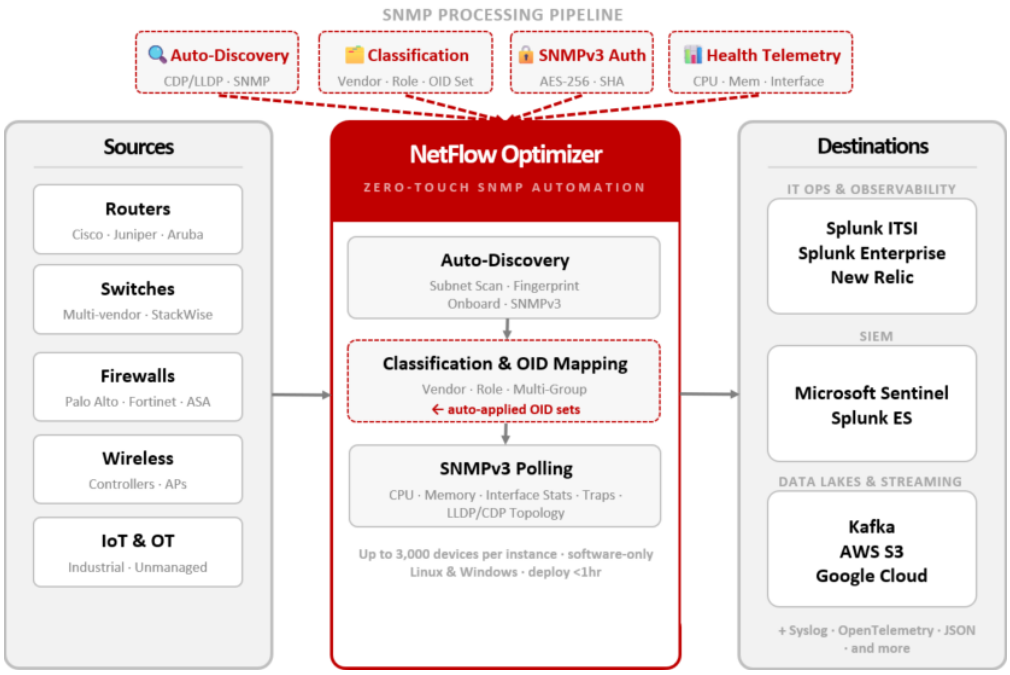
SOLUTION BRIEF

Manual SNMP configuration takes 2–4 hours per device. With NFO it takes minutes.

Every new switch, firewall, or wireless controller requires OID lookup, configuration, and testing before it's monitored. In a network that never stops changing, manual SNMP monitoring is always incomplete. NFO eliminates all of it — autonomous discovery, self-healing inventory, role-based precision.

< 1 hr	3,000	2×/day
From install to devices polling	Devices per NFO instance	Automatic rediscovery — self-healing



The Three Problems with Manual SNMP Monitoring

01 THE VISIBILITY GAP

Always One Device Behind Reality

Manual OID mapping requires someone to identify the device, find the correct OIDs, configure monitoring, and update the inventory — every time a device is added, replaced, or reconfigured. In practice, monitoring is always incomplete. The gaps are exactly where failures and threats hide.

- New devices go unmonitored until someone notices
- Hardware refreshes silently break existing OID mappings
- Multi-vendor environments multiply the configuration burden

02 THE OPERATIONAL COST

Skilled Engineers Doing Spreadsheet Work

Onboarding a single new device manually takes 2–4 hours of OID hunting, configuration, and testing. Hardware refreshes require manual inventory updates. Firewall-specific OID sets require custom configuration. This is not what NetOps engineers were hired to do — and it prevents them from doing higher-value work.

- 2–4 hours per device for manual onboarding
- Hardware refresh triggers full reconfiguration cycle
- Role-specific metrics (firewall, StackWise) require custom OID work

03 THE SCALE PROBLEM

Multi-Vendor Environments Don't Scale Manually

Cisco, Juniper, Palo Alto, Aruba, and dozens of other vendors each implement SNMP differently. Static monitoring tools require per-vendor OID configuration that doesn't transfer between platforms. As environments grow — and as cloud, IoT, and edge devices are added — the manual approach becomes structurally unworkable.

- Per-vendor OID configuration doesn't transfer between platforms
- IoT, cloud, and edge devices add new vendor dialects constantly
- SNMPv3 encryption adds configuration complexity at scale

What's Included — Zero-Touch Automation Features

Zero-Touch Auto-Discovery
Define your IP ranges and NFO scans your network automatically — discovering, fingerprinting, and onboarding every SNMP-capable device without manual intervention. New devices are detected and added within the next scheduled scan. No spreadsheets, no manual OID lookup.

Autonomous Device Classification
NFO analyzes sysObjectID, sysDescr, and sysServices to automatically classify every device by vendor, model, and functional role — routers, switches, firewalls, wireless controllers, and more. The correct OID sets are applied automatically based on classification. No manual configuration required.

Multi-Group Inheritance
A device can belong to multiple groups simultaneously — a Cisco firewall is both a "Cisco" device and a "Firewall." NFO applies the OID sets from all matching groups, ensuring role-specific metrics (firewall session counts, interface error rates) are collected alongside standard vendor metrics automatically.

Self-Healing Inventory
NFO reruns discovery twice daily by default. When hardware is replaced, stacked (Cisco StackWise), or reconfigured, the next scan detects the change and updates classification and OID mappings automatically. Your device inventory stays current without any manual intervention.

SNMPv3 with Configurable Credentials
Full SNMPv3 support with configurable credentials — encryption and authentication settings applied automatically per IP range, accommodating the full range of device requirements across your network. SNMP traps are received and processed with SNMPv3 encryption without requiring pre-registration. Meets security requirements for enterprise and government environments.

Custom OID Sets & User MIBs
For devices or metrics not covered by built-in classification, define custom OID sets and upload vendor MIB files. Custom sets are applied automatically to matching device groups — giving you monitoring precision for specialized hardware without sacrificing the automation model.

Manual SNMP Monitoring vs. NFO Zero-Touch Automation

Task	Manual Workflow	NFO Zero-Touch
New device onboarding	2–4 hours — OID lookup, config, test	**Minutes — auto-discovered, classified, polling**
Hardware refresh	Manual inventory update required	**Automatic — self-healing on next scan**
Multi-vendor OID management	Per-vendor config, no reuse	**Single classification engine, all vendors**
Firewall-specific metrics	Complex manual OID filtering	**Autonomous — role-based group assignment**
StackWise / chassis monitoring	Difficult to scale manually	**Native — auto-detects stack roles on discovery**
SNMPv3 encryption	Manual per-device configuration	**Configurable credentials applied automatically per IP range**
Inventory accuracy	Degrades over time — manual updates	**Always current — twice-daily rediscovery**

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
Devices per instance: Up to 3,000
Scale-out: Add instances; NFO Central manages distributed deployments with no ceiling

See Zero-Touch Discovery working on your own network.

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