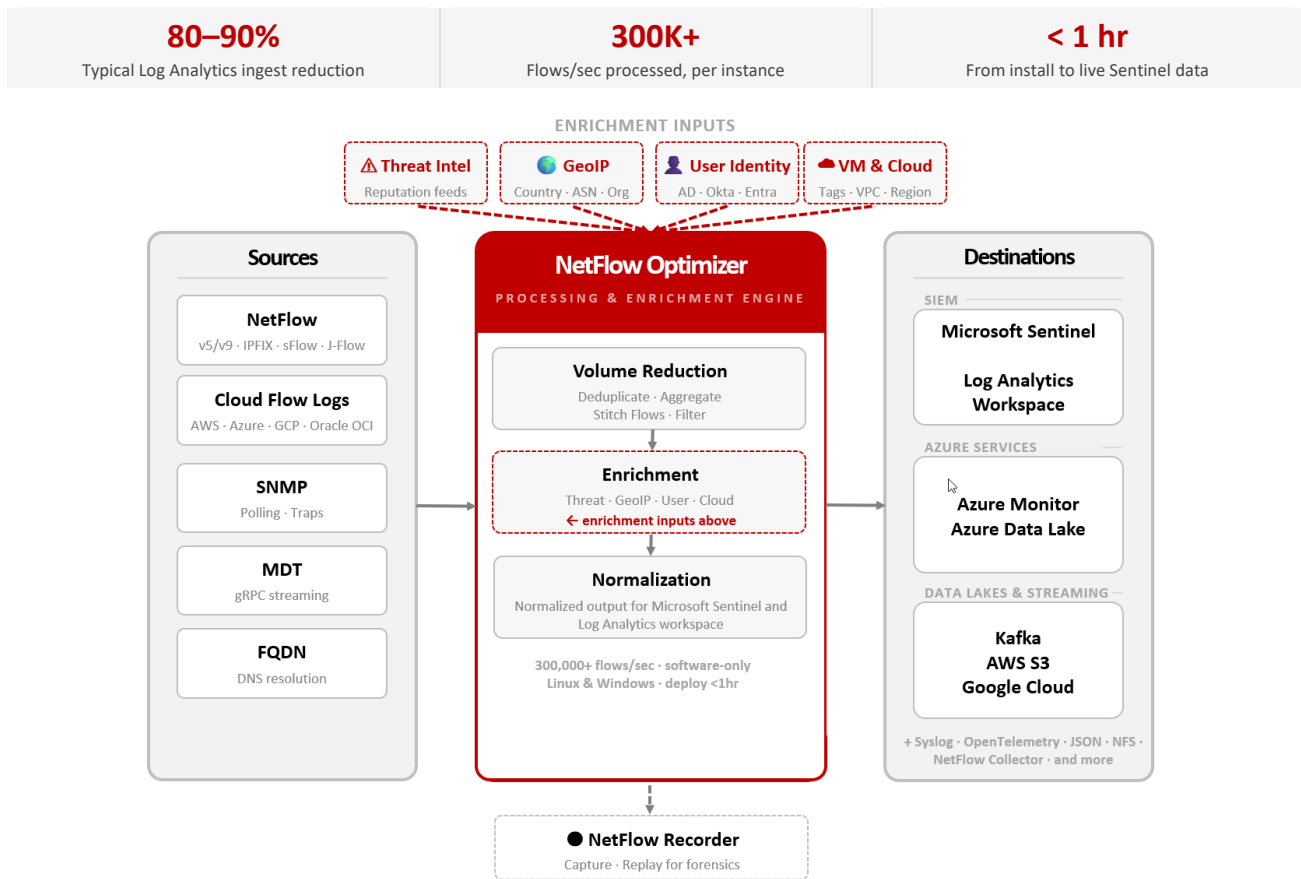




Sentinel sees your cloud. Not your network.

Microsoft Sentinel natively ingests Azure flow logs — but on-premises NetFlow from routers, switches, and firewalls is a blind spot. NFO closes that gap, normalizes every source into one enriched stream, and reduces your Log Analytics ingest bill by 80–90% before data reaches your workspace.



The Network Visibility Gap in Microsoft Sentinel

01 THE GAP	02 THE COST	03 THE CONTEXT
<p>On-Premises NetFlow Is Missing</p> <p>Sentinel natively collects Azure NSG and VNet flow logs. But the majority of meaningful network traffic — from on-prem routers, firewalls, switches, and wireless — generates NetFlow and IPFIX that Sentinel has no native connector for. NFO fills that gap.</p> <ul style="list-style-type: none"> → On-prem NetFlow v5/v9, IPFIX, sFlow, J-Flow — all normalized → Azure NSG/VNet, AWS VPC, GCP, Oracle OCI — already covered → One enriched stream to Sentinel — on-prem and cloud unified 	<p>Raw Flows Are Expensive in Log Analytics</p> <p>Sentinel charges by data ingested into Log Analytics. Raw NetFlow is high-volume, highly redundant — the same conversation reported by multiple devices, hundreds of micro-flows per session. NFO eliminates the redundancy before data hits your billing meter.</p> <ul style="list-style-type: none"> → Deduplication removes cross-device duplicate records → Aggregation collapses micro-flows into single records → Flow stitching adds a further 50% reduction → 80–90% less volume — same analytical coverage 	<p>Raw IPs Tell Half the Story</p> <p>Raw flow records contain IP addresses and port numbers. Sentinel analysts need context — who is behind the IP, where is the remote host, is it a known threat. NFO adds that context inside the pipeline, before data reaches Sentinel.</p> <ul style="list-style-type: none"> → User identity via Active Directory or Microsoft Entra ID → GeoIP location and ASN mapping → Threat intelligence and reputation scoring → VM names and cloud instance metadata

What's Included — Sentinel-Specific Features

Three Pre-Built Sentinel Workbooks

Deployed via ARM templates, customizable via KQL. Three workbooks provide immediate SOC visibility:

- Traffic Overview — top talkers, protocol breakdown
- Malicious Host Communications — threat feed, affected host tracking, accepted vs. rejected traffic
- Critical Port Monitoring — DNS analytics, watchlist for FTP/SSH/RDP/SMB, unauthorized access detection

Unified On-Premises + Cloud Flow Stream

NFO ingests on-prem NetFlow, Azure NSG/VNet flow logs, AWS VPC Flow Logs, GCP VPC, and Oracle OCI — normalizing all sources into a single consistent stream to Sentinel. One Log Analytics table, all network sources, on-prem and cloud.

Enrichment Inside NFO — Before Sentinel

User identity, GeoIP, threat intelligence, and VM metadata are resolved inside NFO before data is sent to Sentinel. Enriched fields arrive ready for analytic rules, hunting queries, and workbook visualizations — no additional enrichment steps in Sentinel.

DDoS Detection with Sentinel Alerting

NFO's built-in DDoS Detector uses proprietary ML algorithms to identify 31 attack types — volumetric floods, application-layer attacks, reconnaissance, and low-and-slow resource exhaustion — in real time. Alerts and attack metadata are forwarded to Sentinel for correlation with other security signals and automated SOAR response.

Ingest Cost Reduction Before the Billing Meter

NFO performs deduplication, aggregation, and flow stitching before data reaches Log Analytics — typically reducing ingest volume 80–90%. On Sentinel's consumption pricing, the NFO license cost is often a fraction of the billing reduction achieved.

Azure Monitor / Log Analytics Delivery

NFO delivers enriched, normalized network telemetry directly to your Log Analytics workspace via the Azure Monitor REST API. No additional agents or forwarders required on your network devices — NFO handles the connection.

Before NFO vs. After NFO in Microsoft Sentinel

Scenario	Without NFO	With NFO
On-prem NetFlow in Sentinel	No native connector — blind spot	Fully ingested, normalized, enriched
Log Analytics ingest volume	High — raw flows, full volume	80–90% lower — before billing meter
Data context in Sentinel	IP addresses only	User, GeoIP, threat — enriched inside NFO before delivery
Analytic rule coverage	Limited — missing on-prem network fields	Full network visibility — on-prem and cloud unified
SNMP device health	Separate tool, not in Sentinel	Same pipeline, same Log Analytics workspace
DDoS detection	No dedicated flow-based detection	Built-in ML detection — 31 attack types including volumetric, application-layer, and low-and-slow — alerts forwarded to Sentinel

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

See NFO filling Sentinel's network visibility gap.

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