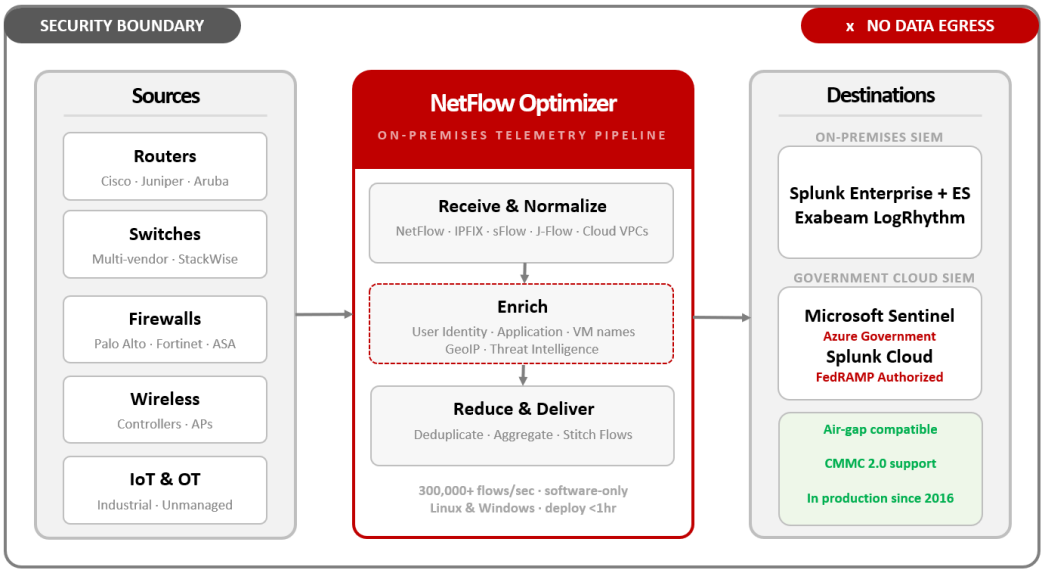
SOLUTION BRIEF

NetFlow Optimizer™ for Government & Public Sector

Network telemetry for classified and sensitive environments.

Most commercial network monitoring tools introduce data egress, cloud dependencies, or proprietary hardware that disqualify them from government and DoD environments. NetFlow Optimizer is software-only, **on-premises, air-gap compatible — and has been in production at federal agencies and DoD enterprises since 2016.**

2016	300K+	< 1 hr
In production at federal agencies & DoD	Flows/sec processed, per instance	Deploy time — no hardware required



Why Most Network Tools Fail in Government Environments

01 THE REQUIREMENT

On-Premises. Air-Gap. Zero Egress.

Government and DoD procurement teams evaluate network tools on architecture and data handling before features. Most commercial tools have cloud dependencies, SaaS components, or vendor-managed infrastructure that disqualify them before the evaluation begins. NFO has none of these.

- Software-only — no proprietary hardware to procure or certify
- On-premises — fits within existing ATO boundary
- Air-gap compatible — no internet connectivity required
- Runs on RHEL 7+, Rocky Linux 8+, Windows Server

02 THE VISIBILITY NEED

Continuous Monitoring for CMMC and FISMA

Network visibility is a foundational requirement across DoD cybersecurity frameworks. CMMC 2.0 Levels 2 and 3 require continuous monitoring and network traffic analysis. NFO delivers enriched network telemetry to your on-premises or government-authorized SIEM — enabling the compliance posture these frameworks require.

- Network telemetry delivery supporting AU family controls
- Device health visibility across all network infrastructure
- DDoS detection — over 30 attack types, proprietary ML
- User identity enrichment resolved before data reaches SIEM

03 THE SCALE CHALLENGE

Multi-Vendor, Distributed, High-Volume Networks

Federal agency and DoD networks span multiple sites, vendors, and classification levels. NFO Central manages distributed deployments with no throughput ceiling — processing 300,000+ flows per second per instance from NetFlow, IPFIX, sFlow, and cloud VPC sources across your entire infrastructure.

- 300K+ flows/sec per instance — unlimited with NFO Central
- NetFlow v5/v9, IPFIX, sFlow, J-Flow — all normalized
- Zero-Touch SNMP — up to 3,000 devices per instance
- Feeds on-premises and government-authorized cloud SIEMs

What NFO Delivers for Government and DoD Teams

On-Premises Telemetry Pipeline — Zero Egress
NFO processes, enriches, and delivers network flow telemetry entirely within your security boundary. No data leaves your environment — enrichment, deduplication, and normalization all happen inside NFO before delivery to your SIEM. Fully compatible with air-gapped networks.

On-Premises SIEM — Splunk ES & Exabeam LogRhythm
For fully on-premises deployments, NFO delivers CIM-compliant enriched network telemetry to Splunk Enterprise Security and Exabeam LogRhythm — both of which can be deployed inside your security boundary with no cloud dependency. Pre-built apps and content provide immediate visibility without custom development.

Government Cloud SIEM — Sentinel, Splunk Cloud & Sumo Logic
For agencies operating in government-authorized cloud environments, NFO delivers enriched telemetry to Microsoft Sentinel on Azure Government, Splunk Cloud and Sumo Logic's FedRAMP Moderate authorized platform. NFO remains fully on-premises — only the enriched output stream is delivered to the cloud SIEM.

DDoS Detection — over 30 Attack Types, Proprietary ML
NFO's built-in DDoS Detector uses proprietary ML to identify over 30 attack types — volumetric floods, application-layer attacks, reconnaissance, and low-and-slow resource exhaustion — entirely within your security boundary. Alerts are forwarded to your SIEM and SOAR platform. In air-gapped environments, the detector identifies anomalous traffic from compromised or misconfigured internal hosts.

Identity & Threat Intelligence Enrichment
NFO enriches every flow record with user identity from Active Directory, GeoIP location, and threat intelligence reputation scores — inside the pipeline, before data reaches your SIEM. Analysts investigate with full context, not raw IP addresses. Enrichment data never leaves your environment.

Zero-Touch SNMP Device Monitoring
NFO automatically discovers, classifies, and monitors every network device across your infrastructure — routers, switches, firewalls, and wireless controllers — without manual OID configuration. SNMPv3 with configurable credentials applied automatically per IP range. Self-healing inventory reruns twice daily, ensuring device coverage stays current across large, distributed government networks without manual intervention.

NFO vs. Typical Commercial Network Monitoring Tools

Requirement	Typical Commercial Tool	NetFlow Optimizer
Deployment model	SaaS or cloud-dependent	**On-premises only — no cloud dependency**
Air-gap support	Rarely supported	**Fully supported — no internet required**
Data egress	Telemetry sent to vendor cloud	**Zero — all processing stays on-premises**
Hardware requirement	Proprietary appliances common	**Software-only — standard Linux or Windows**
ATO compatibility	New boundary often required	**Fits within existing ATO boundary**
CMMC 2.0 support	Partial — cloud components excluded	**Full on-prem telemetry supporting AU controls**
SIEM delivery options	Cloud SIEM only	**On-prem (Splunk ES, LogRhythm) + Gov Cloud (Sentinel, Sumo Logic)**
In government production	Varies	**Federal agencies and DoD enterprises since 2016**

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 **NetFlow throughput:** 300K+ flows/sec at entry-level sizing **SNMP devices:** Up to 3,000 devices per instance **Scale-out:** NFO Central manages distributed deployments with no throughput ceiling

Talk to an engineer who understands government network requirements.

Request a quote for your agency or program or schedule a technical demo with a NetFlow Logic engineer.

Request a Quote
netflowlogic.com/request-a-quote

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