Identity-First APIs: IAM as the Real Platform

Oscar Santolalla. Senior Project Manager, Spinverse

SPINVERSE

Solving global challenges together

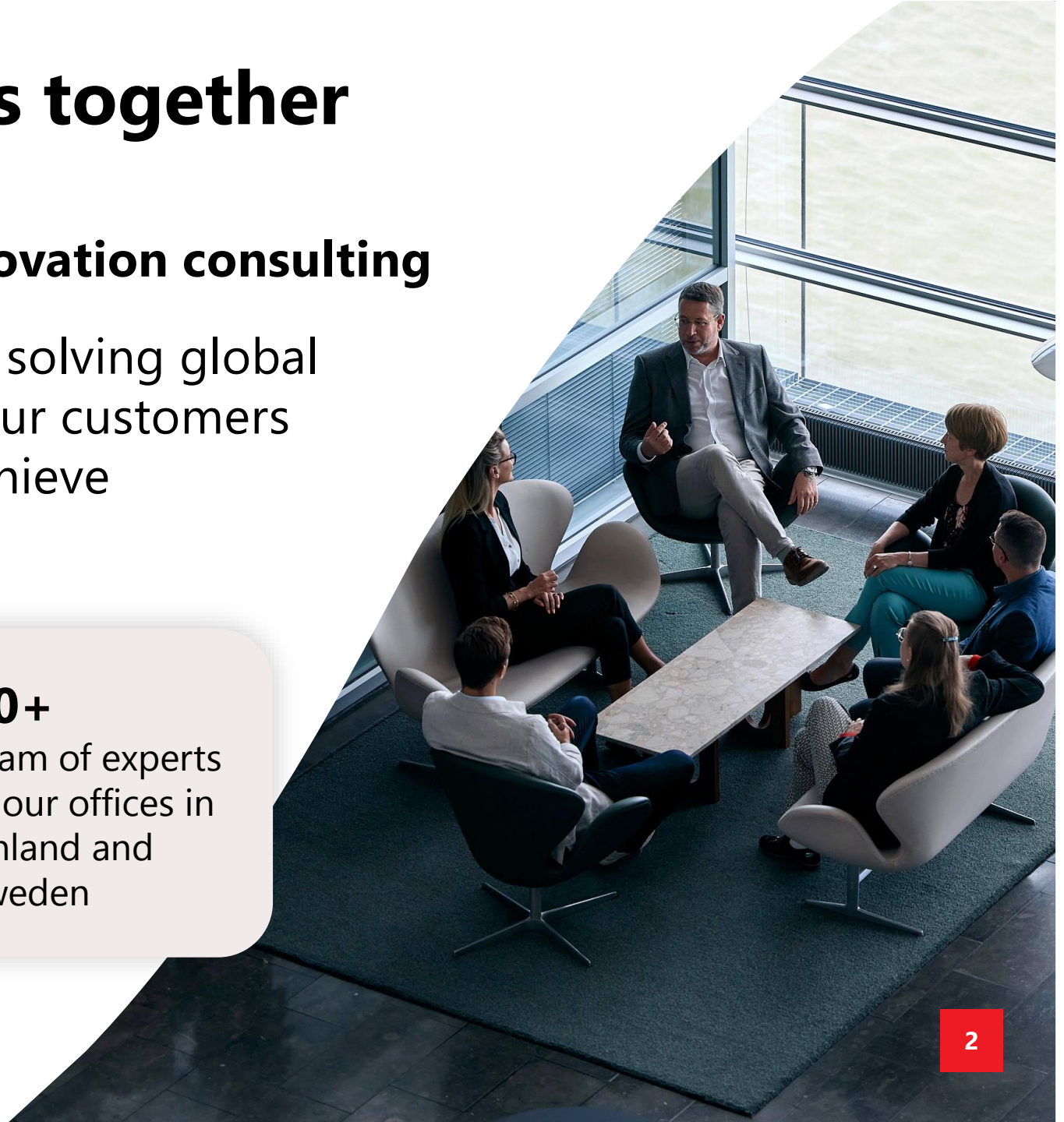
Spinverse is the Nordic leader in innovation consulting

We drive our customers to growth and solving global challenges with innovations. We help our customers ideate, collaborate, get funding and achieve impact with their innovative projects.

€3+ billion
Funding for our customers

5 000+
Organisations engaged in our projects

80+
Team of experts in our offices in Finland and Sweden



SPINVERSE

I. Security weaknesses of APIs

T-Mobile breached by hackers as 37 million customers impacted

The company went through extensive cybersecurity measures after a previous hack.

By Luke Barr
January 20, 2023, 11:57 AM

Hackers steal personal info on 37 million T-Mobile customers Addresses, phone numbers and dates of birth were stolen but the company says credit cards were not exposed.

INNOVATION > CYBERSECURITY

Dell Confirms Database Hacked—Hacker Says 49 Million Customers Hit

By Davey Winder, Senior Contributor. Davey Winder is a veteran cybersecur...
Follow Author

Published May 10, 2024, 05:27am EDT, Updated May 10, 2024, 09:56am EDT

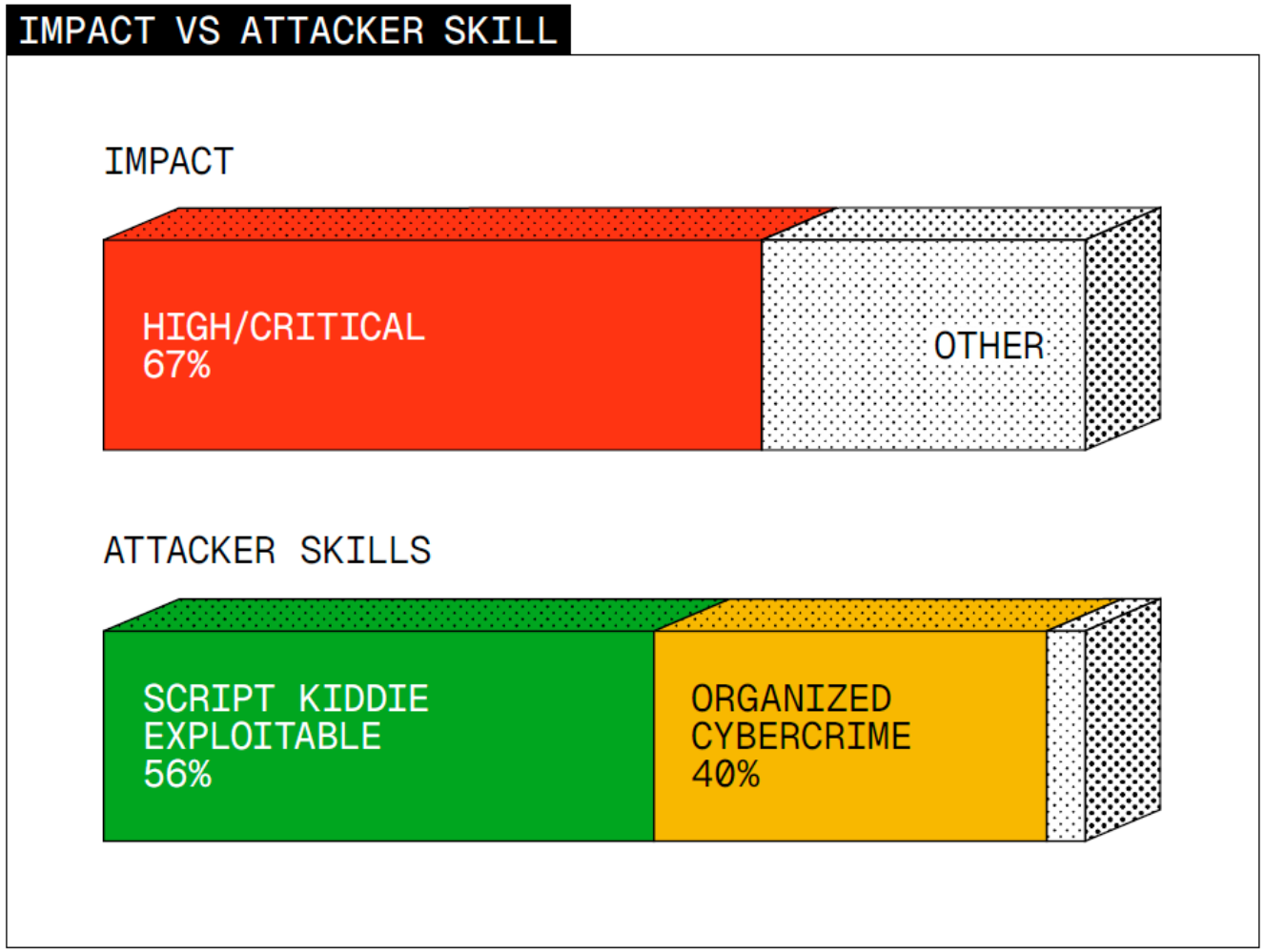
INNOVATION > CONSUMER TECH

Personal Details Of 15 Million Trello Users Up For Sale

By Barry Collins, Senior Contributor. Barry Collins is a tech journalist writing...
Follow Author

Published Jan 23, 2024, 05:12am EST, Updated Jan 23, 2024, 07:59am EST

Most high-impact API vulnerabilities do not require advanced attackers



Source:
Wallarm 2026 API ThreatStats Report

What causes most security vulnerabilities in APIs?

Authorization

OWASP API Security Top 10 — mostly authorization

API1	**Broken Object Level Authorization (BOLA)**	AuthZ
API2	Broken Authentication	AuthN
API3	**Broken Object Property Level Authorization**	AuthZ
API4	Unrestricted Resource Consumption	Other
API5	**Broken Function Level Authorization (BFLA)**	AuthZ
API6	**Unrestricted Access to Sensitive Business Flows**	AuthZ

4 / 6

of the top six risks are authorization failures.

BOLA alone is the #1 API vulnerability

Your homework:

What Broken Object Level Authorization (BOLA) is?

SPINVERSE

BOLA shows that

Nobody takes authorization seriously

SPINVERSE

II. Authorization is not the same as authentication

AUTHENTICATION

"Who are you?"

Login, password, MFA, SSO.
Proves identity — nothing more.

AUTHORIZATION

"What are you allowed to do?"

Roles, scopes, policies, rules.
Enforced at every action.

What is IAM?

What is IAM?

Identity and Access Management

The discipline of deciding who gets to do what, inside your system.

Identity who is making the request
Access what they're allowed to do

IAM is one of many domains within cybersecurity

*Based on **ISC² CISSP** Common Body of Knowledge — the industry standard framework*

D1 Security and Risk Management	D2 Asset Security	D3 Security Architecture and Engineering	**D5 Identity and Access Management (IAM)**
D4 Communication and Network Security	D6 Security Assessment and Testing	D7 Security Operations	D8 Software Development Security

SPINVERSE

In practice, when developers use IAM?

The moments that force a developer to learn IAM:

Add a login page to the app.

Connect our app to Google / GitHub / Apple.

Only admins should be able to delete things.

If authorization is the problem, what is the solution?

Year 2010. The problem was:

“I want to let a 3rd-party photo printing service access my photos stored online, without giving my password”

SPINVERSE

Solution:

A framework that gives an app limited, revocable access to your data without ever sharing your credentials.

SPINVERSE

That framework is OAuth 2.0

The cornerstone of modern authorization frameworks

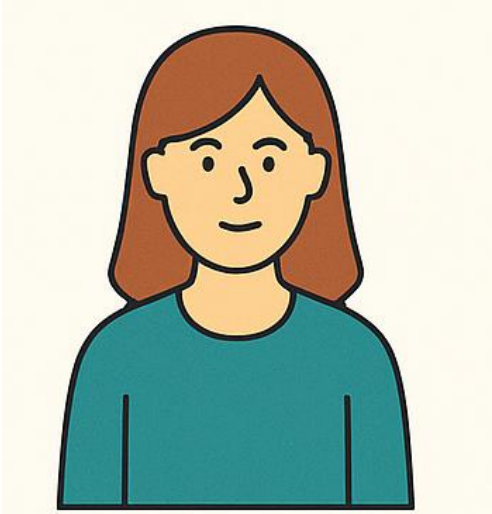
SPINVERSE

OAuth 2.0 uses short-lived access tokens

SPINVERSE

Hotel keycard Analogy

Guest (You) =
The User



Keycard =
Access Token

Hotel room door lock =
Resource Server (API)

Hotel reception =
Authorization Server

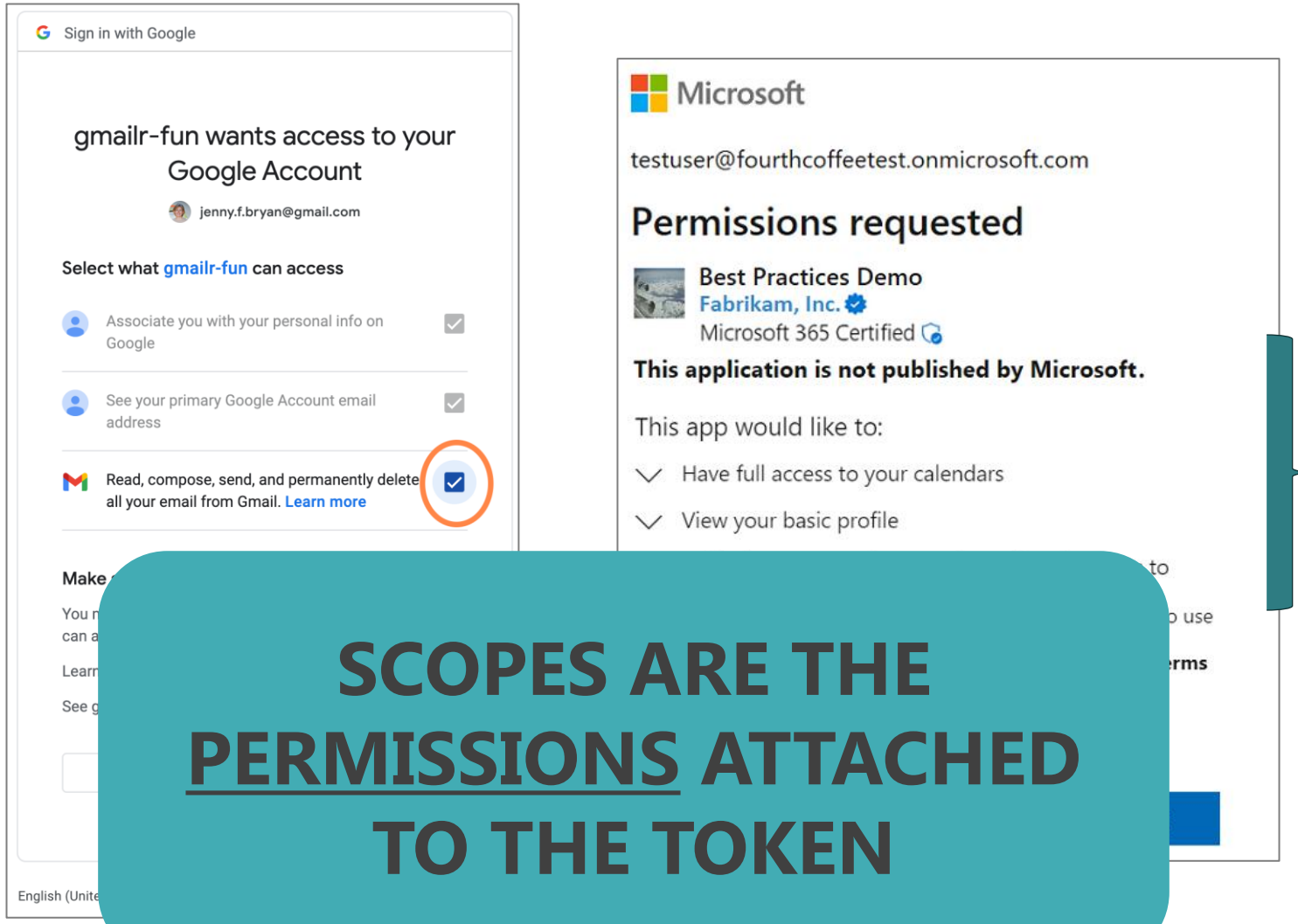
SPINVERSE

In OAuth 2.0, what are scopes?

SPINVERSE

Examples of OAuth consent page

SCOPES

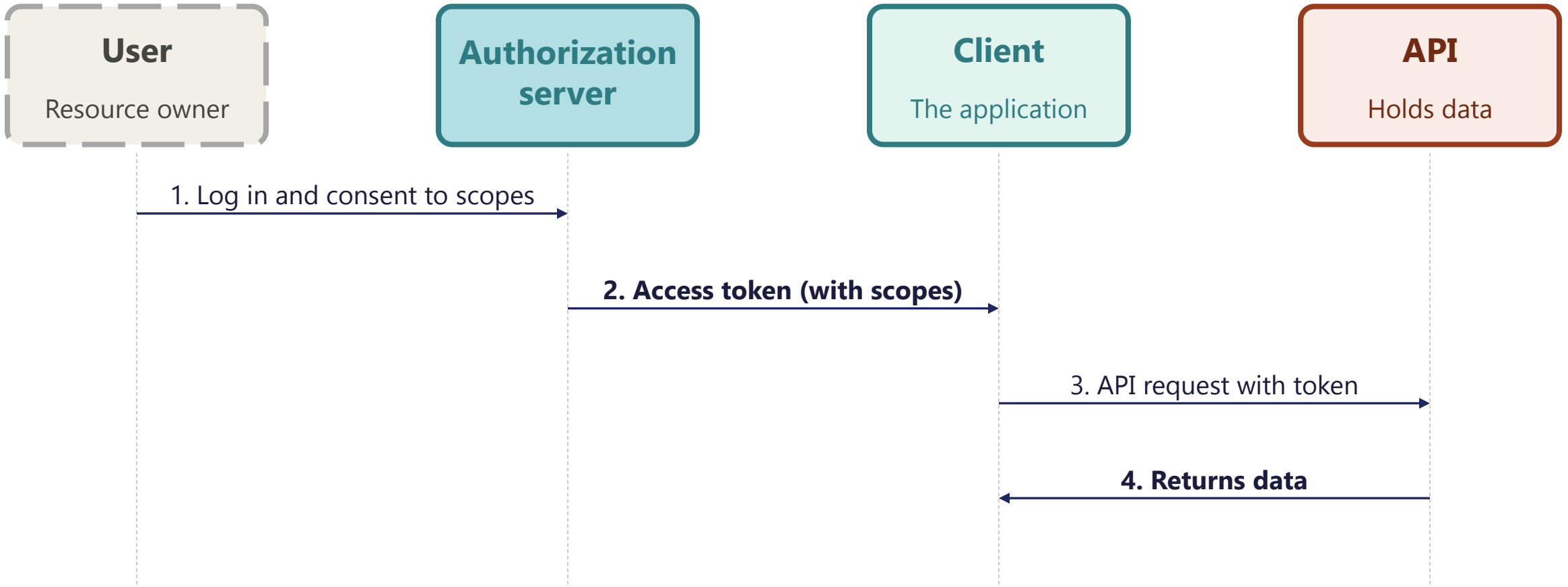


SCOPES

SCOPES ARE THE PERMISSIONS ATTACHED TO THE TOKEN

SPINVERSE

OAuth 2.0. The four-step dance



SPINVERSE

Now,
what happens when AI agents come into the equation?

1. The agent has no identity of its own.

It borrowed your keycard.

Nobody downstream can tell the difference.

When an email arrives, a calendar event is created, a record is updated...

...the receiving system sees one thing:

Alice took this action

Alice's authorized agent took this action

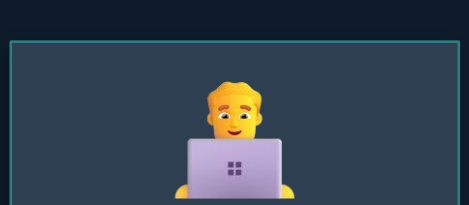
A compromised agent took this action

No audit trail. No accountability. No governance.

2. Traditional authorization works when you can **pre-specify every action.**

AI agents decide what to do at runtime.
You cannot pre-specify it.

Traditional systems: the developer knows every action in advance



developer

knows what the system will do

defines

🔒 **SCOPE — fixed at design time**

```
read:  database_A

write: queue_B
call:  api_1, api_2,
api_3
```

grants

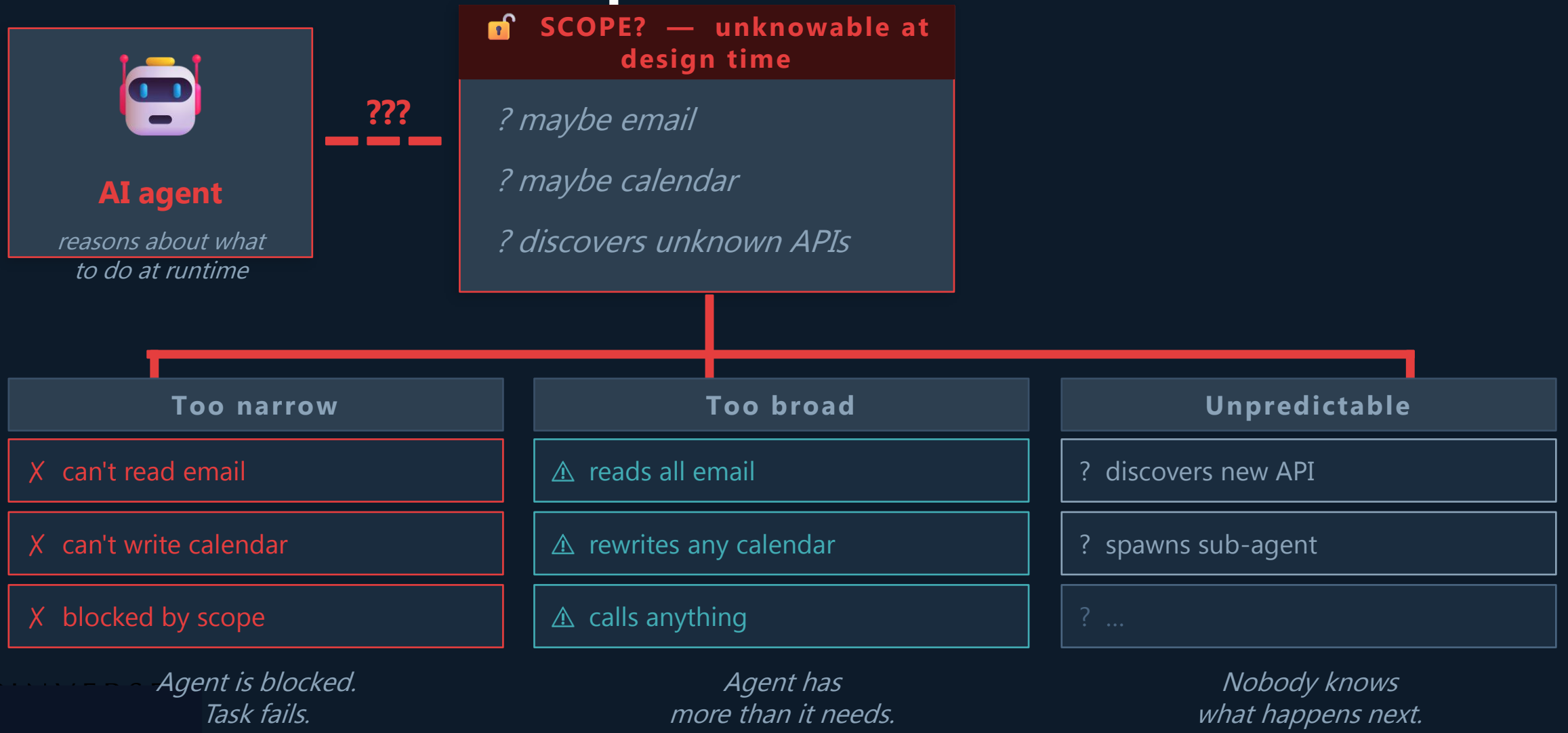
✓ read database_A — *predictable*

✓ write to queue_B — *predictable*

✓ call api_1, api_2, api_3 — *predictable*

Grant exactly those permissions — and nothing more. Static scopes work perfectly here.

AI agents: actions emerge at runtime, nobody pre-specified them

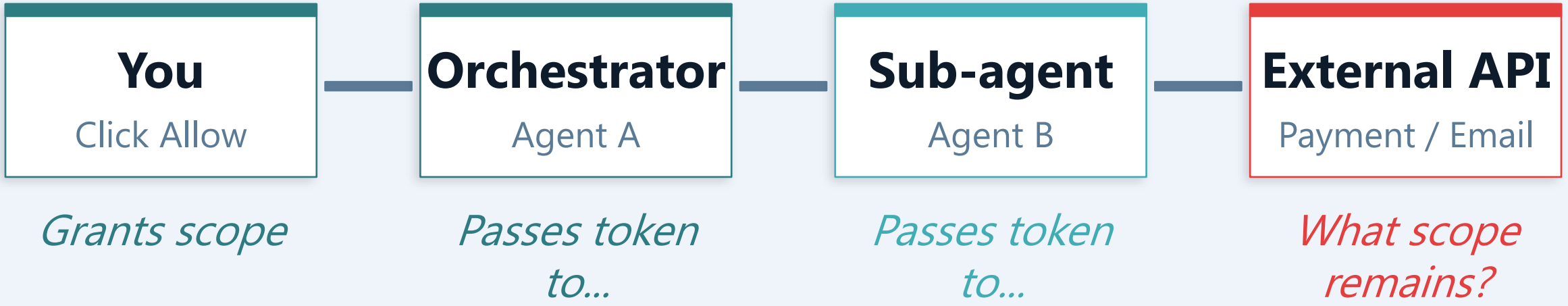


3. Delegation chains dissolve

the original permission boundary.

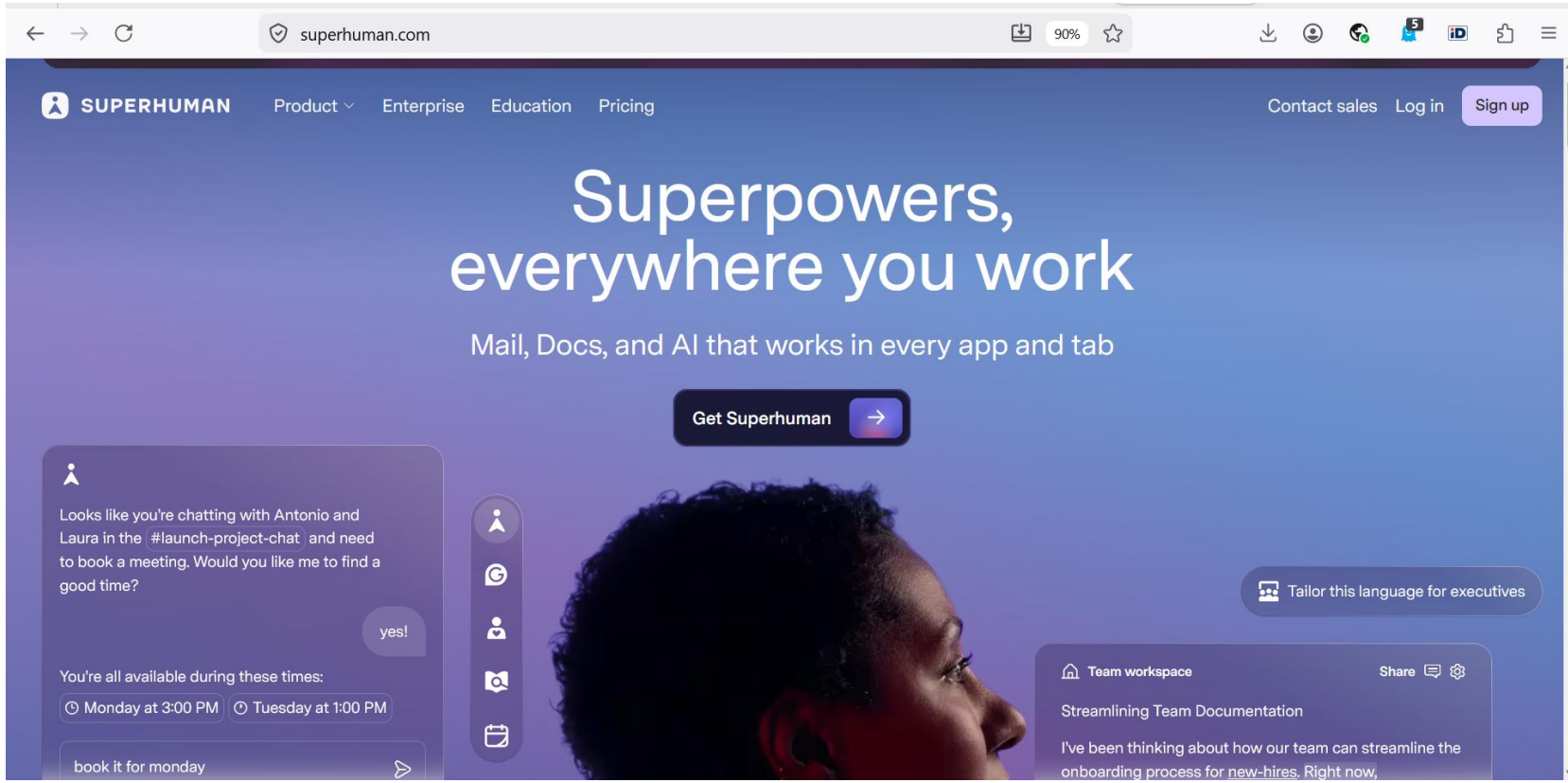
By the last hop, the user's intent and scope are gone.

The Multi-Agent Chain Problem



SPINVERSE

Today, agent applications implement makeshift solutions

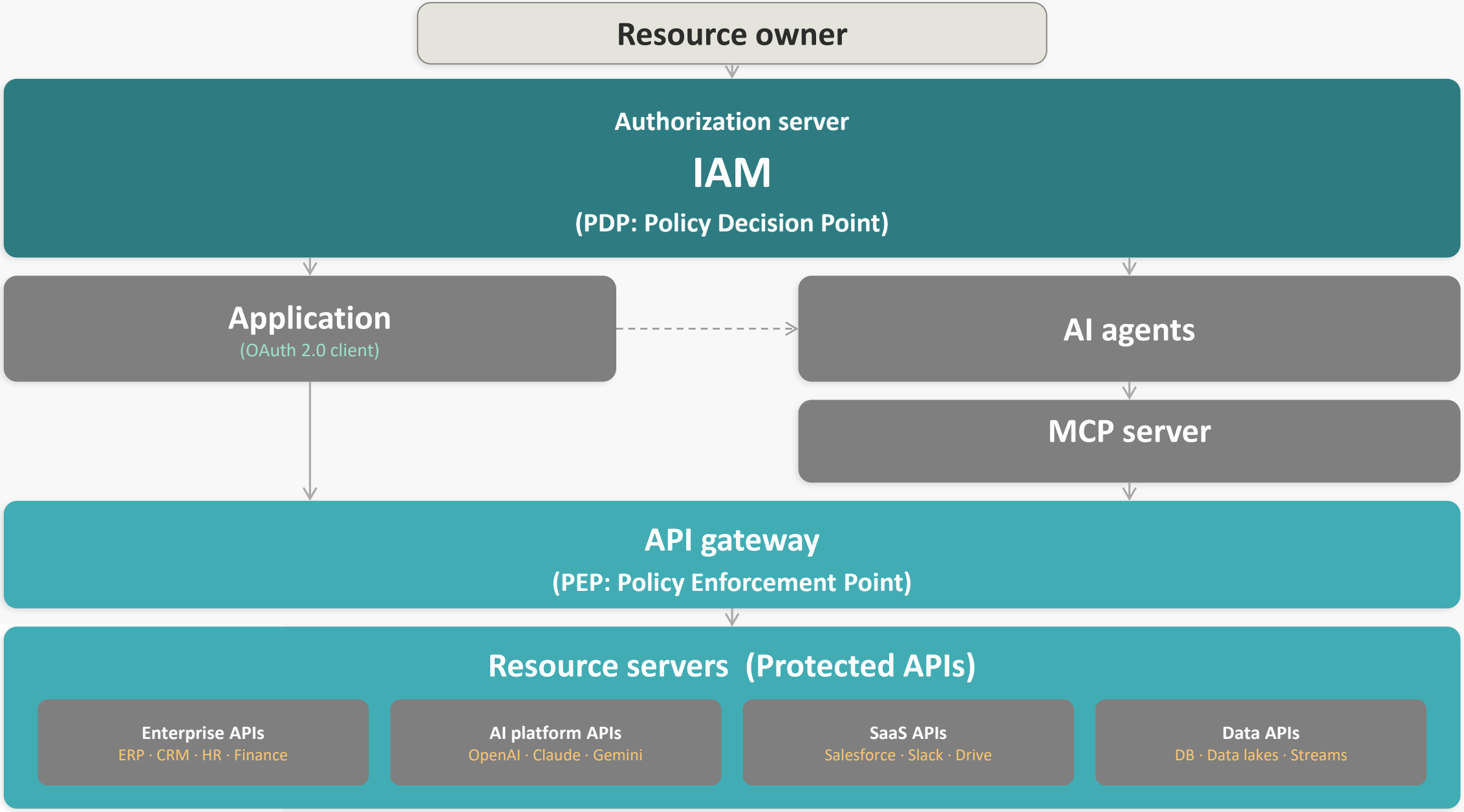


SPINVERSE

III. How IAM becomes the control layer

A control layer is needed.
IAM is needed.

IAM is the Control Layer



AI Agents' authorization problem is not solved yet

RFC 8693 OAuth 2.0 Token Exchange
RFC 9396 OAuth 2.0 Rich Authorization Requests (RAR)
Agent2Agent (A2A) Protocol
...

SPINVERSE

API PROTECTION WITH OAUTH:

AUTHORIZATION CODE GRANT + PKCE

PKCE is a MUST for public clients, recommended for confidential clients

SPINVERSE

OAuth 2.0 expertise should be in-house.

Someone in-house must understand IAM well.

T-Mobile breached by hackers as 37 million customers impacted

The company went through extensive cybersecurity measures after a previous hack.

By Luke Barr
January 20, 2023, 11:57 AM

Hackers steal personal info on 37 million T-Mobile customers Addresses, phone numbers and dates of birth were stolen but the company says credit cards were not exposed.

Teams that understand IAM won’t be in the headlines

Oscar Santolalla
oscar.santolalla@spinverse.com

4.6.2026