



The only Workday *Innovation* Partner you will ever need.

50+

Customers

1,000,000+

Workers using our apps

100+

Countries

FIVE PRODUCTS ON THE WORKDAY MARKETPLACE

Security Plus

Governed role assignments, access reviews & audit evidence. Assign. Review. Prove.



360 Feedback

Multi-rater feedback cycles run end to end inside Workday.



AI Goals Management

AI-assisted goal drafting, alignment and review in Workday.



CLEAN, Data Quality for Workday

Finds, reports and corrects data quality issues across your tenant.



Continuous Education Tracker

Tracks certifications, credits and renewal deadlines per worker.



Security governance for Workday, run inside Workday

Assign. Review. Prove. Do it all without export, external sync or a second identity store to track and maintain.

Every assignment under a business process

- Request, approve, justify, done
- Roles & security group memberships via configurable BPs
- Tracking business justification and full history
- Revocation runs through the same governance

Temporary access that expires by itself

- Flag an assignment temporary and set Assign Until date
- Access is removed when the date passes
- Security freeze for leave, investigation or audit
- Frozen access restores automatically

Reviews & crucial-role certification

- Scheduled reviews route to owners as Workday inbox tasks
- Attestation recorded on the event
- Quarterly or annual campaigns on a four-level criticality scale
- Flagged items feed straight into revocation

Segregation of duties, before and after

- Rule library of conflicting groups & domain permissions
- Starter set for common HCM, Payroll and Financials conflicts
- Every new request checked before approval
- Documented, time-boxed waivers that reopen on expiry

Detection: anomalies, drift, one score

- Dormant access and privilege outliers against job-profile peers
- Roles granted outside the governed process
- Critical-role drift across Sandbox, IMPL and Production
- One Security Check score, trackable quarter over quarter

Answer "why do I have access?"

- Compare two workers' security side by side
- Ask why anyone has access to any report, task or domain
- Get the exact granting chain and full membership path
- Answers in a minute, not an expert investigation



This app is reviewed and approved by Workday experts, confirming compliance with Workday standards, alignment with the product roadmap, and the Incubane's ability to support the app.

What do teams use it for?

SOX and ISO audit readiness

Walk into fieldwork with evidence instead of a war room. Every assignment, review, certification and exception already carries ID, timestamp, justification and approval chain, reportable through Workday reporting. Access-control expectations from ISO 27001 A.5.18 and NIST AC-2 map to running processes, not policy documents.

Crucial-role certification programs

Classify your security groups on a four-level criticality scale, then certify the holders of the top levels quarterly with a named sign-off. Uncertified items escalate and surface as findings. The control does not just exist; it demonstrably operates.

Joiners, movers, leavers without residue

Access follows people through role changes instead of accumulating. Privilege outliers against job-profile peers, dormant access signals and delta reviews keep standing privilege shrinking over time, and the manager's team view makes who-holds-what a routine glance instead of a request to IT.

IMPL drift and consultant access

Implementation tenants accumulate elevated access that quietly diverges from Production. Multi-tenant comparison for critical roles turns that drift into findings with owners, and time-boxed temporary assignments mean consultant access ends when the project does, by itself.

THE WORKDAY SECURITY CHECK

**Can you answer
these in under a
minute?**



How do you assign Workday roles today?



How do you know nothing unusual sits in your IMPL tenant?



How do you make sure access is removed when people change roles?

**If any answer
involves a
spreadsheet
v12finalFINAL, let's
talk.**

How does it work inside Workday?

Runs on your existing security groups and business process framework. App security domains map to your Workday security groups, so there is no new access model to build or audit.

One system of record

Assignments, reviews, findings and evidence live in your tenant as Extend business objects. Worker, org and manager data are read live. No integration to build, no data to duplicate, no second identity store.

Your security model governed, not replaced

It passes review as Workday configuration, not as a new vendor platform. And because it is a security product, every administrative act inside Security Plus is itself a recorded event.

AI on your terms

You connect the language model you control. Prompts are configurable, AI is off by default, and the agent is human-in-the-loop. Nothing is sent to Incubane. An AI Fact Sheet ships with the contract.

Stable across every Workday release

We regression-test the app against both biannual Workday releases before they reach you, and feature updates are included in the license. No version-lag risk, no surprise breakage.

What's included: Core and Platinum

EVERY SUBSCRIPTION INCLUDES THE FULL APPLICATION	Core	Platinum
Full application, all features included	✓	✓
Regression tested every Workday release	✓	✓
Service level agreement	Standard	Enhanced, negotiable
Product roadmap input	1 vote	3 votes
Quarterly business review	Group session	1-1 with a Managing Partner
Implementation team	Delivery team	Delivery team + senior product team
Post go-live configuration support	On request	Up to 40 hours per quarter
Security Agent	—	✓

Security Plus vs standard Workday - Comparison

CAPABILITY	Standard Workday	Incubane Security Plus
Security request workflow	E-mail and tickets, outside Workday	✓ Configurable business process with mandatory justification
Temporary access	Revoked by memory	✓ Auto-expiry on a date, plus temporary security freeze
Access reviews	Manual clean-ups, evidence by hand	✓ Scheduled, routed, attested in the Workday inbox
Crucial-role certification	Not supported	✓ Quarterly or annual campaigns with named sign-off
Criticality classification	Not native	✓ Four-level scale, fully configurable per customer
Segregation of duties	Point-in-time delivered reports	✓ Rule library, preventive checks at request, scheduled scans, waivers
Anomaly detection	None	✓ Assignment and sign-on signals, ungoverned-change alerts
Tenant comparison	Manual, tenant by tenant	✓ Multi-tenant comparison for critical roles, drift as findings
"Why do I have access?"	Expert investigation	✓ Access Explainer traces the exact granting chain
Audit evidence	Assembled by hand, every audit	✓ Every event carries ID, timestamp, justification, approval chain

Standard Workday covers the basics. Our app covers the rest, which is what Audit and IT teams actually ask for.



Ready to see it in your Workday?

[Book a live demo](#)