The Identity Mismodeling Crisis:

Rectifying B2C and Workforce IAM Misuse in B2B Ecosystems

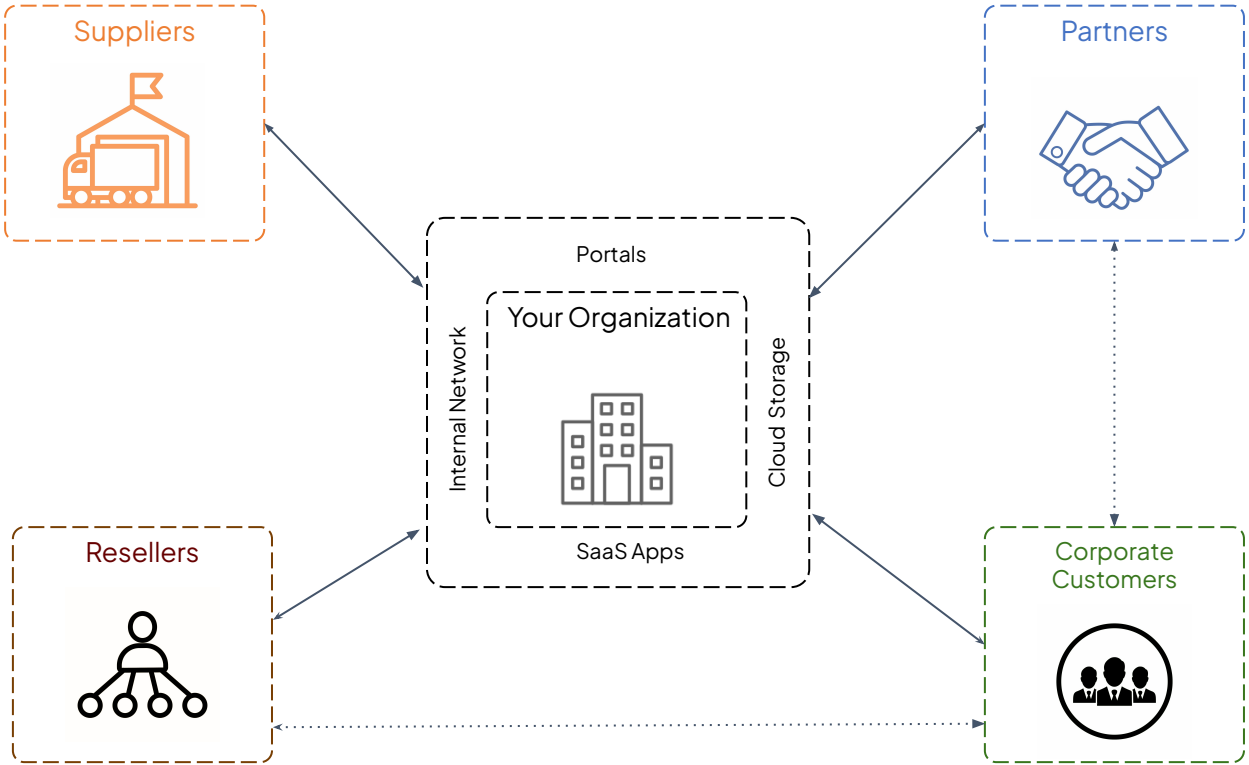
Anuradha Karunarathna

Technical Lead

WSO2

B2B Ecosystem

Collaborations and interactions are multi-faceted, out of the organization's boundary



A decade apart. Third-Party Risk Still Breaks the Enterprise

TARGET RETAIL STORES

December 2013

~40M debit and credit card accounts · 70M PII records

- The Heating, Ventilation, and Air Conditioning (HVAC) vendor Fazio had access to Target's payment system network.
- Attackers phished HVAC vendor credentials.
- Gained access to the TARGET payment system.

Over-privileged third party

CHANGE HEALTHCARE

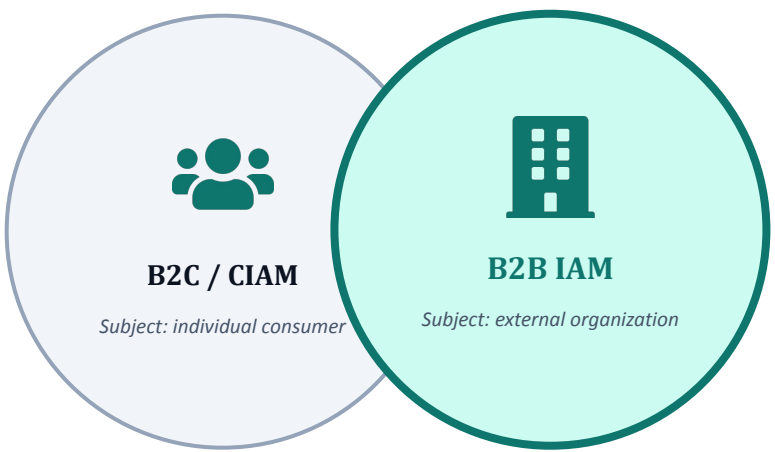
February 2024

~190M individuals affected

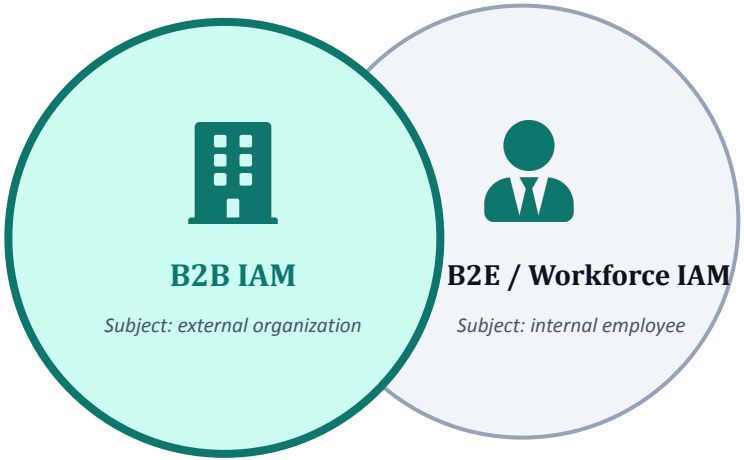
- "Change healthcare" used a third party application "Citrix" to gain remote-access to internal portals
- MFA was not enabled on the Citrix remote-access portal
- Through one stolen credential of an employee, attacker accessed Citrix
- Then, gained access to "Change Health" network through remote access

Under-secured third-party tool

What majority thinks …



If few business customers available, model them along with B2C IAM suite



If few partners available, model them in workforce IAM suite

Functionally it might work

until a third-party organization's requirement stretches the model,
or the pain accumulates over time and finally surfaces as risk.

what about the risk?

OBSERVED IN THE FIELD

Challenges and pain points

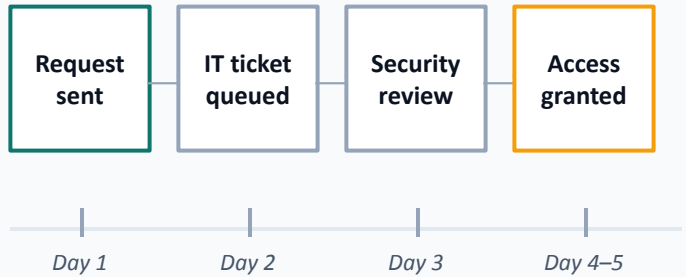
Common problems that surface when B2B is modeled as B2C or workforce.

PAIN POINT #1

Onboarding a partner's new member takes days

- Access requests route through shared IT tickets.
- Approvals are manual, handled by your team, not the partner's.
- Every new seat of partner is a new help-desk ticket for you.
- No self-service path for the partner's own admins.
- End of the day, identity get fragmented. Same user have different credentials to access third party portals.

What the customer experiences

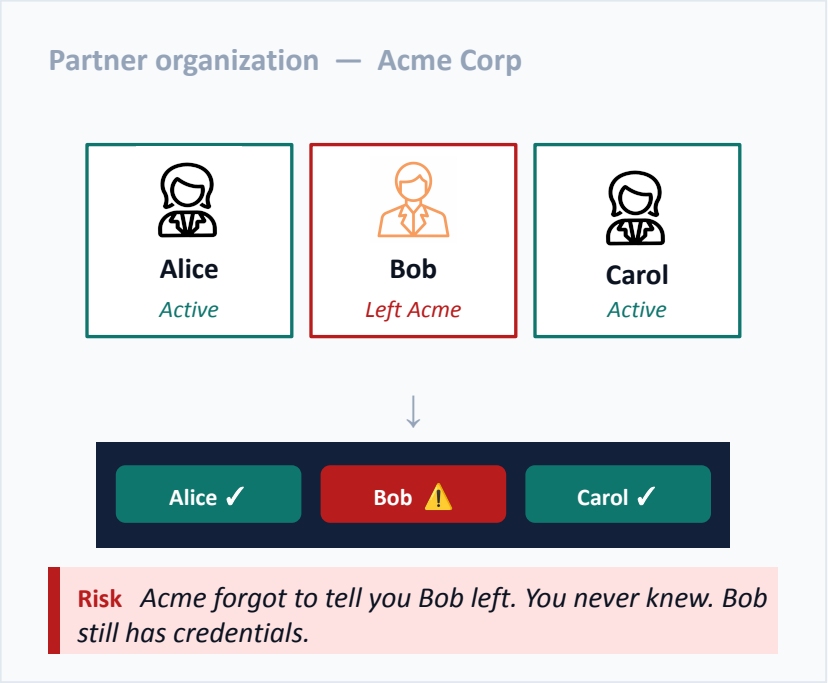


Impact *Partner waits while deals stall. Enterprise buyer loses patience with your onboarding SLA.*

PAIN POINT #2

Partner leavers silently retain access

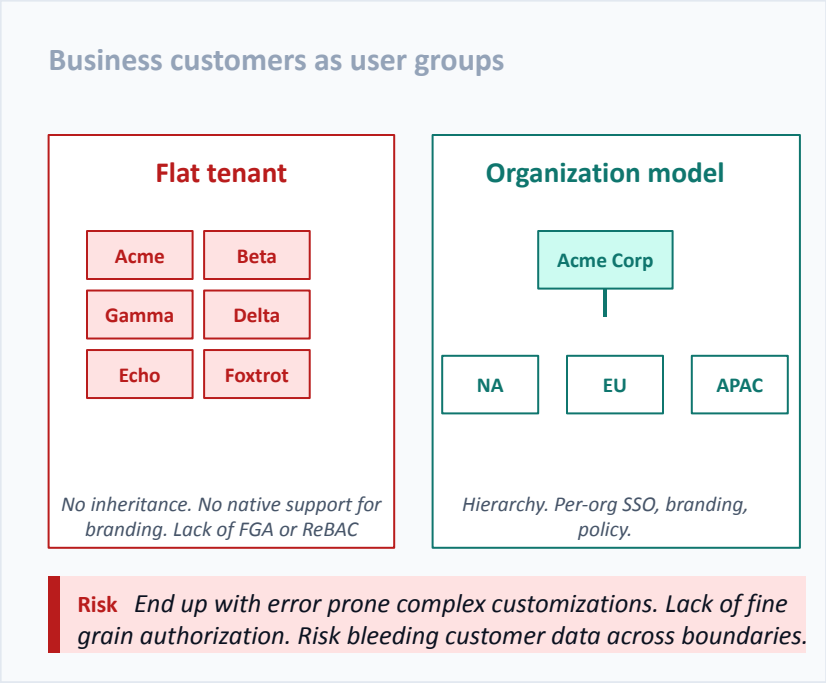
- Deprovisioning depends on the partner telling you someone left.
- No Partner HR to your IS link. Their workforce changes don't reach your IAM.
- Orphaned accounts outlive the employment relationship.
- You learn about it when an auditor finds it, not your system.



PAIN POINT #3

Flat user groups don't scale to many business customers

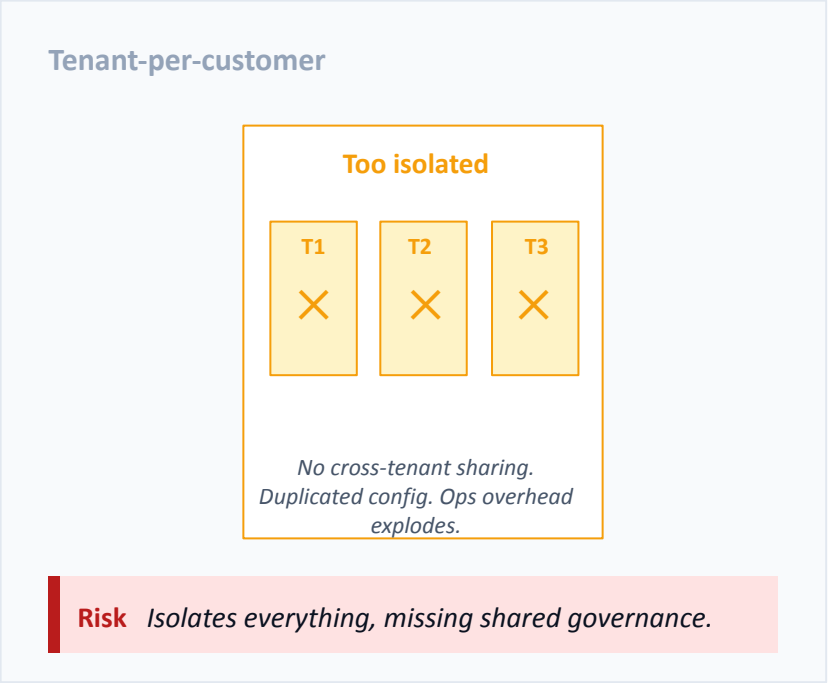
- Each business customer becomes just another group in a shared tenant.
- No parent-child hierarchy for sub-orgs, regions, or business units.
- No Fine Grained Authorization (FGA).
- Group-level access control customization will be complex.



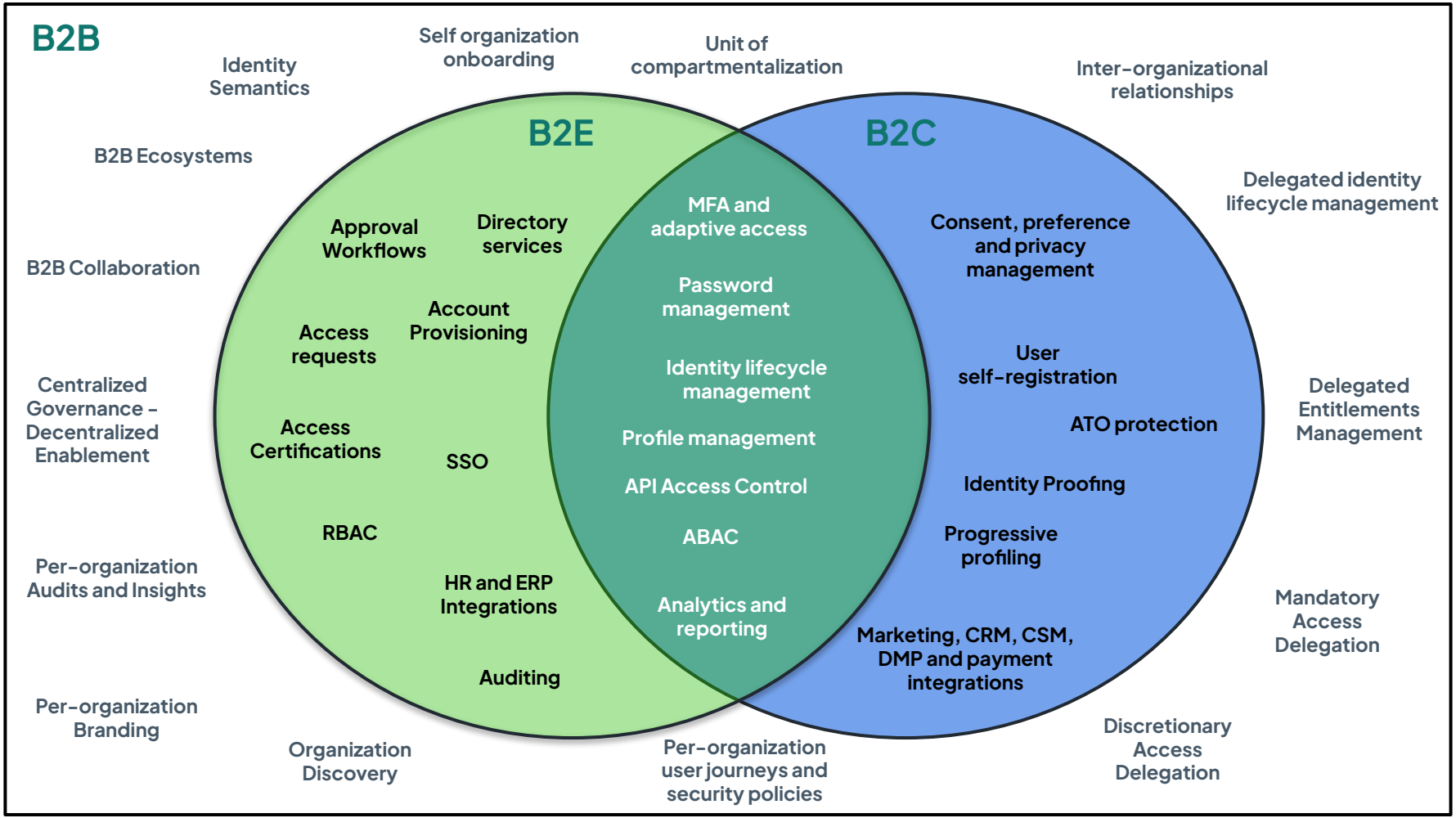
PAIN POINT #4

Tenant-per-customer creates the isolation-sharing dilemma

- Strict isolation duplicates config across every tenant you spin up.
- User identity duplication across different isolated instances.
- Data synchronization and management nightmares.




contractors vendors consultants
partners suppliers
corporate customers Partner IAM
Delegated administration third party identity management
contractors vendors consultants
B2B IAM
Delegated administration third party identity management
B2B IAM vendors consultants
partners B2B IAM Partner IAM
suppliers corporate customers
vendors
corporate customers
Delegated administration Partners
Partner IAM
third party identity management


B2B
Identity Semantics
Self organization onboarding
Unit of compartmentalization
Inter-organizational relationships
B2B Ecosystems
B2E
B2C
Delegated identity lifecycle management
B2B Collaboration
Approval Workflows
Directory services
MFA and adaptive access
Consent, preference and privacy management
Password management
Account Provisioning
Access requests
User self-registration
Identity lifecycle management
Centralized Governance - Decentralized Enablement
Delegated Entitlements Management
Access Certifications
ATO protection
Profile management
SSO
API Access Control
Identity Proofing
RBAC
ABAC
Progressive profiling
Per-organization Audits and Insights
HR and ERP Integrations
Analytics and reporting
Mandatory Access Delegation
Marketing, CRM, CSM, DMP and payment integrations
Auditing
Per-organization Branding
Organization Discovery
Per-organization user journeys and security policies
Discretionary Access Delegation

A reference blueprint

Main characteristics or capabilities expect in a B2B IAM solution

Characteristics of B2B identity solution

Organization identity semantics

Organizations have identity semantics such as attributes.

Name
Legal Identifier
Status after KYB verification
Registration number
Address
|
| – Street Address
| – Town
| – State/Province
| – Postal Code
| – Country
Domain
Email
Subscription

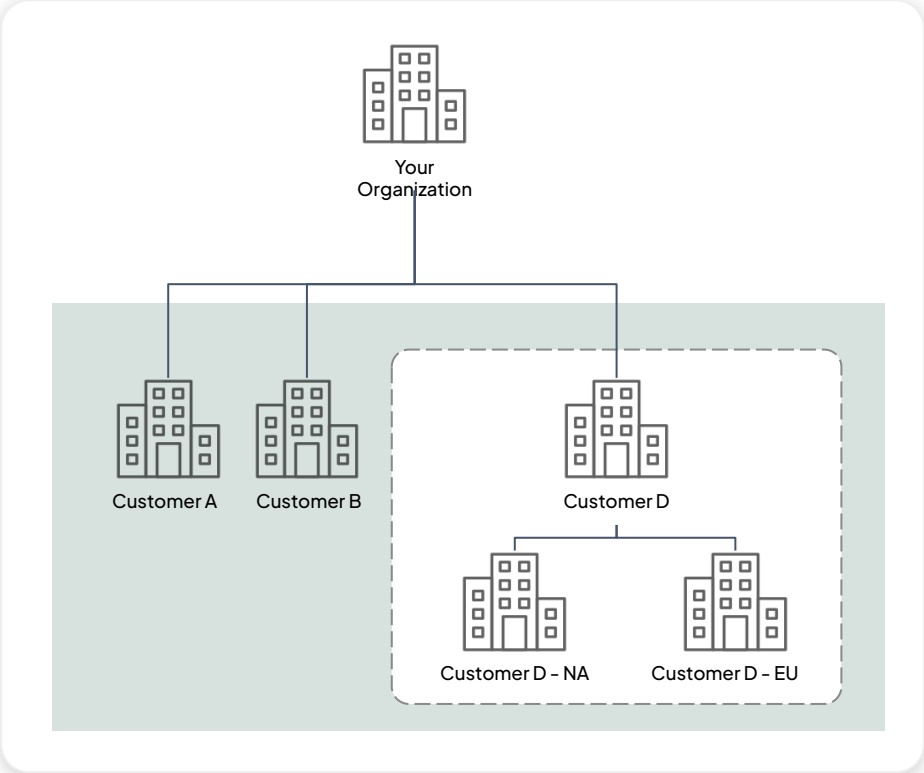
Characteristics of B2B identity solution

Hierarchical organization management

Built-in tenancy for logical compartmentalization of each enterprise customer/partner for

- customization and
- governance

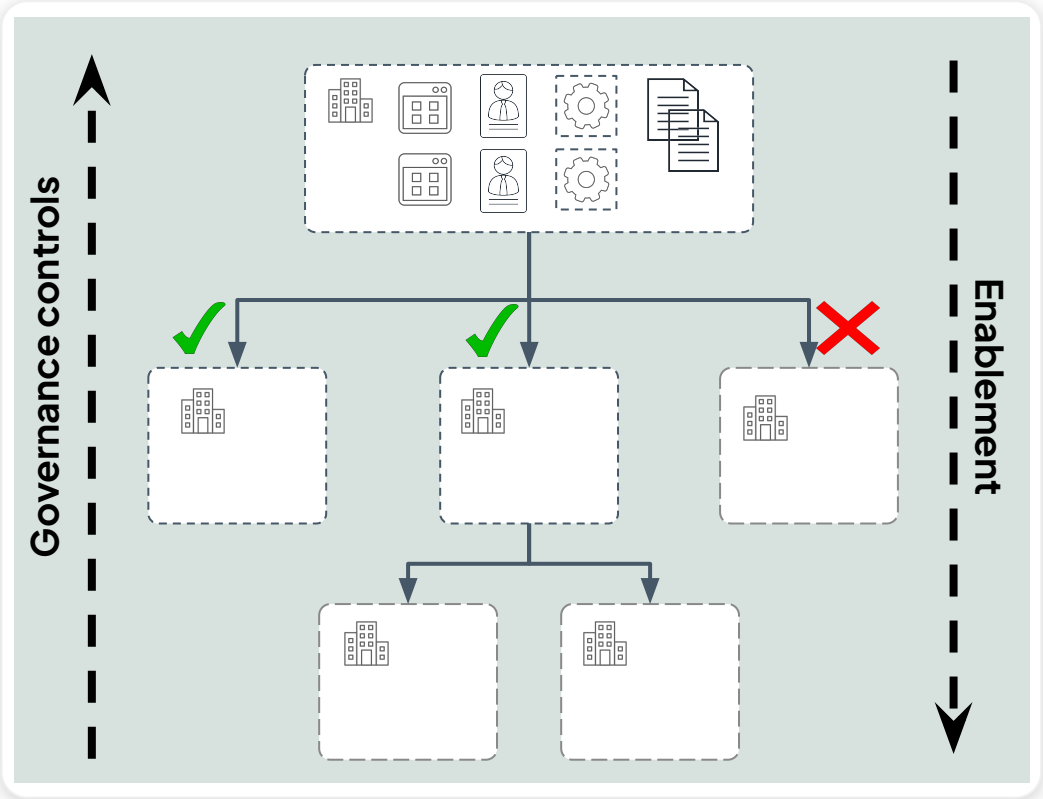
Heterogeneity across the organization is a key



Characteristics of B2B identity solution

Centralized governance - Decentralized enablement

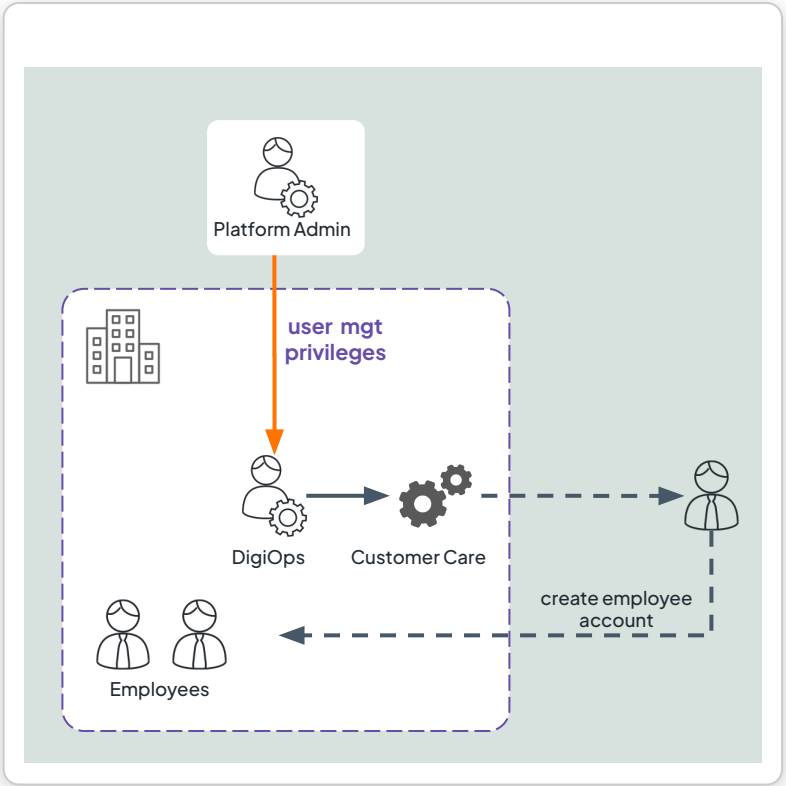
Govern access to your applications and API portfolio by organizations.



Characteristics of B2B identity solution

Delegated user lifecycle management

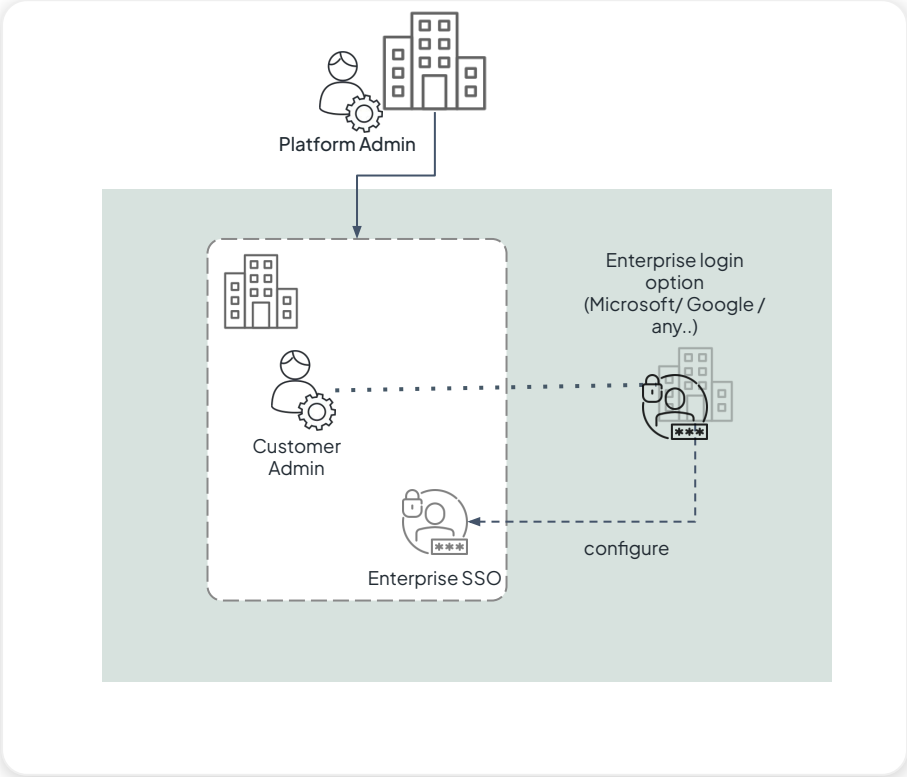
Onboard and manage their own sub-organizations and users.



Characteristics of B2B identity solution

Bring your own Identity Provider (BYOI)

Each customer or partner can optionally use their own IdP, simplifying user onboarding, access management, and lifecycle management.

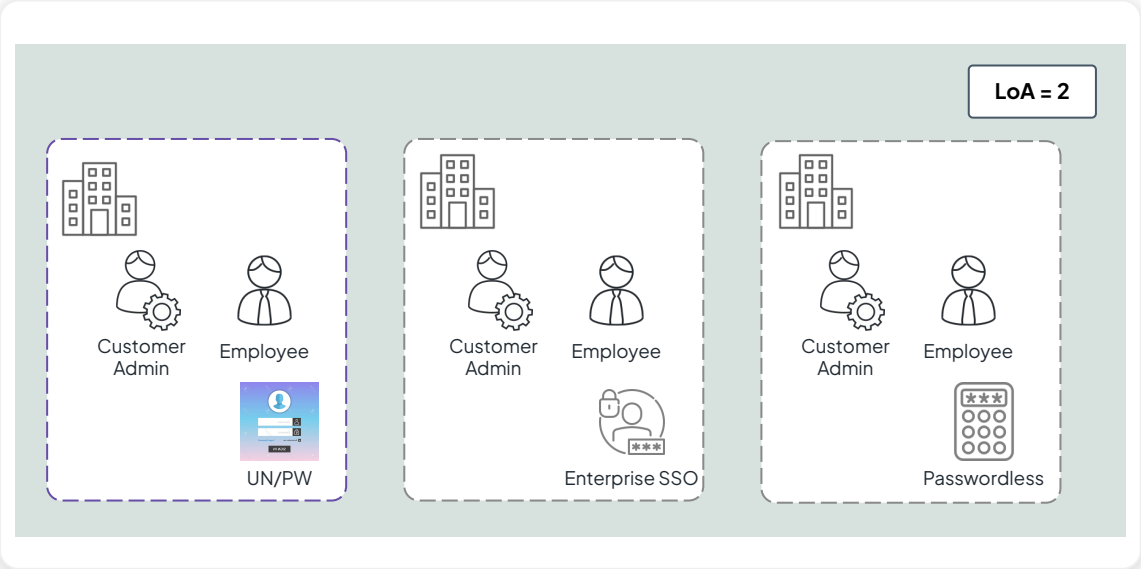


Characteristics of B2B identity solution

Customized log-in, registration and security policies

Variety of authentication options for SSO, social logins, and MFA, while governing the “level of assurance” for each application.

Also able to customize account, password and SSO policies.

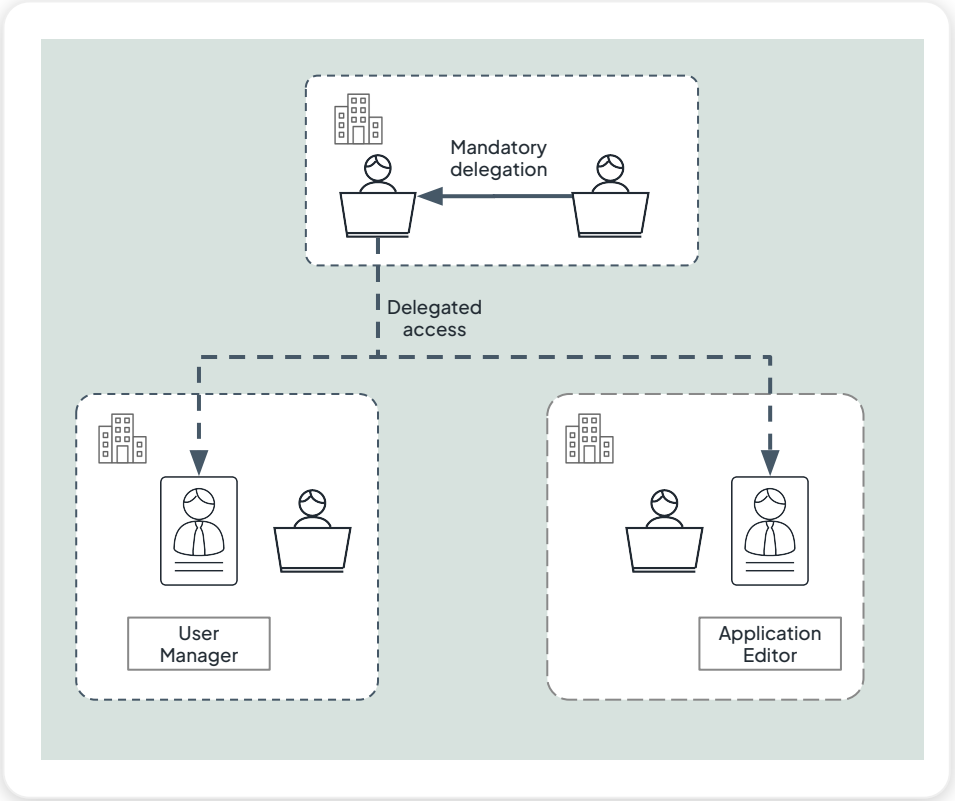


Characteristics of B2B identity solution

Mandatory access delegation

Designate users to act on behalf of customers through mandatory access delegations.

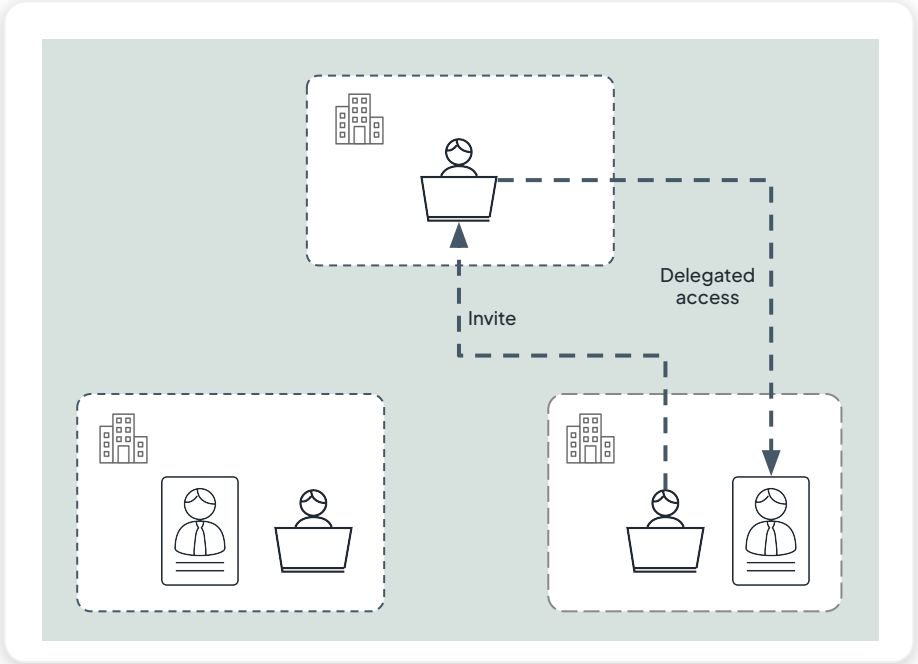
- Same identify being able to access multiple organizations
- Different entitlements per organization



Characteristics of B2B identity solution

Discretionary access delegation

Invite users to act on behalf of customers.



Why drift happens

Why teams land on B2C or workforce tooling even when the shape is B2B.

A QUESTION FOR THE ROOM

When did dedicated B2B IAM solutions first emerge from the vendor landscape?

Analyst recognition came even later *KuppingerCole B2B IAM Leadership Compass and Gartner Partner IAM Innovation Insight both in 2025.*

BEFORE DEDICATED TOOLING EXISTED

Teams improvised. They still do.

Homegrown IAM stretched to fit

Custom modules bolted onto workforce or CIAM stacks.

- Organization context stored as a user claim or attribute.
- Group-based partitioning in a flat user base.
- Per-customer tenant spin-ups with custom sync scripts.

CIAM or workforce tools, reshaped

Single-subject tools adjusted to serve external orgs.

- B2C CIAM for business users —> no org hierarchy.
- Workforce IdP for partners —> same MFA; same session rules for everyone.

THE QUESTION

Tools exist today. Why don't teams pick them?

REASON #1

At selection time, the problem looks B2C IAM needs

Even when the business case is clearly B2B, the requirements surfaced during vendor evaluation all sound like consumer identity needs.

- Customer says they don't need delegated administration today.
- All business customers/partners are expected to use the same login journey.
- No apparent need to vary the password-recovery flow, policies per customer/partner organization.

Think about your next enterprise onboarding. They may need all of the above.

Partners and corporate customers are not uniform: requirements vary with the

- **Trust relationship** and the
- **Third party organization's own IAM maturity**.

REASON #2

Switching to B2B IAM forces major application changes

The identity tool swap is the easy part. The application-layer rewrite it triggers is what stalls adoption.

- Most orgs treat user’s organization as business data, carrying it only as a custom claim in IAM.
- No open standard defines how to communicate an authenticated user's organization in ID or access tokens.
- SCIM has no standard way to carry organization context; vendors all implement it differently.
- Any migration forces changes to auth flows, onboarding, and downstream apps — not just the IAM layer.

REASON #3

B2B plans cost more than B2C plans

Pricing is the usual explanation but in my experience, it is rarely the real one.

B2B Plan ≃ **2.5** x B2C Plan

- Teams that clearly need B2B IAM **have not** chosen B2C over B2B simply because of price.
- Price becomes a factor only when the team doesn't yet see a current need for B2B-specific capabilities.
- By the time the need becomes undeniable (enterprise deal, audit, breach), the cost of not having B2B IAM outweighs the plan difference by orders of magnitude.

THINK

Solid B2B IAM may be the missing piece of your Zero Trust Solution!

Time to Fix the Weakest Link in Your Identity Strategy

Third-party identity is where the breach curve is steepening fastest.

30%

of breaches now involve a third party

Verizon DBIR 2025 (doubled from 15% in 2024)

267

days to identify + contain a supply-chain breach — the longest of any vector

IBM Cost of a Data Breach 2025

B2B IAM is neither
“B2C at scale” nor *“Workforce for externals”*

It is a distinct identity domain
whose first-class subject is the **external organization**,
not the individual.

LET'S DISCUSS

Questions?

Thank You!