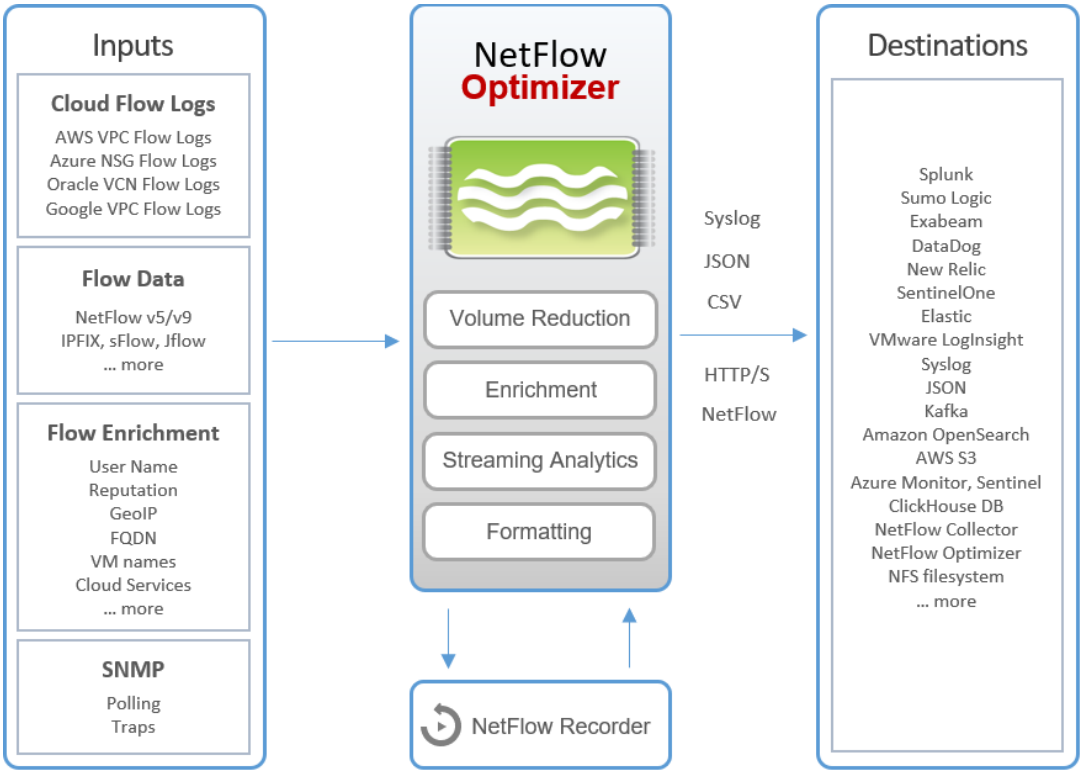
Any Flow Data. Optimized and Enriched. In your Observability Platform.

NetFlow Optimizer enables you to process massive volumes of NetFlow (IPFIX, sFlow, Cloud VPC Flow Logs, etc.) data, optimizing and enriching it in real time - ensuring that you get data where you need it in the right formats.



Benefits

FLOW DATA VOLUME REDUCTION

- Deduplication: report only once, if the same flow is reported by several network devices
- Consolidation: flows from communicating peers are aggregated over configurable period of time (typical reduction is up to 80%)
- Top traffic: configure Top N to reduce volume, keeping 99% accuracy (typical reduction is 95% or more)

FLOW DATA ENRICHMENT

Add information not available in NetFlow records

- DNS names, VM names, User identity
- Cloud instance names, services, regions
- SNMP polling data
- GeoIP at country or city level
- Reputation based on threat lists

FLOW DATA STITCHING AND ANALYTICS

- Combine flow records for client-server conversations
- Report network conversation state (Begin, Continuing, End) and session time
- Machine Learning to detect DDoS attacks and predict network failures

Product Features

MONITORING OF CLOUD FLOW LOGS

- Ability to read AWS VPC Flow Logs from Kinesis or CloudWatch or S3
- Ability to support many AWS accounts, VPCs, and AWS regions with one NFO EC2 instance
- Enrichment of flow records with VPC name, EC2 instance name, DNS name, and AWS region
- Ability to read Azure NSG Flow Logs
- Ability to support many Azure storage accounts, accessing NSG Flow logs via Service Principle or System-assigned Managed Identity
- Enrichment of Azure NSG flow records with Virtual Network name, VM name, DNS name, and Azure region
- Ability to read GCP VCP Flow Logs
- Ability to support many GCP Service accounts and projects
- Enrichment of GCP VCP flow records with VPC Network name, Subnetwork name, Instance name, DNS name, and GCP zone

MONITORING OF NETWORK DEVICE HEALTH

- Identification of hosts and network devices with the most TCP resets
- Identification of overload conditions
- With our SNMP polling
    - CPU utilization
    - Memory utilization
    - Tracking of interface errors
    - Dropped packets counter
    - Flapping interface identification
    - Latency / Jitter

APPLICATION VISIBILITY VIA FLOW DATA FROM

- AWS VPC Flow logs
- Palo Alto Network devices
- Cisco ASA
- Cisco devices generating AVC
- Any exporter based on known destination ports

SECURITY

- Identifies security threats and traces current known threat sources
- Enriches flow data with current Reputation and GEO IP information
- Drill in to see which hosts are affected

TOTAL NETWORK VISIBILITY FOR CUSTOMER OF SPLUNK, SUMO LOGIC, EXABEAM, ELASTIC, AND VMWARE

- Pinpoints physical devices and interfaces impacting VM performance, on a Splunk dashboard
- Reconstructs paths VM-to-VM and VM-to-host conversations over the underlying physical network

UNMATCHED PERFORMANCE

- Capable of processing 1,000,000 flows per second without a single drop
- Can process up to 350,000 flows per second with consolidation

WORKING WITH ANY FLOW DATA

- Capable to process any standard flow protocols
    - NetFlow v5/v9, Flexible NetFlow
    - IPFIX with variable and enterprise fields
    - sFlow (both data records and counter records)
    - J-Flow, Citrix AppFlow, NetStream, etc.

WORKING WITH SNMP DATA

- Flexible and extensible SNMP Polling capabilities
- SNMP Trap support

NETFLOW RECORDER

NetFlow Recorder – enables you to look back in time. You can set rolling *flow capture and replay period of time, and store *flows in memory or on disk, then press <**Replay**> to send these records in syslog or JSON format to your SIEM to gain complete visibility of past network traffic

System Requirements

OPERATING SYSTEM

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

SERVER HARDWARE OR VIRTUAL MACHINE

CPU: 4 CPU or 8 vCPU, 16GB RAM, 20GB disk space