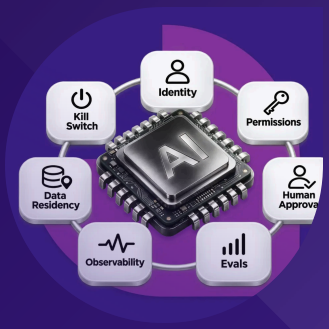
Owned Intelligence in your Microsoft tenant

For heads of IT at utility and energy services contractors: the architecture, data flow and access model, before anything connects.



WHAT YOUR COMPANY GETS

1
Every job's margin before the month closes
Month-End WIP Review, read-only to accounting

2
The right answer for whoever's asking
Employee Answers, scoped by Entra and row-level security

3
One question across every company
The Owner's View, with source rows

4
Your IT team runs your systems. We bring the AI.
Managed team, handed over to your engineer

Runs in your Azure tenant
Your subscription, your billing, code in your repositories from day one.

Permissions from Entra and Power BI

SOC 2 Type II compliant development

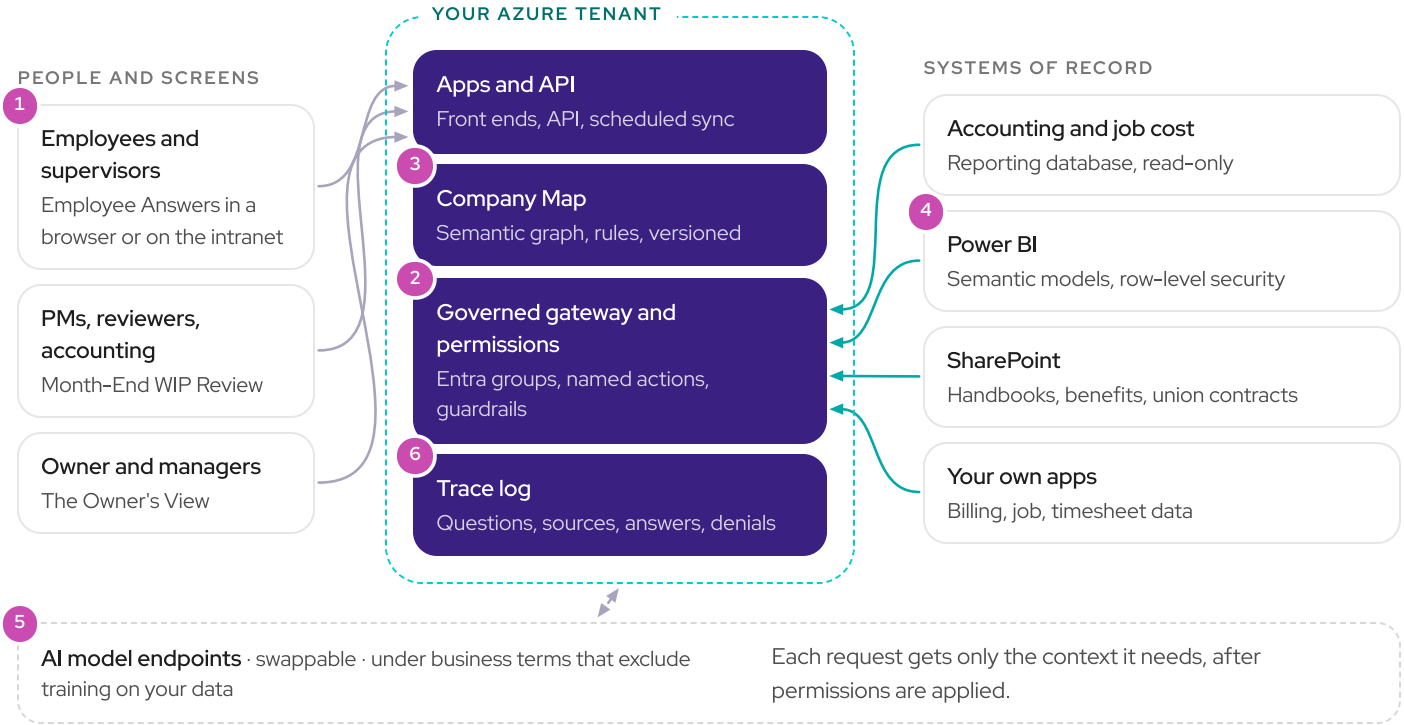
The short version for your security review

Systems of record	Your accounting, payroll, billing and job systems stay the source of truth, unchanged. The layer is read-only to them.
Connections	We read through connections you already have: Power BI semantic models, the accounting system's reporting database, SharePoint, Microsoft Graph and Entra. Nothing new is built into your systems.
Identity	Microsoft Entra single sign-on with your conditional access and MFA policy. Entra security groups set role, company, union and location.
Data access	Power BI queries run on behalf of the signed-in person, so row-level security applies. Documents are filtered by company, role and union before retrieval.

Items marked CONFIRM are confirmed with engineering for your deployment.

ARCHITECTURE AND DATA FLOW

How a question moves through the system

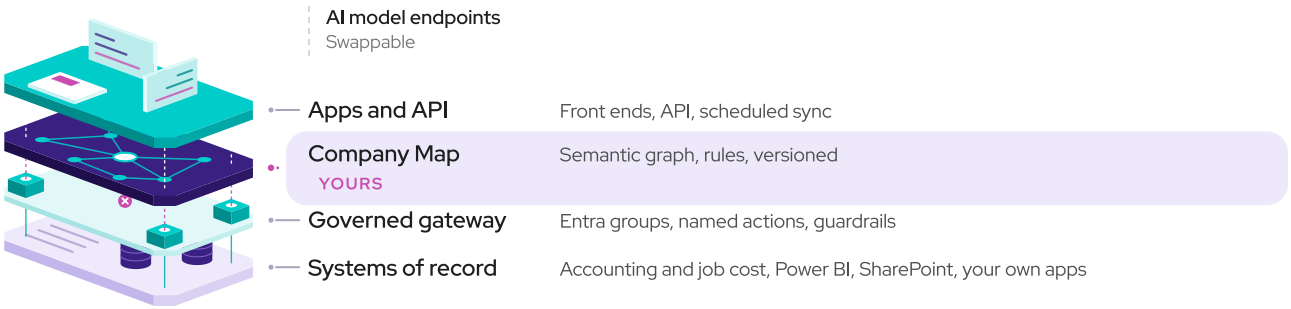


Each hop, in order

1. A person signs in with Microsoft Entra. The layer reads their security groups: role, company, union, location.
2. Guardrails check the question and send sensitive topics to fixed routes (page 5).
3. The scope is resolved first: which companies, jobs, periods or records the question covers, within what this person may see.
4. Data is read on behalf of the person: Power BI under their row-level security, documents filtered by company, role and union.
5. The model drafts an answer from that context. Numbers come from your systems, never from the model.
6. The answer returns with its sources. Everything above is written to the trace log.

Month-End WIP Review is different by design

It contains no AI. It reads the accounting and billing systems on a schedule, for example every 15 minutes. Its own database holds only accruals, statuses, comments, flags and the audit trail. Accounting gets an export file at period lock.



DEPLOYMENT IN YOUR AZURE TENANT

What runs where

COMPONENT	TYPICAL AZURE SERVICE	NOTES
Front ends	Azure Static Web Apps	On your domain
API and sync workers	Azure Container Apps with a container registry	Scaled for month-end load
App database	Azure SQL or Azure Database for PostgreSQL	Stores the app's own records only
Cache	Azure Managed Redis, where needed	Slow-changing lookups
Document search index	A vector index under your account CONFIRM	Tagged by company, role and union
Tracing	An LLM tracing tool such as Langfuse, under your account CONFIRM	Every request and answer
Secrets and monitoring	Key Vault, Azure Monitor and Log Analytics	Alerts to your team and ours

The exact services are written into your architecture document in Validate and reviewed with you before Build.

IDENTITY AND ACCESS

Entra groups decide role, company and union

A mapping table turns Entra groups into a role, companies and union status. Your admins change access in Entra, never in the app.

ENTRA GROUP (EXAMPLE)	ROLE	COMPANIES	UNION SCOPE
AI-HR-Payroll	HR	All	All locals
AI-PeopleOps	People operations (no pay rates)	All	All locals
AI-Mgr-CompanyB	Company manager	Company B	Company B's locals
AI-Supervisor	Supervisor (direct reports via Power BI)	Own company	Own crews' locals
AI-Union-LocalA	Employee modifier	Own company	Local A only

Example group names. Your groups and the mapping table are agreed with your IT and HR leads.

- Offboarding in Entra removes access on the next sign-in
- Users never get direct access to Power BI datasets through the layer; queries run through the API
- NineTwoThree staff access is limited to named engineers, granted by your IT CONFIRM
- Service accounts and app registrations each get least privilege
- Any feature or the whole layer can be switched off by your administrator

HOW PERMISSIONS ARE ENFORCED

Enforced by your systems, not by a prompt

Power BI on behalf of the person asking

The app exchanges the person's sign-in for a Power BI token on their behalf. Every Power BI call runs in that person's context, so your row-level security decides which rows come back.

Documents filtered before retrieval

Handbooks, benefits guides and union contracts are tagged with company, role and union when they're indexed. Retrieval filters on those tags first, so a union employee's question never reaches another local's contract.

CONFIRM WITH ENGINEERING

The governed gateway: the AI never writes database code

This is how we build the layer. Every read goes through the governed gateway:

- Named actions only, from an approved list, for example `job_cost_lines(job, period)` or `sick_time_balance(employee)`
- Allowed fields, values and limits validated on every call
- Run as the person asking, so their Entra groups and Power BI row-level security apply
- A named person approves anything that writes; every call is logged with who asked and what came back

Your architecture document lists the named actions for your deployment and any read paths outside the gateway. Our engineering lead confirms both before you sign off.

What each role sees, as an example

ROLE	BALANCES AND HOURS	PAY RATES	JOB COST	POLICIES AND CONTRACTS
HR and payroll	All companies	All companies	None	All
People operations	All companies	Never	None	All
Company manager	Own company	Own company	Own company	Own company
Supervisor	Direct reports	Never	Own jobs	Own crews' locals
Employee	Self	Self	None	Own company and local

Illustrative. Your permission matrix is written with HR in harness sessions and checked with the Who's Asking Test: 50 questions asked as six people. A correct answer that shows too much fails.

GUARDRAILS

Two checks before an answer, and fixed routes for sensitive topics

- A moderation check and a policy check run on every question; if either fails, the request stops
- Harassment and discrimination go to HR; injuries go to your safety portal with a 911 reminder
- No financial or legal advice; personal issues route to your employee assistance program
- Questions outside the person's scope are refused before any data is read
- Your HR and IT leads own the route list and can change it

LOGGING AND TRACING

- Who asked, when, and from which app
- Which records and documents were read
- What the model returned, latency and cost per request
- Guardrail decisions and permission denials
- Month-End WIP Review audit trail: who changed what, from and to
- Exportable for your auditor

DATA HANDLING

DATA	STORED IN	RETENTION
Accounting, payroll and job records	Your systems. Read when needed. Whether any data is copied, and where, is agreed in IT review.	Your policy
Policy documents	SharePoint, plus a search index under your account	Removed from the index when deleted in SharePoint
Month-end review records	The app's own database in your tenant	Your policy CONFIRM
Questions, answers and traces	The trace log in your tenant or account	Set by you CONFIRM
Model requests	Sent to the model endpoint for the request	Per the provider's business terms

Model terms

Models run under business terms that exclude training on your data. You hold the provider account and pay it directly, with no token markup. Models swap without a rebuild. Your architecture document lists the providers and their terms CONFIRM.

YOUR SOC 2 AUDIT

Change control and repository access your auditor will ask about

AUDITOR'S QUESTION	HOW THE BUILD ANSWERS IT
Who has access to the code?	Repositories sit in your GitHub organization. You grant and remove NineTwoThree engineers by name.
Can one person push to production?	No. Changes go through a pull request with a second reviewer, then QA and UAT environments, then production CONFIRM.
How is infrastructure changed?	As code, in your repository, through the same review path.
Who can reach production endpoints?	Your IT controls network access and private endpoints in your tenant.
How are AI changes tested?	An evaluation suite runs questions by role before release; the Who's Asking Test is re-run after model or permission changes.
Where is it documented?	A site book and design documents in your repository, kept current through handover.

AI-ERA FRAUD

The same AI that fakes a supplier's invoice is already on your people's phones

Contractors move a lot of money to subcontractors, suppliers and payroll, so payment-change fraud and fake invoices are the sharpest risk.

$3,046,598,558

Businesses and individuals reported $3,046,598,558 in business email compromise losses to the FBI in 2025.

FBI IC3 2025 Internet Crime Report

76%

of U.S. organizations experienced attempted or actual payments fraud in 2025, and 74% were affected by business email compromise.

AFP 2026 Payments Fraud and Control Survey

78%

Three in four knowledge workers use AI at work, and 78% of those AI users bring their own AI tools.

Microsoft and LinkedIn 2024 Work Trend Index

Three defenses your IT team owns

- Phishing-resistant sign-in, such as passkeys or security keys (CISA, Oct 2022)
- A call-back rule before changing bank details or resetting access (FBI IC3 PSA I-120324-PSA, Dec 3, 2024)
- Offline, encrypted backups you have restored from (CISA #StopRansomware Guide, Sept 2023)

What we own on the AI side

A written AI policy with the call-back rule, one governed company assistant so work leaves personal chatbot accounts, and permission-scoped answers with every request logged. We don't sell security monitoring, and we don't claim to prevent fraud or phishing.

HANDOVER AND EXIT: YOU ALREADY OWN IT

YOUR AI TEAM, RUN BY NINETWOTHREE

FROM DAY ONE
In your tenant and repositories
Code, Company Map, prompts, evaluations, traces

→

MANAGED
NineTwoThree runs it
A fixed monthly fee, and we carry the delivery risk

→

PAIRING
Your engineer pairs with ours
Takes over the monitoring dashboards and runbooks

→

HANDOVER
Your engineer runs it
Exit means removing our engineers' access
CONFIRM

COMMON SECURITY QUESTIONNAIRE ANSWERS

QUESTION	ANSWER
Do you have SOC 2?	Our development practices are SOC 2 Type II compliant. Documentation on request CONFIRM.
Does the AI write database queries?	We build it so the AI calls named actions through a governed gateway instead CONFIRM .
Is data encrypted?	In transit, yes. At rest, per the Azure services in your architecture document CONFIRM.



It runs in your own Microsoft tenant.

Book a technical session

Your head of IT with a NineTwoThree engineer, 45 minutes, before anything connects. Then a paid validation sprint on your own data, before Build. ninetwothree.co

Book a Job Trace

Confirm before sending (internal: remove this box before the kit goes to a customer)

- Governed gateway: confirm with engineering that the deployment reads only through named actions, and list any read paths outside the gateway (for example model-written Power BI queries under row-level security).
- Search index and tracing: confirm where they run (inside the tenant or under the client's own SaaS account) per deployment.
- Pull-request review, QA and UAT path: confirm for every repository, including infrastructure.
- Staff access: confirm the named-engineer process and timing of removal at handover.
- Model providers and their data terms: list per deployment.
- Default retention for traces and app records; encryption at rest per service.
- SOC 2 documentation: confirm what can be shared and under what NDA.

Microsoft, Entra, Power BI, SharePoint and Copilot are trademarks of the Microsoft group of companies. Other product names are trademarks of their owners. NineTwoThree is an independent company and is not affiliated with or endorsed by Microsoft or any accounting software vendor. This kit describes NineTwoThree's standard approach; your architecture document from Validate governs your deployment. General guidance, not legal or security advice. Copyright © 2026 923 Digital, LLC.