DATASHEET

# Application-to-Network Mapping

Enriching raw flow data with business context for faster, more informed operations

Raw flow data alone is no longer enough to support fast, confident decision-making. A 5-tuple flow record — source IP, destination IP, protocol, and port — confirms that traffic moved, but says nothing about which application generated it, who owns it, or how critical it is to the business. Closing that gap has traditionally meant manual cross-referencing across spreadsheets, CMDBs, and tribal knowledge — a process that can take months and is out of date the moment it's finished.

Selector's App-to-Network Mapping capability replaces that manual effort with a continuous enrichment pipeline. Each flow record is normalized, resolved to a known device or client, and joined against existing sources of truth — IPAM/DNS, CMDB/APM, identity, and network topology — to attach application identity, ownership, environment, and criticality directly to the flow. Where a single source can't resolve a client or application with certainty, Selector aggregates signals across multiple corroborating sources and surfaces a confidence score, so operators always know how much to trust a given mapping rather than treating every result as a binary fact.

## Why 5-tuple Alone Isn't Enough

A raw flow record only contains:

RAW 5-TUPLE RECORD

`Source IP` `Destination IP`

`Protocol` `Port`

SELECTOR ENRICHES EACH FLOW WITH

Application · Owner · Environment

Criticality · Confidence score

Without enrichment, this leaves critical questions unanswered:

- **No app identity** — which service does this traffic belong to?
- **No ownership** — which team or business unit is responsible?
- **No criticality** — is this production, dev, or test?
- **No path visibility** — NAT translation, load balancers, and VIPs can obscure the real source, destination, and route traffic actually takes

> Selector resolves these automatically — including translating NAT'd addresses back to their real source and destination zones — at the speed and scale manual mapping can't match.

## The Enrichment Pipeline

Selector enriches every flow record through a structured pipeline:

### 1 Ingest

Collect raw 5-tuple flow data (NetFlow, sFlow, IPFIX, firewall logs) from across the environment via multi-source ingestion, alongside the underlying infrastructure data (routing, switches/VLANs, load balancers) needed to interpret it.

### 2 Normalize & Resolve

Standardize formats automatically across sources, then apply smart entity resolution to identify the actual devices, clients, and endpoints behind each address — including resolving NAT'd and translated IPs back to real source/destination zones.

### 3 Apply Contextual Linkages

Join the resolved flow against existing systems of record through enterprise joins: IPAM/DNS for hostname resolution, CMDB/APM for application context, and network topology for path and zone information.

### 4 Enrich

Tag each flow with deep metadata — application, owner, environment, and risk/criticality — and generate ML-derived features that prepare the record for downstream AIOps use. Where multiple data sources offer a corroborating but imperfect signal, Selector aggregates across them and assigns a prediction/confidence score to the resulting application or client match, rather than forcing a single brittle source of truth.

### 5 Activate

Deliver AIOps-ready, enriched context (flow ID, application, owner, environment, risk) to power baselining, correlation, and alerting, and make it queryable through dashboards, a visual query builder, or natural language.

## Built on the Systems You Already Run

Selector draws enrichment context from sources already deployed across the environment — each contributing a distinct piece of the resolved flow:

**Observability & Logs**
platforms such as Splunk and Dynatrace contribute traffic history, firewall and routing details, and timestamped flow records

**Network & Infrastructure**
topology and discovery tools contribute path, zone, and device relationship data

**Identity**
SSO/LDAP contributes user and client identity context

**IPAM / DNS**
contributes hostname resolution and address ownership

**Business Context**
CMDB platforms such as ServiceNow contribute application ownership, business unit mapping, and criticality tags

**Custom Data**
CSV, structured portals, and API-delivered sources fill gaps that don't have a system of record

Any data source can be aligned and joined into the model, regardless of format. New sources extend the mapping without requiring a pipeline rebuild.

## A Complete Operational Picture for Every Flow

For any flow, Selector answers three layers of questions that raw telemetry can't:

**What is this flow?**
Application identity (mapping IP to service name), ownership (business unit and team), and environment (production vs. dev/test) — resolved automatically, not looked up by hand.

**Who is impacted?**
Customer/client context for the specific accounts or sources affected, the infrastructure and data centers the flow traverses, and blast radius — the dependent downstream applications that share the same path.

**What should we do?**
Anomaly detection against learned baselines (e.g., surfacing unexpected traffic types), policy validation to catch segmentation violations, and change-risk assessment to determine whether a maintenance window is safe.

This turns flow data from a static record into an operational signal, supporting real-time visibility into client-to-application relationships, drill-down into application-to-application dependencies, and continuous validation of inventory and compliance data through AI/ML-driven anomaly detection across sources.

## Mapping That Keeps Up With the Network

**Automated Discovery**
Selector discovers application and network relationships automatically from live flow data, eliminating manual mapping work

**Continuous Enrichment**
Flow data is enriched automatically, keeping application and ownership maps current as infrastructure changes

**Proactive Validation**
Teams query enriched flow data directly — in natural language — to validate dependencies before they become incidents

By turning flow data into a living, business-aware map, Selector replaces static documentation with a continuously updated source of truth.

## Build a stronger foundation for operations

See how Selector's App-to-Network Mapping helps teams replace “what IP is this?” guesswork with a complete, business-aware view of every flow in the environment. Book a demo at www.selector.ai.

Book a Demo