



DIGITAL PERSONAL DATA PROTECTION • DPDP ACT 2023

# Threatsys DPDP 360

## Compliance Console

Combined feature, workflow and use-case platform for enterprise DPDP operations.

• MADE IN INDIA • MADE FOR INDIA

+91 9668200222    support@threatsys.co.in    www.threatsys.co.in



# Your all-in-one cybersecurity suite, extraordinarily unified

AI SOC, AI GRC, AI CRM, AI AppSec, AI DPDP and AI LMS - unified under a single roof. One platform, one login, one intelligence layer powering every layer of your security posture.



## ***AI-Native Security Operations Console***

AI SIEM, SOAR, FIM and XDR fused into one AI-driven response system with threat hunting and an agentic SOC assistant.



## ***Every risk. One record. All-in-one control.***

Risk, policy and audit converged into one self-updating compliance cycle - audit automation, scoping and evidence.



## ***AI-Mastered DPDP Suite***

Consent, rights, grievance SLAs, notices, DPIAs, vendor risk and evidence for India's DPDP Act, 2023.



## ***Effortless AI-powered delivery management***

Every signal and interaction turned into one relationship - projects, clients and delivery unified in one place.



## ***Automated Application Security Testing***

SAST, DAST, API testing and PTaaS with validated, evidence-backed findings and no false positives across code and cloud.



## ***Building India's cyber-ready workforce***

Enterprise cybersecurity training, compliance awareness and placement-linked skilling through practical learning.

# This deck goes deep on DPDP 360



**AI-Mastered DPDP Suite.** Privacy law decoded and delivered end-to-end - the Made-in-India engine for compliance with India's Digital Personal Data Protection Act, 2023.

SOC 360

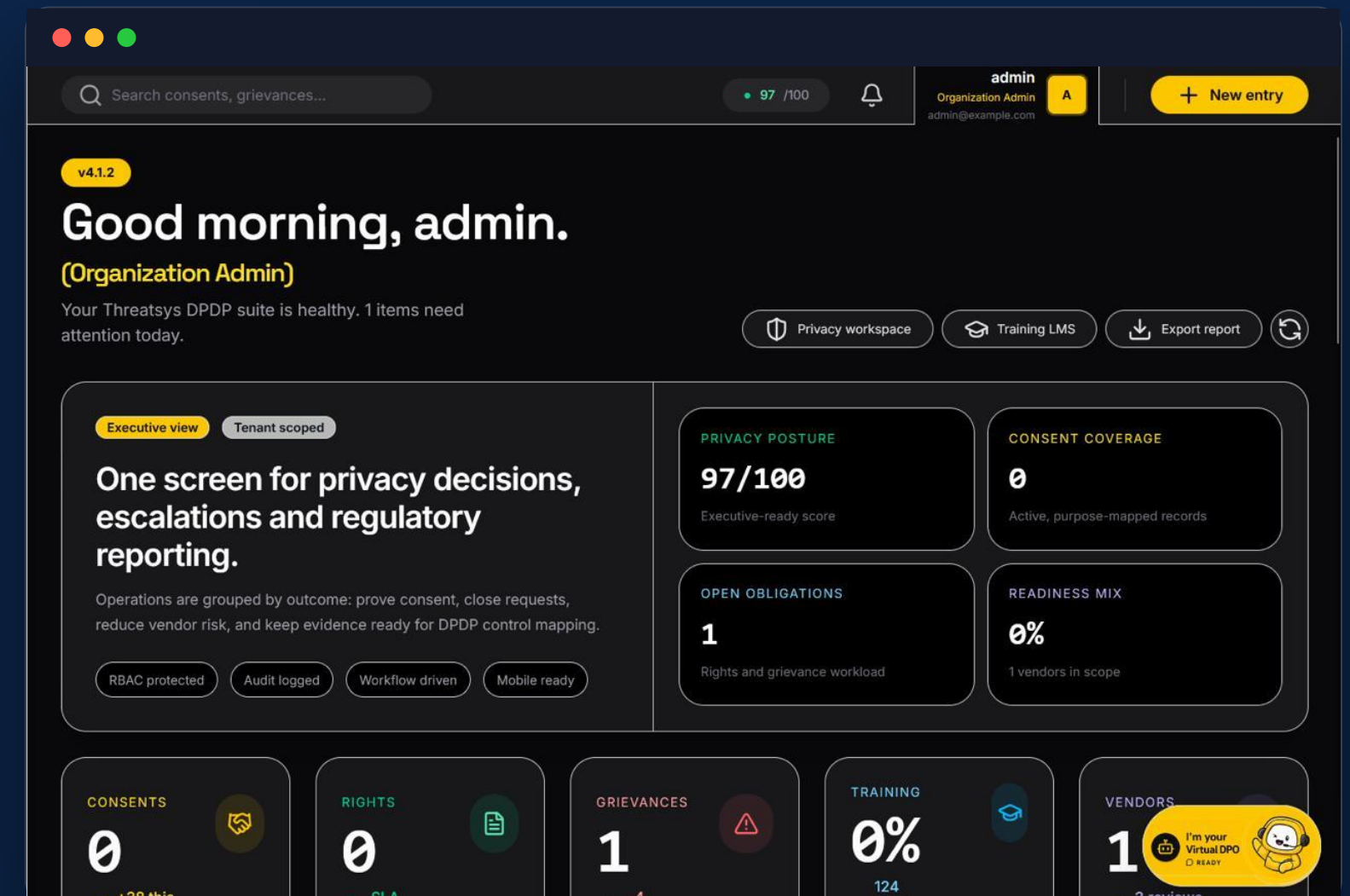
GRC 360

**DPDP 360**

CRM 360

AppSec 360

LMS 360



## OUR UNIQUE STRENGTH

# Made in India, Made for India.

A homegrown DPDP platform engineered to the letter of India's Digital Personal Data Protection Act - not a re-badged foreign privacy tool retrofitted to Indian law.

### Data residency in India

Personal data and evidence stay within Indian jurisdiction and tenant control.

- ✓ Tenant-scoped storage
- ✓ RBAC-protected access

### Aligned to the DPDP Act

Consent, notices, rights and breach duties mapped directly to Indian law.

- ✓ DPBI-ready evidence
- ✓ 23-language notices

### Local build & support

Indian engineering team, language coverage and responsive in-country support.

- ✓ 4-hour expert response
- ✓ CERT-In empanelled team

**CERT-In empanelled**

**PCI QSA authorised**

**Trusted by 1,000+ organisations**

**Noida · Mumbai · Bengaluru · Pune**

# One platform for features, workflows and use-cases

Combined feature, workflow and use-case platform for enterprise DPDP operations.

01

Setup

Presets

02

Operate

DPDP work

03

Automate

n8n hooks

04

Prove

Audit pack

Tenant-aware

RBAC, organization scope and audit baseline.

Board-ready

Risk posture, reports and evidence export.

20+

MODULES

14

WORKFLOWS

24x7

AUDIT

Built on the proven GRC foundation:

Authentication · RBAC · Tenant management · Audit logging · Notifications · Evidence vault · Reports · Automation

# Legal requirements, turned into daily operations

Threatsys DPDP 360 converts DPDP legal requirements into operating workflows, automation, evidence and executive visibility.

01

## Are we compliant?

Obligations, controls, risk scores and readiness reporting.

Obligation map

Readiness score

02

## Can we prove it?

Tamper-evident audit logs, evidence vault and exportable packs.

Hash proof

DPBI-ready

## Business outcomes

Faster audit readiness

Lower privacy operating risk

Repeatable DPDP workflows

Evidence-backed governance

Clear executive reporting

03

## Within SLA?

Consent, grievances, rights, incidents and escalations.

Escalation clocks

Officer queues

04

## Can leadership see risk?

Executive command center, heatmaps and trend analytics.

Live posture

Board export

## ABOUT THE DPDP ACT 2023

India's data protection law: process personal data only on free, informed, purpose-specific consent; honour data-principal rights and grievances within set timelines; report breaches to the DPBI - with penalties for non-compliance. The platform maps each duty to a workflow and defensible evidence.

ONE WORKSPACE, EVERY ROLE

# One tenant-aware workspace for every team

Privacy, legal, security, HR, vendors, auditors and leadership - each sees only the work, evidence and analytics within their permissions and tenant scope.

PR

## Privacy Office

Consent, rights, grievances, DPIA, notices and evidence ownership.

- Consent
- Rights
- DPIA

LE

## Legal & DPO

Obligation mapping, policy approvals and board-ready reporting.

- Obligations
- Policies
- Board report

SE

## Security & GRC

Incidents, vendor controls, processors, transfers and audit proof.

- Incidents
- Vendors
- Audit proof

HR

## HR & Training

Awareness courses, quizzes, certifications and recertification.

- Courses
- Quizzes
- Certificates

BU

## Business Teams

Templates for consent, grievance, vendor and industry onboarding.

- Templates
- Onboarding

LA

## Leadership / Auditor

Privacy score, vendor risk, SLA posture, incidents and trends.

- Dashboards
- Trends
- Exports

# Setup • Operate • Automate • Prove

The simplest way to explain the platform before drilling into modules.

|                                                                                                    |                                                                                                                |                                                                                                        |                                                                                                             |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| <div><div>01</div><div>Setup</div><div>Industry presets, templates, maturity checklist</div></div> | <div><div>02</div><div>Operate</div><div>Consent, grievances, rights, vendors, training, incidents</div></div> | <div><div>03</div><div>Automate</div><div>n8n queues, webhooks, notifications, escalations</div></div> | <div><div>04</div><div>Prove</div><div>Audit logs, evidence vault, regulatory controls, reports</div></div> |
| Tenant profile                                                                                     | Operational tasks                                                                                              | Queue jobs                                                                                             | Control map                                                                                                 |
| Industry setup                                                                                     | Escalations                                                                                                    | Retry history                                                                                          | Evidence packet                                                                                             |
| Workflow templates                                                                                 | Evidence links                                                                                                 | Webhook audit                                                                                          | Timeline                                                                                                    |
| Audit baseline                                                                                     | Executive visibility                                                                                           | Failure alerts                                                                                         | Board report                                                                                                |

From months to weeks. Pre-configured workflows accelerate DPDP readiness without rebuilding privacy operations.

# Complete DPDP module landscape

15+ purpose-built modules on one audit-logged operating layer - built on the proven GRC foundation of authentication, RBAC, tenant management, notifications and evidence vault.

### Governance

Accountability & control mapping

---

- Executive command center
- Onboarding wizard
- Obligation control mapping
- Processing register / RoPA
- PIA / DPIA workflows
- Policy & 23-language notices

### Consent & rights

Cryptographic proof & SLAs

---

- Consent management
- Immutable consent ledger
- Purpose management
- Data Principal rights
- Grievance SLA engine
- Cookie & tracker consent

### Operations & risk

Day-to-day privacy delivery

---

- PII discovery & data intake
- Privacy officer workspace
- Awareness training LMS
- Vendor privacy risk
- DPA management
- Incident & breach

### Platform services

Shared audit-grade backbone

---

- Tamper-evident evidence vault
- Notification service
- n8n workflow automation
- Integration hub
- AI compliance copilot

**15+** DPDP modules

**23** Notice languages

**24x7** Audit readiness

# Executive privacy command center

A board-ready view of privacy posture, risk, SLA health and evidence readiness.

82

Privacy score

Org readiness

11

Open grievances

SLA monitored

7

Vendor risks

High-risk queue

91%

Training

Completion

Executive outputs

Privacy score trends

SLA & breach exceptions

Vendor risk posture

Exportable board report

Live board-ready dashboard →

DPDP

COMPLIANCE MODULE

Dashboard

ROLE WORKFLOW

01 DPO Workspace

02 Executive Dashboard

03 Organization Onboard...

04 Data Inventory

05 Consent Manage...

06 DSR Management

07 Grievance Manag...

08 ROPA Management

09 Retention & Deleti...

10 Vendor Risk

Executive Analytics

admin / Organization Admin

Dashboard

Executive DPDP dashboard

Acme Data Fiduciary governance posture for admin. Board-ready privacy score, risk exposure, decisions, owners and evidence signals by executive profile.

90 days

All departments

Refresh

Export

Board

Risk, accountability, decisions

CEO

Business posture, exposure

CIO

Systems, data, retention

CISO

Incidents, vendors, safeguards

DPO

Rights, consent, compliance

Compliance

Controls, evidence, gaps

Auditor

Evidence, audit readiness

ENTERPRISE SCORE

80%

Overall privacy operating posture

CUSTOMER TRUST

100%

Consent compliance and complaint pressure

VENDOR EXPOSURE

1/1

Third-party concentration risk

TRAINING

100%

Employee awareness completion

CEO command brief

Generated 22 Jul 2026, 12:08 pm. Curated for Business posture, exposure.

Board action register

Owners, urgency and target dates for executive follow-up

# Consent lifecycle and purpose tracking

Used when processing must be tied to valid, current and purpose-specific consent decisions.

- 01

Grant

Capture metadata
- 02

Ledger

Hash proof
- 03

Notify

Event hook
- 04

Renew

Expiry rule
- 05

Withdraw

Revoke use
- 06

Archive

Export evidence

Stored metadata

Identity & timestamp

Purpose & legal basis

IP, device, language

Version & retention

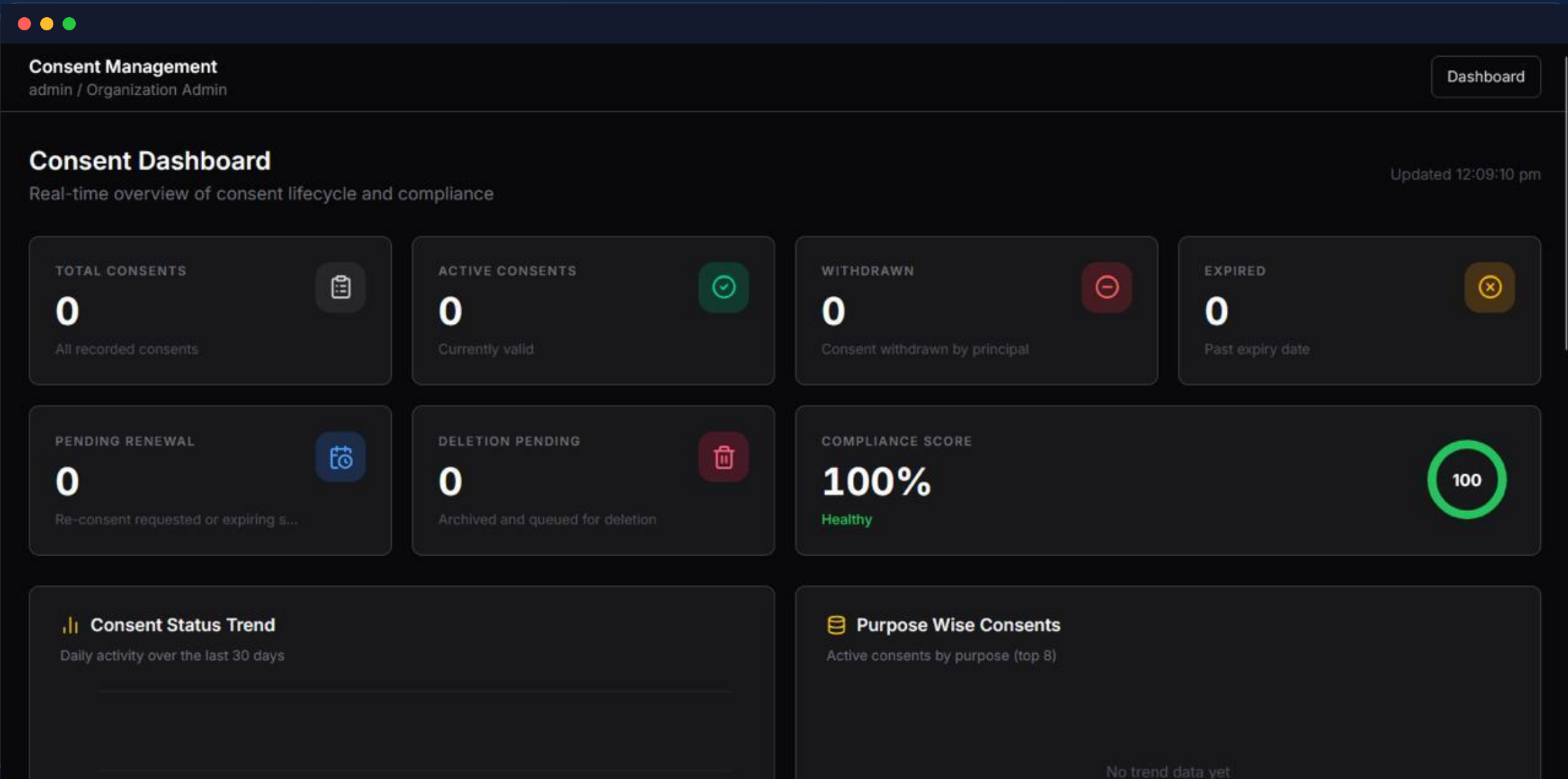
Outputs

Consent status APIs

Purpose-wise analytics

Re-consent campaigns

Tamper-evident snapshots



# Data discovery: the foundation of compliance

Discover and classify personal data across every system to build a comprehensive PII inventory - the foundation every consent, RoPA, rights and risk workflow depends on.

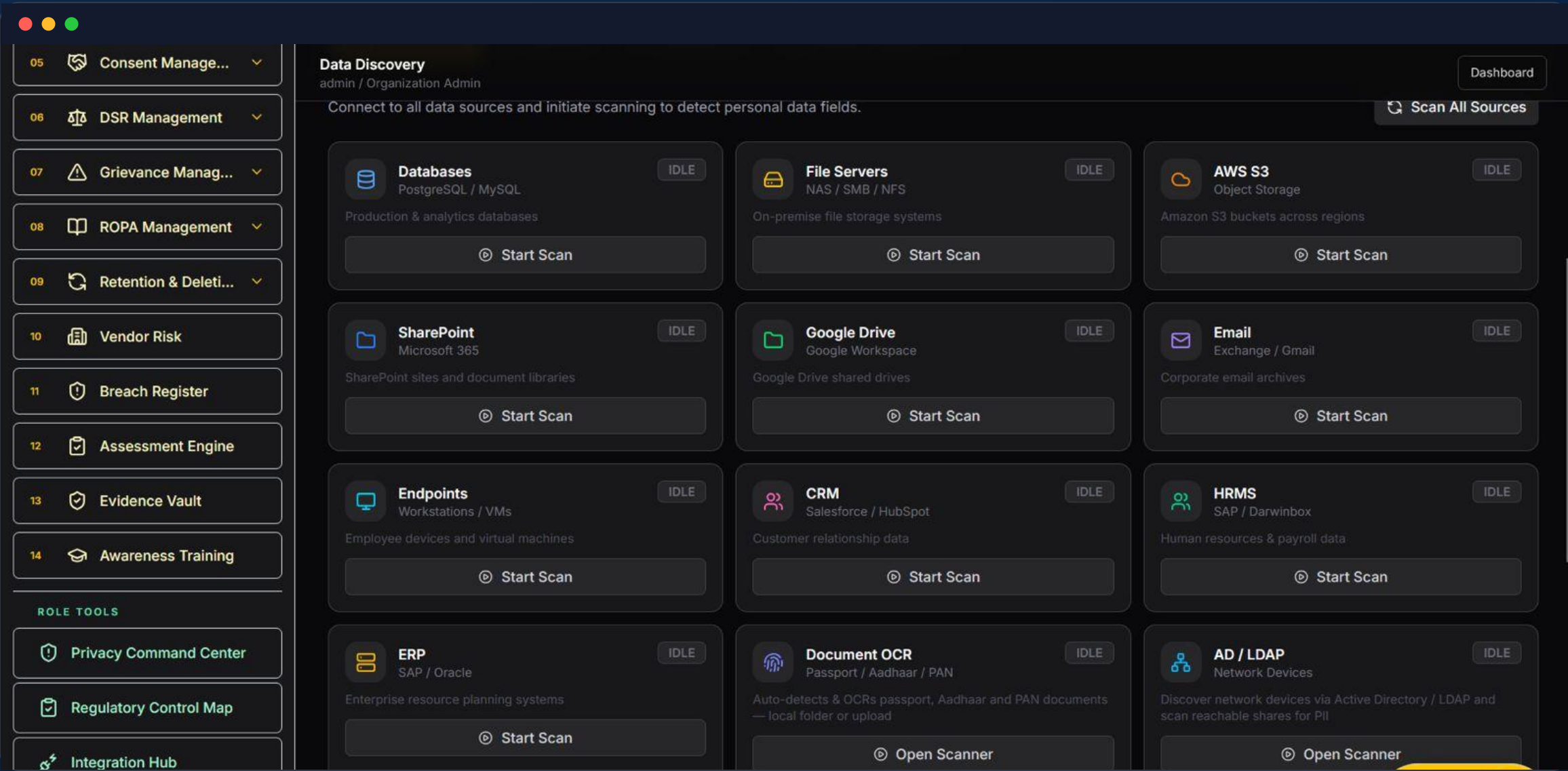


Sources covered

Databases & file servers  
SaaS & cloud apps  
Email & collaboration  
CRM, HRMS & ticketing

Outputs

Classified PII inventory  
Data map & flows  
Sensitivity scoring  
RoPA-ready records



# Rights and grievance SLA operations

- 01 Receive · Portal/API
- 02 Verify · Identity
- 03 Assign · Owner queue
- 04 SLA · Timers
- 05 Escalate · Matrix
- 06 Close · Evidence pack

| Request type         | Platform action                                             | Evidence created   |
|----------------------|-------------------------------------------------------------|--------------------|
| Access / correction  | Verify identity, collect data, approve response             | Response evidence  |
| Erasure / withdrawal | Check lawful constraints, revoke processing, notify systems | Closure proof      |
| Grievance            | Categorize, prioritize, assign officer, monitor SLA         | Immutable timeline |
| SLA breach           | Auto-escalate to manager, compliance officer, leadership    | Escalation trail   |

# Vendor, DPA and third-party privacy risk

Used by procurement, compliance and privacy teams to manage processors, DPAs, assessments and reassessments.

VE

Vendor inventory

Create registry, classify processor role and map data processed.

- Processor registry
- Data mapping

DP

DPA management

Upload, version, approve, track expiry and renewal evidence.

- Versioning
- Expiry alerts

QU

Questionnaires

Dynamic questions, vendor submissions, evidence and risk scoring.

- Self-service portal
- Auto-scored

RE

Reassessment

Periodic schedules, reminders, overdue escalation and tracking.

- Scheduled
- Overdue alerts

RI

Risk heatmap

High-risk vendors, scorecards, compliance trends and review status.

- Scorecards
- Trends

AU

Audit export

Processor registry, DPA evidence, assessment history and scorecard.

- Export-ready
- Audit trail

# Obligations become repeatable controls

| Area                | Use case                                                                | Typical output                  |
|---------------------|-------------------------------------------------------------------------|---------------------------------|
| Processing register | Activities, purposes, data categories, processors, transfers, retention | Inventory & high-risk dashboard |
| PIA / DPIA          | Templates, questionnaires, scoring, mitigation and residual risk        | Assessment pack & heatmap       |
| Policy and notices  | Policy creation, versioning, notices, approvals and acknowledgements    | Published notice history        |
| Obligation mapping  | DPDP duties mapped to controls, owners, gaps and evidence               | Readiness score & gap report    |

**Why it matters:** legal requirements become repeatable controls with measurable accountability and evidence reviewable by auditors, leadership and regulators.

RG

### RoPA register

Records of processing the DPDP Act expects you to maintain.

DP

### DPIA workflows

Scoring, mitigation and residual-risk assessment packs.

PN

### 23-language notices

English and major Indian languages, versioned and published.

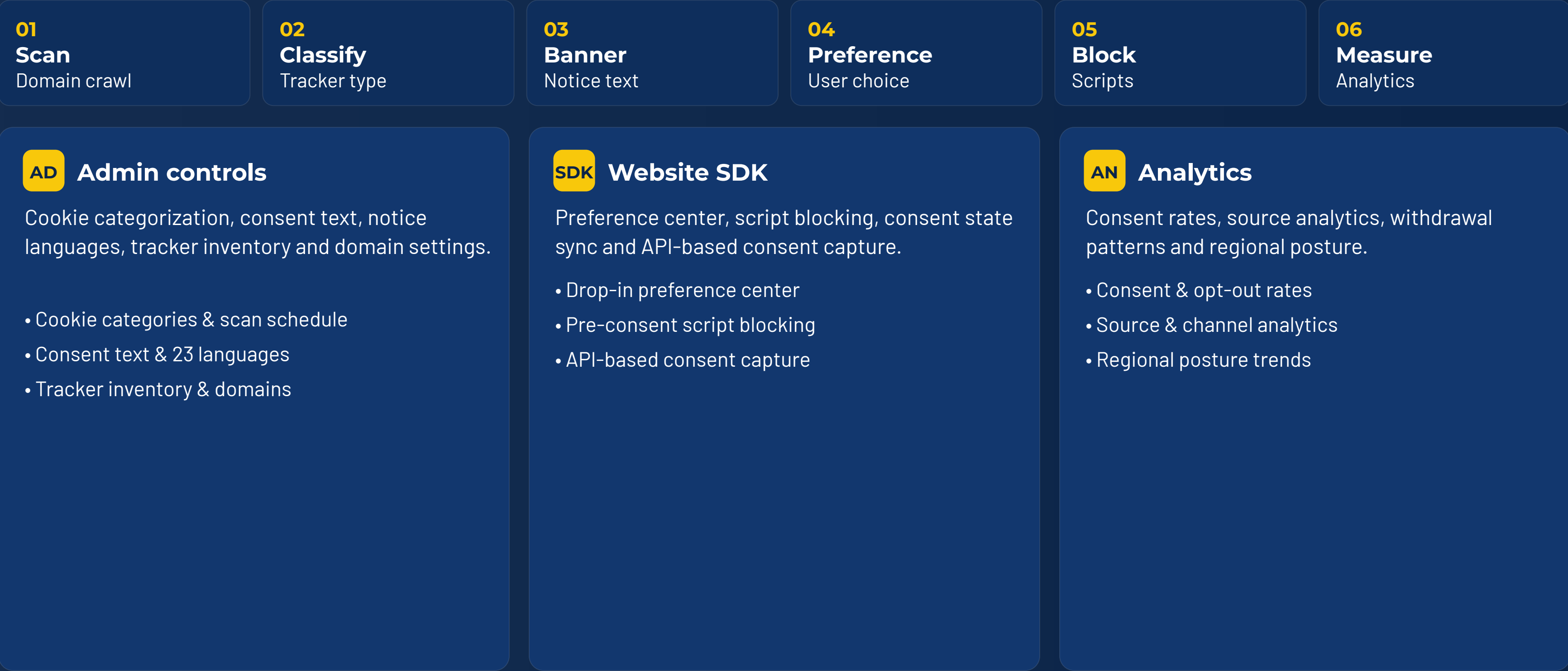
EX

### Executive reporting

Readiness score and gap report for board and DPBI.

# Website cookie and tracker consent

For website privacy operations where banners, preference centers and SDK behavior must be governed centrally.



# Training, quiz and certification engine

A privacy LMS for mandatory assignments, recurring certifications and employee training evidence.

CO

Course management

Video lessons, PDF materials, learning paths and department assignments.

QU

Quiz engine

Question banks, timed assessments, passing thresholds and randomized questions.

CE

Certification

PDF certificates, expiry management, verification and renewal workflows.

CA

Campaigns

Scheduled campaigns, reminders, escalations and annual recertification.

## Outputs & audit evidence

Training history

Per-employee record

Quiz scores

Pass thresholds

Certificates

Verified PDFs

Analytics

Completion rates

Risk scoring

Participation gaps

# Incident, breach and regulatory workflows

- 01 Report · Incident
- 02 Classify · Breach type
- 03 Assess · Impact
- 04 Notify · Stakeholders
- 05 Remediate · Actions
- 06 Export · Report

| Risk signal            | Platform action                                                                                               | Evidence created                    |
|------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------|
| High severity incident | Create incident, classify impact and assign owner<br>Severity scoring · affected data principals · root cause | Incident timeline & evidence bundle |
| Potential breach       | Trigger notification workflow and leadership alert<br>DPBI & data-principal notification decisioning          | Notification decision log           |
| Repeat grievance trend | Analytics flags pattern and recommends control review<br>Recurring categories · SLA breach clusters           | Trend report                        |

## 72-hour clock

Assess



Log



Notify DPBI



Notify principals



Remediate

# Immutable audit logging and evidence vault

Every tenant action produces defensible proof that can be searched, verified and exported.



Coverage

Login & access activity

Consent grant / withdraw events

Rights & grievance fulfilment

Vendor & DPA updates

Policy & notice changes

Admin & RBAC changes

Assurance

Timeline reconstruction

Hash-chain verification

Tamper-evident storage

Full-text evidence search

Evidence export packets

Auditor & DPBI-ready

Why it wins

Defensible, not editable

Every action provable

Withstands scrutiny

One click to evidence pack

# Automation, integrations and AI copilot

## **N8** n8n orchestration

Queue-mode workflows for consent, grievance, vendor, training, notifications and escalations.

Queue jobs

Retry history

Failure alerts

## **IN** Integration hub

Microsoft 365, Google Workspace, Slack, Jira, HRMS, SMTP and webhook ingestion.

M365

Google

Slack

Jira

HRMS

## **NO** Notification service

Email, SMS, in-app and push delivery with templates, retries and tracking.

Email

SMS

In-app

Push

## **AI** AI compliance copilot

DPDP Q&A, policy summaries, grievance categorization and vendor risk insights.

DPDP Q&A

Policy summaries

Risk insights

**Integration principle:** webhook events, tenant context, RBAC, retries, audit logs and failure monitoring are common across every workflow.

# Your Data Protection Officer, on every screen

An always-on AI assistant embedded across the console - "I'm your Virtual DPO" - answering questions, guiding workflows and drafting evidence in context.

QA

DPDP Q&A

Plain-language answers on consent, rights, notices and breach duties.

DR

Drafts & summaries

Generates notices, policy summaries and grievance categorisation.

GW

Guided workflows

Walks users step-by-step through grievances, DSRs and DPIAs.

EV

Evidence & insights

Looks up audit evidence and surfaces vendor-risk insights on demand.

Workflow visibility map

Follow DPDP work from collection through evidence export.

Consent

Purpose ledger

Healthy

Rights

Identity and SLA

Watch

Grievance

Escalations

At risk

Vendors

DPA and risk

Review

Evidence

Vault export

Sealed

Privacy risk heatmap

Board-readable risk signals by DPDP operating domain.

Consent

Version ledger

94

Exposure: Low

Grievance

SLA breach risk

68

Exposure: Medium

Vendors

DPA renewals

61

Exposure: High

Training

Annual campaign

91

Exposure: Low

Incidents

Notification clock

74

Exposure: Medium

Processing

Cross-border map

72

Exposure: Medium

Activity timeline

A single...

Executive reporting pack

Art-friendly indicators for leadership and audit committees.

I'm your Virtual DPO • Ready

I'm your Virtual DPO

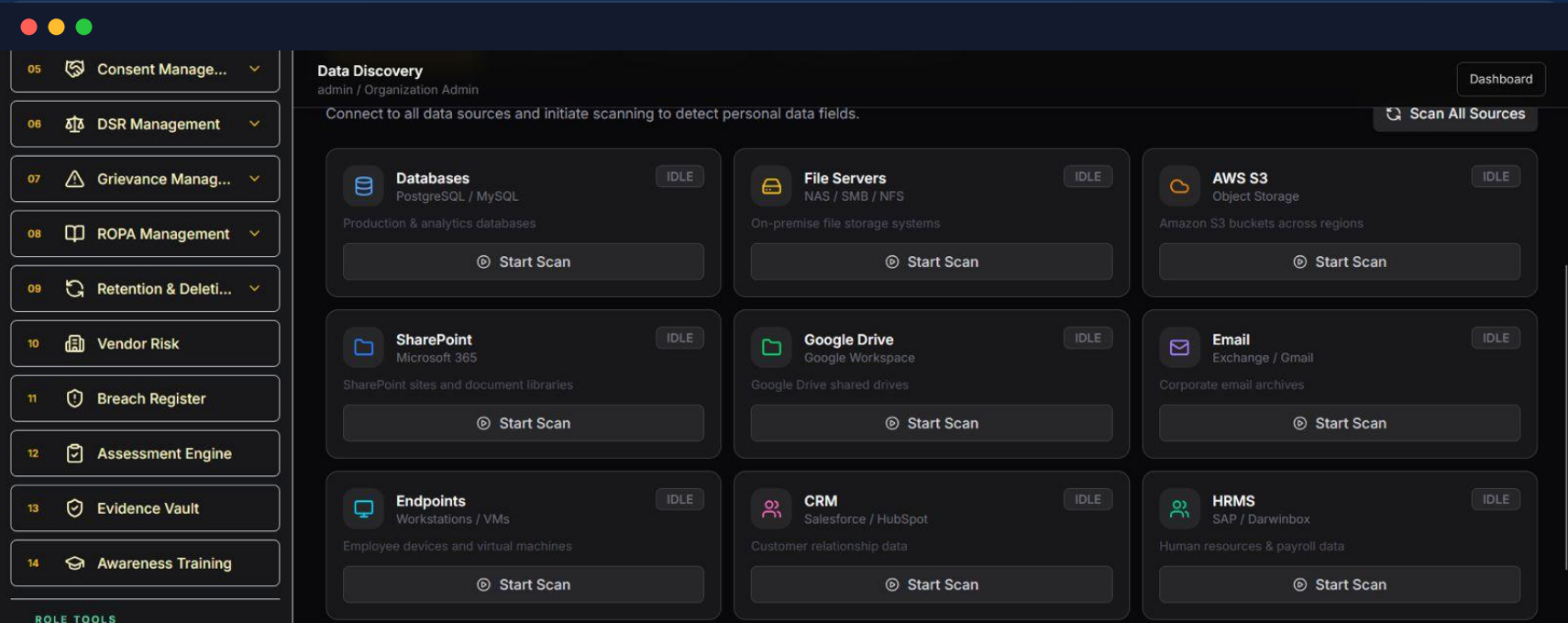
READY

**Always on:** the Virtual DPO travels with every role and screen - tenant-scoped, RBAC-aware and audit-logged like the rest of the platform.

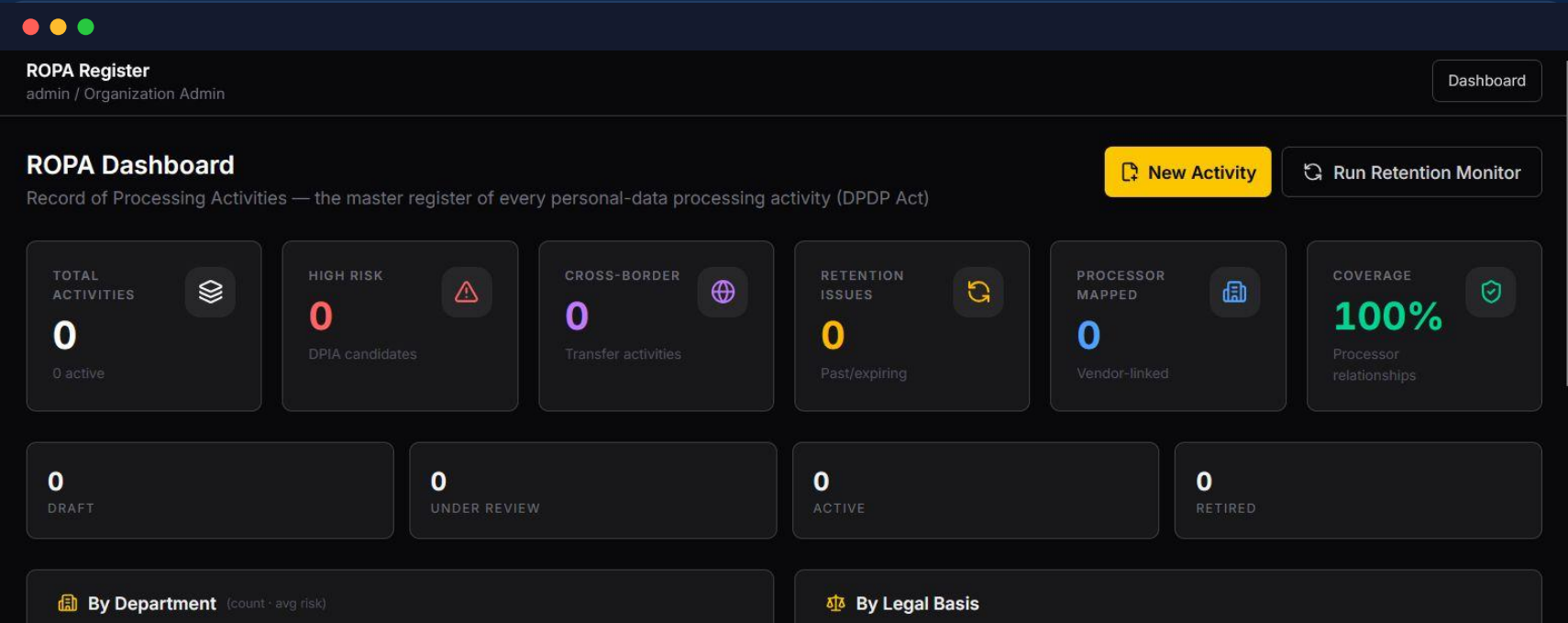
Threatsys DPDP 360

VIRTUAL AI DPO

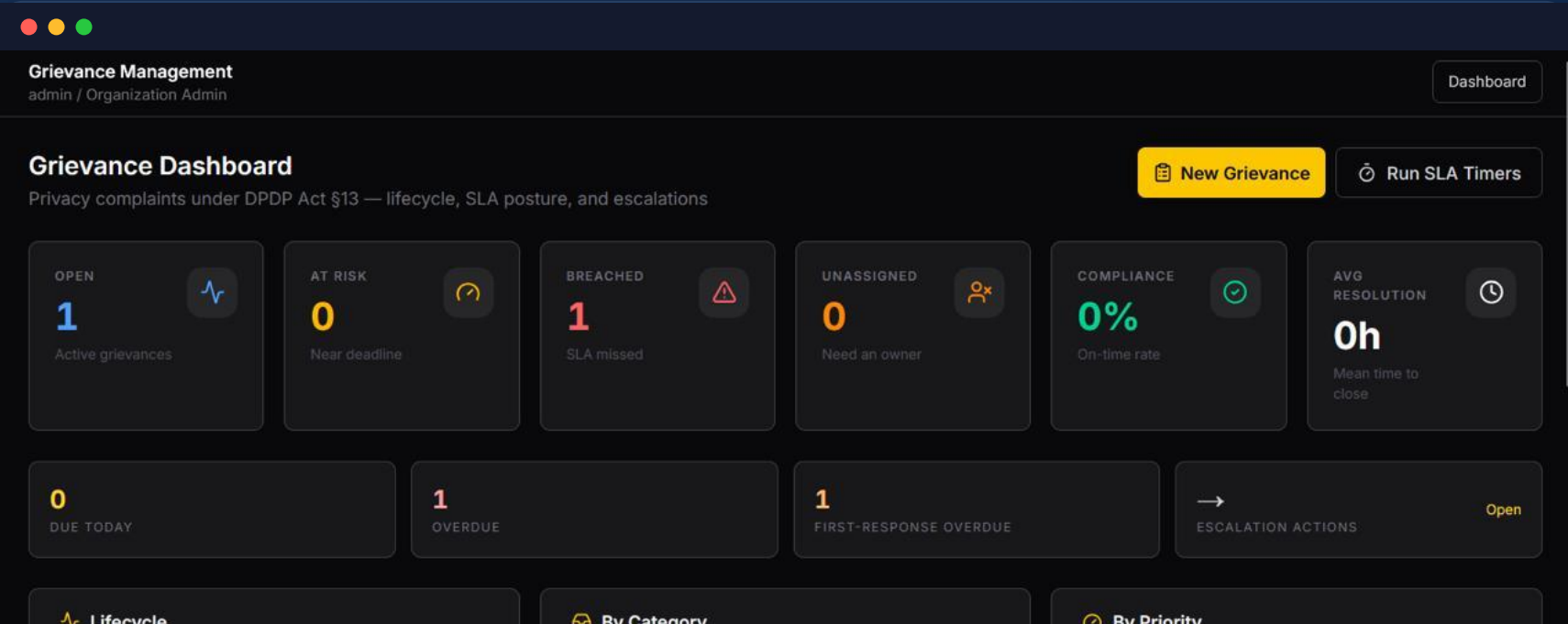
# Discover and operate



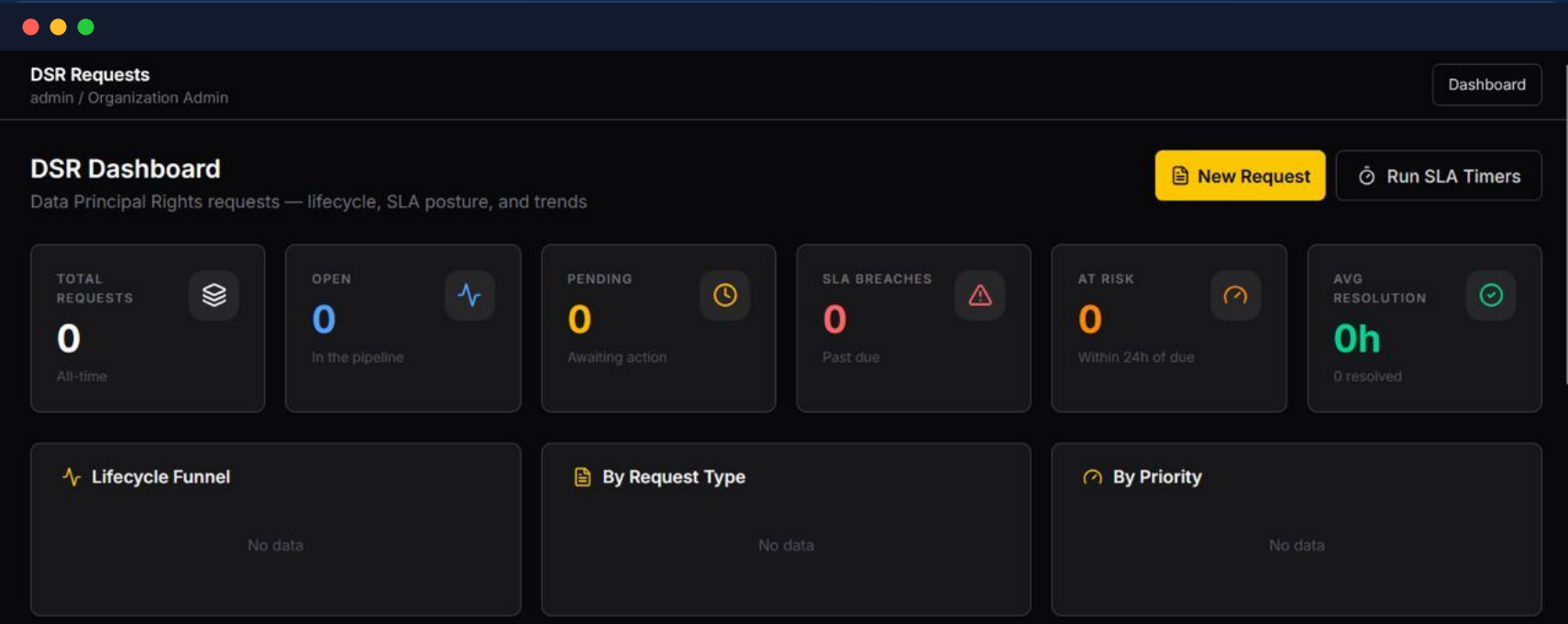
**Data Discovery** - scan every source, auto-classify personal data.



**ROPA Register** - master record of every processing activity.



**Grievance Dashboard** - SLA-tracked complaint lifecycle under §13.



**DSR Requests** - data-principal rights, timers and trends.

# Govern and prove

Vendor Management  
admin / Organization Admin

Dashboard

Privacy vendor operations

DPA governance, dynamic questionnaires, reassessment automation and DPDP risk posture.

Consent timelines

Grievance flow

Training progress

Tenant controls connected

Total vendors

1

Enterprise inventory

High risk

1

Needs privacy review

DPA expiring

0

Next 60 days

Questionnaires

0

0% avg score

Reassessments

0

0 overdue

Privacy command center

Cross-module DPDP operating indicators for executives and privacy officers

Vendor Operations - DPA governance and processor risk posture.

Incident & Breach Management  
admin / Organization Admin

Dashboard

Incident & breach management

Incident intake, personal data impact assessment, 72-hour notification clock, remediation and audit evidence.

ROPA register

Processors

Risk exposure

Tenant controls connected

Open incidents

0

Active investigatio...

Notification due

0

DPBI/data princip...

Overdue

0

Past regulatory de...

ROPA sources

0

Linked activity inv...

Timeline events

0

Evidence-ready e...

Incident intake

Capture event facts, breach classification, affected data and ROPA relationship

Breach command workflow

Triage, impact assessment, notification and remediation states

Incident & Breach - 72-hour notification clock and evidence.

Privacy Officer Workspace  
admin / Organization Admin

Dashboard

07 Grievance Manag...

08 ROPA Management

09 Retention & Deleti...

10 Vendor Risk

11 Breach Register

12 Assessment Engine

13 Evidence Vault

14 Awareness Training

ROLE TOOLS

Privacy Command Center

DPO AUDIT WORKFLOW

Step-by-step DPDP audit modules

Follow the same flow defined in the user manual, with direct access to every DPO review screen.

Audit evidence

01 Executive Dashboard

Review compliance score, SLA pressure, vendor risk and breaches.

02 Data Inventory

Validate data discovery, classification and purpose mapping.

03 Consent Register

Review granted, withdrawn, expired and pending consents.

04 ROPA Register

Verify processing purpose, legal basis and retention period.

05 DSR Requests

Approve access, correction, erasure and withdrawal responses.

06 Retention Review

Approve delete, archive and exception handling evidence.

07 Vendor Risk

Check DPA status, assessments and high-risk processors.

08 Breach Register

Review impact assessment, notifications and closure evidence.

09

10

11

DPO Workspace - step-by-step DPDP audit modules.

Search consents, grievances...

97 /100

admin  
Organization Admin  
admin@example.com

+ New entry

CONSENTS

0

+38 this week

RIGHTS

0

SLA governed

GRIEVANCES

1

-4 resolved

TRAINING

0%

124 employees certified

VENDORS

1

3 reviews due

Compliance command center

Live operating view across core DPDP controls

Module score 97

Today's queue

Actions routed from consent, grievance and vendor workflows

Command Dashboard - one live operating view across controls.

# Recommended client presentation flow

Use this sequence to show the application as a working privacy operations platform.

**01**  
**Website**  
Public page

**02**  
**Create**  
Account

**03**  
**Login**  
Console

**04**  
**Operate**  
Use case

**05**  
**Export**  
Evidence

## Demo storyline

- 1 · Create or log into a tenant workspace from the **[DPDP portal URL]**.
- 2 · Show executive dashboard: privacy score, consent posture, grievances and vendor risk.
- 3 · Record a consent event, withdraw it and show immutable ledger history.
- 4 · Create a Data Principal or grievance request and show SLA escalation visibility.
- 5 · Open vendor risk, DPA tracking or DPIA to show enterprise controls.
- 6 · Export an audit or board report as operational evidence.

**Tip** Open the secure console live at **[DPDP portal URL]** - real screens land better than slides.

# Rollout phases and client value

A practical implementation path from tenant foundation to operational assurance.

**Phase 1** • Weeks 1-2

**Foundation**

- Tenant onboarding & industry preset
- RBAC and user roles
- Initial policies and purposes
- PII discovery & data intake

**Phase 2** • Weeks 3-6

**Operations**

- Consent, rights, grievance
- Vendor and DPIA workflows
- Training campaigns
- Notices in 23 languages

**Phase 3** • Weeks 7+

**Assurance**

- Audit evidence vault
- Executive & DPBI reporting
- Integrations and automation
- Continuous compliance

**Client value**

**Faster operations**

Months to weeks

**Stronger accountability**

Clear ownership

**Lower risk**

Fewer penalties

**Defensible evidence**

Audit-ready

# What the client can see live

A working DPDP operations platform with login, tenant workspace, dashboards, workflows, evidence and export-ready reporting.

- ☒ Account creation and tenant setup

☒ Vendor, DPA and risk dashboards
- ☒ Executive command center

☒ Evidence vault and audit export
- ☒ Consent ledger and purpose tracking

☒ Automation, integrations and AI copilot
- ☒ Public website and secure login



# Thank **you**

• MADE IN INDIA • MADE FOR INDIA

CALL

**+91 9668200222**

EMAIL

**support@threatsys.co.in**

WEB

**www.threatsys.co.in**