ENTERPRISE IAM 18-WEEK PROGRAM · 2024

Reimagining enterprise access without the friction.

An AI-powered Identity & Access Management platform designed for the four humans caught inside every access decision: the employee, the admin, the auditor, and the security lead.

2.6d → 11m	ACCESS LATENCY
−74%	MANUAL APPROVALS
SUS 84	USABILITY SCORE
92%	TASK SUCCESS

CHAPTER 01

Overview

SecureVault is an AI-powered Identity & Access Management platform that helps enterprises move from reactive access chaos to proactive, least-privilege security.

Modern organizations use hundreds of SaaS tools. Every joiner, mover, and leaver triggers a cascade of permission changes — and today those changes are handled by tickets, spreadsheets, and tribal knowledge.

As Senior Product Designer, I owned end-to-end UX for the platform: discovery research, information architecture, cross-role workflows, AI interaction design, prototyping, usability testing, and the enterprise design system.

KEY TAKEAWAYS

- 18 weeks · 4 personas · 3 design sprints
- 26 research interviews across 9 organizations
- Shipped v1 to 12 design partners · 92% task success

BEFORE	AFTER
× Slack DMs and email chains for access	✓ Self-service with AI-recommended roles
× IT manually approves 200+ tickets/week	✓ 74% of approvals fully automated
× 47-item nav · low task success	✓ 9-item IA · 89% task success
× Audit prep = 3 weeks of spreadsheets	✓ Audit answers in seconds, framework-mapped
× No visibility into privilege drift	✓ Drift detection with blast-radius scoring

CHAPTER 02

The Business Problem

Access is broken. Slow for employees, painful for IT, invisible to compliance, and dangerous for security.

IT teams reported spending 30–40% of weekly capacity on manual approval tickets. Employees waited an average of 2.6 business days to gain access to tools they needed on day one.

Compliance teams could not answer basic audit questions — who has access to what, why, and since when — without weeks of manual reconciliation. Meanwhile permission sprawl was quietly expanding the blast radius of every credential.

KEY TAKEAWAYS

- 2.6 day average request-to-access latency
- $4.2M average annual cost of over-permissioning
- 68% of audits flagged 'excessive privileges'

Employee
WAITING

IT Manager
OVERLOADED

Security
BLIND SPOTS

Compliance
NO EVIDENCE

Four roles, one broken workflow. Every arrow between them is a ticket.

CHAPTER 03

Research & Discovery

Market analysis, competitive teardown, stakeholder interviews, and generative user research framed the opportunity.

Market Research — The IAM market is projected to reach $32B by 2028, but mid-market adoption is throttled by product complexity. Buyers want Okta-grade governance with Notion-grade usability.

Competitive Analysis — I audited Okta, Microsoft Entra, SailPoint, Saviynt, and JumpCloud. Consistent gaps: shallow AI, weak self-service, and dashboards built for auditors, not humans.

Stakeholder Interviews — 11 sessions with CISOs, IT Directors, and Compliance leads surfaced a shared frustration: every existing tool assumes the admin, never the employee.

User Research — 15 diary studies and contextual inquiries with employees revealed the emotional cost of waiting for access: blocked onboarding, missed deadlines, and workarounds that quietly leaked data.

KEY TAKEAWAYS

- 4 primary personas validated across 9 orgs
- Journey mapping revealed 14 friction points
- Service blueprint exposed 6 silent handoffs

	AI DEPTH	SELF-SERVICE	AUDIT UX	TIME-TO-VALUE
Okta	Partial	Strong	Partial	Partial
MS Entra	Partial	Partial	Weak	Weak
SailPoint	Partial	Weak	Strong	Weak
JumpCloud	Weak	Partial	Weak	Partial
SecureVault	Strong	Strong	Strong	Strong

CHAPTER 04

Personas & Journeys

Four archetypes anchored every design decision — each with distinct goals, tools, and success metrics.

Priya — Security Administrator. Wants least-privilege by default and clear signals when drift occurs. Success = time-to-detect anomalies.

Marcus — IT Manager. Juggles 200+ tickets a week and wants automation he can trust. Success = approvals per hour without incidents.

Elena — Employee. Just wants the tools to do her job on day one. Success = access in minutes, not days.

David — Compliance Officer. Must prove to auditors that the org is in control. Success = a single, defensible source of truth.

KEY TAKEAWAYS

- Personas grounded in real transcripts
- Journey map became the north star in exec reviews
- Blueprint aligned Security, IT, and People Ops

Priya
SECURITY ADMIN
Detect drift fast
Splunk · Okta · PagerDuty

Marcus
IT MANAGER
Trustworthy automation
Jira · Slack · ServiceNow

Elena
EMPLOYEE
Tools on day one
Slack · Notion · Figma

David
COMPLIANCE
Defensible source of truth
Vanta · Drata · Excel

CHAPTER 05

Information Architecture & Flows

I restructured the product around three mental models: Requests, Roles, and Risks. Everything a user does maps to one of them.

The previous prototype exposed 47 top-level nav items. I collapsed them into 9 semantic categories using tree-testing with 24 participants — success rate rose from 41% to 89%.

User flows were designed role-by-role: employee self-service, admin approval, compliance audit, and security investigation. Each flow was rehearsed against real transcripts before wireframing.

Wireframes progressed from lo-fi paper to interactive Figma prototypes across three iterations, validated in moderated tests with 18 participants.

KEY TAKEAWAYS

- Nav reduced 47 → 9 items
- Task success 41% → 89%
- 3 wireframe rounds · 18 usability sessions

Request → AI Match → Risk Score → Approval → Provision → Audit Log

Every request follows a single canonical flow, instrumented end-to-end.

CHAPTER 06

AI-Powered Design Decisions

AI is the differentiator — but only when it earns trust. I designed three AI surfaces around transparency and reversibility.

AI Permission Recommendations — peer-based ML suggests roles for new hires based on team, title, and behavior clusters. Every suggestion shows confidence, rationale, and a one-click override.

Risk Detection — anomaly models flag unusual privilege usage: impossible travel, dormant admin re-activation, over-permissioned service accounts. Alerts are ranked by blast radius, not just probability.

Access Request Workflow — employees describe intent in plain language; AI maps it to the smallest sufficient role, routes to the correct approver, and predicts approval likelihood.

Audit Timeline — a queryable, immutable ledger. Compliance can ask 'who accessed prod between March 4–6?' and get an answer in seconds, mapped to SOC2, ISO 27001, and HIPAA.

KEY TAKEAWAYS

- Every AI action shows confidence + rationale
- One-click override on 100% of suggestions
- Audit queries: 5 days → under 60 seconds

AI SURFACE LIVE SAMPLE

Permission Recommendations

Peer-based ML suggests the smallest sufficient role.

Design · Editor CONFIDENCE 94%

8 of 9 peers on Design team hold this role.

Figma · Commenter CONFIDENCE 88%

Matches title 'Product Designer'.

Notion · Member CONFIDENCE 72%

Used by 6 similar new hires in 30 days.

Confidence · rationale · one-click override on every action.

AI SURFACE LIVE SAMPLE

Risk Detection

Anomalies ranked by blast radius, not just probability.

HIGH **Impossible travel · admin@a...**
LON → SFO · 22 min

MED **Dormant admin re-activated**
Idle 94 days · Prod DB

LOW **Over-permissioned service ac...**
18 unused scopes

Confidence · rationale · one-click override on every action.

AI SURFACE LIVE SAMPLE

Audit Timeline

Immutable ledger · queryable in plain English.

REQUEST 09:42
Elena requested Figma · Editor

AI 09:43
AI matched role · risk score 12

APPROVE 09:44
Marcus auto-approved (policy #14)

AUDIT 09:44
Provisioned · logged to SOC2 CC6.1

Confidence · rationale · one-click override on every action.

CHAPTER 07

Design System & Accessibility

SecureVault ships with an editorial, WCAG 2.2 AA design system used across 240+ screens.

Tokens — 12 semantic color roles, 4 elevation levels, an 8pt spatial grid, and a type scale tuned for data density. Themable for light, dark, and high-contrast.

Components — 68 primitives, from data tables and permission graphs to risk badges and approval chains. Each ships with keyboard maps, ARIA patterns, and motion tokens.

Accessibility — audited against WCAG 2.2 AA with a screen-reader partner. Every interactive surface reachable by keyboard; every data viz has a tabular

KEY TAKEAWAYS

- 240+ screens on one token system
- WCAG 2.2 AA · tested with assistive tech users
- Documentation adopted by 3 downstream teams

fallback and non-color status cues.

COLOR TOKENS

Cream
Ink
Coral
Sage
Amber
Paper
Line
Muted

TYPOGRAPHY

Fraunces

Inter · JetBrains Mono

Editorial serif for headlines, geometric sans for UI density.

ACCESSIBILITY

WCAG 2.2 AA

Keyboard maps, ARIA patterns, screen-reader tested, high-contrast mode, non-color status cues.

CHAPTER 08

Results & Reflection

SecureVault moved the numbers that matter to security, IT, employees, and compliance — simultaneously.

Business Results — access request latency dropped from 2.6 days to 11 minutes median. Manual IT approvals fell 74%. Audit prep collapsed from 3 weeks to 2 hours. NPS from IT admins climbed to +58.

Usability Testing — 92% task success across 4 role types, SUS score 84. Employees described it as 'the first security tool that feels like it's on my side.'

Reflection — the hardest problem was not AI, it was trust. Every decision — copy, confidence, reversibility, defaults — had to earn the right to be automated. Enterprise UX is not about hiding complexity; it is about revealing it responsibly.

KEY TAKEAWAYS

- Access latency: 2.6d → 11m
- Manual approvals −74% · Audit prep −99%
- SUS 84 · NPS +58 · 92% task success

2.6d → 11m
REQUEST LATENCY

−74%
MANUAL APPROVALS

3w → 2h
AUDIT PREP

+58
IT ADMIN NPS

USER FLOWS & JOURNEYS

Four humans. Four journeys. One system.

Every SecureVault decision was rehearsed against the real path each role walks — from the emotional lows of waiting for access, to the highs of a clean audit close.

Elena · Employee

"I start Monday and I still don't have Figma."

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05	STEP 06
Day 1 · Onboard	**Search tool in SecureVault**	**AI suggests role**	**One-click request**	**Auto-approved in 11m**	**Working by lunch**
● FRUSTRATED	● CURIOUS	● RELIEVED	● CONFIDENT	● DELIGHTED	● PRODUCTIVE

Marcus · IT Manager

"200 tickets a week. I need signal, not noise."

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05	STEP 06
Morning queue	**Risk-ranked inbox**	**Bulk approve low-risk**	**Review flagged edge cases**	**Policy rule created**	**Queue at zero**
● OVERLOADED	● FOCUSED	● EFFICIENT	● DELIBERATE	● EMPOWERED	● CALM

Priya · Security Admin

"Where is privilege quietly drifting today?"

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05	STEP 06
Command center opens	**Anomaly cluster surfaces**	**Blast radius scored**	**Revoke + auto-notify**	**Policy pushed to drift check**	**Incident closed**
● ALERT	● FOCUSED	● INFORMED	● DECISIVE	● CONFIDENT	● ASSURED

David · Compliance

"Auditors arrive Friday. I need the story, mapped."

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05	STEP 06
Open audit workspace	**Query timeline in plain English**	**Framework auto-map (SOC2/ISO)**	**Evidence bundle exports**	**Auditor walkthrough**	**Zero findings**
● ANXIOUS	● CURIOUS	● RELIEVED	● PREPARED	● CONFIDENT	● VINDICATED

End-to-end swimlane · Access request → audit

CANONICAL FLOW

EMPLOYEE: Request tool → AI suggests role → Submit

SECUREVAULT AI: Match peers → Score risk → Route approver

IT / APPROVER: Inbox ranked → Review + approve → Provision

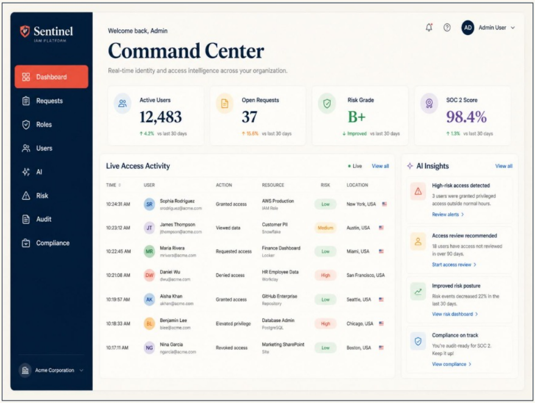
COMPLIANCE: Immutable log → Framework map → Evidence ready

FOUR LANES · ONE CONTINUOUS SYSTEM OF RECORD.

DELIVERABLES

Six screens · one flow.

The final visual system, expressed across the six moments that matter most in enterprise IAM — from request to audit.



Welcome back, Admin

Command Center

Real-time identity and access intelligence across your organization.

Active Users	Open Requests	Risk Grade	SOC 2 Score
12,483	37	B+	98.4%
↑ 4.2% vs last 30 days	↑ 15.6% vs last 30 days	↓ Improved vs last 30 days	↑ 1.3% vs last 30 days

Live Access Activity · Live View all

TIME	USER	ACTION	RESOURCE	RISK	LOCATION
10:24:31 AM	SR Sophia Rodriguez srodriguez@acme.com	Granted access	AWS Production IAM Role	Low	New York, USA
10:23:12 AM	JT James Thompson jthompson@acme.com	Viewed data	Customer PII Snowflake	Medium	Austin, USA
10:22:45 AM	MR Maria Rivera mrivera@acme.com	Requested access	Finance Dashboard Looker	Low	Miami, USA
10:21:08 AM	DW Daniel Wu dwu@acme.com	Denied access	HR Employee Data Workday	High	San Francisco, USA
10:19:57 AM	AK Aisha Khan akhan@acme.com	Granted access	GitHub Enterprise Repository	Low	Seattle, USA
10:18:33 AM	BL Benjamin Lee blee@acme.com	Elevated privilege	Database Admin PostgreSQL	High	Chicago, USA
10:17:11 AM	NG Nina Garcia ngarcia@acme.com	Revoked access	Marketing SharePoint Site	Low	Boston, USA

AI Insights View all

High-risk access detected
3 users were granted privileged access outside normal hours.
Review alerts ›

Access review recommended
18 users have access not reviewed in over 90 days.
Start access review ›

Improved risk posture
Risk events decreased 22% in the last 30 days.
View risk dashboard ›

Compliance on track
You're audit-ready for SOC 2. Keep it up!
View compliance ›

STEP 01 / 06

Admin Command Center

Unified security posture, live risk telemetry, and cross-team access queue.

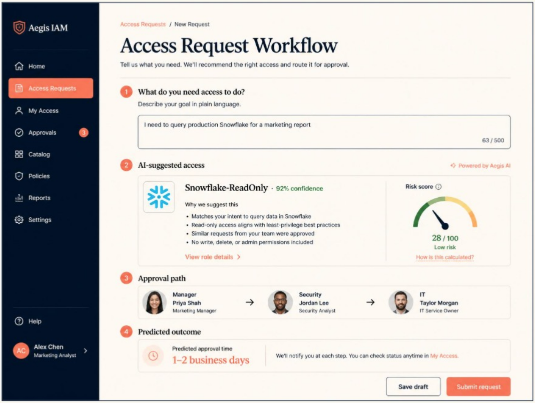
1600 × 1200

STEP 02 / 06

Access Request Workflow

Employee self-service with AI-suggested roles, risk score, and approver chain.

1600 × 1200



Access Requests / New Request

Access Request Workflow

Tell us what you need. We'll recommend the right access and route it for approval.

1 What do you need access to do?
Describe your goal in plain language.

I need to query production Snowflake for a marketing report
63 / 500

2 AI-suggested access · Powered by Aegis AI

Snowflake-ReadOnly · 92% confidence

Why we suggest this
- Matches your intent to query data in Snowflake
- Read-only access aligns with least-privilege best practices
- Similar requests from your team were approved
- No write, delete, or admin permissions included

View role details ›

Risk score: 28 / 100
Low risk
How is this calculated?

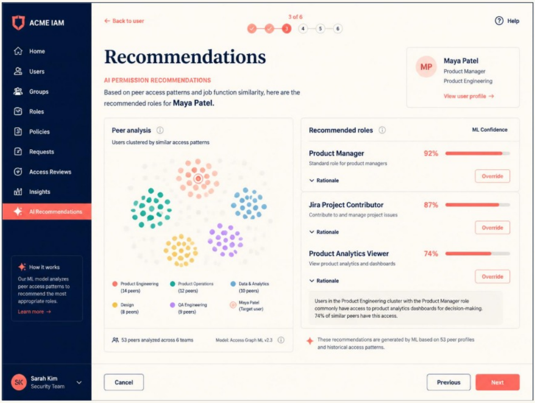
3 Approval path

Manager
Priya Shah
Marketing Manager
→
Security
Jordan Lee
Security Analyst
→
IT
Taylor Morgan
IT Service Owner

4 Predicted outcome

Predicted approval time
1–2 business days

We'll notify you at each step. You can check status anytime in My Access.



Recommendations

AI PERMISSION RECOMMENDATIONS

Based on peer access patterns and job function similarity, here are the recommended roles for **Maya Patel.**

MP **Maya Patel**
Product Manager
Product Engineering

Peer analysis
Users clustered by similar access patterns

🟥 Product Engineering (14 peers)
🟩 Product Operations (12 peers)
🟦 Data & Analytics (10 peers)
🟨 Design (8 peers)
🟪 QA Engineering (9 peers)
◎ Maya Patel (Target user)

53 peers analyzed across 6 teams
Model: Access Graph ML v2.3

Recommended roles — ML Confidence

Role	ML Confidence
Product Manager Standard role for product managers	92%
Jira Project Contributor Contribute to and manage project issues	87%
Product Analytics Viewer View product analytics and dashboards	74%

Users in the Product Engineering cluster with the Product Manager role commonly have access to product analytics dashboards for decision-making. 74% of similar peers have this access.

These recommendations are generated by ML based on 53 peer profiles and historical access patterns.

How it works
Our ML model analyzes peer access patterns to recommend the most appropriate roles.

Sarah Kim
Security Team

STEP 03 / 06

AI Permission Recommendations

Peer-based, ML-driven role suggestions with confidence scoring.

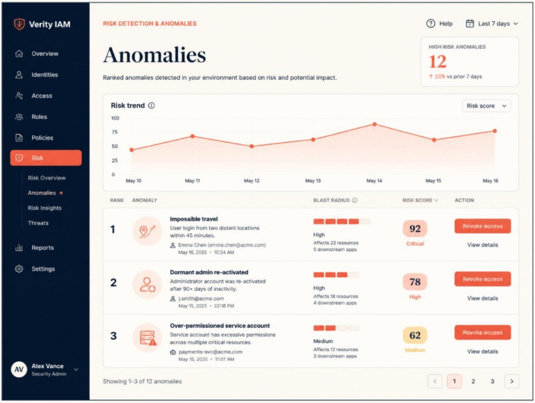
1600 × 1200

STEP 04 / 06

Risk Detection & Anomalies

Real-time detection of unusual privilege usage across the org.

1600 × 1200



RISK DETECTION & ANOMALIES

Anomalies

Ranked anomalies detected in your environment based on risk and potential impact.

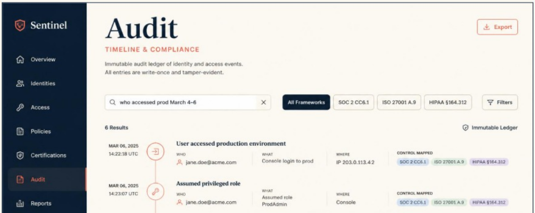
HIGH RISK ANOMALIES
12
↑ 20% vs prior 7 days

Risk trend

RANK	ANOMALY	BLAST RADIUS	RISK SCORE	ACTION
1	**Impossible travel** User login from two distant locations within 45 minutes. Emma Chen (emma.chen@acme.com) May 16, 2025 • 10:24 AM	High Affects 23 resources 5 downstream apps	92 Critical	Revoke access View details
2	**Dormant admin re-activated** Administrator account was re-activated after 90+ days of inactivity. j.smith@acme.com May 15, 2025 • 02:18 PM	High Affects 18 resources 4 downstream apps	78 High	Revoke access View details
3	**Over-permissioned service account** Service account has excessive permissions across multiple critical resources. payments-svc@acme.com May 15, 2025 • 11:07 AM	Medium Affects 12 resources 3 downstream apps	62 Medium	Revoke access View details

Showing 1–3 of 12 anomalies

AV Alex Vance
Security Admin



Audit

TIMELINE & COMPLIANCE

Immutable audit ledger of identity and access events.
All entries are write-once and tamper-evident.

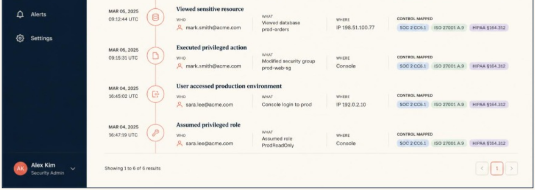
who accessed prod March 4–6

6 Results

		WHO	WHAT	WHERE	CONTROL MAPPED
MAR 06, 2025 14:22:18 UTC	**User accessed production environment**	jane.doe@acme.com	Console login to prod	IP 203.0.113.42	SOC 2 CC6.1 ISO 27001 A.9 HIPAA §164.312
MAR 06, 2025 14:23:07 UTC	**Assumed privileged role**	jane.doe@acme.com	Assumed role ProdAdmin	Console	SOC 2 CC6.1 ISO 27001 A.9 HIPAA §164.312

STEP 05 / 06

Audit Timeline & Compliance



MAR 05, 2025
09:12:44 UTC

Viewed sensitive resource

WHO mark.smith@acme.com
WHAT Viewed database prod-orders
WHERE IP 198.51.100.77
CONTROL MAPPED SOC 2 CC6.1 ISO 27001 A.9 HIPAA §164.312

MAR 05, 2025
09:15:31 UTC

Executed privileged action

WHO mark.smith@acme.com
WHAT Modified security group prod-web-sg
WHERE Console
CONTROL MAPPED SOC 2 CC6.1 ISO 27001 A.9 HIPAA §164.312

MAR 04, 2025
16:45:02 UTC

User accessed production environment

WHO sara.lee@acme.com
WHAT Console login to prod
WHERE IP 192.0.2.10
CONTROL MAPPED SOC 2 CC6.1 ISO 27001 A.9 HIPAA §164.312

MAR 04, 2025
16:47:19 UTC

Assumed privileged role

WHO sara.lee@acme.com
WHAT Assumed role ProdReadOnly
WHERE Console
CONTROL MAPPED SOC 2 CC6.1 ISO 27001 A.9 HIPAA §164.312

Showing 1 to 6 of 6 results

Immutable audit trail mapped to SOC2, ISO 27001, and HIPAA.

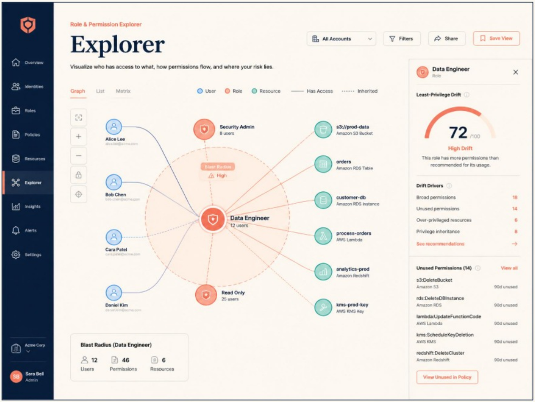
`1600 × 1200`

STEP 06 / 06

Role & Permission Explorer

Visual permission graph, blast radius, and least-privilege drift.

`1600 × 1200`



Role & Permission Explorer

Explorer

Visualize who has access to what, how permissions flow, and where your risk lies.

Blast Radius (Data Engineer)

Users	Permissions	Resources
12	46	6

Data Engineer
Role

Least-Privilege Drift

72 /100

High Drift

This role has more permissions than recommended for its usage.

Drift Drivers

Broad permissions	18
Unused permissions	14
Over-privileged resources	6
Privilege inheritance	8

See recommendations →

Unused Permissions (14) View all

s3:DeleteBucket Amazon S3	90d unused
rds:DeleteDBInstance Amazon RDS	90d unused
lambda:UpdateFunctionCode AWS Lambda	90d unused
kms:ScheduleKeyDeletion AWS KMS	90d unused
redshift:DeleteCluster Amazon Redshift	90d unused

View Unused in Policy