80–90% less data in your SIEM. 100% of the visibility.

NFO sits between your network and your SIEM — deduplicating, enriching, and reducing flow volume before it reaches your ingest meter.

80–90%	300K+	3,000	< 1 hr
SIEM ingest reduction	Flows/sec per instance	SNMP devices/instance	Time to deploy

VOLUME REDUCTION

Reduces SIEM ingest by 80–90% using:

- → Intelligent Aggregation
- → Deduplication
- → Flow Stitching (additional 50% reduction)
- → Top N Traffic Analysis

ENRICHMENT

Transforms raw IPs into actionable intelligence:

- → User identity (AD, Okta, Entra ID)
- → Threat intelligence & reputation
- → GeoIP & ASN mapping
- → VM names & cloud metadata
- → CIM format normalization

INTEGRATIONS

Delivers enriched data to:

- → Splunk, Sumo Logic (free apps)
- → Microsoft Sentinel, CrowdStrike
- → Elastic, Exabeam, SentinelOne
- → Datadog, New Relic
- → Kafka, S3, ClickHouse, OpenSearch

SOURCES

Flow Data: NetFlow v5/v9, IPFIX, sFlow, J-Flow
Cloud Flow Logs: AWS VPC, Azure NSG/VNet, Google VPC, Oracle OCI
Device Telemetry: SNMP Polling & Traps, Model-Driven Telemetry (MDT)*
Enrichment Feeds: Active Directory, Okta, Entra ID, GeoIP, Threat Intel

DESTINATIONS

SIEM & Security: Splunk (ES, ITSI), Microsoft Sentinel, CrowdStrike, Sumo Logic, Exabeam, SentinelOne, Elastic
IT Ops & Observability: Datadog, New Relic, VMware Aria
Data Lakes & Streaming: AWS S3, Amazon OpenSearch, Azure Monitor, ClickHouse, Kafka, OpenTelemetry

PRODUCT HIGHLIGHTS

ZERO-TOUCH SNMP DISCOVERY

Define IP ranges — NFO automatically discovers every device, classifies it by vendor and role, applies the correct OID sets, and starts polling. No manual OID mapping. No spreadsheets. Reruns twice daily to stay current as your network changes.

INTELLIGENT VOLUME REDUCTION

Deduplication, intelligent aggregation, and flow stitching reduce SIEM ingest by 80–90% — while preserving 100% of investigative value. Flow stitching alone adds a further up to 50% reduction by merging unidirectional records.

CONTEXT ENRICHMENT

Every flow is enriched with user identity, threat reputation, GeoIP, and cloud/VM metadata before it reaches your SIEM. Analysts investigate with full context — no manual lookups, no pivot to external tools.

DDOS DETECTION

Built-in DDoS Detector identifies volumetric and low-and-slow attacks in real time — analyzing flow patterns to surface scrubbing recommendations and alert your SOC before impact.

MULTI-CLOUD VISIBILITY

Ingest flow logs from AWS VPC, Azure NSG/VNet, Google VPC, and Oracle OCI alongside on-premises NetFlow — normalized into a single enriched stream. One pipeline for your hybrid environment.

NETFLOW RECORDER

Capture and replay flows from memory or disk to your SIEM for forensic lookback. When an incident occurs, you can reconstruct exactly what moved on the network — before the alert fired.

MODEL-DRIVEN TELEMETRY (MDT)

Accepts gRPC-based telemetry from Cisco and Juniper devices for sub-second streaming metrics — complementing SNMP polling with real-time push-based visibility.

UNMATCHED PERFORMANCE

Entry-level deployment starts at 2 CPUs / 8 GB RAM. A single high-performance instance processes 300,000+ flows per second. Add instances via NFO Central to scale without limit.

SYSTEM REQUIREMENTS

Linux: RHEL 7+, Rocky Linux 8+
Windows: Windows Server 2019, 2022, 2025
Software-only — no proprietary hardware required.

SIZING GUIDANCE

Entry level: 2 CPUs, 8 GB RAM, 20 GB disk
At this configuration: 300K+ flows/sec, up to 3,000 SNMP devices
Scale-out: Add instances; NFO Central manages distributed deployments with no throughput ceiling

See NFO cut your SIEM costs — in your own environment.

Start a free trial with your own network data, or schedule a technical demo.

netflowlogic.com/free-trial | netflowlogic.com/request-a-demo