Distributed and Delegated Access Management

Hans Zandbelt

Identiverse 2023 – Las Vegas – Version 1.0 – June 1, 2023

“Identity and Access Management Market to Surpass USD 39.26 Billion by 2030 Driven by Increasing Reliance on Digital Platforms and Automation”

Research by SNS Insider
May 15, 2023

Overview

- A brief history of Web Access Management
- The Rise of the Cloud
- The Era of New Identity and API Security Protocols
- Migrating Legacy Web Apps to the Cloud
- Models for Modern Access Management
- Centralized vs Distributed Delegated Access Management
- Summary

A brief history of Web Access Management

- Enterprise domain access on-prem
  - For SSO and access
- Single cookie, domain/enterprise-wide
  - Course grained…
- Centralized Management
  - Change requests through IT
- Proprietary protocols and plugins
  - Agents…

In Real Life...

- Adapt your app for SSO
  - consumer enterprise SSO token
- Register your app
  - to the central IT organization
- Wait until it is onboarded
- Changes?
  - Repeat 1-2
- *Ineffective, time-consuming, waste of resources, frustrating process*

And Then There are Agents

- Proprietary code
  - Closed source
- Proprietary protocol
  - vendor-specific
- Limited application support
  - What about the rest…

So… this means:

Access control is enforced through a central component that only works for tightly coupled applications in the enterprise network.

Application access management is delegated to a “generic centralized party” that has no in-depth application knowledge or interest(!) and does not really know how to qualify specific requests.

The Rise of the Cloud and Mobile

- Adoption of SaaS
  - Apps are no longer just on-prem
- Infrastructure-as-a-Service
  - In “public”, shared datacenters
- Identity is the new perimeter
  - Enterprise network -> zero trust
  - Mobile workers (Covid)
- Mobile Apps (native)

The Era of new Protocols

- New protocol developments
  - Driven by Saas, Cloud and Mobile
  - REST/JSON vs XML/SOAP/RPC
- Password anti-pattern
  - May have worked intra-enterprise
- OAuth 2.0 and OpenID Connect
  - (delegated) tokens
  - REST/JSON/Mobile friendly

Agents? What agents?

- Open & Standards-based
- Open Source
- Wide adoption
  - all applications…
- Legacy apps supported
  - header-based

Migrating Legacy Web Apps to the Cloud

- Legacy Web Apps
  - Cannot be changed
  - No knowledge or people (anymore)
  - May rely on headers
- Externalize AuthN & AuthZ
  - To a (multi-function) gateway
  - Identiverse 2019
- Leverage modern protocols
  - Without app changes(!)

Models for Modern Access Management

- Mix Intra-domain/Cloud-hosted apps
- SSO to corporate IDP (AD, Azure AD)
- Access Management externalized
  - Gateway/Proxy Tier
- Decentralized Entitlements
  - No app groups/roles/entitlements in AD
  - No duplicated/indirect management
- Application Owners own access!

Two-Tiered Enterprise Access Management

- Tier 1 “core and course grained”
  - Centralized accounts and SSO
- Tier 2 “application specific and fine grained”
  - Application specific access control
  - Managed by application owners
- Employee and customer facing
- On-prem, hosted and SaaS

Access Management Tier 1

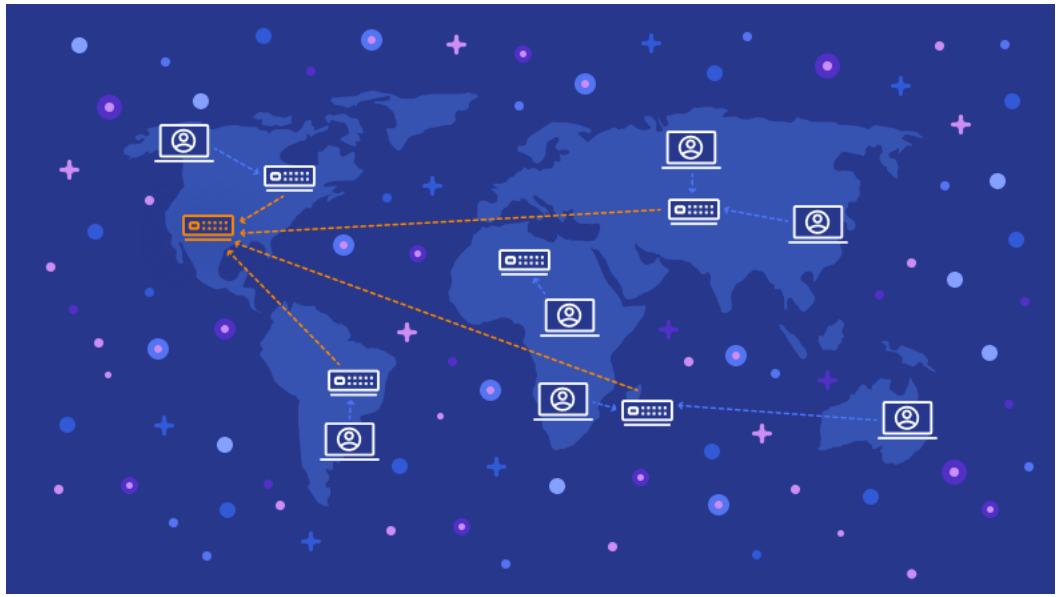
- Operated by central IT
- User account management
  - lifecycle
- Authentication Management
  - Passwords
  - 2 factor
- Identity Provider
  - SAML/OpenID Connect SSO
- Application onboarding

Access Management Portal

- Part of (central) Tier 1
- A webapp for app owners
  - manage access to their app
  - SSO into it (of course!)
- Backend integration with Tier 2
  - Push out gateway configuration
  - Config management based
- Custom/hosted, appliance, SaaS

Access Management Tier 2

- Reverse Proxy Layer
  - SSO and Access Control
  - Clustered / Segmented (app)
- Provided by central IT
  - Operational Management
- (Delegated) Configuration
  - Central IT
  - Application Owners

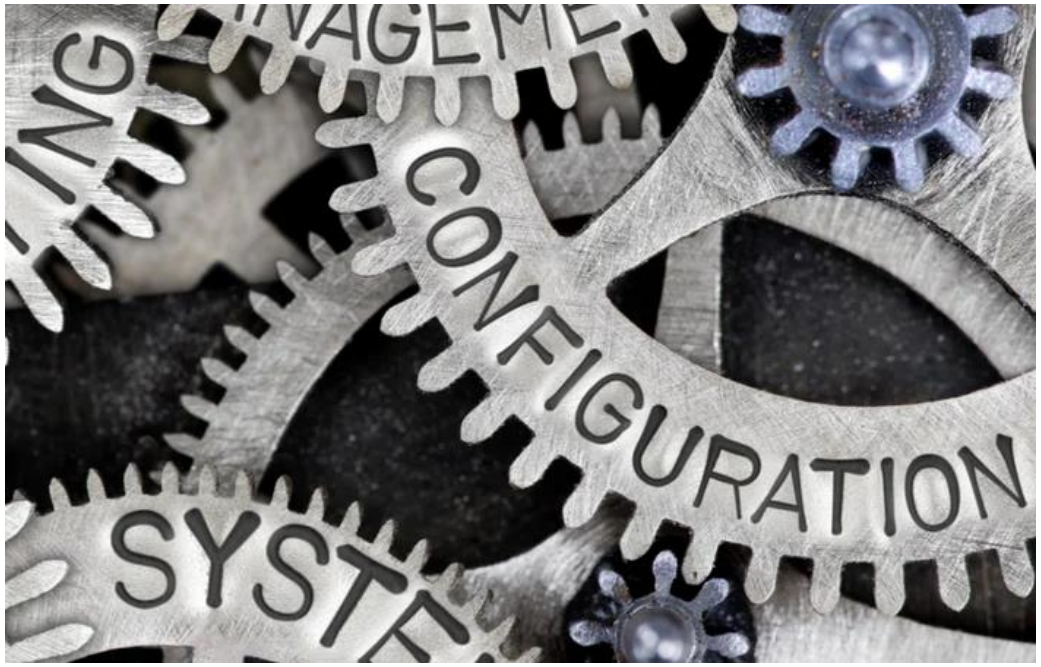


Access Management Configuration

- Central Authoritative source
- Distributed storage and enforcement
  - local database/directory, and/or embedded in the application
- Users: application specific entitlements (based on Tier 1 roles)
  - Users: application specific roles
  - Access: application specific rules

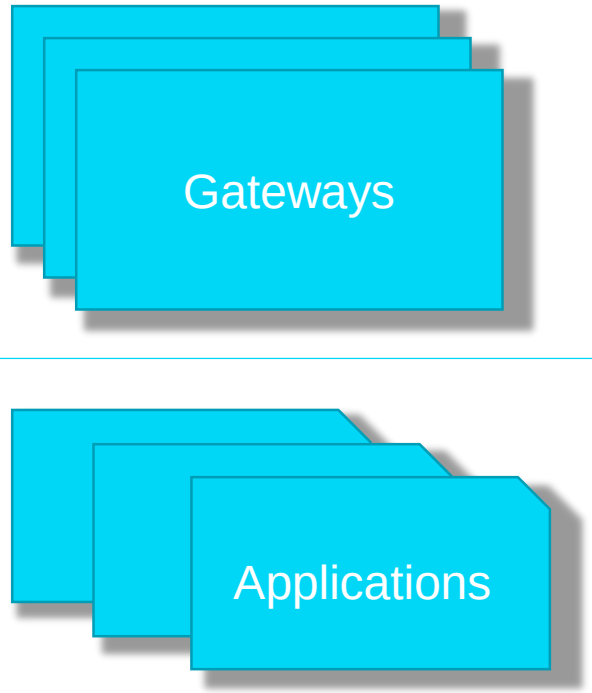
Access Gateway Configuration

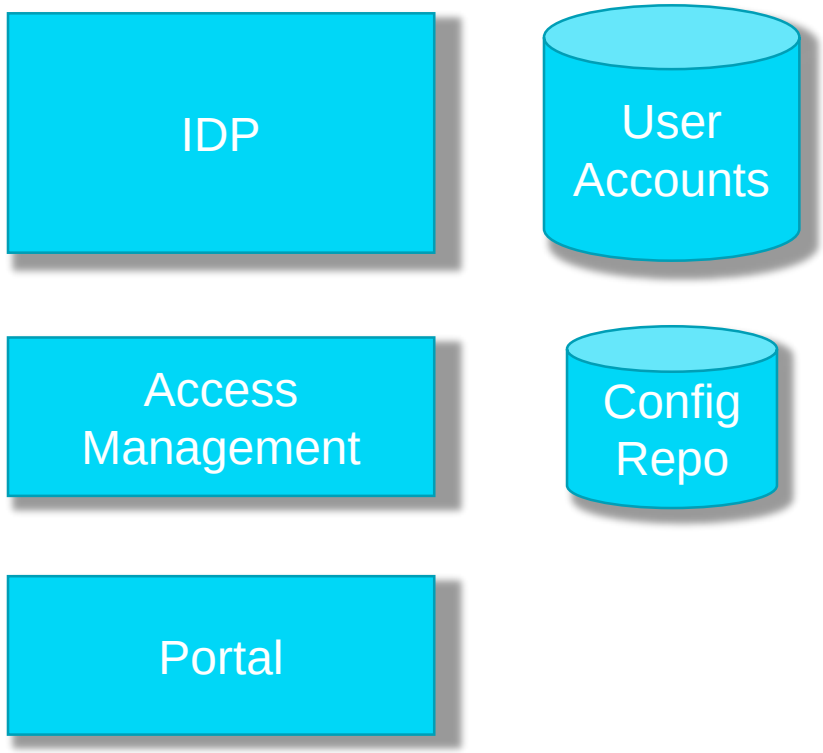
- Puppet/Ansible based
- Central storage of config files
  - Version management
- Pushed out to gateways
  - Dynamic scaling
- Manual is an option
  - Small scale start/fallback



Tier 2 (Gateway/App)

Tier 1 (IDP/SSO)



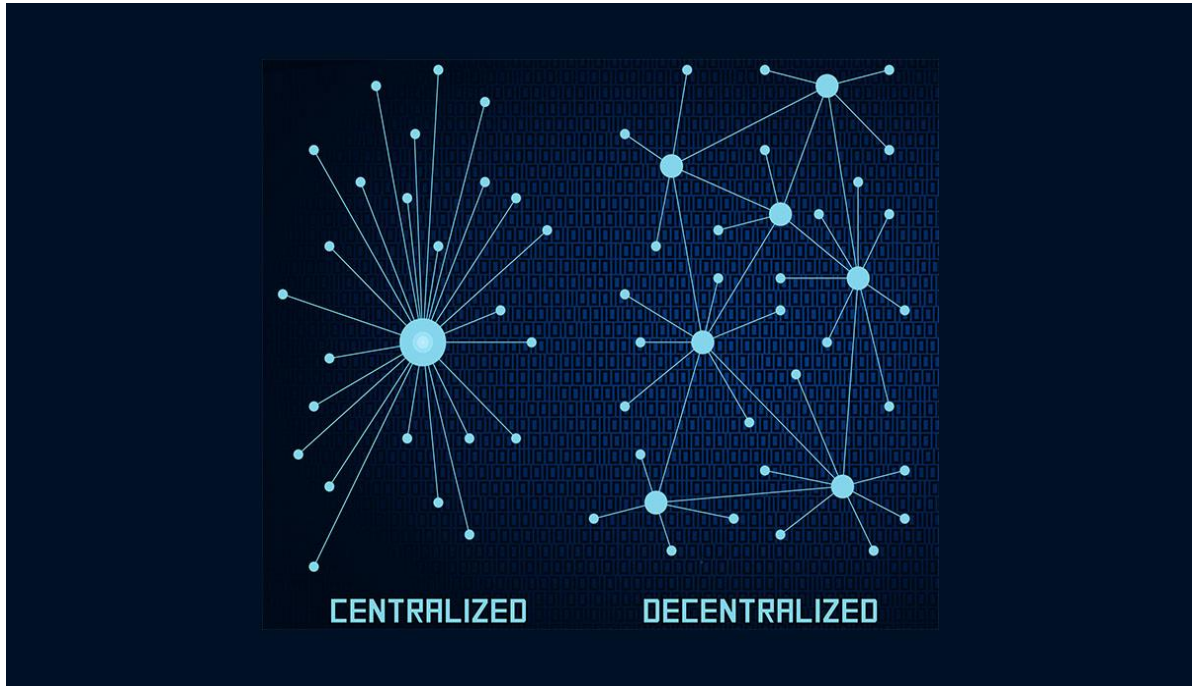


Centralized vs Delegated Access Management

- Access Management config
  - left to app owners in-app, or:
  - done by centralized IT
- Allow shifting…
  - Based on org/responsibilities
  - App type
  - Infrastructure requirements
  - Knowledge

Centralized vs Distributed Access Enforcement

- Distributed Access Control
  - Externalize configuration and enforcement
  - Outsourcing to a dedicated component
  - Good for app (see 2019)
  - Allowing shifting…
- Cloud ready
  - Independent of callbacks to central server

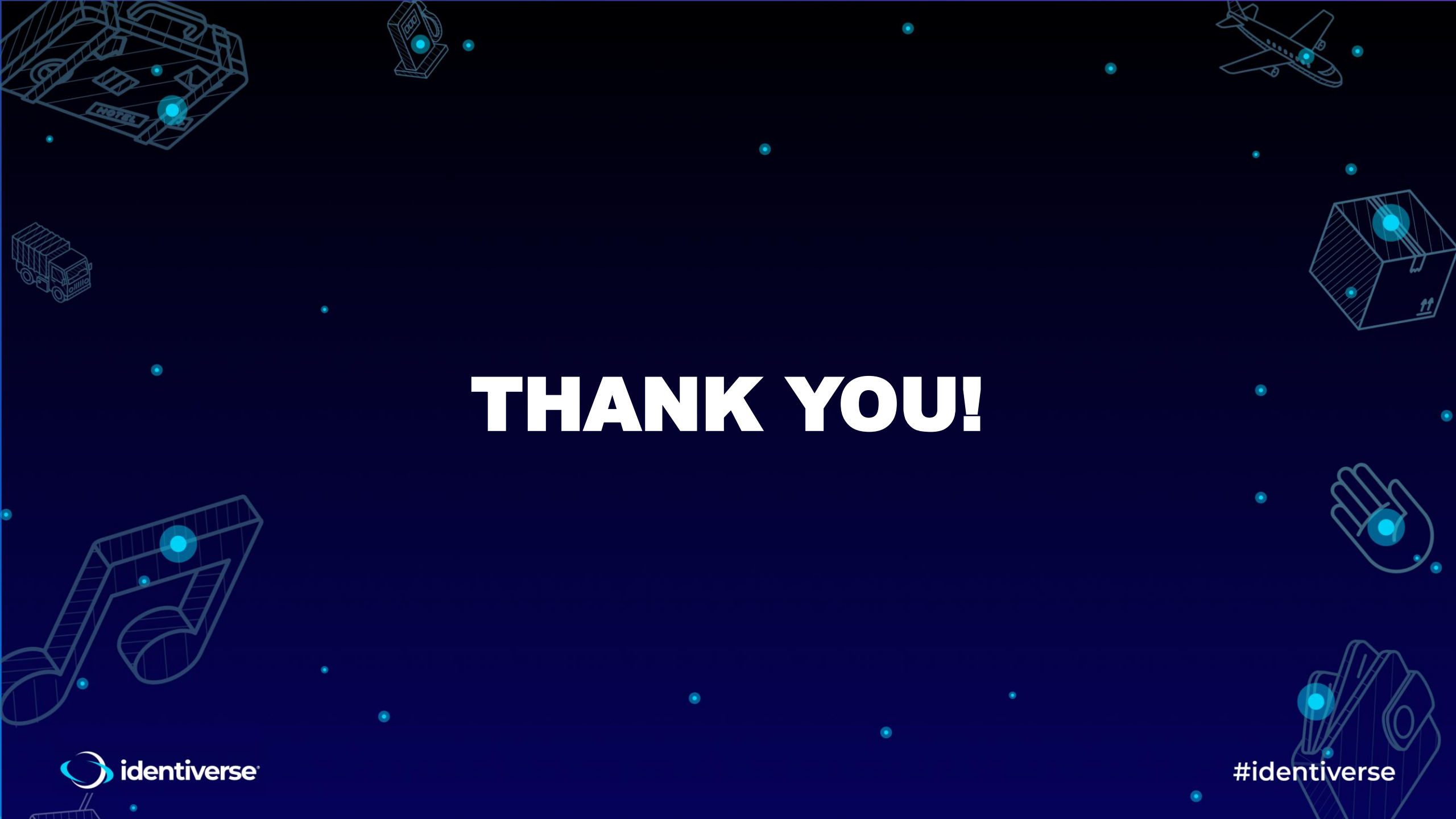


Conclusions / Takeaways

- Modern Access Management for Distributed applications across Cloud and On-Premises can be handled through a dedicated access gateway
- Configuration of distributed Access Management can be achieved through **container configuration management**
- Shifting between **delegated** and **centralized** access management is possible by delegating the container configuration
  - Through a web portal and/or (developer/access) APIs

Questions

- Are you (your company) providing this?
  - No, (apart from a simple gateway) this is the description of an approach, a way of thinking to plan for the future
  - It is likely that you already do a part(s) of this yourself today…
- Do we need to build this ourselves?
  - Possibly, some have already, it depends on your specific needs
  - In the end, doing this (i.e. access config management) through a person/team is also an implementation (no code, no GUI and no backend) but would effectively be similar to classic WAM with the same challenges
- Can we purchase this from another company?
  - Possibly, parts for sure, Amazon ALB APIs, PingCentral Portal, DataWiza SaaS Proxy


THANK YOU!
identiverse
#identiverse

Hans Zandbelt

CEO

OpenIDC / ZmartZone