midwest
architecture community
collaboration

Identity Hunting:
Access and Governance
in a Decentralized Enterprise

by Joseph Solinsky, CISSP

Agenda

The Midwest Architecture Community Collaboration's (MACC) purpose is to bring all domains of architecture together to share information and techniques of interest to all of us. It is our shared belief that through collaboration, we can better understand and promote the significance of architecture to business success.

Today's IT infrastructure presents novel challenges to maintaining continuity across decades of innovation, from the mainframe years up to contemporary, external Software as a Service platforms. This presentation will explore interfacing technologies and processes to govern and interconnect heterogeneous user stores and trust external identities. Different integration strategies will be compared and supporting technologies will be reviewed, based off successful deployments.

Your Security Architecture, circa 2017

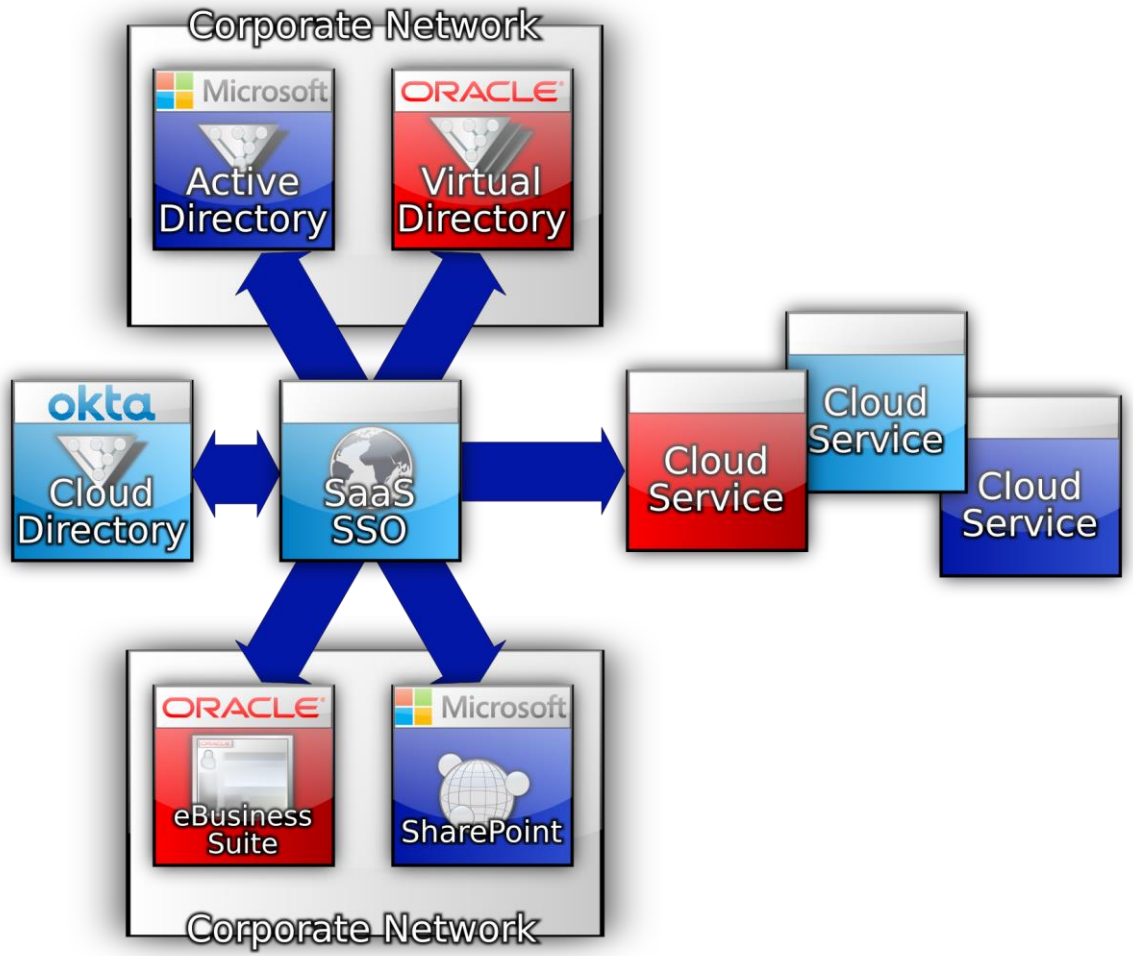
- There is no Firewall
- You do not control the desktop
- You do not own all the user accounts
- You do not own all the hosting systems
- Other businesses hold your confidential, restricted, and highly restricted information
- You and your competitors may be using the same servers
- You gave up control over patch management of your critical systems

Identity is a Moving Target

- Central IT has embraced Shadow IT
  - Access Management uses certain standards
  - But identity provisioning still has to happen
- Central systems need to be related
  - Interoperability
  - Synchronization and Reconciliation
  - Single Sign-On
- Regulations still apply to Software as a Service

midwest architecture community collaboration

New Habitats of Access Management



midwest architecture community collaboration

Paths and Perimeters of Information

- Software as a Service is territorial movement
  - This eliminates traditional perimeters
  - Identity information is exchanged externally
  - Governance is spread to partner obligation
- Identities travel across territories daily
  - Positive identification requires protocols
  - But identities at rest are more reliable than those in transit

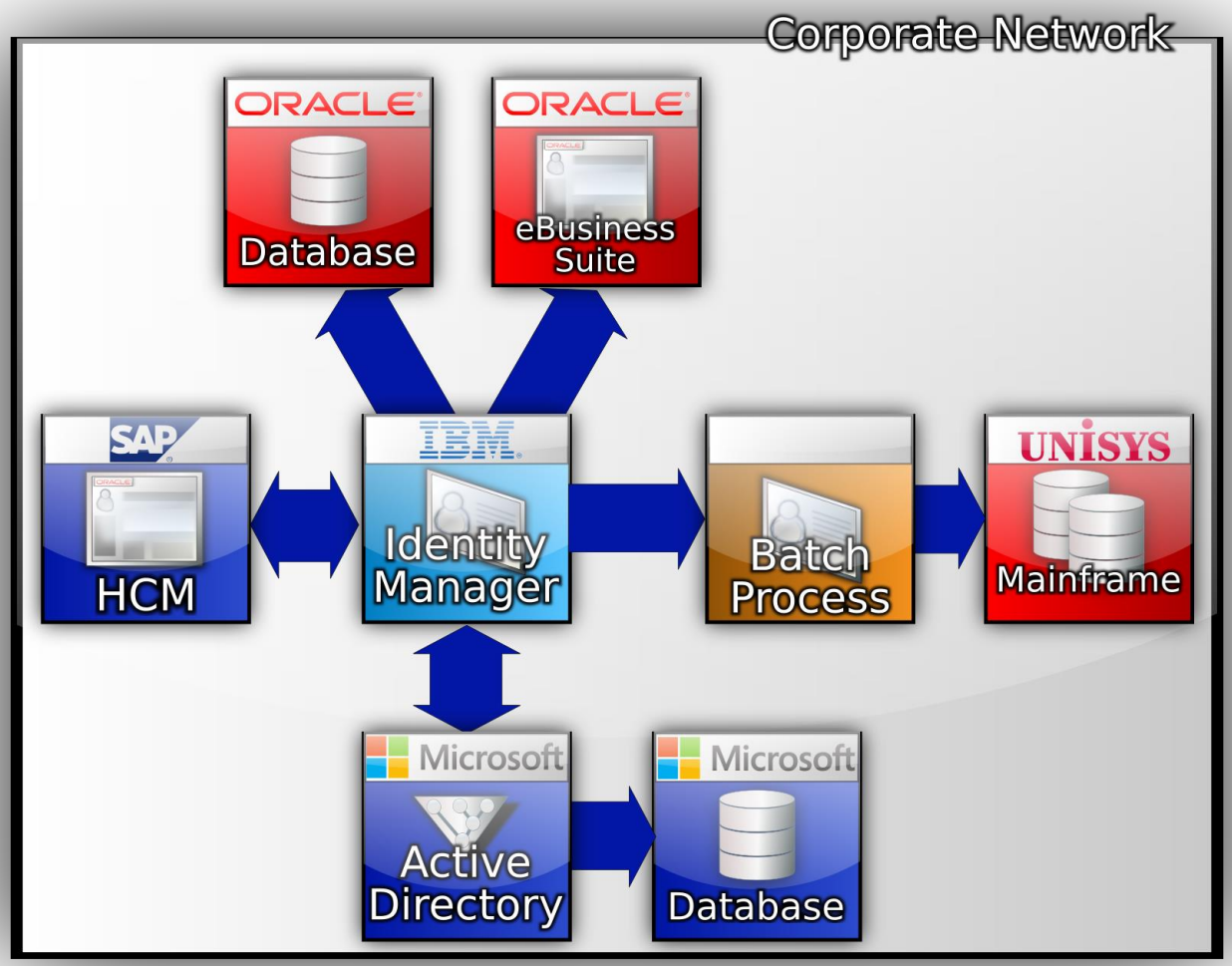
midwest architecture community collaboration

Where Identities are Born

- Traditionally, identities are formed in an HR Management System
- Software as a Service platforms offer this
  - Workday and many others
  - On-premises vendors like Oracle are shifting to SaaS architecture
- Provides a baseline of employees
  - Audits and compliance origins
  - Initial accounts and roles

midwest architecture community collaboration

Traditional Identity Birthplaces



midwest architecture community collaboration

Access Management Traditionally

- Web and Application Access
  - Tokens or cookies
  - Agents
  - Proxies
- Original Federation patterns
  - Identity Provider (IDP), Service Provider(SP), Hub & Spoke
- Policy Management
  - Security or application-based administrators
  - Centralized policy for integrated applications

midwest architecture community collaboration

Access Management in SaaS

- Application Access
  - Pure Federation or Stashed Credentials
  - Access Management systems still required for SP
  - Application Servers support federation or use a proxy
  - Agents are internal only, when needed by Access Management System
- Federation Model is Essential
  - Gateway instead of Hub & Spoke
  - IDP, SP elements remain

midwest architecture community collaboration

Using SaaS for all Access Management Policies

- Administrators should be centered with the SaaS SSO provider:
  - security, and population-based administrators
  - Definitions may not align with on-premises patterns
- Centralized policy for both SaaS and integrated applications
  - Policies may multiply – combinations become an instance:

	Corp. Users	Customers	Vendor/ Contractors
Financials App. (Internal)	App. #1		
Human Resources (SaaS)	App. #2		App. #5
Company Portal (SaaS)	App. #3	App. #4	App. #6

midwest architecture community collaboration

Split domain Access Management Policies

- Keeping some on-premises
  - No externally sourced accounts means policies can stay put
  - Multi-domain tokens require you to build default-deny policies
- Account synchronization strategies
  - Slows down policy change effectiveness
  - Expect synchronization failures – this is the internet!
- Movement towards SaaS is a stampede
  - Expect this architecture to be in flux
  - Communicate to executive leadership full impact of decisions

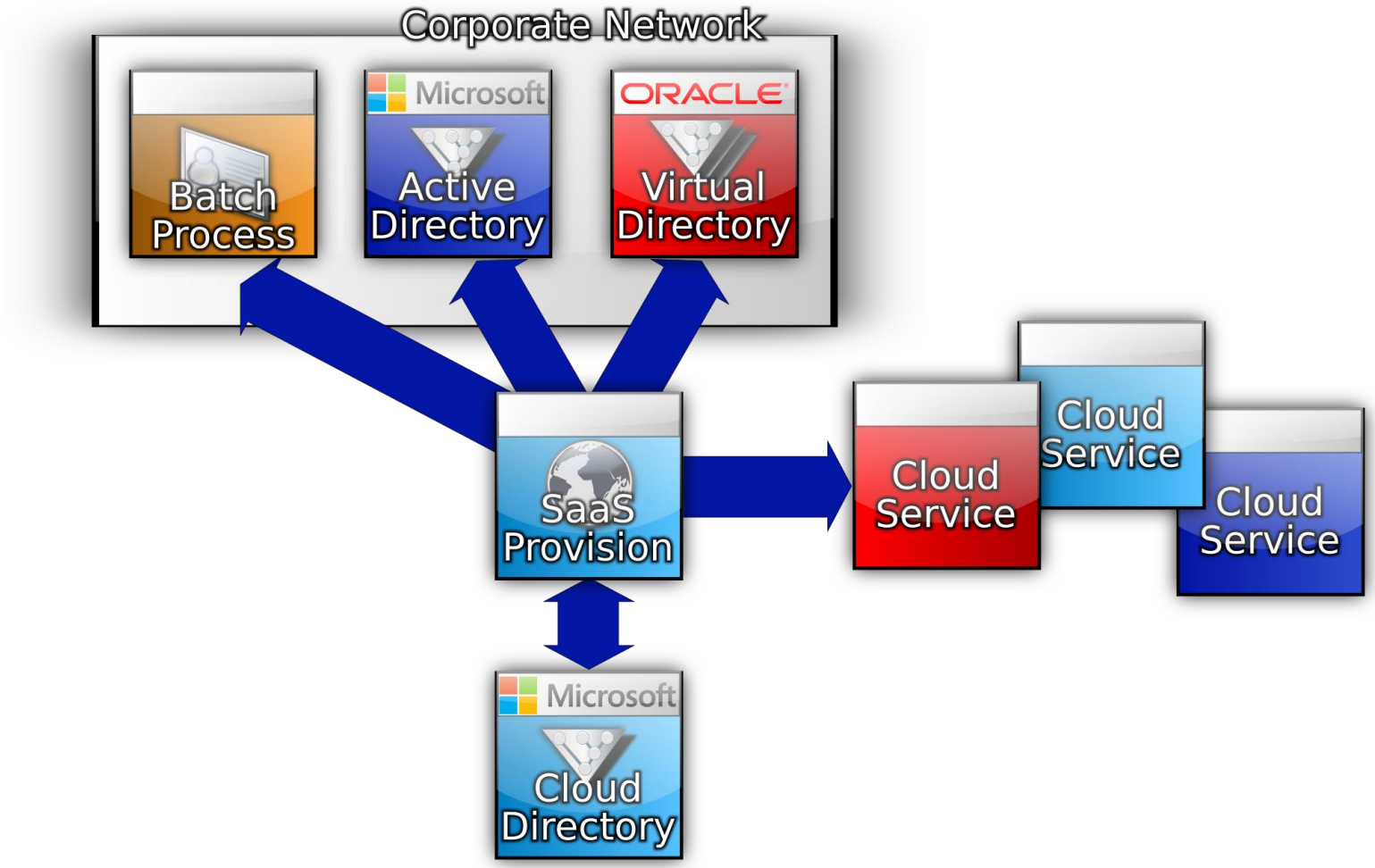
midwest architecture community collaboration

New Birthplace for Identity

- Some Identity Governance is now external
  - Fewer regulatory controls
  - New complexity stems from the IDP trust model
- Decentralized identities shifts life-cycle management
  - SaaS life-cycle patterns multiply as Access Management policies did
  - External processes still need to be understood and monitored
- Role and privilege assignments still require provisioning
- Micro Services/API can couple with external identity provisioning

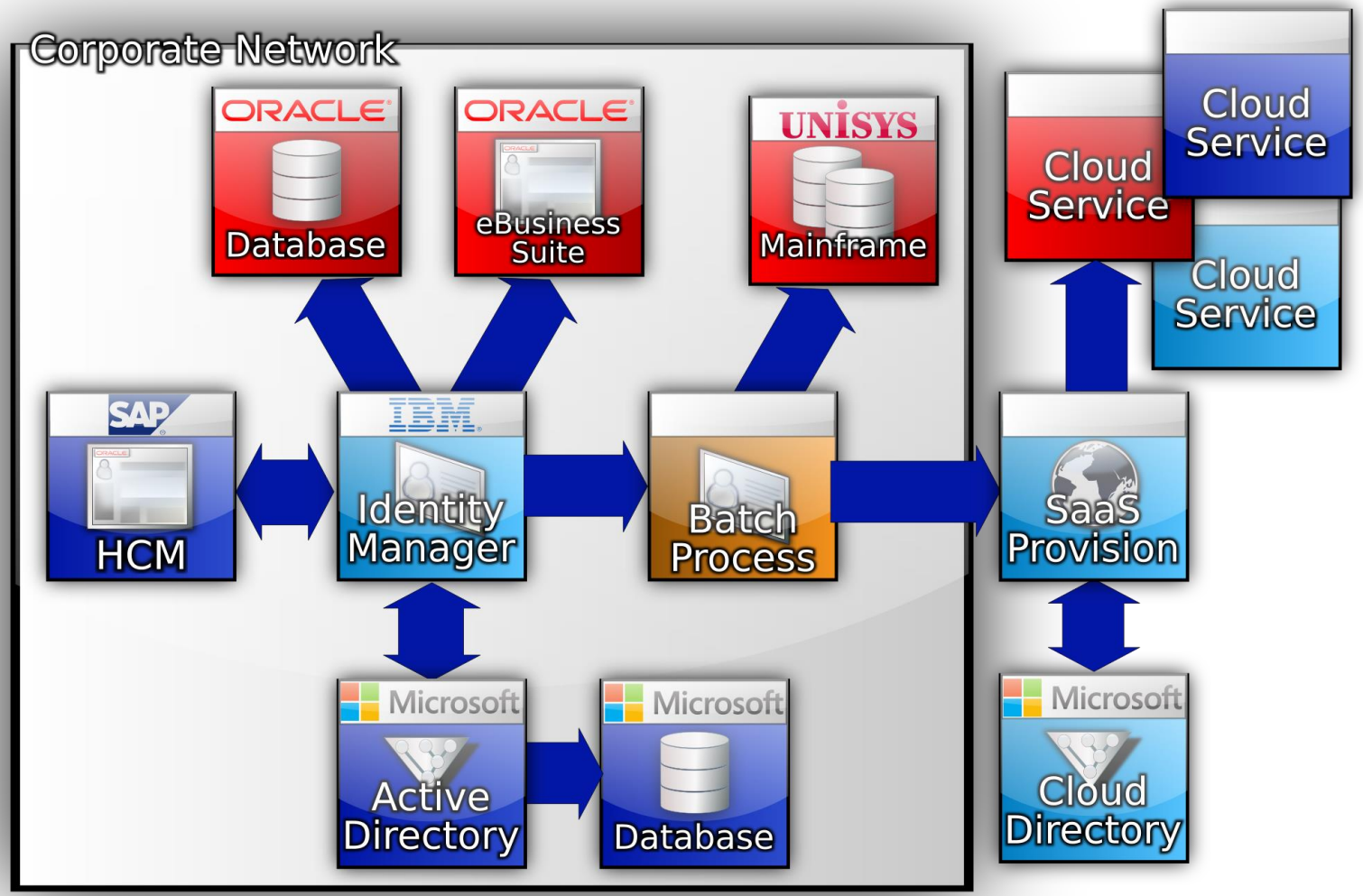
midwest architecture community collaboration

New Identity Spawning Grounds – Green Field



midwest architecture community collaboration

New Identity Spawning Grounds – Woodland



midwest architecture community collaboration

SaaS Provisioning Guidance

- Beware of what connectors exist versus what isn't understood
- Micro-services is often sales-speak for “requires coding effort”
- SaaS providers rarely understand on-premises application provisioning
- Gravitate towards open standards for provisioning
  - Traditional SPML
  - SCIM and variants
  - SAML provisioning profile
- Are your grounds now centered on one SaaS provider?

midwest architecture community collaboration

SaaS Audit

- This is the hairy part of SaaS
- Focus on consolidation
  - Auditors are expensive and so is their time
  - They may not know where to look
- Audit functions built around only what the service offers
  - Ask questions relevant to your audit obligations, e.g.:

  are there records of SaaS provider-level access to your system?

  - What integration exists to your audit repositories?
- Determine what audit customizations exist with the provider

midwest architecture community collaboration

SaaS Compliance

- It is the job of an architect to understand compliance requirements when making and integrating SaaS technologies
- Read your compliance obligations and create domains to focus on
  - Typical C, I, A goals
  - Security layers: out in the open now
  - Encryption, certificate management increase in complexity
  - Ask the vendor to provide answers before you buy anything
  - Identity proofing is increasingly important
  - Quarterly Access Reviews need owners, enforcers

Telling Your Identity Hunting Story

- Traditions are overturning
  - Perimeter territories are suddenly open
  - Identities and services are now externally provided
- Everything that's new is built on the old
  - Access Management uses the same core, but now there's two
  - Identity Governance will trace differently from before
- Audit and Compliance requirements did not go away
  - Additional effort is required to mitigate complexity increases
  - Understand and communicate impact in these areas

midwest
architecture community
collaboration

Connect with me

- Joseph Solinsky
- jcsky@visi.com

https://www.linkedin.com/in/joseph-solinsky

midwest architecture community collaboration