uControl

USE CASE · DISCOVER

Network & Topology Intelligence

See how everything connects — and what an outage will really hit.

A list of assets tells you what you have. A topology tells you what happens when one fails.

Most inventories are flat. They record devices but not how they connect — so impact analysis, change planning and security investigations fall back on tribal knowledge and out-of-date diagrams.

> **uControl builds the map from reality, not memory.**
> uControl **Insights** discovers devices and ingests NetFlow/IPFIX to see real communication paths; uControl **Core** assembles them into a live topology of typed relationships you can traverse for impact and dependency.

Executive summary

Network & Topology Intelligence turns raw discovery and passive flow data into an interactive map of your estate and how it communicates. Insights provides the discovery and the flow; Core turns it into typed relationships and topology you can traverse.

The map is live — flow-derived edges age out automatically — so it reflects how the estate actually behaves, not how a diagram once described it.

The business challenge

Connectivity is the hardest thing to keep accurate:

- Network diagrams are outdated the moment they're drawn
- Dependencies live in people's heads
- Segmented and OT networks resist active scanning
- Nobody owns the whole picture
- Impact analysis is guesswork under pressure

So change breaks things it shouldn't, and incidents take longer to trace.

The uControl approach

uControl derives topology from evidence. Insights discovers devices and reads NetFlow/IPFIX to materialise real traffic paths — no active scan, no credentials; Core assembles typed relationships and an interactive topology you can traverse hops from any asset.

How it works

Passive flow discovery Insights

Insights ingests NetFlow/IPFIX to materialise assets and their real communication paths without touching the device — ideal for OT and segmented networks.

Relationship modelling Core

Core detects and types the relationships across hardware, software and network — no scripting required.

Live topology map Insights

An interactive graph with flow-derived traffic edges that age out automatically, so the map stays true to current behaviour.

Impact & dependency analysis Core

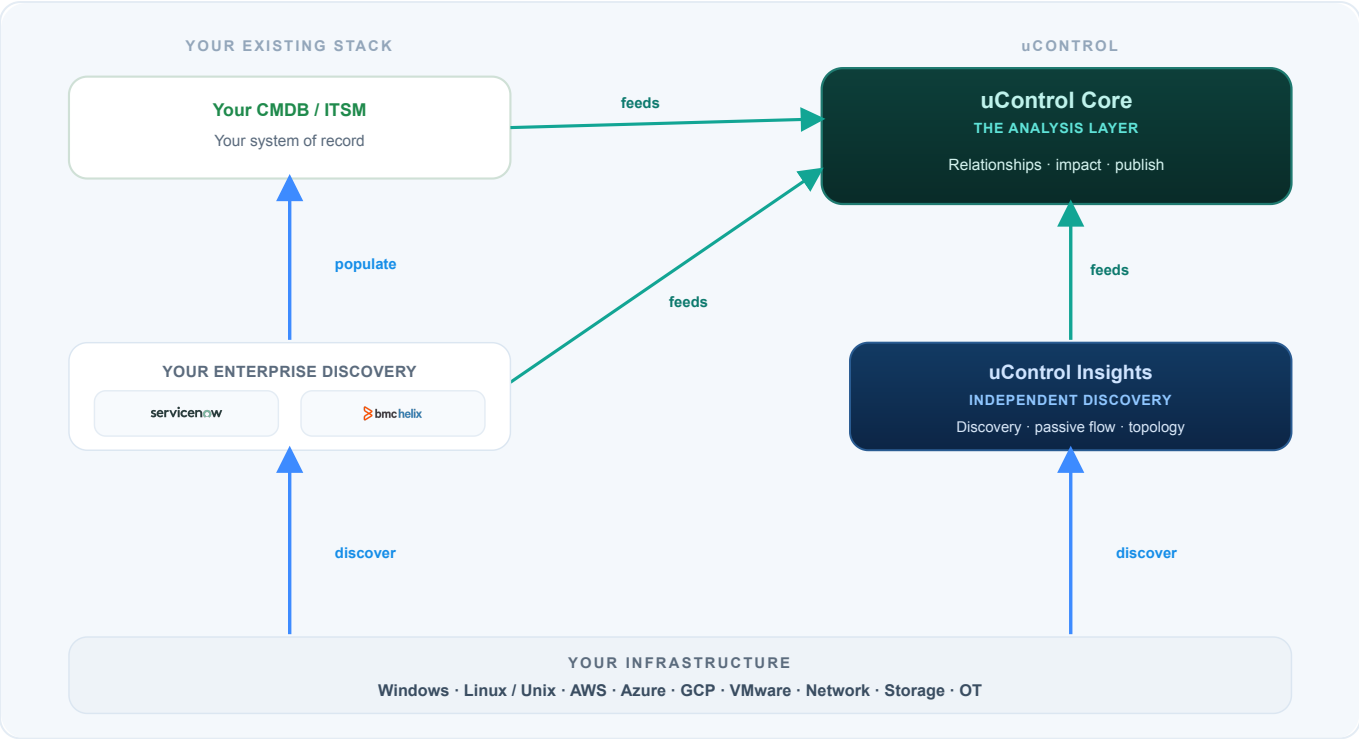
Traverse from any asset to see what depends on it, and what it depends on — before you change or during an incident.

Blind-spot detection Core

Core flags traffic to hosts that were never scanned, surfacing shadow-IP and coverage gaps.

Reference architecture

Your enterprise Discovery populates your CMDB, while uControl Insights discovers independently. uControl Core takes feeds from your Discovery, your CMDB and Insights to do the analysis.



Customer journey

1 Discover
Insights discovers devices and begins reading network flow.

2 Materialise
Passive flow surfaces assets and their real communication paths.

3 Model
Core assembles typed relationships and a live topology.

4 Analyse
Traverse impact and dependencies from any asset.

5 Maintain
Flow-derived edges age out so the map stays current.

Key capabilities

- ✓ Passive NetFlow/IPFIX discovery (Insights)
- ✓ No-code relationship detection (Core)
- ✓ Interactive live topology map (Core)
- ✓ Traffic edges that age out automatically
- ✓ Upstream/downstream impact analysis (Core)
- ✓ Shadow-IP & blind-spot detection (Core)
- ✓ OT-safe, credential-free path discovery
- ✓ Typed relationships across the estate
- ✓ Traverse from any asset in clicks

Business benefits

- ✓ Know what an outage or change will really hit
- ✓ Trace incidents faster with real paths
- ✓ Plan change against evidence, not diagrams
- ✓ See dependencies no scan-only tool finds
- ✓ Understand security blast radius
- ✓ Keep the map current automatically

Illustrative scenario

Segmented manufacturing network — illustrative

A team could not risk active scanning across sensitive production networks, and had no reliable dependency map.

uControl Insights read network flow to materialise the OT assets and their communication paths passively, and Core assembled a live topology — revealing cross-segment dependencies and shadow-IP hosts that active scanning had never safely reached.

Frequently asked questions

Do you need to actively scan sensitive networks?

No — passive NetFlow/IPFIX analysis materialises assets and paths with no active scan and no credentials, which is ideal for OT and segmented networks.

How does the map stay accurate?

Flow-derived traffic edges age out automatically, so the topology reflects current behaviour rather than a one-off snapshot.

Can I see what a change will impact?

Yes — Core lets you traverse upstream and downstream dependencies from any asset before you make a change.