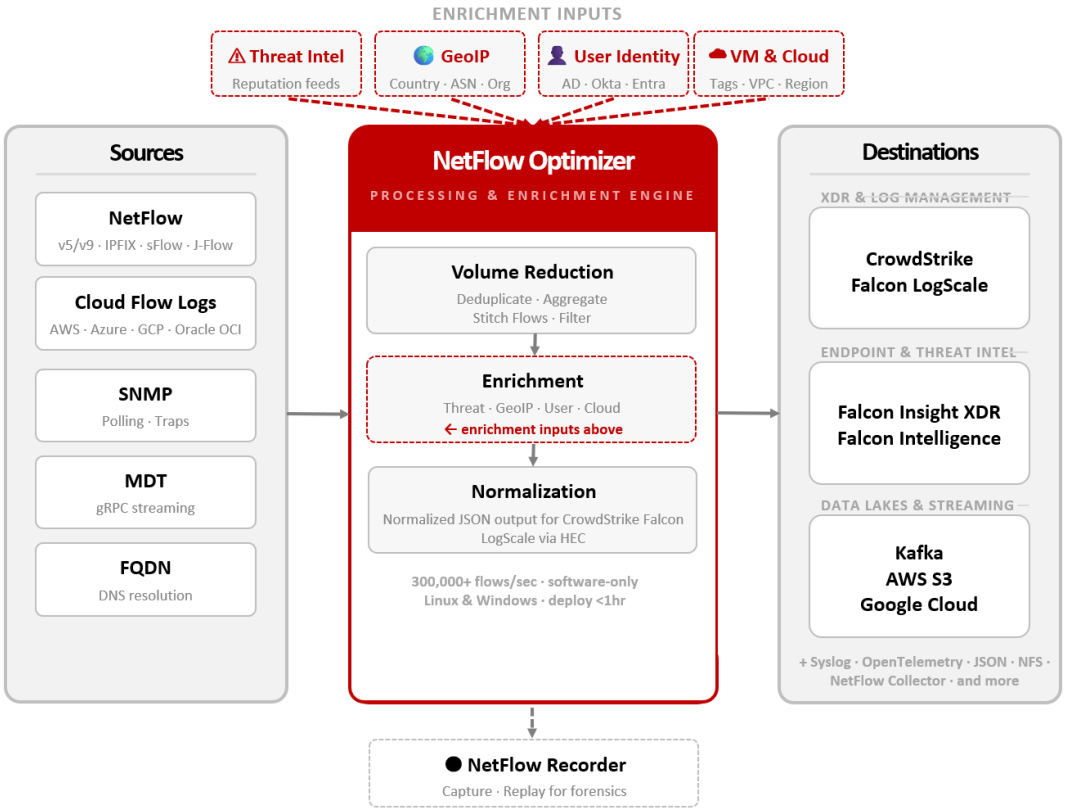
INTEGRATION GUIDE

NetFlow Optimizer™ + CrowdStrike Falcon LogScale

CrowdStrike sees the endpoint. Not the network between them.

CrowdStrike Falcon is a world-class EDR — but endpoints are not the whole story. Lateral movement crosses unmanaged devices, IoT, and network segments that agents can't touch. NFO adds the network visibility layer **Falcon doesn't have — delivering enriched, normalized NetFlow directly to Falcon LogScale.**

80–90%	300K+	< 1 hr
Typical LogScale ingest reduction	Flows/sec processed, per instance	From install to live LogScale data



The Network Visibility Gap in CrowdStrike Falcon

01 THE BLIND SPOT

Unmanaged Devices Have No Agent

CrowdStrike Falcon excels at endpoint visibility — but IoT devices, printers, industrial controllers, and legacy systems can't host a Falcon agent. When a threat actor moves laterally through your network, these blind spots are the path of least resistance. NFO provides network-layer visibility for every segment, with or without an agent.

→ East-West lateral movement fully visible — regardless of agent coverage

→ Unmanaged IoT, OT, and legacy devices covered via NetFlow

→ Correlated alongside Falcon endpoint alerts in a single platform

02 THE COST

Raw NetFlow Is Expensive and Risky to Ingest

Falcon LogScale can ingest raw NetFlow — but raw UDP flows sent over the public internet to a SaaS platform is a security risk. And the volume is prohibitive. NFO acts as a secure local gateway: it aggregates, enriches, and pushes structured JSON to LogScale via HTTPS, solving both problems before data leaves your network.

→ Secure HTTPS delivery — no raw UDP over the public internet

→ 80–90% volume reduction — stays within LogScale license limits

→ Structured JSON optimized for LogScale's index-free architecture

03 THE CONTEXT

Multi-Vendor Normalization Before LogScale

Cisco, Palo Alto, Juniper, AWS, Azure — every vendor implements NetFlow differently. Raw collection forces analysts to write complex vendor-specific queries. NFO normalizes all sources into a single consistent schema before data reaches LogScale, so threat hunting works across your entire hybrid environment.

→ NetFlow v5/v9, IPFIX, sFlow, J-Flow — all normalized

→ AWS VPC, Azure NSG, GCP, Oracle OCI flow logs — same pipeline

→ Single standardized schema — query once across all sources

What's Included — LogScale-Specific Features

Structured JSON via LogScale HEC
NFO delivers enriched NetFlow data to the LogScale HTTP Event Collector (HEC) as structured JSON — optimized for LogScale's index-free architecture. Sub-second LQL query performance across terabytes of network telemetry.

East-West Lateral Movement Detection
NFO provides continuous network flow visibility across all segments — including unmanaged devices Falcon agents can't reach. When a threat actor moves laterally, NFO captures every connection so analysts can trace the full attack path in LogScale.

Identity-Enriched Network Records
NFO resolves IP addresses to Active Directory, Microsoft Entra ID, or Okta user identities before data reaches LogScale. Analysts hunt by username, not IP — eliminating lookup overhead during active investigations.

Exfiltration Detection Alongside EDR
Falcon sees a suspicious process reading files. NFO sees the gigabytes of data moving laterally across the network. Together in LogScale, analysts get the full picture: what happened on the endpoint and what left the building — correlated in a single query.

SNMP Device Health in LogScale
SNMP Pro delivers device health telemetry — CPU, memory, interface stats, SNMP traps — to LogScale alongside flow data. Zero-Touch Discovery classifies devices automatically. Network and security context in the same platform.

DDoS Detection with LogScale Alerting
NFO's built-in DDoS Detector uses proprietary ML algorithms to identify over 30 attack types — volumetric floods, application-layer attacks, reconnaissance, and low-and-slow resource exhaustion — in real time. Alerts and attack metadata are forwarded to LogScale for correlation with Falcon endpoint signals and automated response workflows.

Before NFO vs. After NFO in CrowdStrike Falcon LogScale

Scenario	Without NFO	With NFO
Unmanaged device visibility	Blind spot — no Falcon agent possible	**Full NetFlow coverage — every conversation captured**
NetFlow delivery to LogScale SaaS	Raw UDP over internet — security risk	**Secure HTTPS via NFO — enriched JSON, no raw flows**
LogScale ingest volume	High — raw flows, full volume	**80–90% lower — aggregated before HEC delivery**
Multi-vendor normalization	Vendor-specific queries required	**Single schema — all sources normalized inside NFO**
Lateral movement detection	Endpoint-only — network path invisible	**Full east-west visibility across managed and unmanaged devices**
Identity context in LogScale	IP addresses only	**User identity resolved inside NFO — hunt by name, not IP**
SNMP device health	Separate tool, not in LogScale	**Same pipeline, same LogScale repository**

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
Throughput: 300K+ flows/sec at entry-level sizing
Scale-out: Add instances; NFO Central manages distributed deployments with no throughput ceiling

See the network layer CrowdStrike can't see.

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