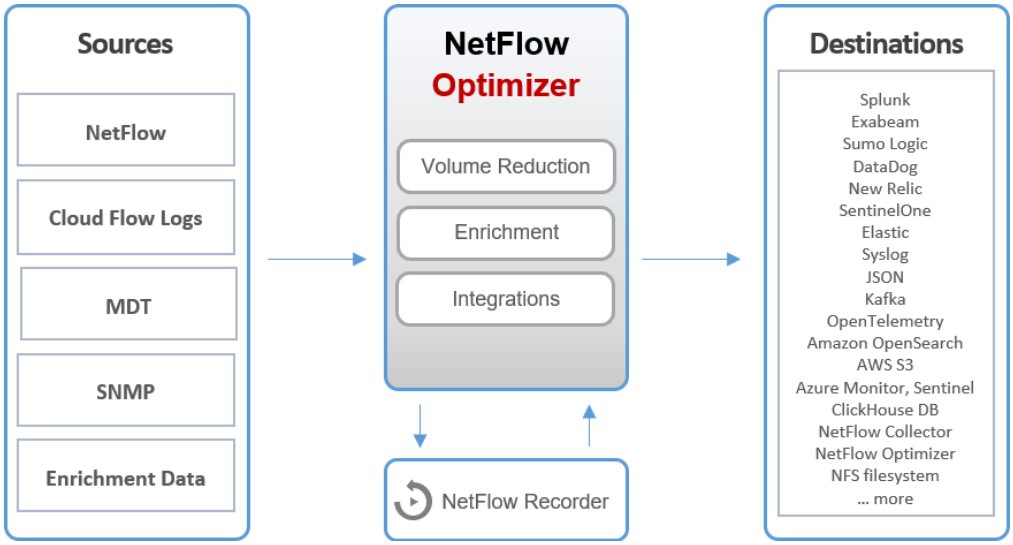
DATA SHEET

NetFlow Optimizer™

Any Flow Data. Optimized and Enriched. In your Observability Platform.

NetFlow Optimizer enables you to process massive volumes of NetFlow (IPFIX, sFlow, Cloud Flow Logs, etc.) data, optimizing and enriching it in real time. This ensures you get actionable insights directly in your observability platform.



Core Functions

VOLUME REDUCTION

Deduplicate and aggregate flows to minimize data volume (typical reduction is 80% or more).

ENRICHMENT

Add vital context like Username, Applications, VM names, GeoIP, SNMP data, and Reputation.

INTEGRATIONS

Seamlessly connect with a wide range of data sources and observability platforms,

Sources & Destinations

SOURCES

- **Flow Data:** NetFlow v5/v9, IPFIX, sFlow, Jflow, etc.
- **Cloud Flow Logs:** AWS VPC, Azure NSG and VNet, Oracle VCN, Google VPC
- **Enrichment:** Username, Applications, Reputation, GeoIP, VM names, Cloud Services
- **SNMP and MDT:** Polling, Traps, Metrics

DESTINATIONS

- **SIEM/Observability Platforms:** Splunk, Sumo Logic, Microsoft Sentinel, Exabeam, DataDog, New Relic, Elastic, SentinelOne, VMware LogInsight
- **Data Lakes & Databases:** AWS S3, Amazon OpenSearch, Azure Monitor, Azure Sentinel, ClickHouse DB

Product Highlights

EFFICIENT NETFLOW VOLUME REDUCTION

- Use advanced techniques like deduplication, intelligent aggregation, and flow stitching to address overwhelming data volumes, reducing storage needs and speeding up analysis.

ADVANCED CLOUD MONITORING

- Gain complete visibility into your cloud and hybrid environments. NFO monitors cloud flow logs for a unified view for security and performance analysis.

TOTAL NETWORK VISIBILITY

- Pinpoint physical devices and interfaces impact VM performance on dashboards from platforms like Splunk, Sumo Logic, Exabeam, and others.

MODEL-DRIVEN TELEMETRY (MDT)

- Enables more granular and real-time network visibility by accepting MDT input, which is a new industry standard for collecting network data.

FLOW DATA SUPPORT

- Process any flow protocol, including NetFlow v5/v9, Flexible NetFlow, IPFIX (with variable and enterprise fields), sFlow, J-Flow, and more.

INTELLIGENT NETFLOW ENRICHMENT

- Transform raw IP address data into actionable intelligence. NFO enriches flows with user identities, application details, VM names, geolocation, and threat intelligence.

SECURITY

- Identifies security threats by tracing known sources and enriching flow data with real-time Reputation and GeoIP information. You can drill down to see which hosts are affected.

NETWORK DEVICE HEALTH

- Monitor the health of your network devices with SNMP polling. Identify hosts with the most TCP resets, overload conditions, interface errors and discards.

UNMATCHED PERFORMANCE

- Capable of processing 1,000,000 flows per second without a single drop. It can process up to 500,000 flows per second with consolidation.

NETFLOW RECORDER

- Look back in time by capturing and replaying flows from memory or disk to your SIEM, gaining complete visibility of past network traffic.

System Requirements

SYSTEM

- Linux kernel 2.17+ (RHEL 7+, Rocky Linux 8+, etc.)
- Windows: Windows Server 2016, 2019 (64-bit)

SIZING GUIDANCE

- CPU: 2 cores, 4vCPUs, 16GB RAM, 20GB disk space

Stop Drowning in Flow Data

See how NetFlow Optimizer can cut your data volume by 80% or more and enrich your flows for better visibility. Visit netflowlogic.com/contact/ today!