Case Study

Five minutes of access. Years of hidden risk, surfaced in days.

A real Salesforce org, an anonymised look, and why it matters for yours

In a few days, Nextview shows where your Salesforce org carries security risk, technical debt and AI readiness gaps — ranked by severity and effort.

nextview...

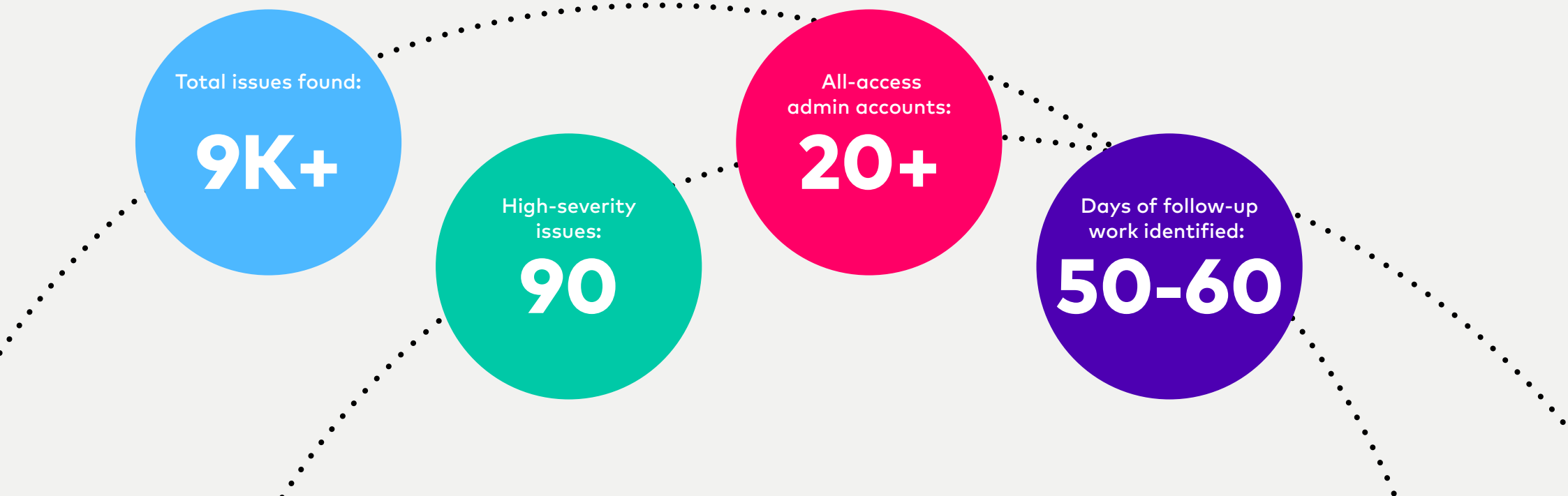
salesforce

The Org Scan is performed by Nextview specialists, combining scan data with Salesforce architecture expertise. It's not a self-service tool; it's an expert-led assessment with prioritised output.

The setup

A major European leisure travel company had been running Salesforce for years. They asked us a simple question: is our *Salesforce platform an accelerator, or an anchor?* They suspected things had grown messy over the years, but nobody could say how messy. Or what it was costing them. So we ran an Org Scan on their live environment. The admin spent about two minutes granting access. Within days, we had a complete picture.

Here is what the numbers looked like when te results landed.



The headline: a "Very Good" org that was quietly carrying real risk

The org scored 71 out of 100. A healthy "Very Good" rating, in line with comparable organisations. On paper, nothing was on fire. That is exactly why this case is instructive: even a well-run org was sitting on issues that no one had visibility of.

8,959 issues identified.
90 of them high-severity.
7 of those fixable fast.

The point was never the volume. It was the speed of impact. By separating signal from noise, we isolated the small number of items that genuinely threatened security and stability — and the handful that could be fixed immediately for an instant improvement.

For leadership, the scan changed the discussion. Instead of debating whether Salesforce needed attention, the team could see which risks mattered, which fixes were quick, and which improvements belonged on the roadmap.

What was hiding in plain sight

Security exposure that mattered.

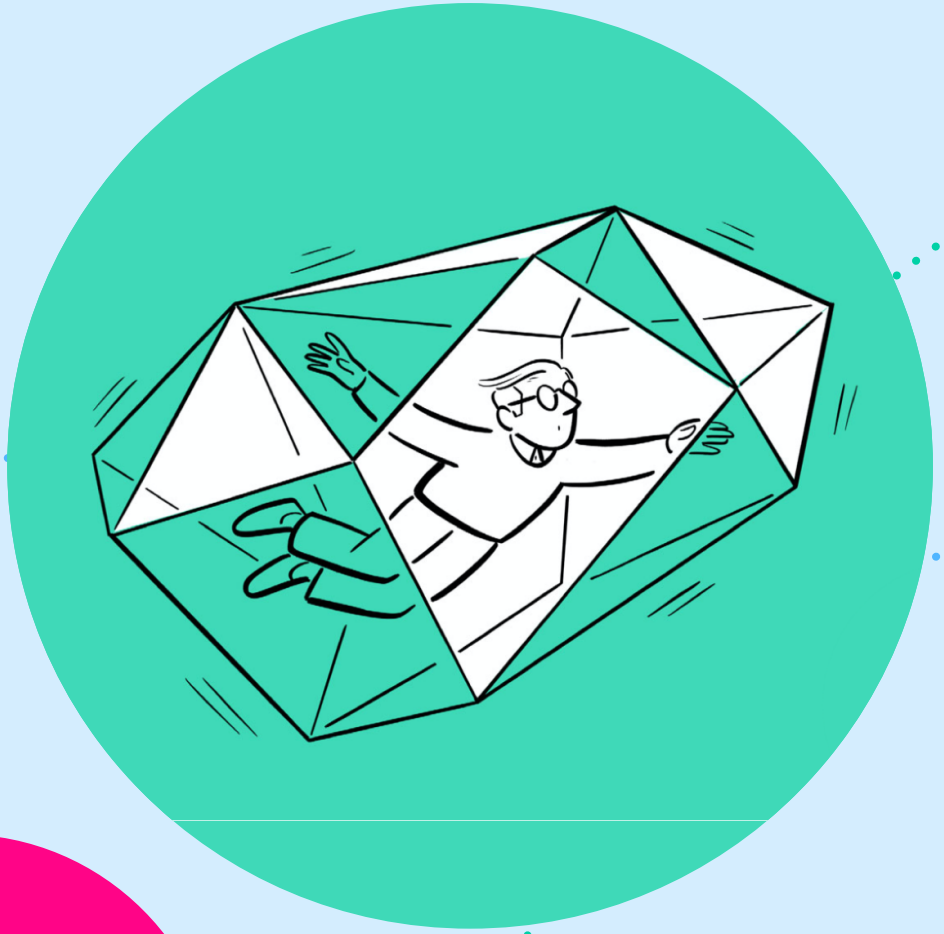
Connected apps set to self-authorise, widening the attack surface beyond what Salesforce recommends. Apex code vulnerable to SOQL injection, a route to data exfiltration. Missing clickjack and HttpOnly protections, leaving the door open to phishing and session hijacking. Real risks, hiding in plain sight.

Technical debt accumulating silently

Apex classes running on outdated API versions. Installed packages out of date, some never security-reviewed, some deprecated entirely. Each one a quiet liability that no one had time to address.

Clutter that slows everyone down

Custom fields nobody uses, old integration fields from tools long gone. "Ghost fields" drag on performance and bury the data that actually matters. Every user feels it, no one knows where to start.



The part that changes the conversation: what it would take to fix it

Findings on their own create anxiety. The value is in the answer to *"so what do we do?"* From the scan, we built a costed, three-month roadmap: every recommendation sized into fixed work packages, quick wins first, the long tail of technical debt scheduled after. No guesswork, no open-ended estimate, no scope creep. Because the plan is built on metadata facts, not assumptions.

What this unlocks

Remediation is not the end goal. It is the entry point. Once the org reaches a clean, governed baseline, a very different set of conversations becomes possible.

Agentforce readiness.

AI agents need a secure, well-structured org to operate in. Closing permission gaps and cleaning metadata is not optional groundwork. It is the prerequisite for any responsible AI deployment.

Faster release cycles.

Removing deprecated packages and outdated Apex reduces the blast radius of every Salesforce seasonal release. Fewer compatibility surprises means faster, safer deployments.

Adoption recovery.

Cleaning up ghost fields and unused page layouts directly improves what sales reps and agents see every day. Fewer distractions means higher data quality and better reporting.

Audit and compliance confidence.

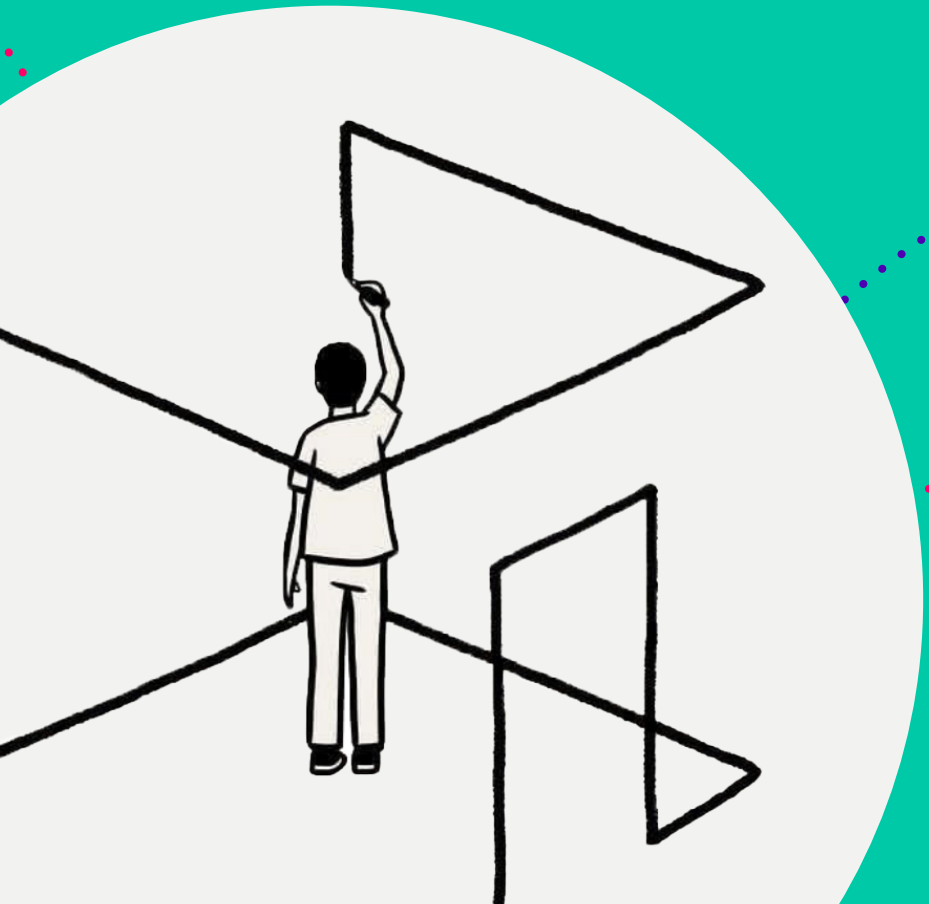
An org with known, governed permissions and a clean installed-package inventory is an org that can answer hard questions from security teams, auditors, or regulators. Quickly and accurately.

The Agentic Era isn't coming. It's here.

This organisation, like most, wanted to move on to Agentforce. But AI is only as trustworthy as the data and metadata beneath it. An org cluttered with technical debt and loose permissions doesn't make AI an asset. It makes it a liability waiting to happen.

The scan doubled as an AI-readiness baseline: a precise view of exactly what to clean up before you let agents or your customers interact with your Salesforce data.

The question isn't whether you'll deploy AI. It's whether you'll do it on a foundation you trust.



What you expect

A clear view of security exposure
AI readiness signals for Agentforce
Quick wins separated from roadmap items

nextview...

salesforce

This was their org. Curious what we'd find in yours?

The first Org Scan is free. Your admin grants access in minutes. Nextview returns a prioritised view of your org within days.

Request your Org Scan → https://nextviewconsulting.com/nextview-advantage