

Unearthing the Ghosts in Your Org:
A Practical Guide to Auditing Salesforce Technical Debt

Mike Rogan
Wayfinder

Thank you to our sponsors:

Sunrise HCM
Plauti
TITAN
Trailblazer COMMUNITY
Really Good Emails
PHAROS
ForceClaw
Ascend TECHNOLOGIES
Nutrient
SoClo INVENTORY
COPADO
SurveyVista

ABOUT ME

What qualifies me to be your ghost hunter:

- Salesforce consultant, customer, alum
- In the ecosystem 17 years
- Focus on regulated industries and data strategy, AI readiness, and governance



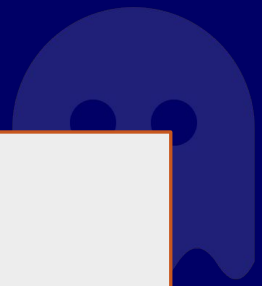
Mike Rogan
Founder, Wayfinder

THE HAUNTING BEGINS

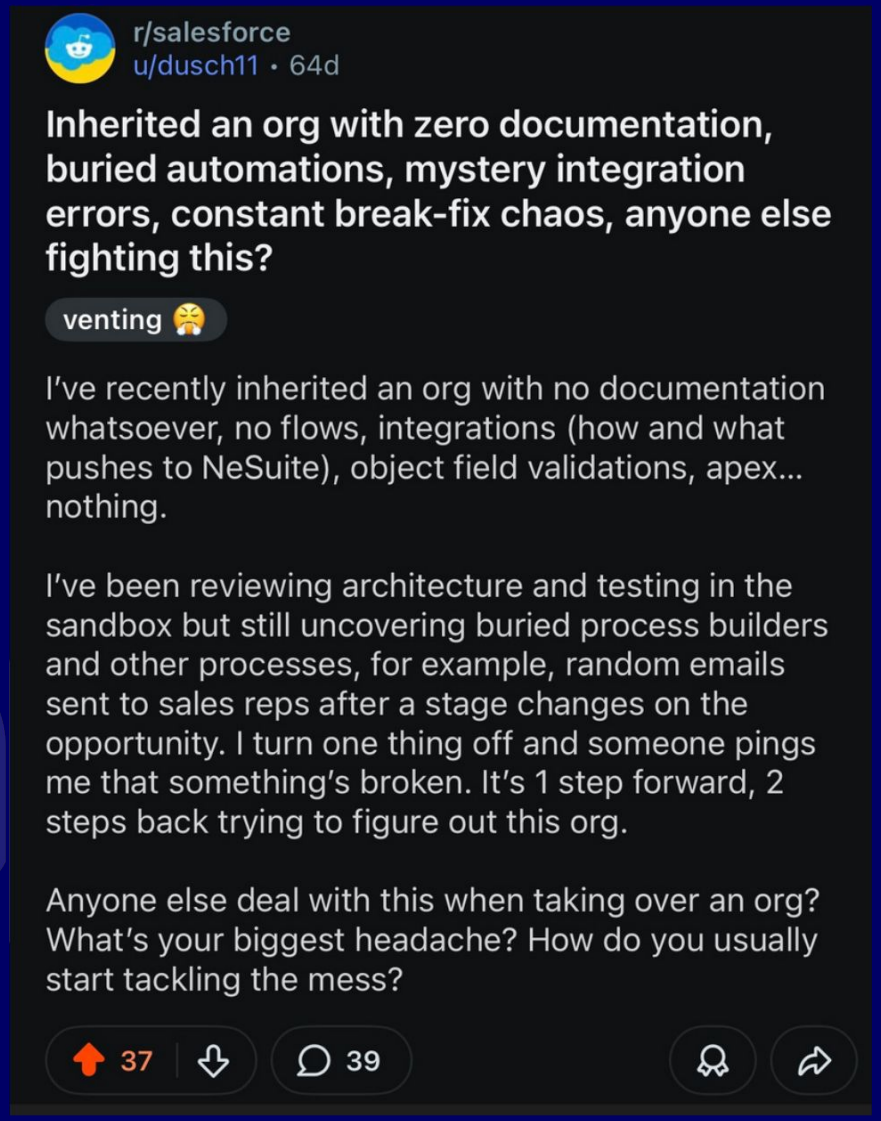
You didn't build this org.
But now it's your problem.

New job | Promotion | Acquisition | Consultants

No documentation. Half the builders are gone. The ghosts have moved into your org.



This session is the survival guide nobody gave you.


r/salesforce
u/dusch11 • 64d
Inherited an org with zero documentation, buried automations, mystery integration errors, constant break-fix chaos, anyone else fighting this?
venting 😤
I've recently inherited an org with no documentation whatsoever, no flows, integrations (how and what pushes to NeSuite), object field validations, apex... nothing.
I've been reviewing architecture and testing in the sandbox but still uncovering buried process builders and other processes, for example, random emails sent to sales reps after a stage changes on the opportunity. I turn one thing off and someone pings me that something's broken. It's 1 step forward, 2 steps back trying to figure out this org.
Anyone else deal with this when taking over an org? What's your biggest headache? How do you usually start tackling the mess?
37
39

YOU'RE NOT ALONE

That Reddit post isn't an outlier. It's the norm.

2%

say their org is clean and well-maintained

56%

say technical debt is their biggest challenge

31%

say it's severe enough to slow their day-to-day work

87% of us are living in a haunted house.

Source: Salesforce Ben 2026 Admin Survey

TODAY'S HUNT

Two hauntings. Forty minutes.

PART 1

The ghosts you inherited

Audit an org you didn't build using native tools, third-party apps and Claude.

~20 min

PART 2

The ghosts AI is creating

Agents, MCP connections and AI-built metadata and how to govern them.

~15 min

WRAP

Your toolkit + Q&A

What to do Monday morning. Then your questions.

~5 min

Both parts answer one question: is your org ready for AI?

MEET YOUR GHOSTS — AND WHAT THEY'RE COSTING YOU

What They Look Like	What They Cause
Abandoned data with no owner	AI hallucinations → lack of adoption/trust
Orphaned fields on every layout	Security gaps → audit failures, breach exposure
Integrations nobody remembers	Open doors → unauthorized access
Licenses unused for years	Storage and license bloat → surprise bills

Deloitte estimates technical debt eats **21–40% of IT spending.** Unmanaged ghosts get expensive.

THE GHOST HUNTING KIT

Three ways to catch a ghost:

01

Native Tools

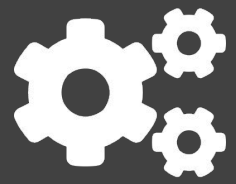
What you already have in Setup, now with AI built in



02

Third-Party Apps

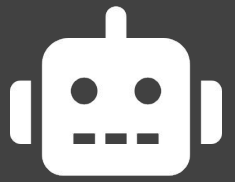
Purpose-built for the mess



03

GenAI + MCP

Governed access to your live org (be careful)



Run all three. Some ghosts only show up when you shine a different light.

Free tools already in Setup: These ghosts don't require a budget to find.

Tool	What It Finds
Security Center Essentials	NEW: free security dashboard with your Health Check score. One permission to turn on (EE and up).
Setup with Agentforce	NEW: ask the Setup agent about health score, licenses and storage. GA since May; needs Agentforce.
Setup Audit Trail	Who changed what, and when. Keeps only 180 days, so export it. Winter ’27 adds its own permission.
Connected Apps + External Client Apps	Forgotten integrations, stale tokens. New Connected Apps are blocked since Spring ’26; inventory the old ones.
Org Check	Automations, Apex, Profiles — including Process Builders still firing

First Ghost to Catch: Open Security Center Essentials today. One permission. You will find something haunting.

When the ghosts are too deep for native tools, you need something built for the mess.

Elements

Best for:

Process maps & documentation

Challenge:
Steep Learning Curve

Hubbl

Best for:

Org health & benchmarking

Challenge:
Diagnostic Focus

Metazoa

Best for:

Migrations & merges

Challenge:
Desktop App

4 Questions That Narrow It Down:

1. Do you need dependency mapping or just documentation?
2. What's your org complexity — objects, automations, users?
3. One-time audit or ongoing governance?
4. NEW: Does the vendor offer an MCP server yet?

Don't bring a thermal camera when a flashlight will do the job.

GENAI

AI is powerful but lacks access to tribal knowledge. Some ghosts only live in people's heads.

Feed AI the metadata and the human context. Let it help reconcile what's haunting your org.

Bad prompts summon the wrong ghosts.

❌ "Audit my production Salesforce org" is not a prompt. It's a séance.

SUMMONING CLAUDE — WITHOUT SUMMONING CHAOS

The pace of change is scary. Be a smart ghost hunter.

Claude can now reach your live org two governed ways. Both run under the permissions you already have.

Export or Connect → **Feed** → **Analyze** → **Act**

Salesforce Hosted MCP Servers

GA since April 2026 · Enterprise Edition and up

Servers ship disabled — an admin turns each one on in Setup

Salesforce in Claude

Open beta since Sept 2026 (Claudeforce)

An admin connects it once through AgentExchange; sales skills first to be enabled at launch, others follow

Export is still the safest start. You see what the LLM sees.

Connecting? Enable one read-only server, authenticate through an External Client App, and open access only when your governance is ready. ALWAYS start in sandbox!

BETTER TOGETHER: HEALTH CHECK + CLAUDE

The prompt that catches ghosts hiding in plain sight

PROMPT

```
"Here is my Salesforce Health Check export. My org supports a B2B sales team of about 80 users
and we use Experience Cloud for partner-facing deal registration. Please:
(1) Summarize what this score means in plain English — as if explaining it to a VP of Sales
who has never heard of Salesforce Health Check.
(2) Identify the three highest-risk items and explain the real-world business consequence of
each — not just that it fails a benchmark.
(3) Give me a prioritized action list: what I can fix today (no budget, no developer) vs. what
needs planning or escalation.
(4) Draft a two-paragraph executive summary I can paste into a Slack message to my CTO."
```

How this helps: One CSV. Four outputs. No code. No MCP. Claude turns a 62/100 score into a CTO-ready escalation, three named risks, and a same-day action list.

DEMO: LIVE ORG + CLAUDE VIA HOSTED MCP

The prompt that hunts ghosts without an export

PROMPT

```
"You're connected to my Salesforce sandbox through the read-only Hosted MCP server. Do not
create, update, or delete anything. Context: B2B sales team, ~80 users, solo admin, no change
management.
(1) Find active Standard users who haven't logged in for 90+ days. Group them by license —
what are we paying for that nobody uses?
(2) List active custom flows (no managed-package namespace) that have no description, and the
object each one fires on.
(3) Flag anything that is a security or compliance exposure, regardless of effort.
(4) Bucket every finding: Quick Win, Strategic, Low Priority, Don't Look Now. Then draft three
sentences for my CTO."
```

How this helps: Live answers under your existing permissions and you can check every query Claude ran. Remember: Use a read-only MCP!

BACKUP · DEMO 1

Here's what that looks like live.

Same read-only connection, same prompt, recorded in the sandbox.

Drop your 60–90 second screen recording here

Insert → Video → This Device. Set it to play automatically, full screen.

NOT EVERY GHOST IS WORTH CHASING

Quick wins buy you credibility. Strategic projects need the budget conversation.. This matrix is how you earn it.

	LOW EFFORT	HIGH EFFORT
HIGH IMPACT	**Quick Wins** High impact, easy wins Security gaps, license waste	**Strategic Projects** Plan carefully Complex automations, org cleanup
LOW IMPACT	**Low Priority** Low impact, low effort Document and defer	**Don't Look Now** High effort, low impact Not worth starting here



Feed your findings to Claude with org context → it scores, ranks, and tells you which ghosts to chase first.

AI readiness = clean data × governance

GOVERNANCE →

Locked, but cluttered

Controls in place, but AI reasons over bad data. Confidently wrong.

AI-ready

Trusted data. Owned agents. Automate here.

Ghost town

Where most inherited orgs start. Fix both, beginning with Part 1.

Haunted house in waiting

Great data, open doors. One forgotten token from a breach.

DATA QUALITY →

LOW EFFORT HIGH EFFORT

~20%

of admins consistently get strong executive support for tech debt

Salesforce Ben 2026 Admin Survey

Part 1 fixes the data axis.

Part 2 fixes the governance axis.

Nobody owns the risk. That's the real readiness gap.

PART 2 · THE NEW HAUNTING

AI is creating even scarier ghosts right now.

Governance is the AI readiness test most orgs are failing. Every agent and MCP connection is tomorrow's haunted house.

> *“If you can build things faster, that doesn't necessarily mean you're going to build better things faster.”*
>
> Paul Battisson, Salesforce MVP — in Salesforce Ben's “2026: The Year of Technical Debt, Thanks to Vibe Coding”

MEET THE NEW GHOSTS — AI-MADE, MACHINE-SPEED

What They Look Like	What They Cause
Agents nobody owns or governs	Actions nobody can explain
MCP servers switched on and forgotten	Doors left open to every connected client
Tokens from every AI tool someone tried	Year-long access by default, spiraling costs
AI-built flows, fields and prompts — no description	Next year's undocumented automation
One shared "AI" integration user	No attribution, maximum blast radius

AI doesn't invent new kinds of technical debt. It creates the old kinds at machine speed.

THIS ALREADY HAPPENED

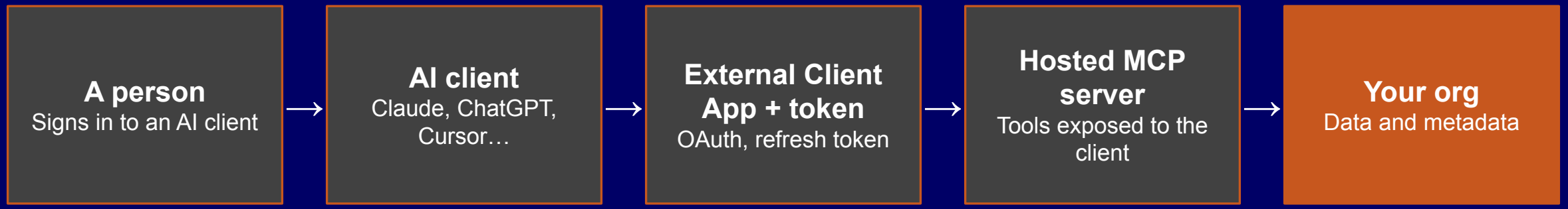
One forgotten integration. 700+ haunted orgs.

Mar–Jun 2025	Aug 8–18, 2025	Aug 20, 2025	Aftermath
Attackers sit inside the vendor's GitHub, then reach Drift and its customers' OAuth tokens	Stolen Drift tokens pull Salesforce data: contacts, opportunities, cases	Salesforce and Salesloft disable every Drift integration worldwide	700+ orgs affected. AWS keys, Snowflake tokens and passwords sitting in case notes went too.

The ghost transcended the org. It was a token for an integration nobody was watching. Every AI client you connect is one more.

HOW ONE MCP CONNECTION LEAVES RESIDUE

Every connection is a door. Access leaves a trail.



THE QUESTION TO ASK AT EACH HOP

Who approved this tool?	Is it on your allowlist?	Lives 1 year by default	Is it still switched on?	What did it read — or write?

Tools run with the connected user's permissions: CRUD, field-level security and sharing all apply. Your permission model is the last line of defense.

Prompt injection

Instructions hidden in a record, email or case that the agent reads — and obeys.

Spooky because: The attack arrives as data.

Tool poisoning

A malicious or careless MCP server whose tool descriptions steer the agent.

Spooky because: You trusted the tool, not the text.

Over-permissioned agents

The agent runs as a shared admin or integration user with View All or Modify All.

Spooky because: It can reach everything you can't explain.

Unchecked autonomy

Writes and deletes with no human checkpoint and no log anyone reviews.

Spooky because: Nobody notices until a customer does.



Agents inherit whatever access you hand them. Hand them the least required.

LOCK THE FRONT DOOR — HOSTED MCP HARDENING CHECKLIST

Straight from Salesforce's own guidance (Developers Blog, June 30, 2026):

1

One External Client App per AI client

Claude, ChatGPT and Cursor each get their own. Easier to scope, audit and kill.

2

Grant the mcp_api scope — not api

"Access Salesforce hosted MCP servers" only. Not the keys to the whole API.

3

Limit who can connect

App policy: only users with an "MCP Client User" permission set. Add IP ranges.

4

Shorten refresh tokens

Default is one year. Production deserves less.

5

Activate only the servers you need

They ship off. Keep it that way for everything you aren't using.

6

No shared integration users

Every person signs in as themselves, so every action has a name on it.

You can't govern what you can't see. Four places to look:

Where to look	What you'll see
Event Monitoring	Event Log File Browser → API Total Usage → filter API_CLIENT_CATEGORY = SALESFORCE_HOSTED_MCP. Check USER_NAME, CLIENT_IP, STATUS_CODE.
OAuth Usage (Setup)	Every app holding tokens, and who holds them. Revoke one token — or all of them — per app.
Setup Audit Trail	Metadata changes by the people who connect AI tools. AI-built changes show up as theirs.
Transaction Security Policy Accelerator	Salesforce Labs app (March 2026): prebuilt real-time policies for data loss, access and integrations. Needs Shield Event Monitoring.

Ghost-hunter habit: Review the MCP event logs on the same monthly cadence as Security Center Essentials.

THE AGENT GOVERNANCE FRAMEWORK

Name it. Scope it. Watch it. Retire it.



NAME IT	SCOPE IT	WATCH IT	RETIRE IT
Every agent and AI client has a human owner, a purpose and its own External Client App. *Watch for: Agentic Identity (agents as first-class identities, announced Dreamforce '26)*	Least privilege. Read-only first. mcp_api scope. A human approves before writes and deletes. *Start with the read-only server; earn your way to write.*	Event Monitoring for MCP traffic. OAuth Usage monthly. Agentforce Observability for your own agents. *Watch for: MCP Risk Scores on servers Agentforce consumes (announced)*	Every pilot gets an end date. Revoke tokens, deactivate servers, remove permission sets. *Quarterly: Anything without an owner gets exorcised.*

If you can't name the owner, it's already a ghost.

DEMO: 2 HUNT THE GHOSTS YOUR AI LEFT BEHIND

The prompt that audits the auditors

PROMPT

```
"You're connected to my org through the read-only Hosted MCP server. Do not change anything.
(1) Query OauthToken: list every app holding tokens — app name, user, last used, use count. Flag
anything unused for 60+ days.
(2) Query SetupAuditTrail for the last 30 days, limited to users who hold tokens for AI tools.
Group changes by user and action.
(3) List flows and permission sets created in the last 30 days with no description, and who created
each.
(4) Find users with API Enabled plus Modify All Data or View All Data. Which of them also connect
AI tools?
Return a ghost list: owner, risk, and one recommended action each."
```

How this helps: The ghosts AI creates are queryable. Hunt them with the same connection that made them: read-only.

BACKUP · DEMO 2

Here's what that looks like live.

Same read-only connection, same prompt, recorded in the sandbox.

Drop your 60–90 second screen recording here

Insert → Video → This Device. Set it to play automatically, full screen.

AI READINESS SCORECARD — CAN YOU ANSWER YES?

- ☑ Do you know every AI tool that holds a token to your org?
- ☑ Does each one have its own External Client App?
- ☑ Is nobody connecting through a shared integration user?
- ☑ Are production refresh tokens shorter than a year?
- ☑ Are only the MCP servers you use switched on?
- ☑ Can you see MCP traffic in your event logs?
- ☑ Does every agent have a named human owner?
- ☑ Do AI-built flows and fields get descriptions before deploy?



Every "no" is a ghost in the making. Fix the cheap ones this week.

YOUR GHOST HUNTING TOOLKIT — TAKE THIS HOME

1

Run the native sweep today

Security Center Essentials, Setup Audit Trail, Connected Apps and ECAs, Org Check — these ghosts are in plain sight.

2

Match the tool to the haunting

Elements, Hubbl, or Metazoa — get a trial to shine the right light on the right ghost. Don't overdo it.

3

Feed Claude evidence, not wishes

Export the files — or connect read-only through Hosted MCP. The ghost is in the data, not the prompt.

4

Govern the agents before they haunt you

One ECA per client, mcp_api scope, short tokens, an owner for every agent. Watch the logs.

5

Name your poltergeists. Prioritize based on business impact.

You're not just auditing — you're making the case to leadership for remediation.

RESOURCES + CONTINUE THE GHOST HUNT

You inherited the haunting. You don't have to live with it.

Tools in the kit:

Elements	Hubbl	Metazoa
Claude	Hosted MCP	Event Monitoring

Deck &
Bonus Materials

Connect:

Mike Rogan | mike@wayfinder.cc | /in/mikerogan

Got ghosts? Let's talk.

Q&A

Unearthing the Ghosts in Your Org:
A Practical Guide to Auditing Salesforce Technical Debt

Mike Rogan
Wayfinder

#2026-breakout-unearthing–the-ghosts-in-your-org-how-to-audit-salesforce-technica

Thank you to our sponsors:

Sunrise HCM
Plauti
TITAN
Trailblazer COMMUNITY
Really Good Emails
PHAROS
Nutrient
SoClo INVENTORY
ForceClaw
Ascend TECHNOLOGIES
COPADO
SurveyVista

NORTHEAST DREAMIN' · OCTOBER 29, 2026

Unearthing the Ghosts in Your Org:

A Practical Guide to Auditing Salesforce Technical Debt

BONUS SLIDES

Mike Rogan | mike@wayfinder.cc | /in/mikerogan

NORTHEAST DREAMIN' · OCTOBER 29, 2026

Unearthing the Ghosts in Your Org:

A Practical Guide to Auditing Salesforce Technical Debt







Your org has ghosts. This is how you find them.

Mike Rogan | mike@wayfinder.cc | /in/mikerogan

WAYFINDER

Via Salesforce CLI (metadata as XML)

Metadata Type	What Claude Does With It
Flows	Plain-English summary, dead paths, risk flags
Apex Classes	Governor limit risks, hardcoded IDs, deprecated APIs
Permission Sets	Over-permissioning, Modify All / View All exposure
Validation Rules	Logic docs, conflicting rules, deleted field refs

Via CSV Export (no CLI required)

Export Source	What Claude Does With It
Setup Audit Trail	High-risk change patterns, external user flags
License Manager	Unused licenses by last login date
Connected Apps / ECAs	Forgotten integrations, over-scoped OAuth, migration list
Login History	Shared credentials, inactive-but-authenticated users

Third path: Salesforce Hosted MCP Servers (GA April 2026) let Claude query your org. Start with the read-only server — and be careful.

FIVE WAYS CLAUDE HELPS YOU FLUSH OUT GHOSTS

Use Case	What You Feed It	What You Get Back
Flow Documentation	*Flow XML*	Plain-English summary, risk flags, ready-to-paste description
Apex Review	*Apex class file*	Plain-English explanation, developer escalation recommendation
Audit Trail Analysis	*Setup Audit Trail CSV*	Risk-prioritized change summary, ready to present
Tribal Knowledge Capture	*Interview notes + Flow XML*	Reconciled process doc, discrepancies flagged automatically
Prioritization	*Findings list + org context*	Scored action list, quick wins, executive escalation items

WHAT CLAUDE CAN'T DO — KNOW YOUR TOOLS, KNOW YOUR LIMITS

✕ Can't save you from yourself

Live access is real now: Hosted MCP (GA) and Salesforce in Claude (beta) both act under your permissions. Use guardrails — start read-only.

✕ Can't watch the ghost move

Reads Flow logic but can't observe how it behaves against live data

✕ Can't be 100% accurate

Treat all outputs as first drafts — validate before you act on them

✕ Can't haul unlimited luggage

Very large orgs may require chunking exports into batches

Claude is the ghost detector — not the ghost hunter.
MCP handed it a key to the front door. You still decide which rooms it can enter.

KEEP THE GHOSTS FROM COMING BACK

You can stop the haunting.

Every Flow gets a Description.

Name it. Describe it. Future admins won't inherit a mystery.

Every change gets a record.

Slack thread, ticket ref, Setup comment. No undocumented changes.

Retire the unsupported.

Process Builders and Workflow Rules move to Flow — on purpose, one at a time.

Monthly native sweep.

Security Center Essentials plus a Setup Audit Trail export. The trail only keeps 180 days.

Every integration is an ECA.

No new Connected Apps. Inventory the old ones before they become ghosts.

Claude maintains living docs.

Run it at audit time and as the org evolves. Ghosts love stale documentation.

The best ghost is the one that never gets a chance to haunt.