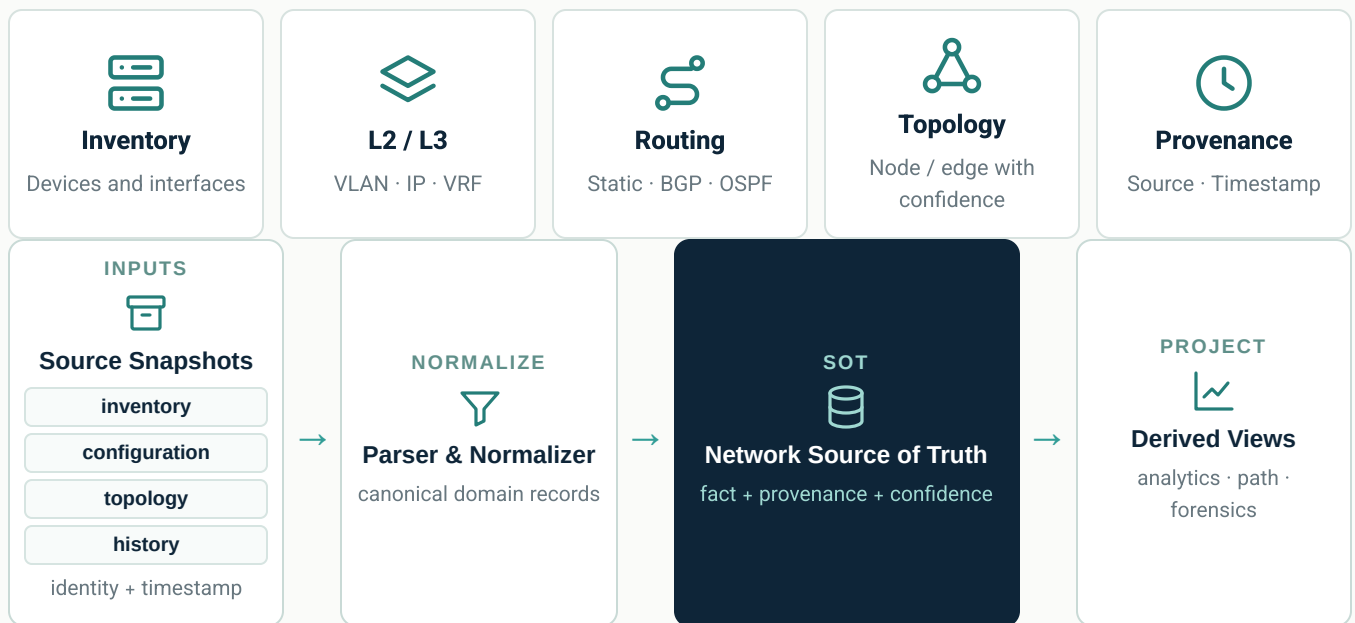


4SO Network

Technical Brochure

Network Source of Truth with Provenance & Confidence

Turns scattered network information into a machine-readable model: inventory, interfaces, L2/L3, routing, topology and history are kept with clear provenance, and inference never silently becomes fact.



Inference never silently becomes fact

A relationship derived only from naming or a diagram stays a candidate until it is corroborated.

Projection ≠ Authority

Summaries, path views and forensics are built over source records and never create a second authority.

Turn the network into data you know exactly how far to trust.

CAPABILITY SNAPSHOT

Capability Snapshot

Network data is broken down into analyzable domains

The goal is to turn config dumps into an operational model that supports queries, correlation and forensics.



Device Inventory
A structured model independent of the source format



Interface Model
Interfaces, descriptions and bundles



VLAN and Port-channel
Segments, membership and aggregation



IP and VRF
Addressing and routing context



Routing Facts
Static, BGP and OSPF for path analysis



Topology
Node/edge with source and confidence



Service Dependencies
DNS, time, AAA and logging



Provenance and History
Timestamp, source and change history

Data ownership boundary

- A configuration fact belongs to that source's snapshot 
- A topology fact belongs to its own diagram source 
- A candidate relationship is not definitive until corroborated 
- A derived view is only a projection 

Operating principles

- Raw configuration containing secrets never reaches output 
- Confidence is never separated from provenance 
- A diff shows the change, not its cause 
- No device commands or live configuration changes 



Core contract: Source Snapshot → Parse → Normalize → Correlate → Classify → Review → Derived View — every stage keeps the path back to the source.

AUTHORITY MODEL

Authority Model

The source matters; so does the confidence

Instead of a flat table that treats everything as definitive truth, data is classified by its origin and extraction method.

FACT —————

What the source actually stated;
valid only within the scope of that
snapshot and timestamp.

source-scoped · timestamped

FACT —————

What the source actually stated;
valid only within the scope of that
snapshot and timestamp.

source-scoped · timestamped

FACT —————

What the source actually stated;
valid only within the scope of that
snapshot and timestamp.

source-scoped · timestamped

CANDIDATE —————

Inferred from naming, descriptions or diagrams; recorded with its confidence and inference method.

bounded inference · confidence

CANDIDATE —————

Inferred from naming, descriptions or diagrams; recorded with its confidence and inference method.

bounded inference · confidence

CANDIDATE —————

Inferred from naming, descriptions or diagrams; recorded with its confidence and inference method.

bounded inference · confidence

DERIVED

A summary, path or analysis over source records; it does not create a second authority.

projection · reproducible

DERIVED

A summary, path or analysis over source records; it does not create a second authority.

projection · reproducible

DERIVED

A summary, path or analysis over source records; it does not create a second authority.

projection · reproducible

SYNTHETIC RECORD SHAPES

FACT	
domain	interface
source	config snapshot
observed	timestamp
class	fact

FACT	
domain	interface
source	config snapshot
observed	timestamp
class	fact

The diagram illustrates the relationship between a candidate and its associated domain, method, confidence, and state. It consists of a central box labeled "CANDIDATE" with four arrows pointing to four separate boxes: "domain", "method", "confidence", and "state".

```
graph TD; CANDIDATE --> domain; CANDIDATE --> method; CANDIDATE --> confidence; CANDIDATE --> state;
```

The diagram illustrates the relationship between a candidate and its associated domain, method, confidence, and state. It consists of a central box labeled "CANDIDATE" with four arrows pointing to four separate boxes: "domain", "method", "confidence", and "state".

```
graph TD; CANDIDATE --> domain; CANDIDATE --> method; CANDIDATE --> confidence; CANDIDATE --> state;
```

DERIVED	
domain	path view
inputs	L2 · L3 · routing
lineage	source manifest
authority	none

DERIVED	
domain	path view
inputs	L2 · L3 · routing
lineage	source manifest
authority	none

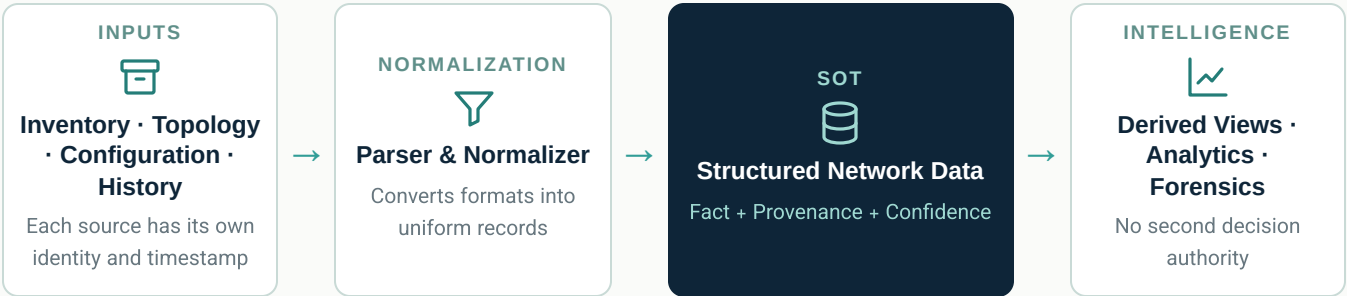
Domain	Example records	Authority / Confidence	Use
Inventory	Device identity, platform/role, source mapping	Fact within the snapshot scope	Inventory and normalization
Interfaces / L2	Interface, VLAN, port-channel	Config-derived + timestamp	Link-layer analysis
L3 / Routing	IP/subnet, VRF, static, BGP, OSPF	Observed or config-derived record	Path and policy analysis
Topology	Node, edge, link candidate	Fact Candidate Derived	Correlation without turning inference into truth
Dependencies	DNS, time, AAA, logging	Source-owned relation or bounded inference	Service dependency analysis
History	Snapshot identity, change context	Timestamp + provenance	Forensics and comparison

ARCHITECTURE OVERVIEW

Architecture Overview

The pipeline must preserve provenance, not erase it

Sources are ingested separately, parsers normalize them, and the single source of truth keeps records with their provenance and confidence.



Evidence type	Classification	Usage rule
Configuration snapshot	Fact within the snapshot scope	Valid only with its own source and timestamp
Topology / diagram	Source-scoped fact	A relationship in a diagram does not prove the live network state
Naming / description	Candidate	An inferred link, role or site is not definitive before corroboration
Multi-source	Confidence-bearing	Origins and supporting evidence stay attached to the relation
Derived view	Projection	Built from source-owned data; not a second SoT
Historical compare	Change context	Shows change; does not claim an incident's cause without evidence



Reproducible

Parsers and generators rebuild output from the manifest



Secret-safe

Credential values are removed from the dataset



Ambiguity visible

Conflicts and unknowns are never hidden

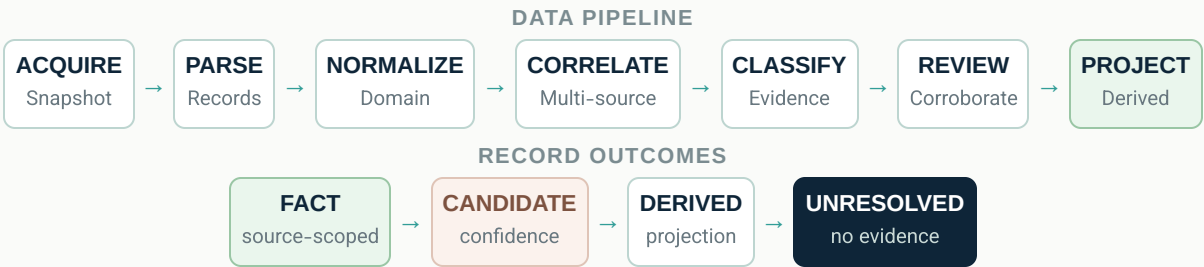
 **Correlation:** a relation built from several sources carries the source identity, timestamp, confidence and supporting evidence with it; correlation does not remove source ownership.

ACTION & WORKFLOW CONTRACT

Action & Workflow Contract

Core action: turning evidence into an analyzable model

This product applies no change to the live network; its core workflow is evidence management and classification.



Action	Admission	Execution	Success	Failure / Recovery
Ingest Snapshot	Source identity, hash and timestamp	Parser reads only that source's data	Every record traces back to its snapshot	A failed parse never overwrites the previous source
Normalize	Parser for device, interface, L2/L3, routing	Conversion to the canonical model	Identity and source mapping preserved	Unknown fields are never fabricated
Correlate	Match key and provenance on both sides	Build the relation without removing ownership	Supporting sources can be shown	Conflicts are not hidden or collapsed
Infer Candidate	A hint for bounded inference	Candidate with confidence and method	Distinguishable from fact and reviewable	Never reaches authority without corroboration
Review	Independent evidence or operator confirmation	Assessment with additional evidence	Classification kept with its trace	No evidence = unresolved
Export Safe View	Snapshots and sensitivity policy	Projection from existing records	Reproducible, with no second SoT	Public output removes sensitive data



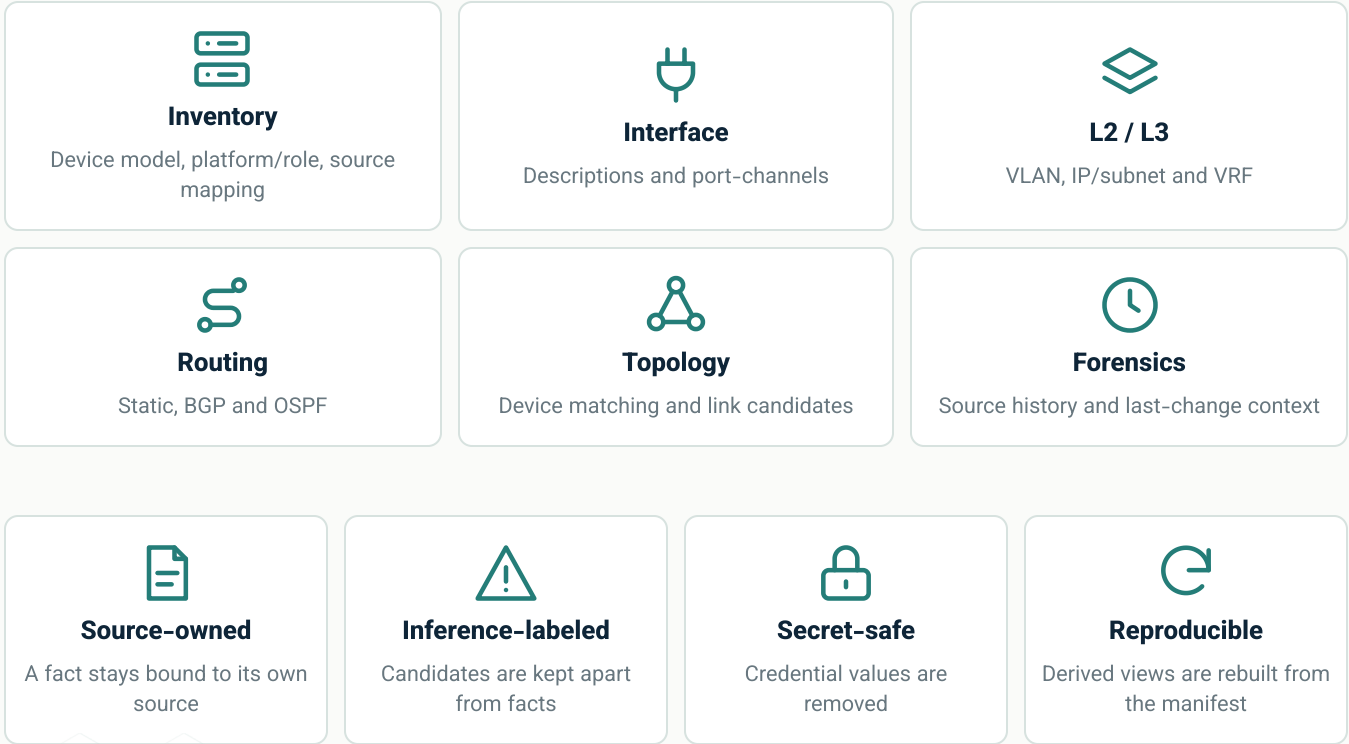
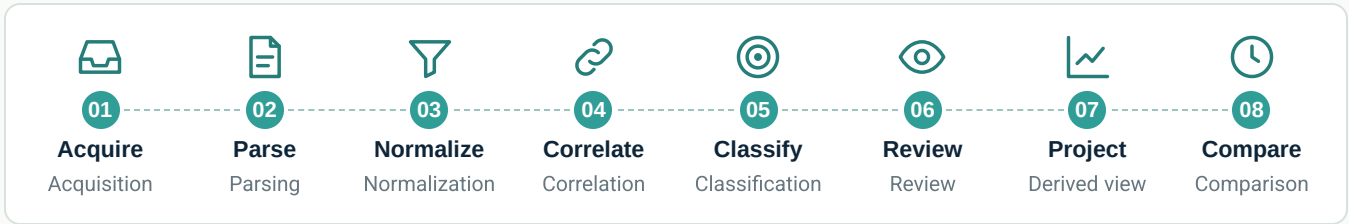
Projection ≠ Authority: summaries, path views, analytics or forensics are built from several sources, but the original fact stays bound to its own source and timestamp.

LIFECYCLE

Lifecycle & Data Profiles

Network data has a quality lifecycle too

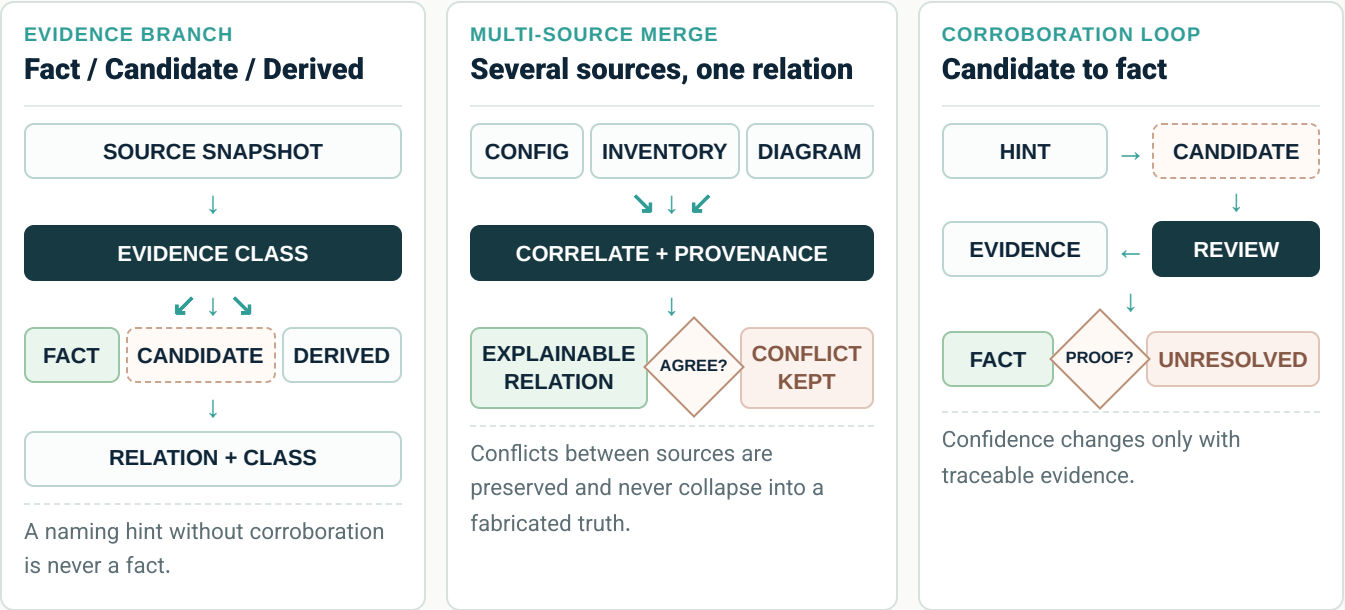
Until a snapshot has been parsed, classified and correlated it is only raw input; a derived result does not take the place of a fact until it has been reviewed.



DEEP TECH WORKFLOWS

Data-Quality Failure Semantics

Ambiguity must be visible, not hidden



Failure Domain	Detection	Product Behavior	Recovery
Stale snapshot	Source timestamp and history	The fact stays scoped to that snapshot	Acquire a newer source
Parser gap	Schema or parse error	A missing field stays missing	Extend the parser and regenerate
Source conflict	Mismatch during correlation	No silent winner is chosen	Keep the conflict and its evidence
Weak inference	Low confidence	Never promoted to fact	Independent corroboration
Sensitive content	Detection and redaction	The value is removed	Only metadata remains

Path analysis: if link or routing evidence is incomplete, confidence drops; the system never fabricates a missing path.

ACTION & OPERATIONS CATALOG

Action & Operations Catalog

The operations catalog is data engineering for the network

Acquire •

- ingest snapshot
- verify manifest
- history sync



Parse •

- devices
- interfaces
- L2
- L3
- routing



Correlate •

- device match
- topology match
- link candidate



Quality •

- classify
- conflict review
- secret redaction



Analyze •

- subnet view
- routing view
- dependency view



Forensics / Export •

- snapshot diff
- provenance trace
- safe summary



Security and Sensitivity

Credential values are removed from generated datasets



Secret findings only as redacted metadata



Queries and exports follow the sensitivity policy



Observability and Evidence

Data freshness from timestamps and history



A parse error is a data-quality signal



Every derived report is traceable via its manifest



Action safety: the operations catalog is data-centric; no general device command or live configuration change is claimed.

Network data whose provenance and trustworthiness are clear.

4SO Network is built for decisions on network data, with provenance and confidence as part of the model itself.

