The four adaptive identity problems

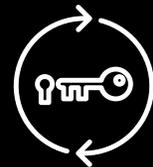**From**

To

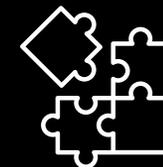Human governance - Policy-time, static

Real-time governance

Protecting AI: agents & machines

Universal & dynamic privilege (JIT / real-time auth)

Threat management: Identity + SOC

What is important for you?

1 Market Leader

2 Innovation – 200m$ in R&D

3 Huge customer base - reference

4 Great local team

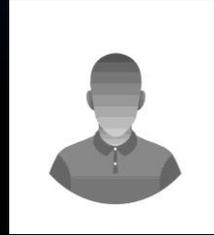5 Great partners - experience

Great local team

Florian Koeppli
RVP Sales

Partner Manager
TBH

Tim Hintermann
SE Mgr

Jerome Mathew
Sales

Nicolas Taffignon
Sales

Anna Gillitzer
Sales

Raymond Huber
SE

SE joining in April

Diturin Mzi
Sales

Gary Cuenoud
Sales

Francesco Staibano
Demand Generation

Technical Advisor joining in April
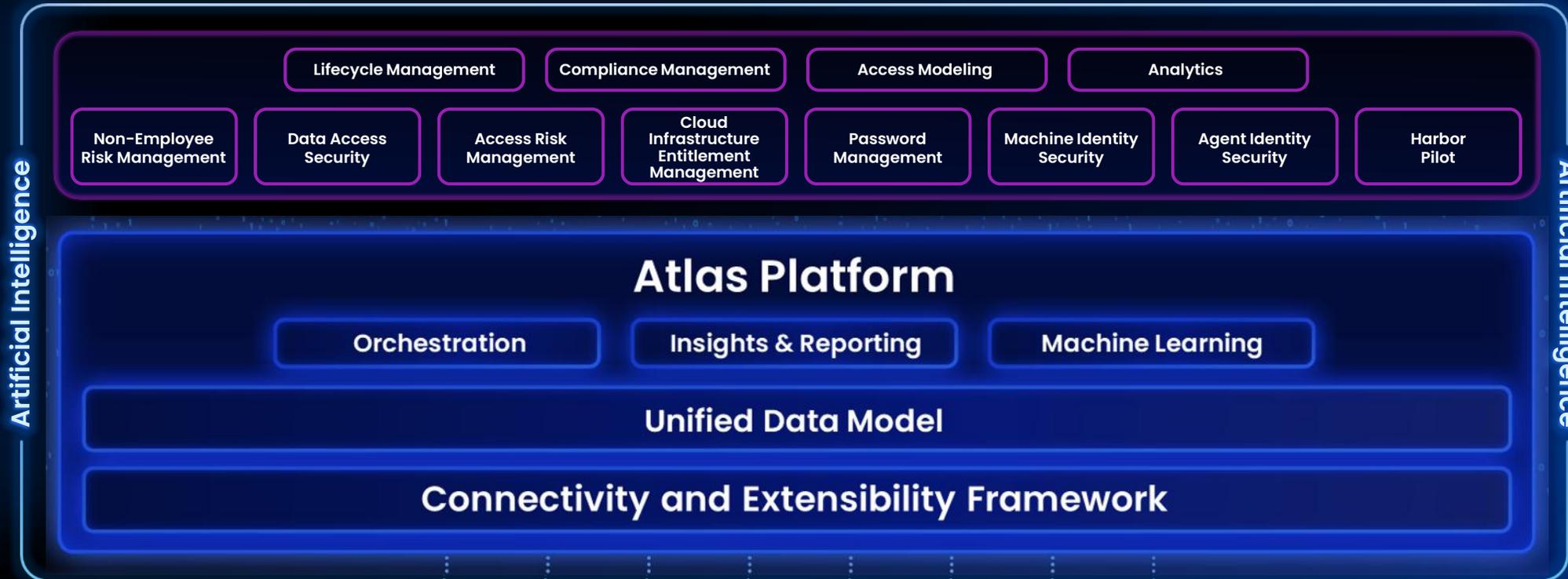
The SailPoint Platform

Employees **Non-Employees** **Machines** **Agents**

Providing comprehensive coverage of all enterprise identities

Lifecycle Management | Compliance Management | Access Modeling | Analytics

Non-Employee Risk Management | Data Access Security | Access Risk Management | Cloud Infrastructure Entitlement Management | Password Management | Machine Identity Security | Agent Identity Security | Harbor Pilot

Agentic User Experience

Harbor Pilot

Artificial Intelligence

Atlas Platform

Orchestration | Insights & Reporting | Machine Learning

Unified Data Model

Connectivity and Extensibility Framework

Artificial Intelligence

Shared Signals Framework (SSF) & Dedicated integrations

jamf paloalto
proofpoint CROWDSTRIKE

5

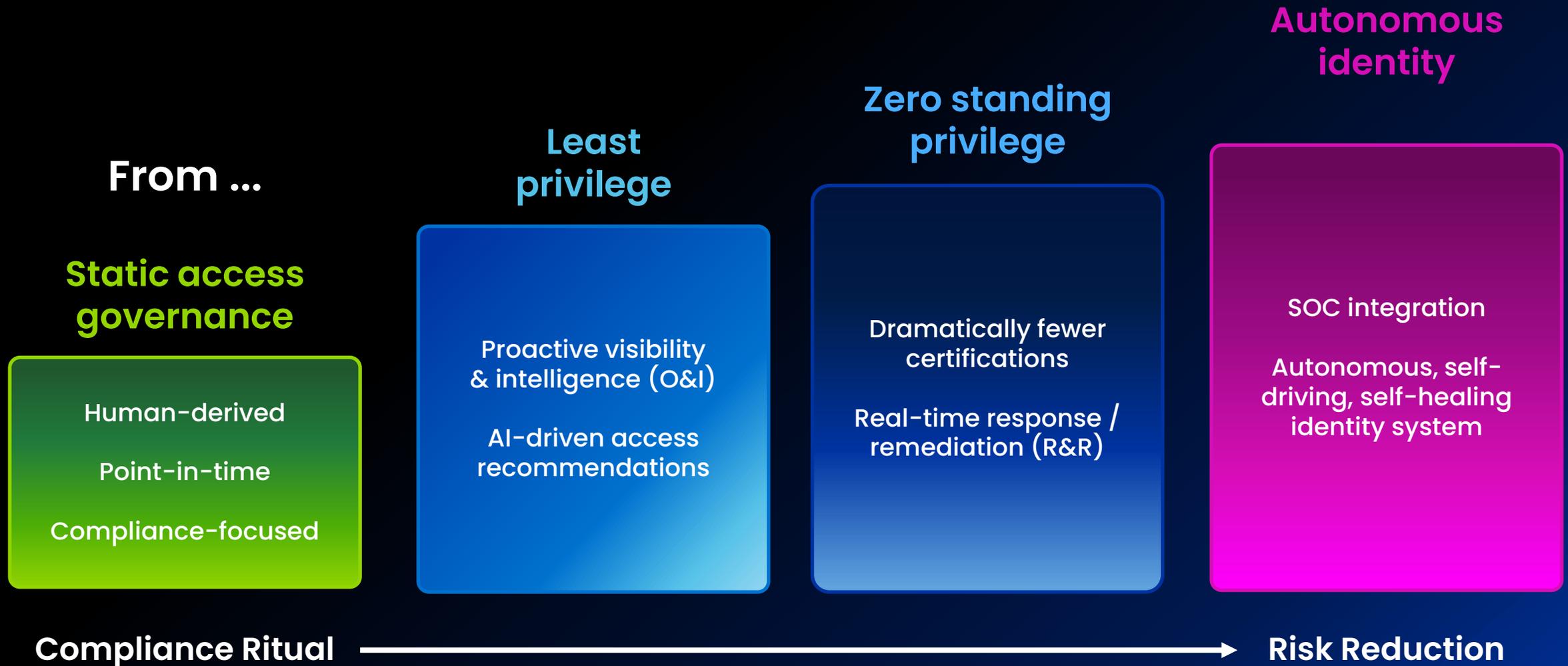# SailPoint's approach to Agent Identity Security

Agents are **a new form of identity**

Agents **cannot be governed in isolation**

SailPoint provides a **unified control plane** to govern agents, and how they interact with humans, machine, and data

SailPoint's Platform Advantage

- Data Access Security
- Non-Employee Identity
- Machine Identity
- Employee Identity
- Agent Identity

SailPoint Atlas

Governed on a unified control plane

Real-time governance

From ...

Static access governance

Least privilege

Zero standing privilege

Autonomous identity

Human-derived	Proactive visibility & intelligence (O&I)	Dramatically fewer certifications	SOC integration
Point-in-time			Autonomous, self-driving, self-healing identity system
Compliance-focused	AI-driven access recommendations	Real-time response / remediation (R&R)	

Compliance Ritual ──────────────▶ **Risk Reduction**

Real-time AI governance and security framework

Protection & trust
Prevent misuse including prompt & response security, guardrails and agent real-time monitoring

Visibility & risk analysis
Discover machines, agents, and shadow AI across all systems

Real-time auth
Grant just-in-time access based on policy, context, and intent

Ownership & user management
Assign owners and manage who can access each agent

Governance & lifecycle management
Provision, certify, and retire agent identities with auditability

Introduction to the Framework: https://www.sailpoint.com/blog/sailpoint-framework-governing-ai-agents

SailPoint Shadow AI Remediation

Real-Time Visibility

- Understand how employees use shadow AI tools like ChatGPT, Claude, and Gemini.

- Monitor document uploads and interaction frequency in real-time.

Remediation & Oversight

- Block unauthorized uploads or redirect users to approved tools.

- Gain centralized oversight to help ensure compliance and reduce security gaps.

Easy Install & No User Impact

- Users keep working with no experience change, unless misuse occurs.

- IT easily deploys a browser extension via device management tools, e.g., Intune or JAMF.
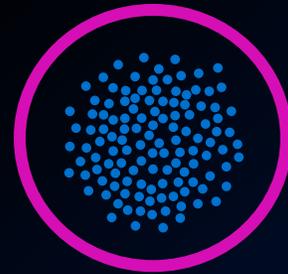
Introduction to the topic: https://www.sailpoint.com/blog/sailpoint-shadow-ai-remediation
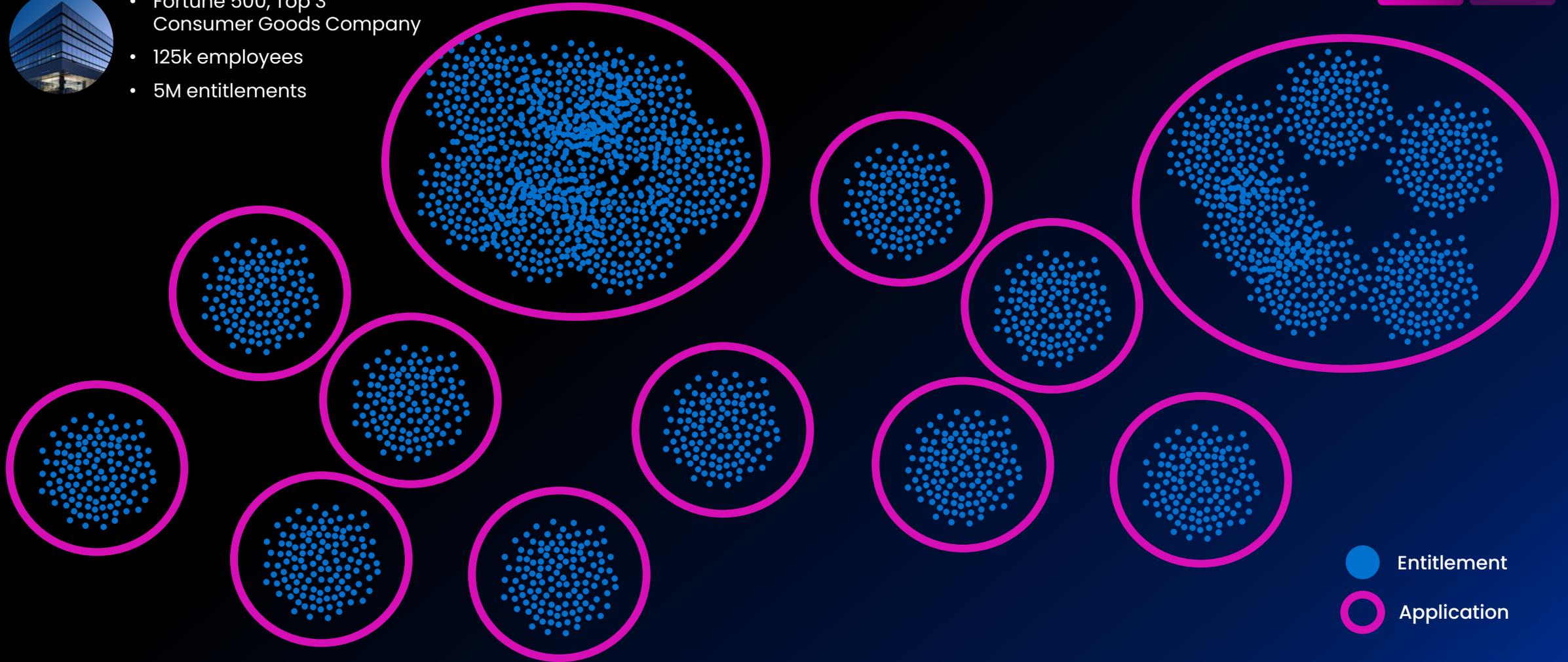
Privilege context
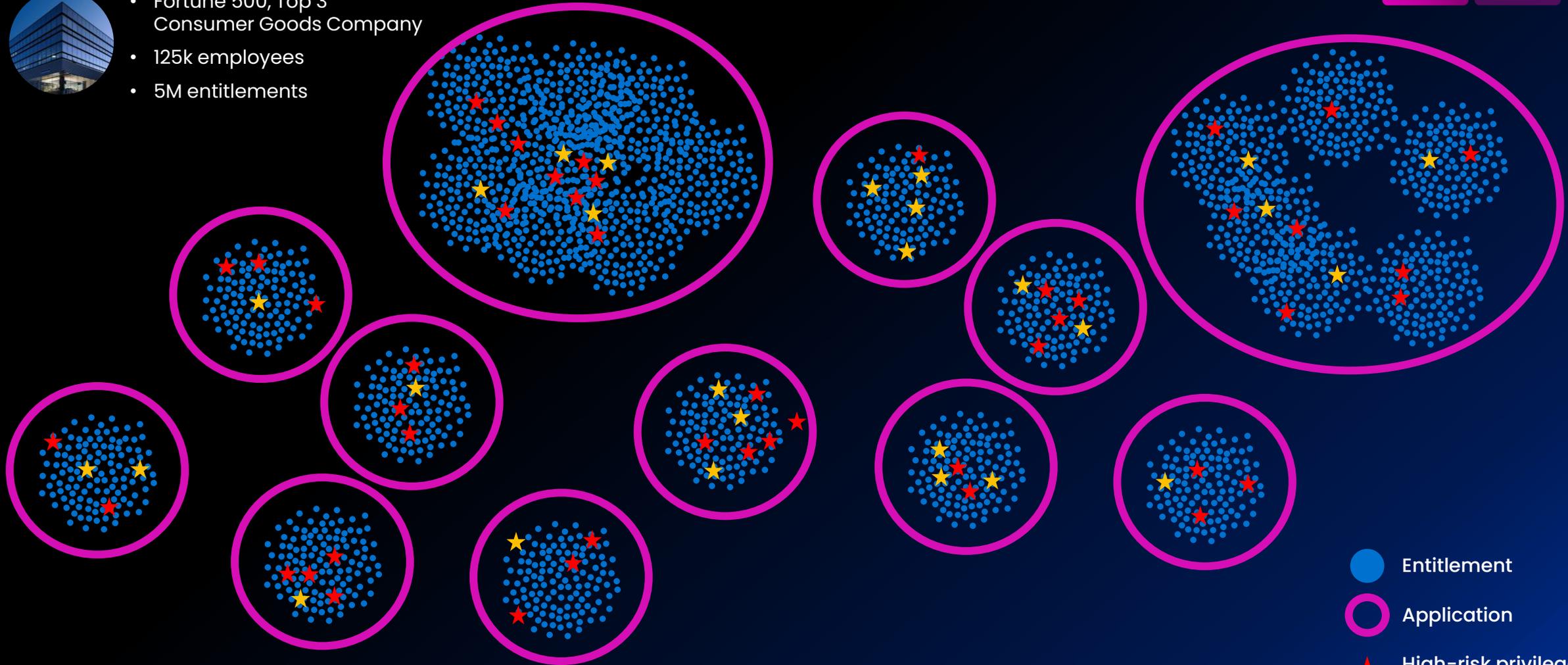

Entitlement

Application

Privilege context

- Fortune 500, Top 3 Consumer Goods Company
- 125k employees
- 5M entitlements

Entitlement

Application

Privilege context

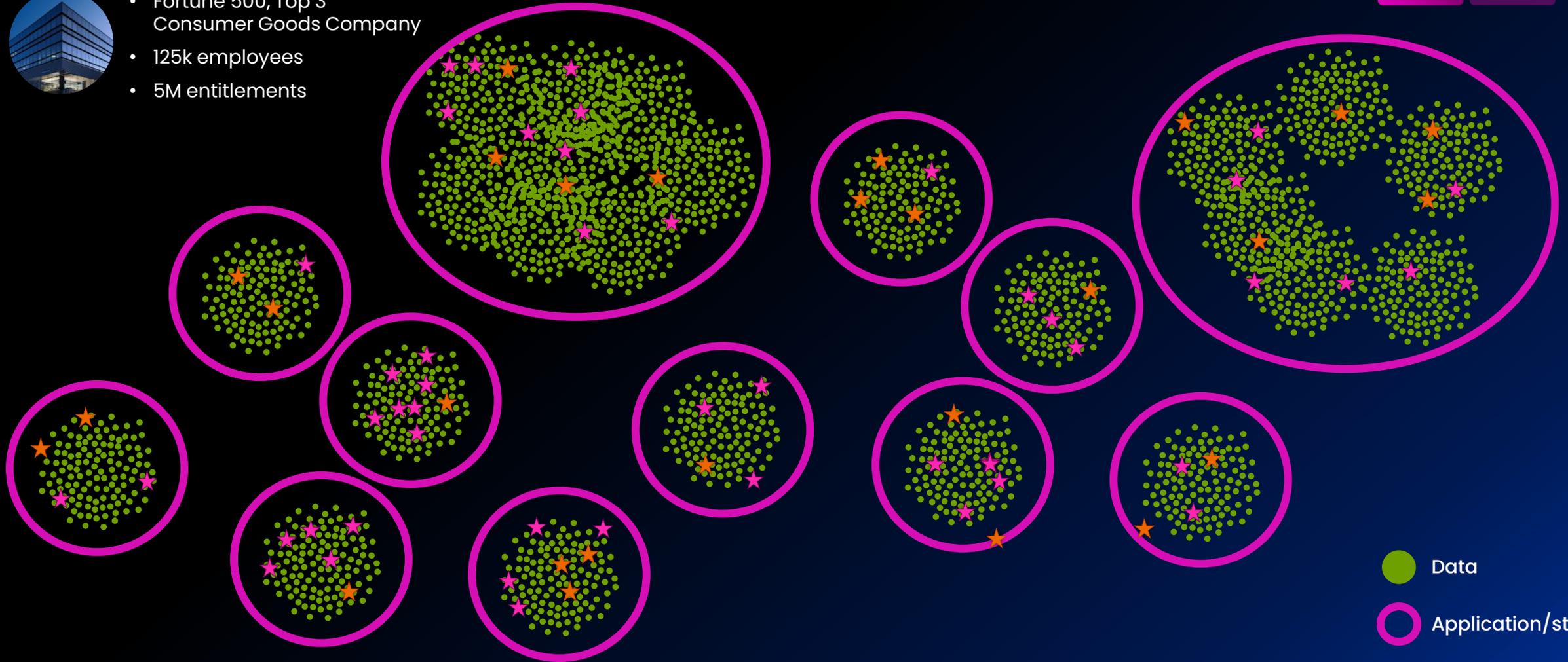- Fortune 500, Top 3 Consumer Goods Company
- 125k employees
- 5M entitlements

Entitlement

Application

High-risk privilege entitlements

Medium-risk privilege entitlements

Privilege context

- Fortune 500, Top 3 Consumer Goods Company
- 125k employees
- 5M entitlements

Legend:
- 🟢 Data
- ⭕ Application/storage
- ⭐ Sensitive data
- ⭐ Internal data

Threat Management (Identity + SOC)

Signal
Indicators: Real-time identity signals describing user access, privileges, and behavior.

Context
Correlating identity data to explain risk, impact, and security prioritization.

Action
Precise, targeted remediation that reduces risk without disrupting business operations.
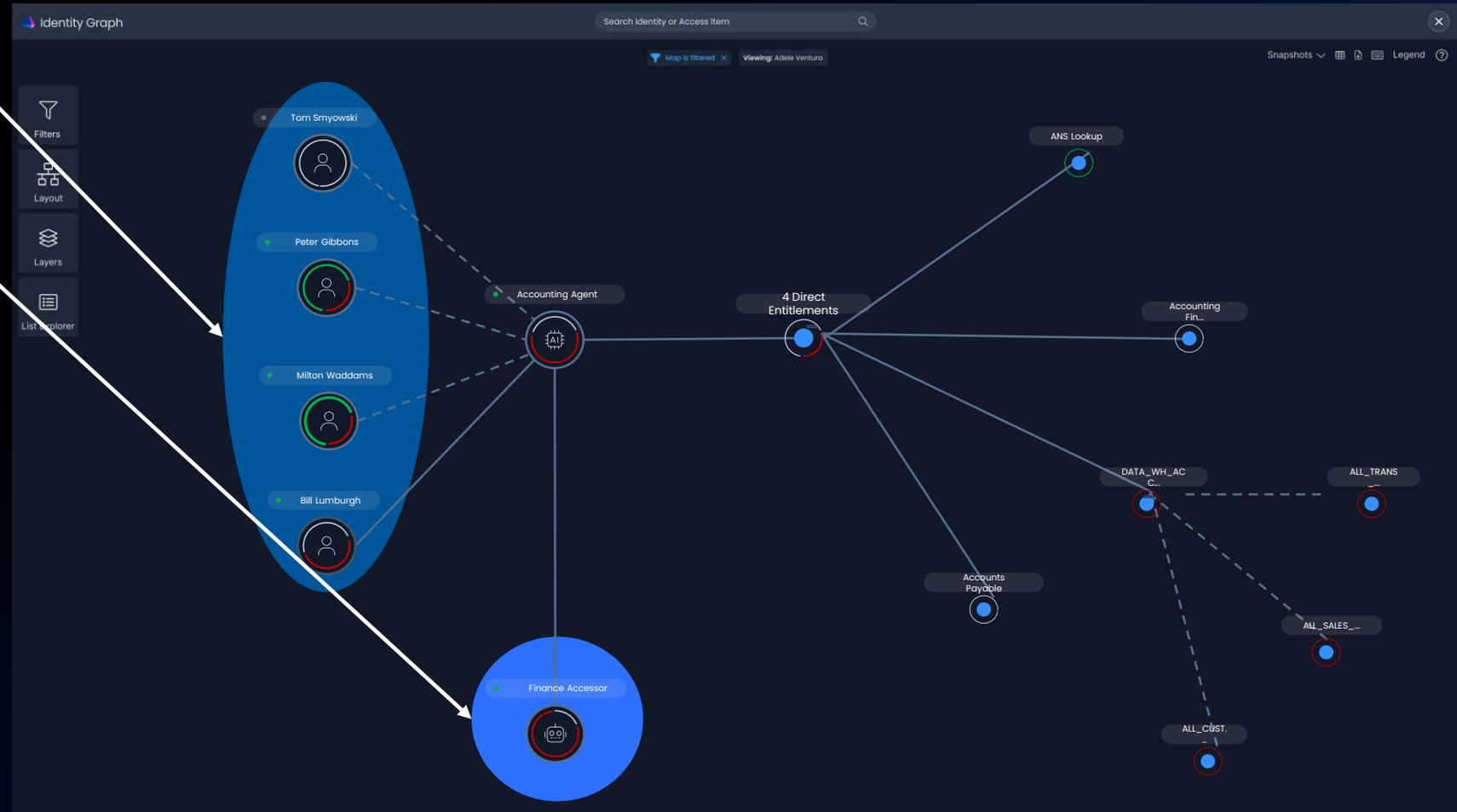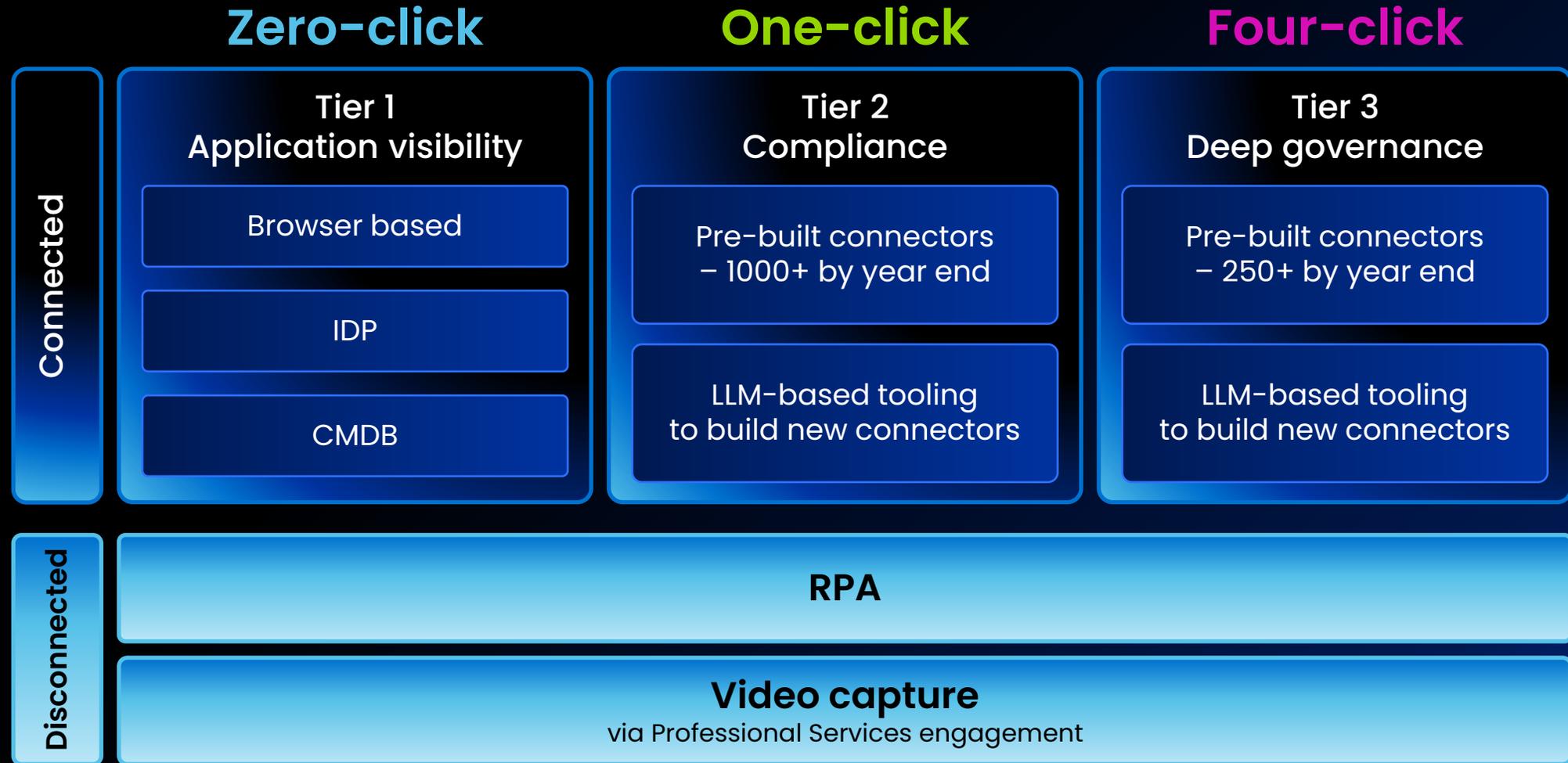
SailPoint Observability & Insights

Humans

Machines

Benefits:
- Visibility, Insight, Control
- Improved identity hygiene
- Faster incident response
- Strong governance & compliance

https://www.sailpoint.com/products/identity-security-cloud/atlas/add-ons/observability-insights

SailPoint's connectivity solution: 0, 1, 4

Zero-click

One-click

Four-click

Connected

Tier 1
Application visibility

Browser based

IDP

CMDB

Tier 2
Compliance

Pre-built connectors
– 1000+ by year end

LLM-based tooling
to build new connectors

Tier 3
Deep governance

Pre-built connectors
– 250+ by year end

LLM-based tooling
to build new connectors

Disconnected

RPA

Video capture
via Professional Services engagement

Thank you