uControl

USE CASE · TRUST

Configuration Governance

Govern change to your CMDB with sign-off and an audit trail.

Automated CMDB updates are only an asset if you can trust — and prove — every change.

Uncontrolled write-back is how CMDBs lose credibility: silent changes, no ownership, no record of who changed what or why. Governance is what makes automation safe.

> **uControl governs every change.**
> uControl **Insights** provides the discovery evidence, and uControl **Core** routes every configuration change through owner sign-off, respects blackout windows, and records a full audit trail — no silent write-backs.

Executive summary

Configuration Governance makes CMDB change deliberate and defensible. Insights supplies the evidence; Core validates candidate changes, routes them to owners for confirmation, respects change policy, and logs every action.

You get the benefit of automated maintenance without surrendering control of your system of record.

The business challenge

Ungoverned CMDB change is risky:

- Silent write-backs no one approved
- No clear ownership of CIs and services
- Changes that ignore change-freeze windows
- No audit trail of who changed what
- Automation that erodes trust rather than building it

So teams either over-trust or switch automation off entirely.

The uControl approach

uControl puts owners in control. Insights and Core surface candidate changes with evidence; Core routes them to the right owner, enforces blackout windows and change policy, and records a defensible audit trail for

every write-back.

How it works

Owner sign-off Core

Owners confirm changes before the CMDB is updated — no silent write-backs.

Tag & drift rules Core

Rules identify candidate CIs for a service and flag deviations from your standard.

Change-policy controls Core

Blackout windows and controlled publishing respect your change process.

Full audit trail Core

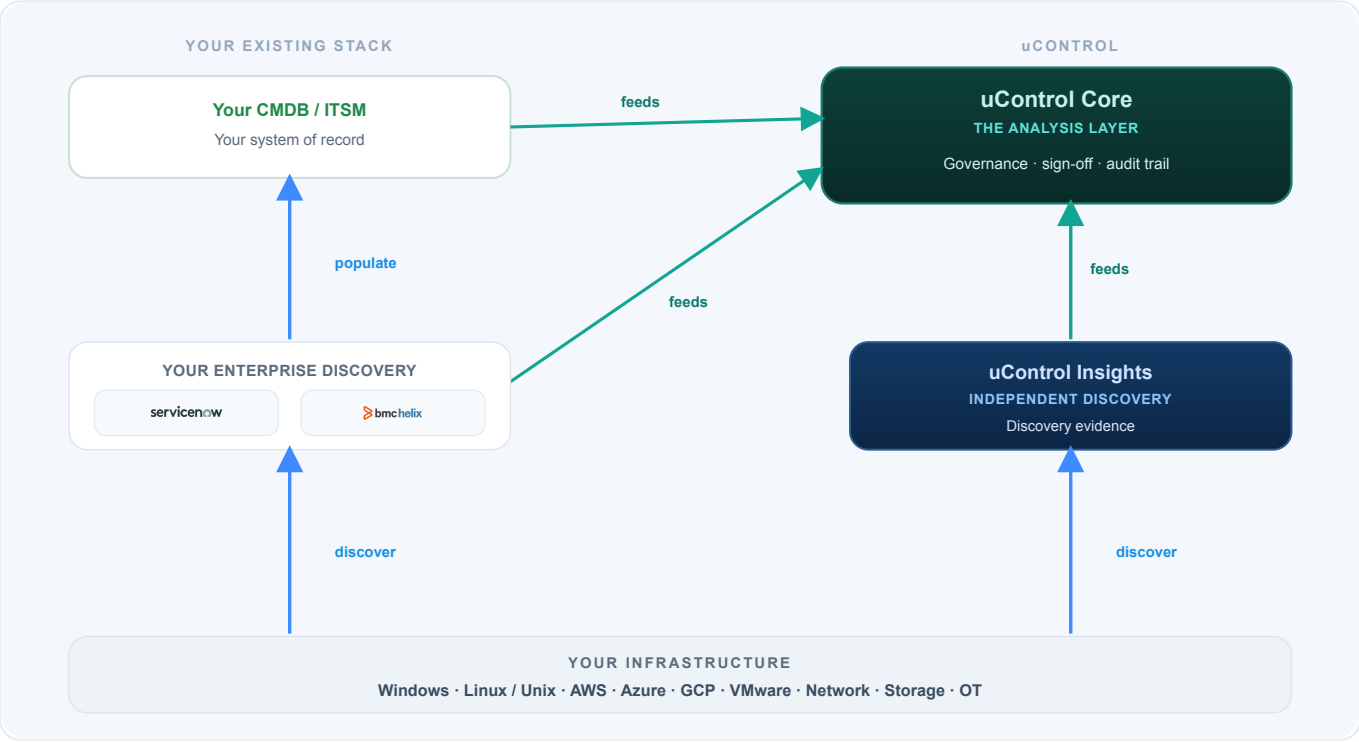
Every edit, submission and approval is logged with actor, timestamp and before/after value.

Discovery evidence Insights

Insights provides the discovery that justifies each proposed change.

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. **Detect**
   Core surfaces a candidate change with supporting evidence.
2. **Route**
   The change goes to the responsible owner.
3. **Review**
   The owner approves or rejects with a reason.
4. **Apply**
   Approved changes write back within policy windows.
5. **Evidence**
   Every action is logged for audit.

Key capabilities

- ✓ **Owner sign-off before write-back (Core)**
- ✓ **Tag & drift rules (Core)**
- ✓ **Blackout windows & controlled publishing (Core)**
- ✓ **Full audit trail (Core)**
- ✓ **Role-based access (Core)**
- ✓ **Discovery evidence per change (Insights)**
- ✓ **Service-ownership modelling (Core)**
- ✓ **Defensible change history**
- ✓ **Governed automation**

Business benefits

- ✓ **No silent, unapproved changes**
- ✓ **Clear ownership and accountability**
- ✓ **Change that respects your policy**
- ✓ **A defensible audit trail**
- ✓ **Safe, trusted automation**
- ✓ **Confidence for audit and compliance**

Illustrative scenario

Audited enterprise — illustrative

Auditors questioned how CMDB changes were controlled and evidenced.

uControl routed every reconciled change through owner sign-off within defined windows and logged each action with before/after detail — giving the organisation a defensible governance trail and the confidence to automate CMDB maintenance safely.

Frequently asked questions

Can changes be applied automatically?

Only with control — owners confirm changes before write-back, and blackout windows respect your change policy.

Is there a full audit trail?

Yes — every edit, submission and approval is logged with actor, timestamp and before/after value.

Who approves changes?

The CI or service owner — access is role-based and enforced, so only the right people can sign off.