.
- Answers with charts in the chat and suggested next steps.
- 25+ network-specific tools built on ntopng and nDPI.



Availability

Works with Anthropic, OpenAI or a local LLM.

Asking The New Questions In Plain English



PQC

Which hosts still negotiate TLS without post-quantum key exchange?



AI Traffic

Which hosts used AI services last week and how much data did they send?



Change

What new hosts and services appeared since last Monday?



Compromise

Which hosts changed behaviour in the last 24 hours, and why?

NOC-friendly: questions, not queries.



Integration: ntopng inside NetEye

- ntopng acts as collector for NetEye interfaces and satellites.
- Single sign-on with roles: administrator and non-privileged.
- Restrictions: allowed interfaces and allowed networks.
- pcap-download permission for controlled packet evidence.
- Retention managed within the platform.



Enterprise Ready

Multi-tenant access control allows safe sharing of network data.



Takeaways

- Beyond flows and alerts: crypto, AI, change and compromise.
- The same network data empowers NOC, SOC and application teams.
- ntopng adds Layer 7 intelligence, and nAnalyst adds the why, to NetEye.
- Next step: pilot PQC inventory and change reporting on one site.
- **Questions and discussion.**



Thank you

Luca Deri @lucaderi

<https://www.ntop.org>

