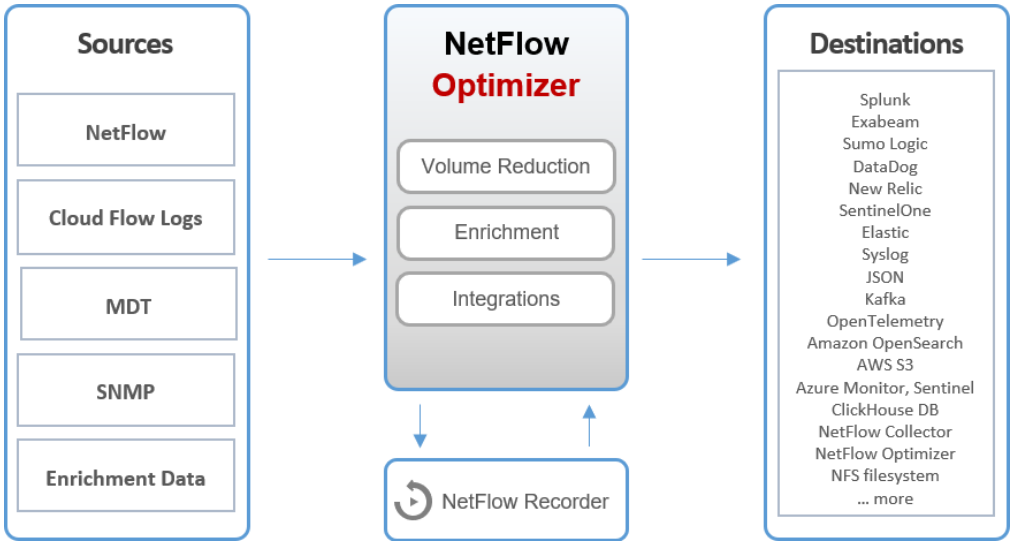
Any Flow Data. Optimized and Enriched. In your Observability Platform.

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 User Name, VM names, Applications, GeoIP, SNMP data, Security 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:** User Name, Reputation, GeoIP, VM names, Cloud Services
- **SNMP:** Polling & Traps

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

- Address the challenge of overwhelming data volumes by intelligently reducing data without sacrificing critical insights. NFO uses advanced techniques like Deduplication, Intelligent Aggregation, Top N analysis, and Flow Stitching to minimize storage needs and accelerate analysis.

INTELLIGENT NETFLOW ENRICHMENT

- Transform raw IP address data into actionable intelligence by correlating it with other data sources. NFO enriches flows with User Identities, Application Details, Virtual Machine (VM) Names, IP address geolocation, and Threat intelligence feeds.

ADVANCED CLOUD MONITORING

- Transform raw IP address data into actionable intelligence by correlating it with other data sources. NFO enriches flows with User Identities, Application Details, Virtual Machine (VM) Names, IP address geolocation, and Threat intelligence feeds.

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.

TOTAL NETWORK VISIBILITY

- Pinpoint physical devices and interfaces impacting VM performance on dashboards from platforms like Splunk, Sumo Logic, Exabeam, and others. Reconstruct VM-to-VM and VM-to-host conversations over the physical network.

NETWORK DEVICE HEALTH

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

MODEL-DRIVEN TELEMETRY (MDT) SUPPORT

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

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.

FLOW DATA SUPPORT

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

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: 4 physical cores, 16GB RAM, 20GB disk space