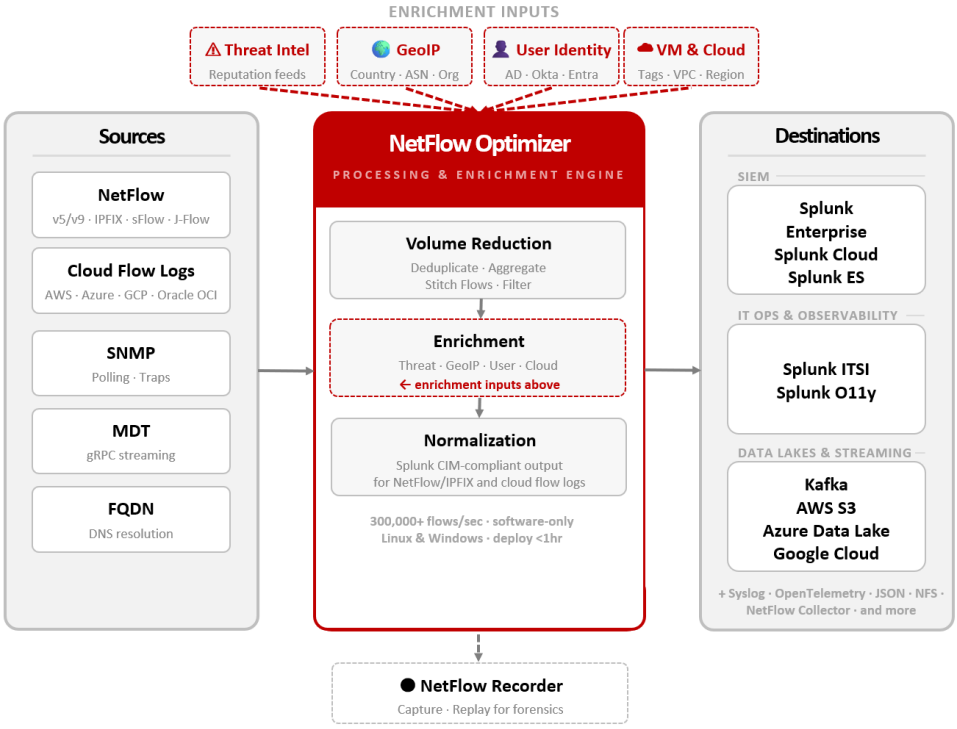
INTEGRATION GUIDE

NetFlow Optimizer™ + Splunk Integration

NetFlow is binary. Splunk can't ingest it. NFO changes that.

Without a processing layer to decode and normalize it first, network flow telemetry never reaches your SIEM. NetFlow Optimizer decodes, enriches, and normalizes raw flow data before Splunk ingestion — **giving Splunk network telemetry for the first time**.

< 1 hr	300K+	80–90%
From install to live Splunk data	Flows/sec processed, per instance	Typical reduction in raw flow volume reaching Splunk



The Three Problems NFO Solves for Splunk

01 BINARY COMPATIBILITY

Making NetFlow Viable in Splunk

Splunk cannot ingest binary NetFlow exports. NFO decodes raw binary records and delivers structured, CIM-compliant output that Splunk indexes immediately.

- → Binary converted to JSON or syslog key=value
- → NetFlow v5/v9, IPFIX, sFlow, J-Flow
- → Cloud flow logs: AWS, Azure, GCP, OCI
- → CIM-compliant from day one — no manual field mapping

02 CONTEXT

Enriched Data, Not Naked IPs

Raw flows show IP addresses. NFO adds the context Splunk needs for detection, investigation, and AI/ML — before data lands in your index.

- → User identity via AD, Okta, Entra ID
- → Application name via device DPI (Cisco NBAR2, Palo Alto App-ID, Fortinet, SonicWall
- → Cyber threat intelligence & reputation scoring
- → GeoIP, ASN, and location mapping
- → VM names and cloud instance metadata
- → Reverse DNS (FQDN)

03 DATA NORMALIZATION

Sustainable at Enterprise Scale

Raw NetFlow volume is inflated by structural redundancy. NFO eliminates it before the data reaches Splunk, making full-fidelity network telemetry sustainable at any scale.

- → Aggregation collapses flows with shared key attributes
- → Flow stitching unifies ingress/egress into single bidirectional records
- → Deduplication removes multi-hop cross-collector duplicates
- → Result: full network visibility in Splunk — at manageable volume

info@netflowlogic.com | sales@netflowlogic.com 1-650-308-8887 www.netflowlogic.com

What's Included — Splunk-Specific Features

NetFlow & SNMP Analytics App
A free, pre-built app on Splunkbase with ready-to-use dashboards for network traffic analysis, firewall monitoring, cloud visibility, and SNMP device health. No dashboard configuration required.

Technology Add-On (TA-netflow)
Ensures NetFlow data lands in Splunk with correct CIM-compliant field names and sourcetype. Normalization happens inside NFO — the TA ensures Splunk indexes it correctly and makes it immediately compatible with all Splunk apps.

Zero-Touch SNMP Device Monitoring
Automatically discovers, classifies, and polls SNMP devices — sending device health KPIs (CPU, memory, interface stats, traps) directly to Splunk alongside flow data, in a single pipeline.

Content Pack for Splunk ITSI
Extends NFO data into Splunk IT Service Intelligence — adding service health views, glass tables, and KPI monitoring driven by enriched NetFlow and SNMP device metrics.

Splunk Enterprise Security Integration
CIM-compliant output maps directly to Splunk ES correlation searches and notable event workflows. Enriched fields — user, threat score, GeoIP — are available immediately in ES risk-based alerting.

Splunk Observability Cloud (OTel)
NFO's OpenTelemetry output delivers enriched NetFlow and SNMP device metrics directly to Splunk Observability Cloud — bringing network-layer visibility into the same platform as your application and infrastructure telemetry.

Before NFO vs. After NFO in Splunk

SCENARIO	WITHOUT NFO	WITH NFO
NetFlow in Splunk	Not possible — Splunk cannot ingest binary data	**Full fidelity, structured, enriched — indexed immediately**
Flow volume reaching Splunk	N/A — no NetFlow in Splunk	**Lean, high-fidelity stream — structural redundancy removed before ingestion**
CIM compliance	N/A	**Automatic — NFO normalizes inside the pipeline**
ES correlation searches	No network context fields available	**User identity, threat scores, GeoIP — full investigative context for ES correlation**
SNMP device health in Splunk	Separate tool, separate dashboard	**Same pipeline, same Splunk app**
Splunk search performance	N/A	**Fast — lean, enriched, normalized records**

SYSTEM REQUIREMENTS	SIZING GUIDANCE
Linux: RHEL 7+, Rocky Linux 8+ **Windows:** Windows Server 2019, 2022, 2025 *Software-only — no proprietary hardware required.*	**Entry level:** 2 CPUs, 8 GB RAM, 20 GB disk **Throughput:** 300K+ flows/sec at entry-level sizing **Scale-out:** Add instances; NFO Central manages distributed deployments with no throughput ceiling

Add network telemetry to your Splunk environment for the first time.

Start a free trial with your own network or schedule a technical demo with a NetFlow Logic engineer.

Start Free Trial
netflowlogic.com/free-trial

Schedule a Demo
netflowlogic.com/request-a-demo