uControl

USE CASE · DISCOVER

Discovery Assurance

Prove your CMDB is complete — and keep it that way.

How do you know your CMDB is actually complete?

Enterprise Discovery platforms such as ServiceNow Discovery and BMC Helix Discovery are very good at finding and maintaining Configuration Items. But they can only report on what they can reach. Devices on unknown subnets, systems missing credentials, segments behind firewalls and infrastructure that appeared after the last scan simply don't show up — and nothing flags their absence.

The result is a CMDB that looks complete but quietly isn't. Change management, automation and operational decisions are all built on data with blind spots nobody can see.

> **Discovery Assurance gives you a second opinion.**
>
> uControl **Insights** discovers your estate independently; uControl **Core** then continuously compares that view against your CMDB and reports the difference — coverage gaps, unreachable segments, stale records and newly appeared infrastructure — so you can trust your operational data, and prove it.

Executive summary

Most organisations treat CMDB completeness as an assumption rather than a measurement. Once enterprise Discovery is live and Configuration Items are flowing, coverage is rarely questioned — until an incident hits a system nobody knew existed, or an audit asks for evidence that can't be produced.

Discovery Assurance provides an independent, continuous check on that completeness. uControl **Insights** discovers the estate on its own terms; uControl **Core** reconciles what it finds against the CMDB and highlights the difference. Instead of trusting that Discovery found everything, organisations gain objective evidence of what is covered, what is missing and what has gone stale — turning CMDB confidence from a hope into a measurable, defensible position.

The business challenge

Enterprise Discovery is only as complete as the access it is given. Every real environment quietly works against that:

- New subnets and sites are added but never included in scan ranges
- Credentials expire, rotate or were never supplied for some systems
- Firewall and segmentation changes cut off previously reachable networks
- Cloud and virtual resources appear and disappear between scans

- Acquired or shadow infrastructure is never registered as a target

None of these produce an error. Discovery simply reports on what it can see, and the gaps stay invisible. The downstream cost is familiar: incidents on unknown assets, change requests that miss dependencies, automation that acts on incomplete data, and audits that can't be evidenced. The CMDB is trusted precisely because no one has an independent way to challenge it.

Why traditional approaches fall short

Where organisations do try to assure coverage, they usually do it from inside the same tool that created the gap. Discovery reports on its own scan results. Coverage is estimated from expected IP ranges that may themselves be incomplete. Periodic manual audits sample a fraction of the estate and are out of date the moment they finish.

The problem is structural: a Discovery engine cannot flag what it never reached. Asking it to prove its own completeness is asking it to find its own blind spots. Genuine assurance requires an independent source that discovers the estate a different way and continuously, then compares.

The uControl Insights approach

uControl **Insights** runs its own lightweight, agentless discovery across the environment — including passive network-flow analysis that surfaces assets from traffic alone, with no scan or credentials. uControl **Core** then reconciles that independent view against the enterprise CMDB and reports the delta:

- Assets uControl found that are *not* in the CMDB — coverage gaps
- CIs in the CMDB that uControl no longer sees — potentially stale or decommissioned
- Active subnets and segments outside any known scan range — dark space
- New infrastructure that has appeared since the last enterprise scan

Because it runs continuously, Discovery Assurance doesn't just produce a one-off audit — it keeps proving completeness as the estate changes.

How it works

Independent discovery

Agentless network discovery plus passive NetFlow/IPFIX analysis builds a picture of the estate that doesn't depend on the same credentials, ranges or reachability as the enterprise engine.

Coverage reconciliation

uControl compares its findings against the CMDB via API, matching on identity and surfacing what each source has that the other doesn't.

Gap & blind-spot detection

Assets live in traffic but never scanned, subnets outside known ranges, and credential-blocked systems are flagged as coverage gaps with the evidence behind them.

Drift & staleness

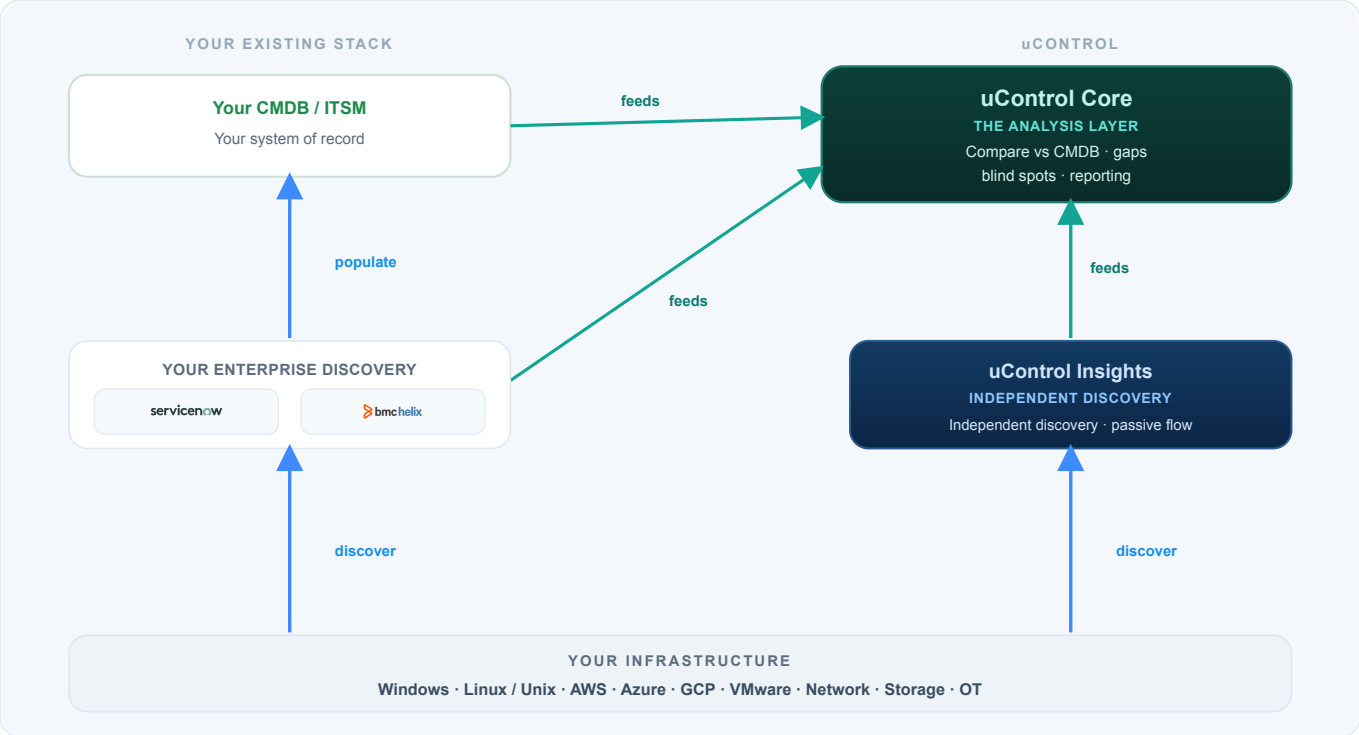
CIs the CMDB still lists but that no longer appear in discovery are highlighted as candidates for refresh or decommission.

Assurance reporting

Executive dashboards and alerts express coverage as a measurable figure over time, and notify owners — in the UI and on Microsoft Teams — when it slips.

Reference architecture

Discovery Assurance sits alongside enterprise Discovery as an independent check — it does not replace the CMDB or the engine that populates it.



uControl Insights becomes the operational intelligence layer that continuously validates the completeness of the data your CMDB depends on.

Customer journey

1. **Baseline**
   Run uControl Insights to build an independent view of the estate.

2. **Compare**
   Reconcile that view against the enterprise CMDB via API.

3 **Surface**
Review coverage gaps, dark space and stale records with the supporting evidence.

4 **Remediate**
Extend scan ranges, resolve credential and firewall gaps, and correct stale CIs.

5 **Assure**
Keep the comparison running so completeness stays measured as the estate changes.

6 **Report**
Share coverage trends and assurance evidence with stakeholders and auditors.

Key capabilities

- ✓ **Independent agentless discovery (Insights)**
- ✓ **Passive network-flow discovery (Insights)**
- ✓ **CMDB coverage reconciliation (Core)**
- ✓ **Coverage-gap and dark-space detection (Core)**
- ✓ **Unknown-subnet identification**
- ✓ **Stale / decommissioned CI detection (Core)**
- ✓ **Continuous assurance, not one-off**
- ✓ **Coverage scoring over time**
- ✓ **Executive assurance dashboards**
- ✓ **Teams alerts when coverage slips**
- ✓ **API comparison with ServiceNow and BMC Helix**
- ✓ **Evidence-ready audit reporting**

Business benefits

- ✓ **Measurable, defensible CMDB completeness**
- ✓ **Blind spots surfaced before they cause incidents**
- ✓ **Reduced risk in change and automation decisions**
- ✓ **Evidence ready for audit and compliance**
- ✓ **Coverage maintained as the estate evolves**
- ✓ **Greater stakeholder confidence in operational data**

Expected business outcomes

- Fewer incidents on unknown or unmanaged assets
- More reliable impact analysis and change planning
- Higher trust in CMDB-driven automation
- Faster, evidenced audit responses
- A CMDB that stays complete, not just complete on day one

Illustrative scenario

Financial-services organisation — illustrative

An organisation with a mature ServiceNow CMDB assumed coverage was effectively complete. Running uControl Insights alongside it as an independent check revealed several active subnets at two regional sites that had never been added to the Discovery schedule, plus a block of CIs that had not been seen in months.

The coverage gaps were added to the Discovery ranges and the stale records reviewed for decommissioning — closing blind spots that had gone unnoticed for over a year, and giving the team a coverage figure they could report with confidence.

How it complements ServiceNow

ServiceNow Discovery finds infrastructure and maintains Configuration Items. Discovery Assurance complements it by independently confirming that what should have been discovered actually was — feeding coverage gaps and stale-CI candidates back so the ServiceNow CMDB becomes measurably, not assumed, complete.

How it complements BMC Helix Discovery

BMC Helix Discovery delivers deep discovery and dependency mapping. Discovery Assurance adds an independent completeness check on top — validating coverage over time and surfacing the environmental blind spots that no single engine can flag about itself.

Frequently asked questions

Does Discovery Assurance replace our CMDB or Discovery engine?

No. It is an independent check that runs alongside them, proving completeness and surfacing gaps — it doesn't populate or replace the CMDB.

How does it find things enterprise Discovery misses?

It discovers a different way — agentless scanning plus passive network-flow analysis that surfaces assets from traffic with no credentials — so it isn't limited by the same ranges, credentials or reachability.

Does it work with both ServiceNow and BMC Helix?

Yes. It reconciles its independent discovery against either CMDB via API, and can run before, during and after an implementation.

Is this a one-off audit?

No. Assurance runs continuously, so coverage stays measured as the estate changes rather than being proven once and forgotten.