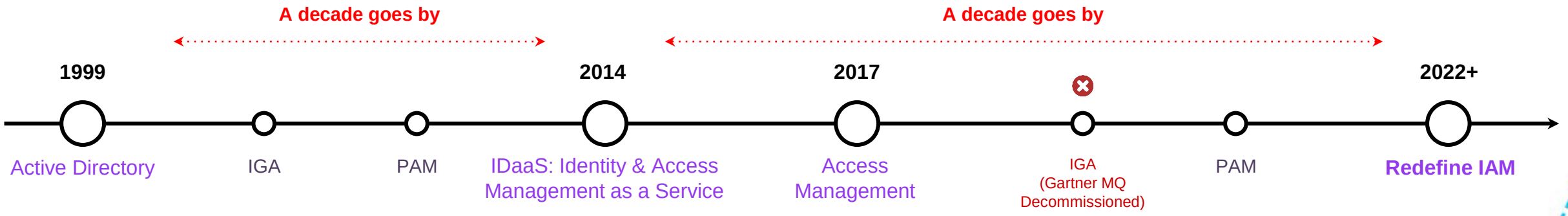
IGA Strategies for Achieving Least Privilege

Rich Dandliker: Chief Strategist, Veza
David Tyburski: CISO, Wynn Resorts

Identity needs a second act: Authentication ->Authorization

Gartner Magic Quadrant throughout the years



Beyond IAM to true Access Controls:

- Implementing MFA is not the “security cure-all” some had hoped for
- Authorization is the next frontier of IAM to secure access to data

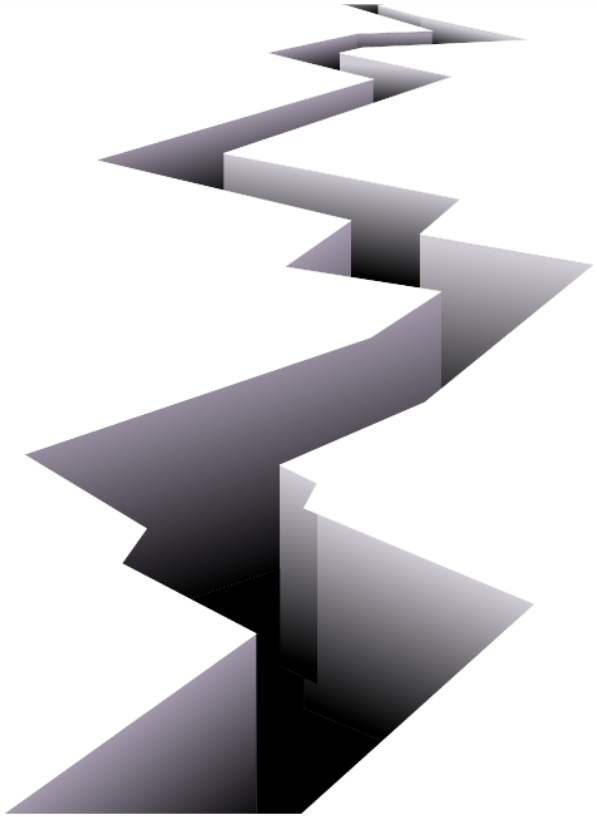
Customer Problem:
Can anybody get to least privilege?

Teams

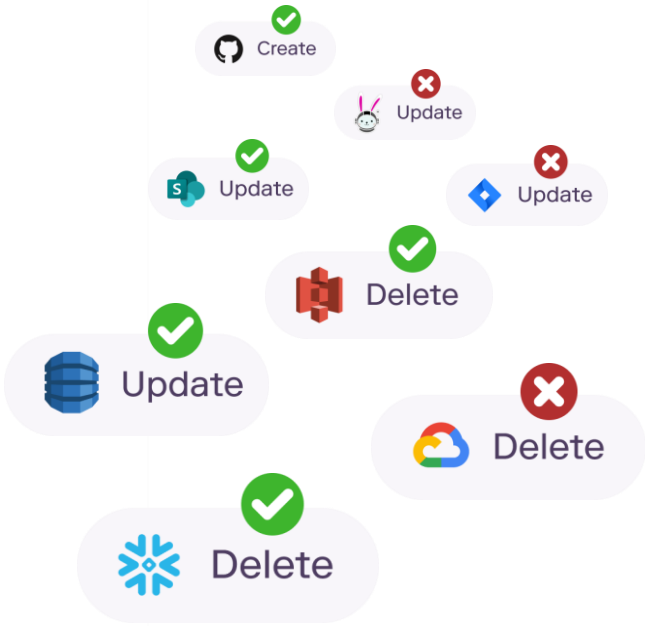
Identity Teams
How do I build secure Access Management processes?

Security Engineering
How do I find and fix privilege violations?

Compliance
How do I automate audit and regulatory reporting and controls for continuous compliance?



Least Privilege



Securing access to data: high complexity problem

Identity, cloud IAM, and access permissions are disconnected

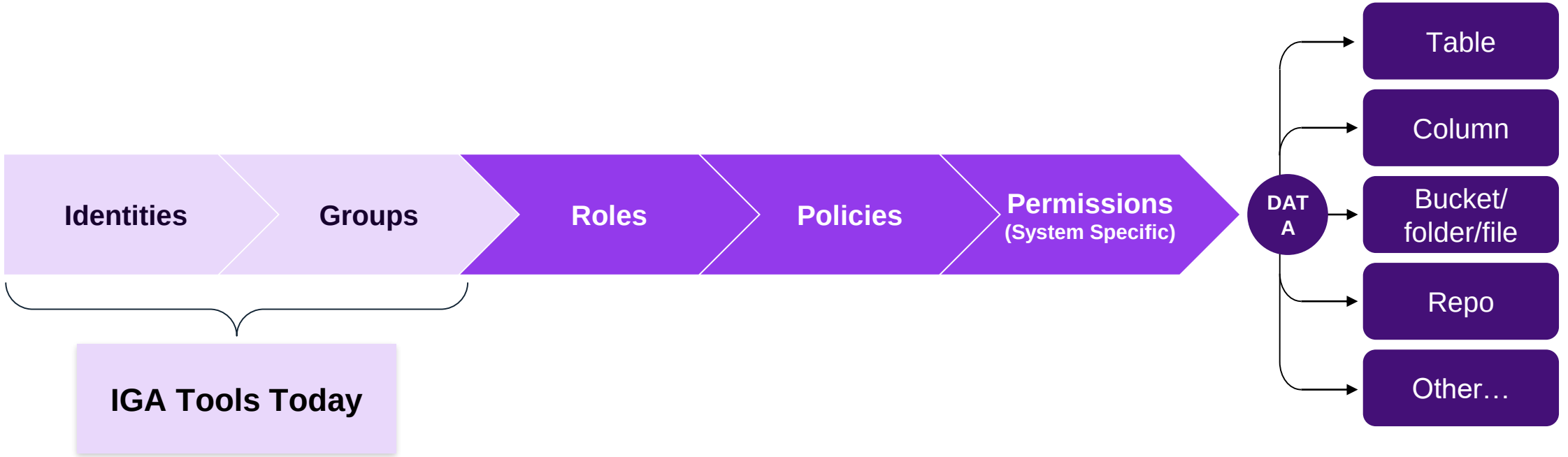
Identity Providers | **IAM Systems** | **Data Systems, SaaS Apps & Resources**

Massive number of combinations

Users x Groups	X	Roles x Policies	X	Permissions x Services x Granular Objects
• Okta, Azure AD, Google, Ping • Cloud identity, Service Accounts & Local Users		• AWS IAM • GCP IAM • Azure RBAC		• 500+ Data Systems • 5000+ Apps • 500+ Services

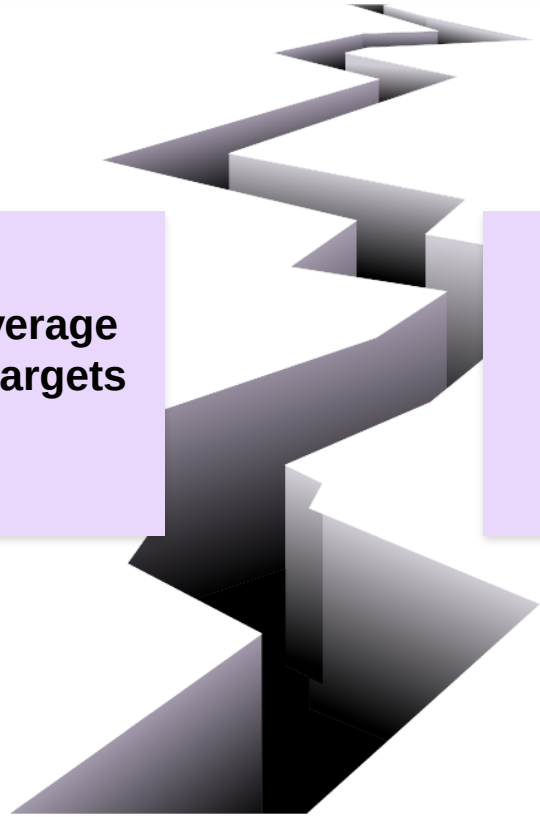
Lack of Common Language / Canonical Data and Object Model

One key way IGA solutions today fall short…



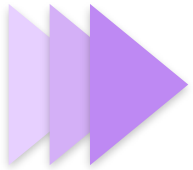
...but there are even more IGA gaps

- Don't go beyond group and role names
- System-specific permissions hard to understand
- Narrow coverage for certain targets only
- Identities often based on HR system only- no contractors, partners, etc.
- Integrations are slow and costly
- Human identities only- no service accounts



Fundamental security goal:

Securing access
to enterprise data



Who can and should take what action on what data?

AUTHORIZATION

Authorization use cases

1. **Access Review Automation.** Run periodic campaigns to see if users should still have access. Certify and recertify entitlements. Perform resource level certifications. Applies to any SaaS app, custom apps, any system.

2. **Privileged Access Violations.** Monitor any apps and systems for new access that would violate policies. E.G. local users or admins created by circumventing provisioning/SSO. Protect against insider threats.

3. **Cloud IAM Misconfigurations.** Investigate access to sensitive resources through cloud IAMs. Applies to AWS, GCP, Azure. Identify IAM misconfigurations. Validate access for human identities and service accounts.

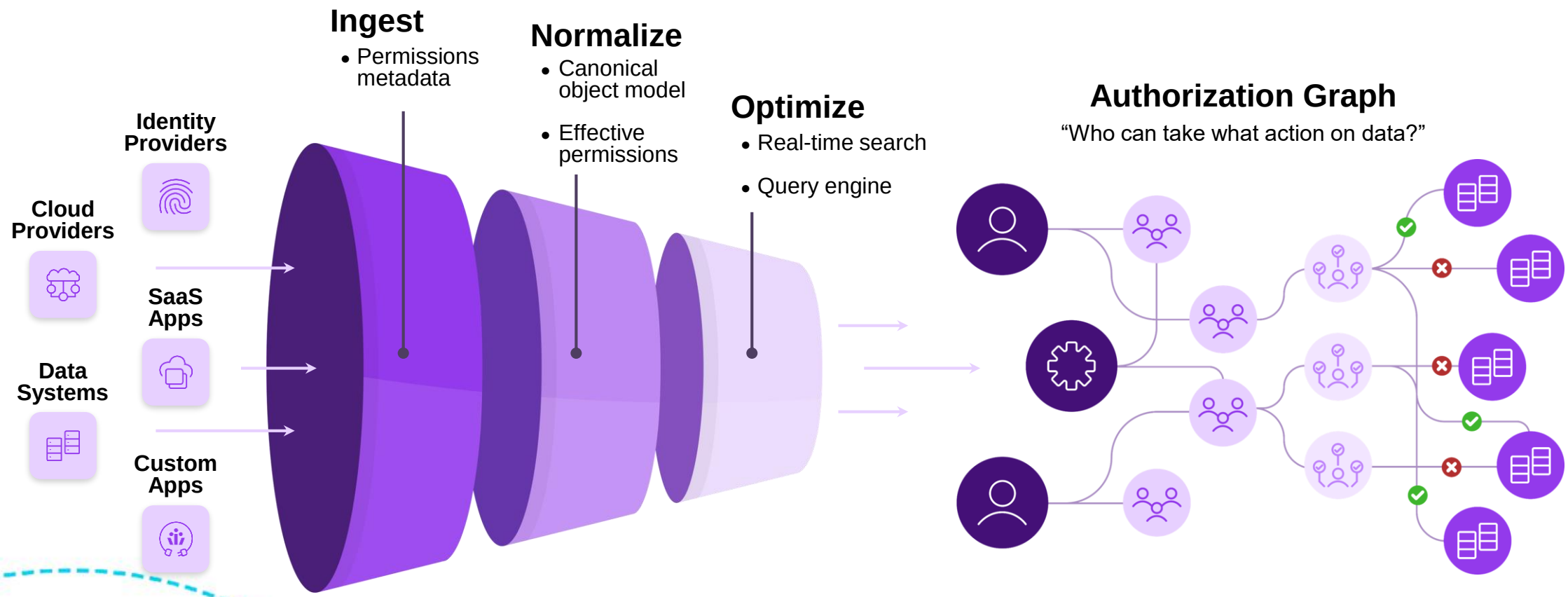
4. **Structured & Unstructured Data Access**. Bring governance to data stores, cloud data lakes, monitoring for activity monitoring. Applies to SharePoint, Box, Snowflake, Databricks, Redshift, BigQuery.

5. **SaaS Access Governance.** Bring governance to data in SaaS apps, meet audit and achieve continuous compliance (SOX, ISO, etc.) on SaaS apps (SFDC, GitHub, GitLab, Box, NetSuite, etc.).

Blackstone intuit CROWDSTRIKE F1000 Bank zoom Robinhood chime LiveRamp Expedia Meritage Homes

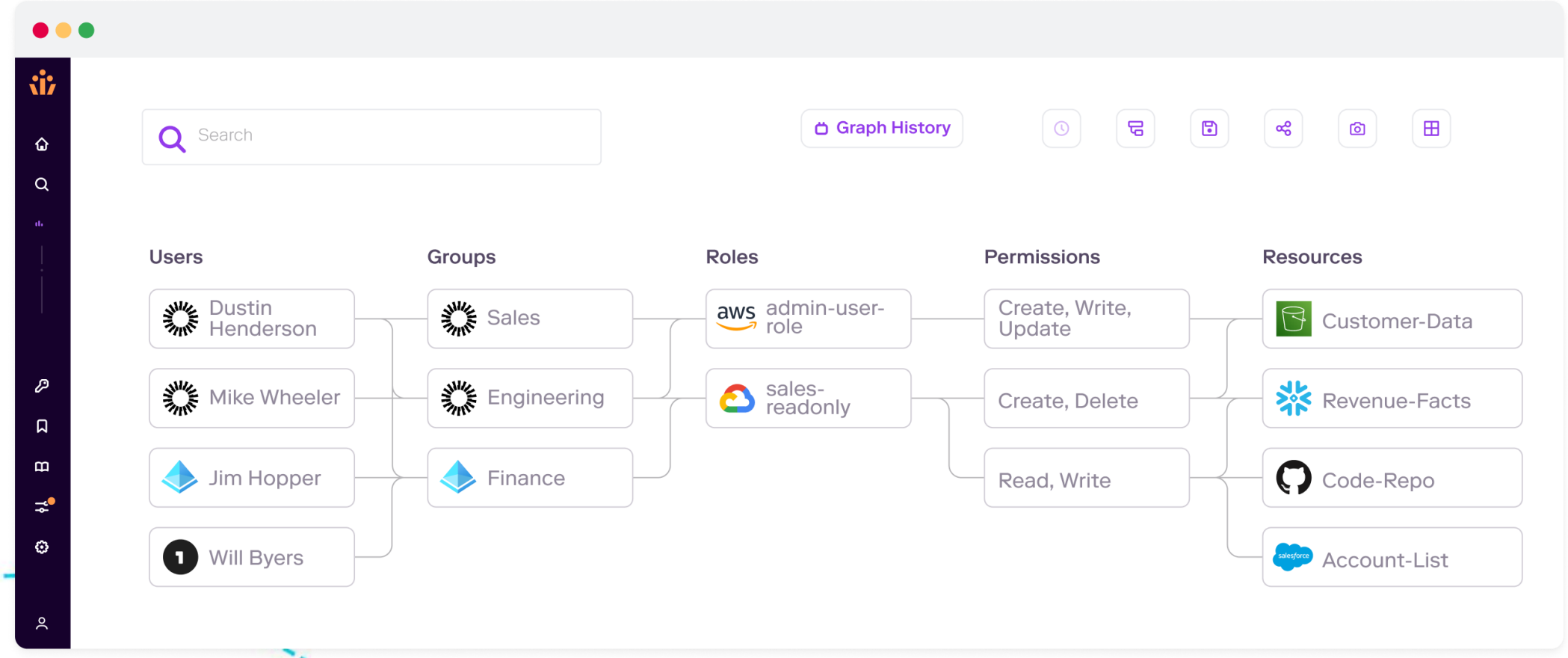
Perspective on a Potential Solution

Step 1: A graph data model to understanding the reality of access

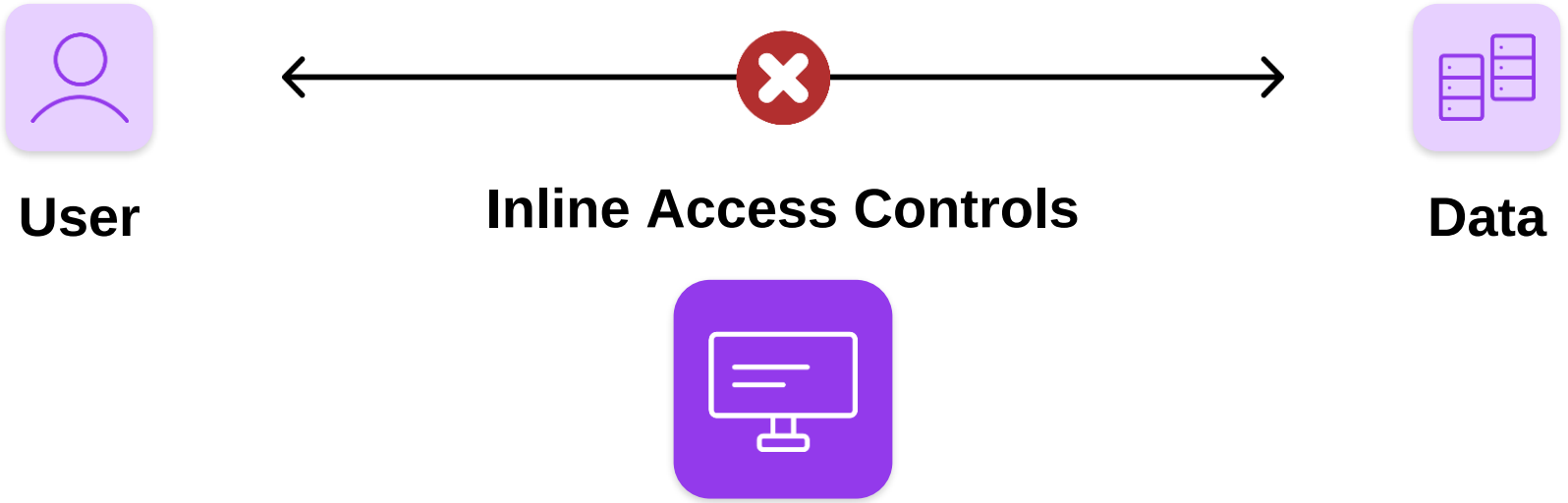


Power of the authorization graph

Employees | Service Accounts | Partners | Contingent Workers | Bots | APIs



Step 2: Address architectural issues with in-line deployments



- Slow deployment
- Downtime risk
- Added points-of-failure
- Increased policy complexity

Roadmap for evolution

Visualize

Who has access to what Data?

Authorization Metadata Graph

“Table Stakes” Functionality

- Integrations (Data, SaaS Apps, Services)
- Enterprise Scale
- Search and Query Engine

Remediate

How and what do I need to fix in data access and entitlements?

Monitoring and Workflows for Access Control

Increasing Operational Relevance

- Intelligent Access Reviews
- Lifecycle Workflows
- IaC inspection and monitoring for “Shift-Left” protection and integration

Control

How do I implement secure and consistent policies across my entire data infrastructure?

Consolidated Authorization Standard

Advanced Capabilities

- Provisioning
- AI / ML based RBAC Recommendations
- RBAC Aware Policy Engine

David Tyburski
Chief Information Security Officer

Use Cases

- Access Review Automation
- Privileged Access Violations
- SaaS Access Governance

PeopleSoft (Custom IdP)
Okta
Oracle Apps
SharePoint
AWS IAM

30K Identities

400 Custom Apps

The Need: Identity Orchestration

- Manual processes don’t scale
- High stakes: regulatory compliance and customer trust

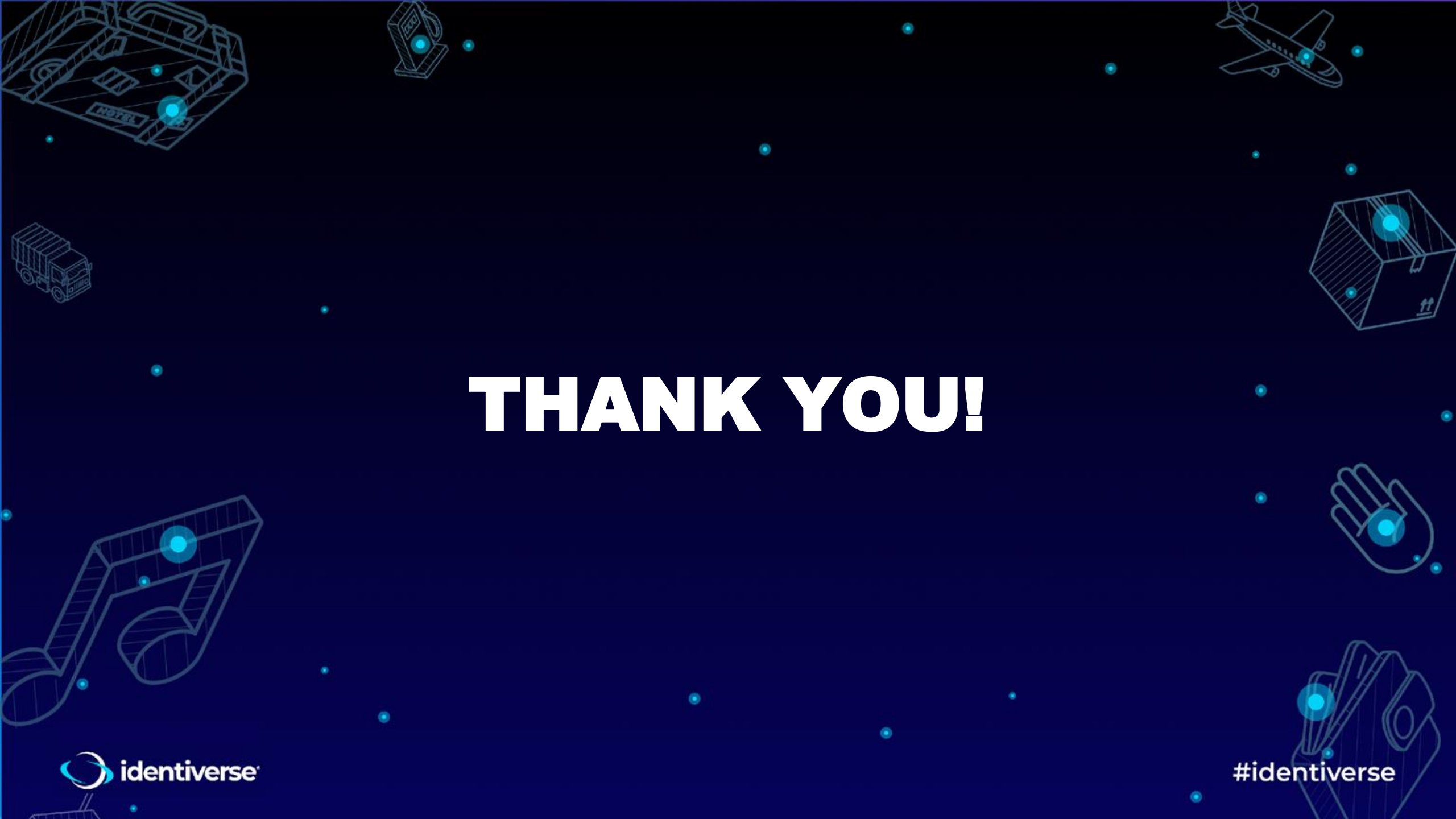
Existing Solutions Fall Short

- Proliferation of shadow accounts
- Access requests don’t account for separation of duties

Our Solution

- ECARF: custom access request portal
- “The Matrix”: rules governing who SHOULD get what access
- Authorization Graph: the “check and balance” across it all


Q&A


THANK YOU!
identiverse
#identiverse