Red Hat SSO & Azure Active Directory

RHUG 2018

Sebastien Perreault

Senior Solutions Architect


Identity and SSO

Wikipedia as the “authoritative source” for definitions:

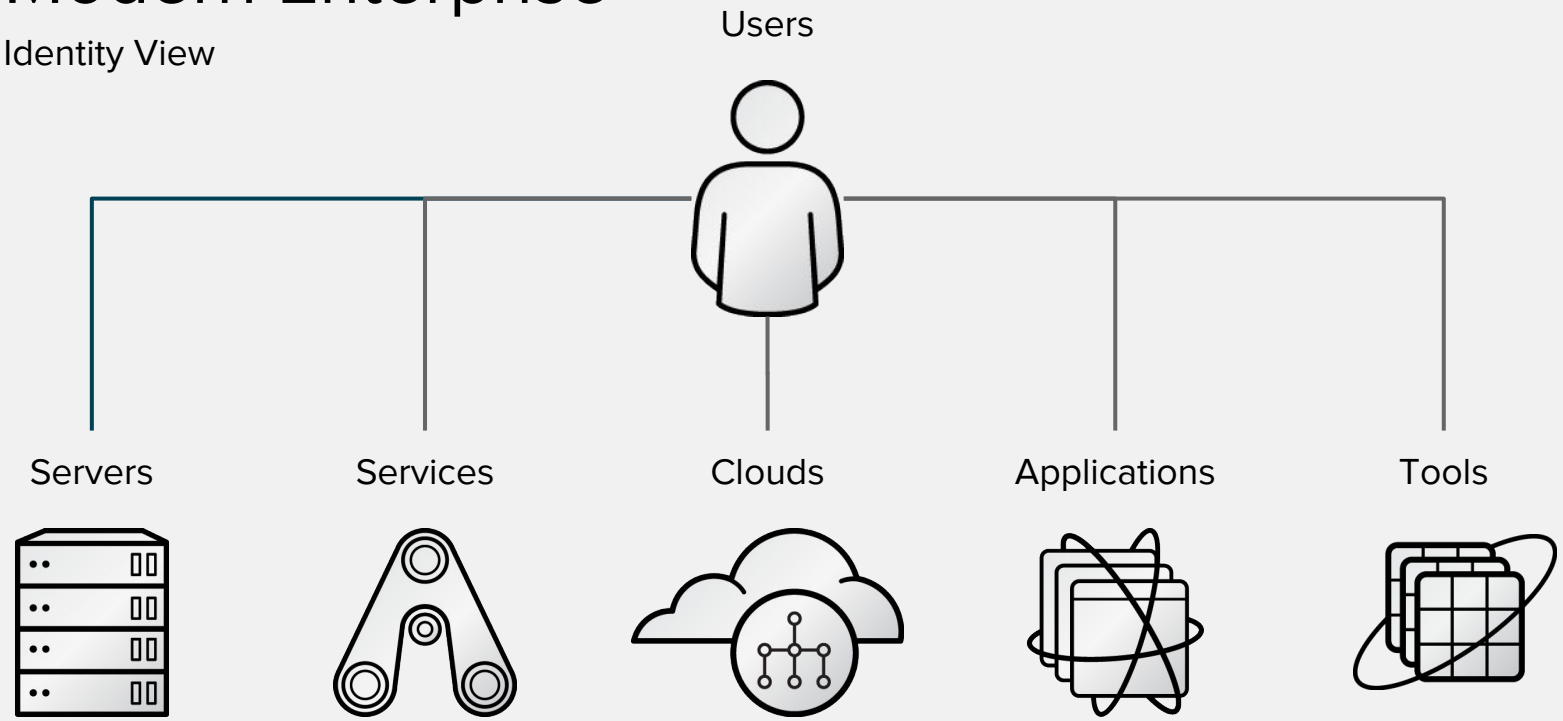
Identity Management - (noun)

“Identity management (IdM) describes the management of individual principals, their authentication, authorization, and privileges within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime and repetitive tasks.”

Wikipedia

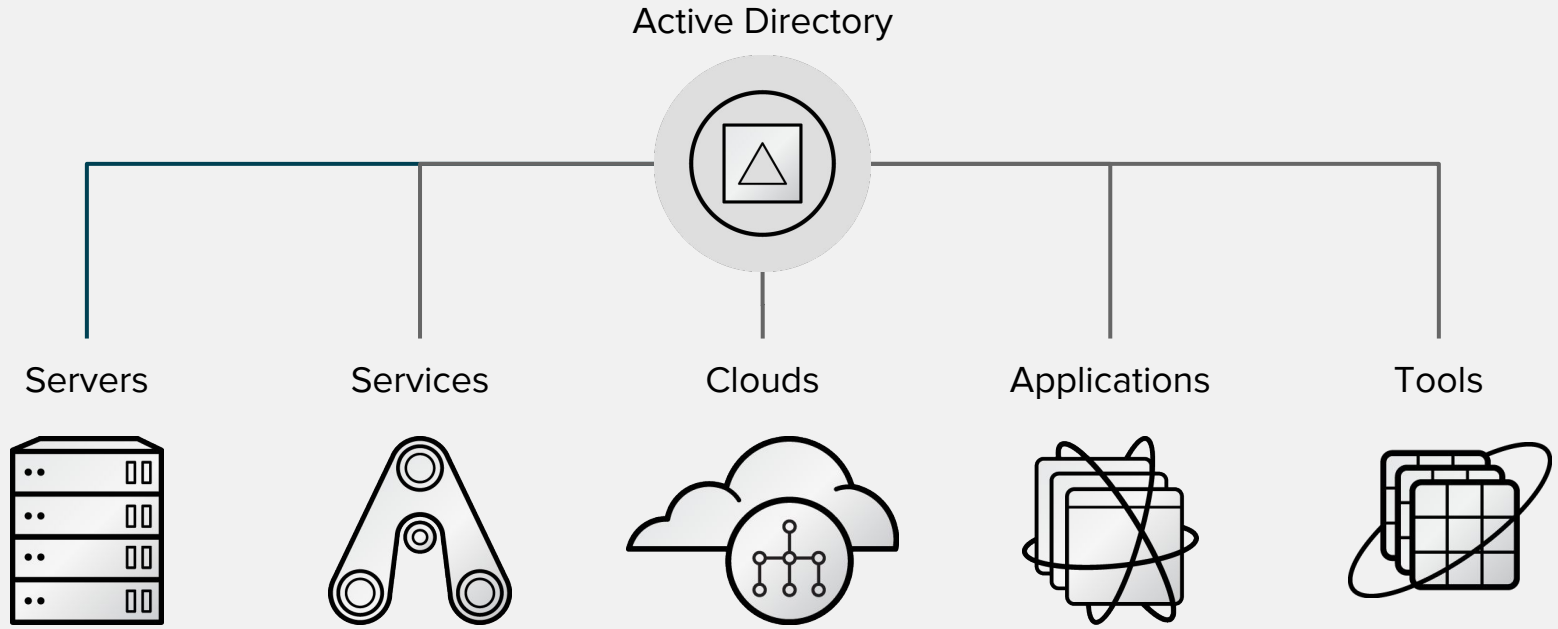
Modern Enterprise

Identity View



Modern Identity Model

Active Directory based solution



Users

In Modern Enterprise

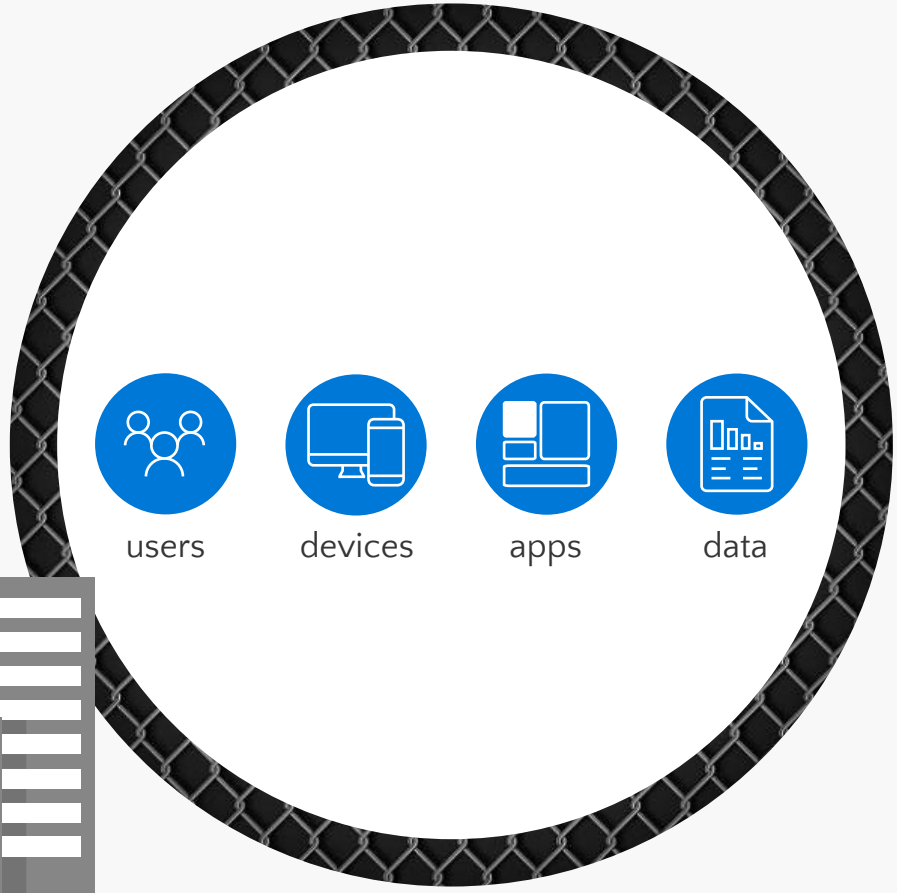
Internal Namespace

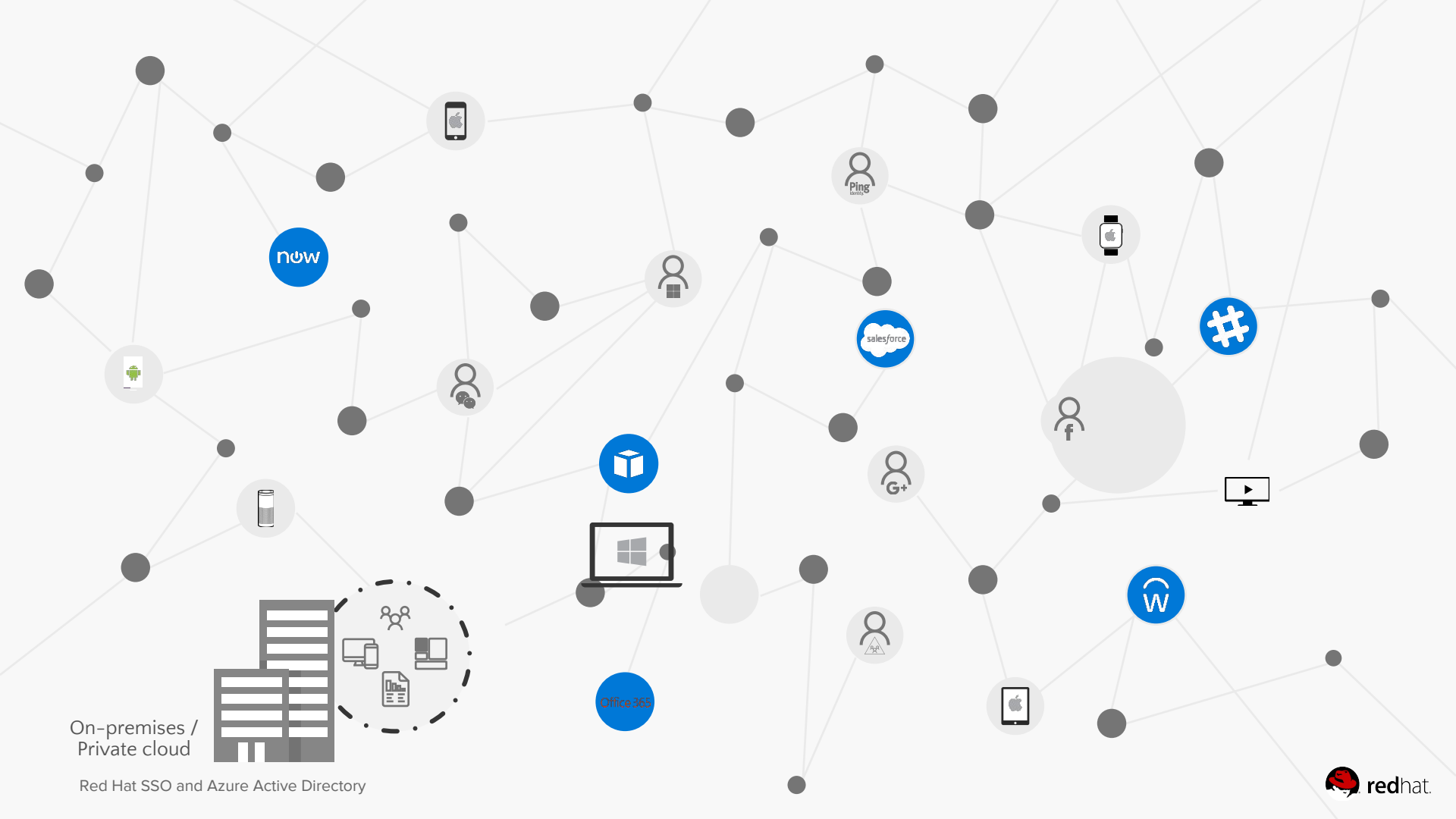
Employees
Contractors

External Namespace

Customers
Partners

THE WORLD BEFORE
MOBILITY & CLOUD





Red Hat SSO and Azure Active Directory

redhat.


Identity
Is the new control plane
On-premises /
Private cloud


How to deal with SSO

Some of the standards listed here!

Overview

- Platform level:
  - ~~NTLM~~ - old, weak crypto, should not be used
  - **Kerberos** - old, went a long way, recommended
- Application level:
  - ~~OpenID~~ - old, has weaknesses, should not be used
  - **SAML** - old, proven, recommended, challenges with mobile
  - **OpenID Connect (OIDC)** - modern, proven, recommended for new applications

Protocols

OpenId Connect

- JSON
- Simpler
- Bearer token

When to use

- Default
- Single-page apps, mobile
- REST services

SAML

- XML
- More mature

When to use

- Monolithic applications
  - Or you don’t need end-to-end auth
- If your apps already support SAML
- If you have requirements OpenID Connect doesn’t support

You can use both!

How to deal with SSO

Bottom Line

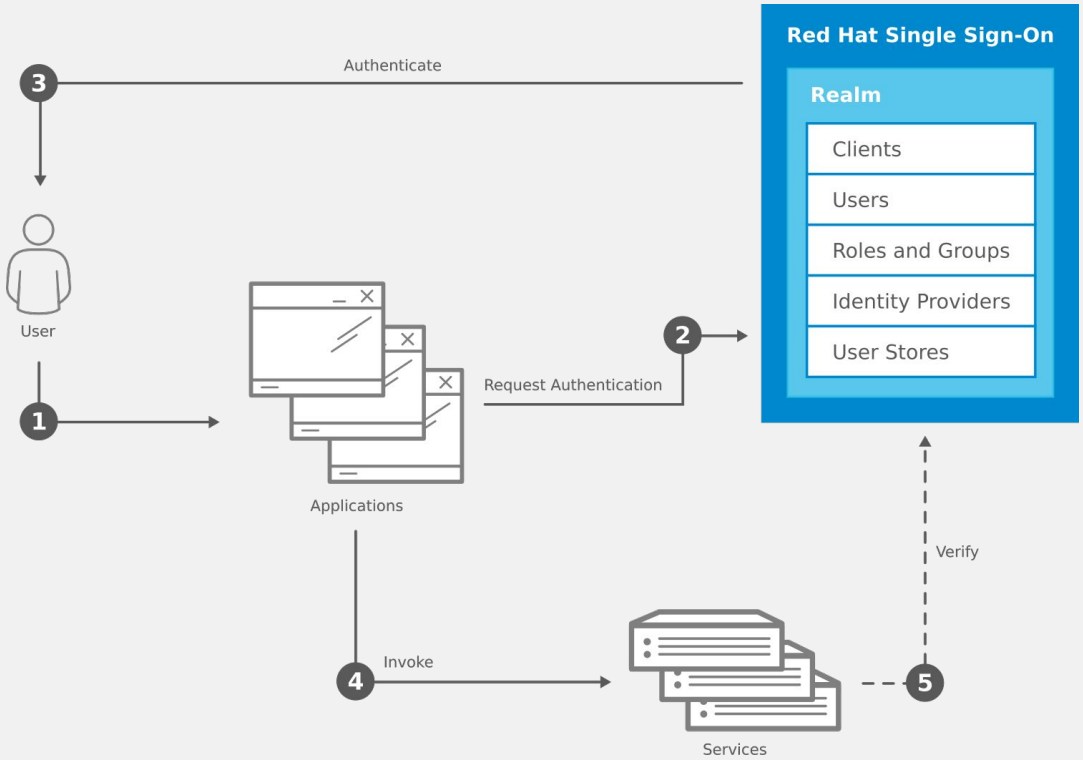
Use combination of Kerberos, SAML, OIDC and a combination of them based on the use case.

Federation is the key

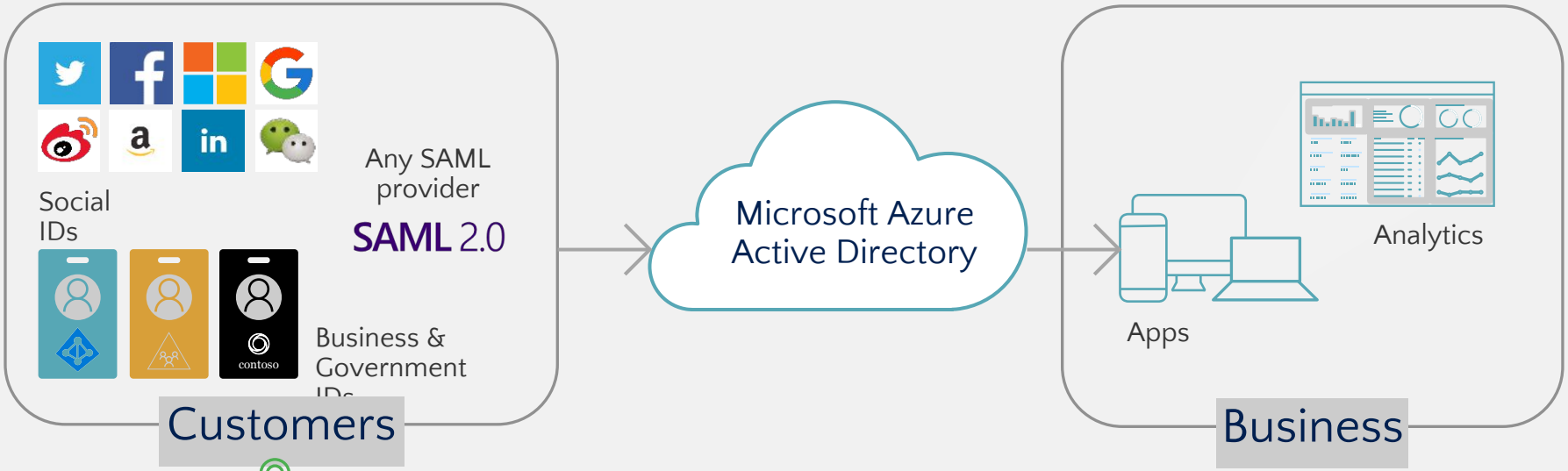

Concepts

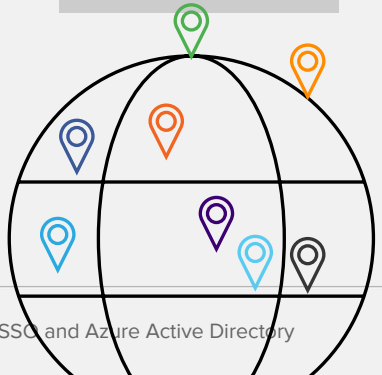

Jiheuheu Land
Anghulard Land
Nhodedjyhès Land
Mikhroservices Land

Concepts



Azure Active Directory B2C

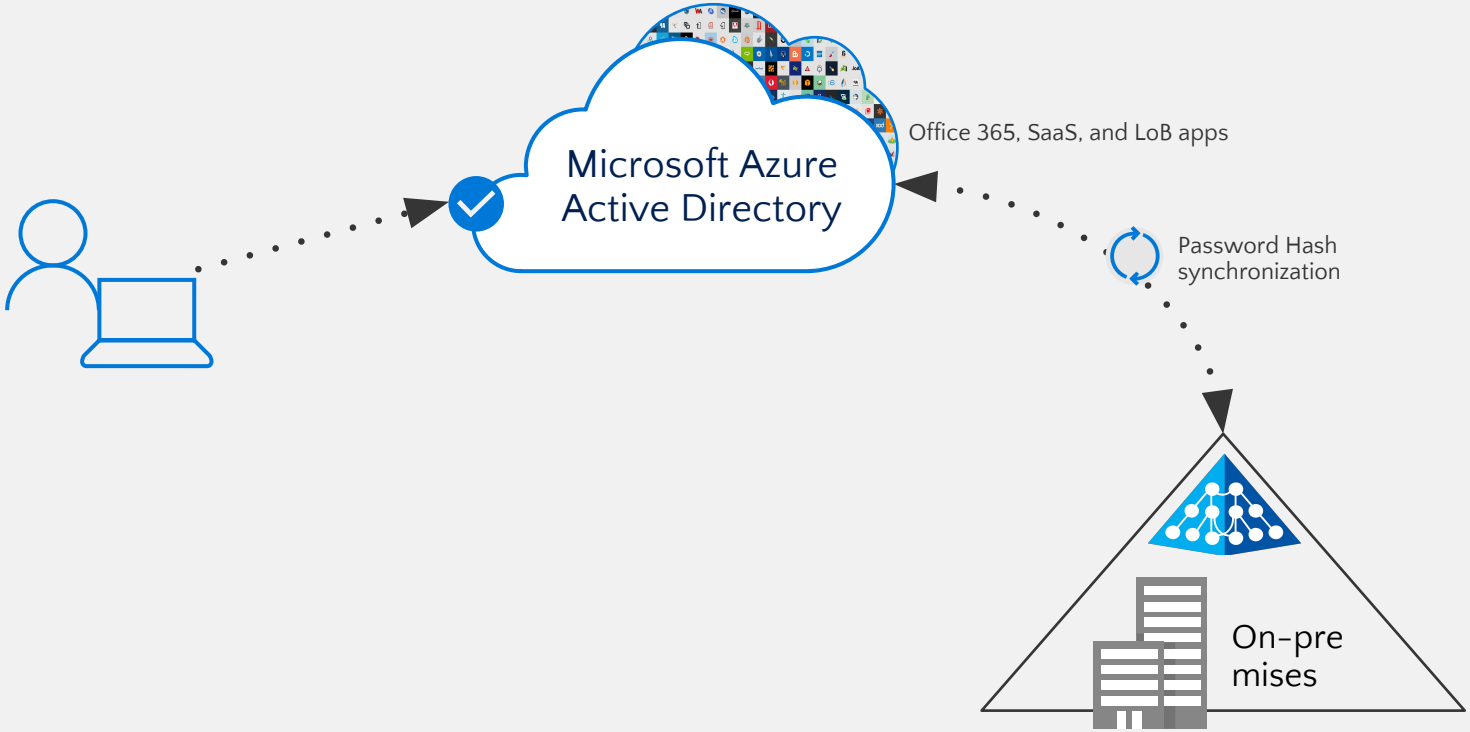




- Securely authenticate your customers using their preferred identity provider
- Capture login, preference, and conversion data for customers
- Provide branded (white-label) registration and login experiences

Azure AD Connect authentication options

Password Hash synchronization



Adapters

Red Hat Single Sign-On

- Client-side JavaScript
- JBoss EAP
- JBoss Fuse
- Node.js
- Servlet Filter
- Spring Boot

Keycloak (community)

- Jetty
- Spring Boot 2
- Spring Security
- Tomcat
- WildFly


Demo Time !

Microsoft Azure AD - Cheatsheet

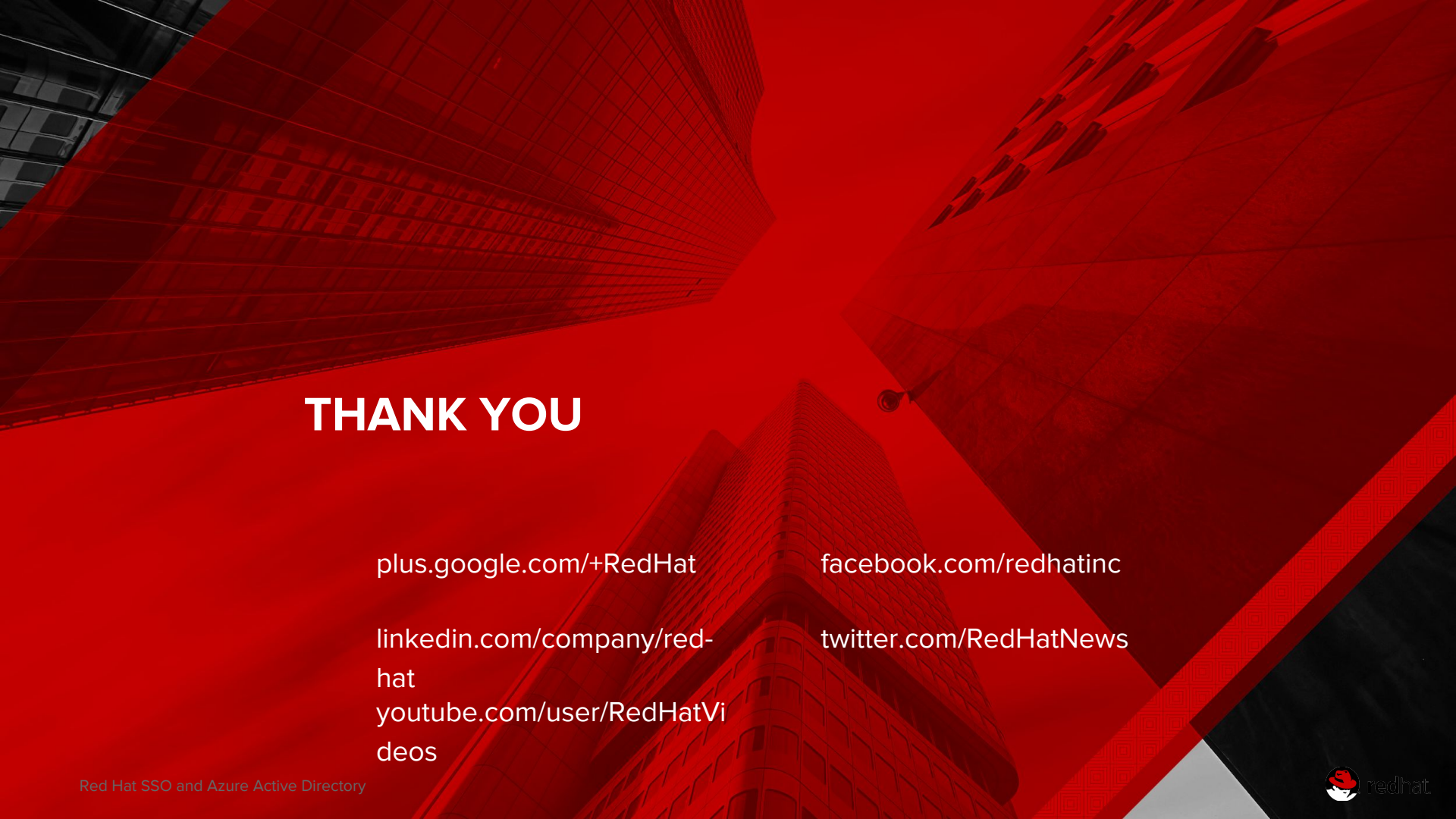
- iDP Mapping

  firstName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

  lastName: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Questions?

Finally


THANK YOU
plus.google.com/+RedHat
facebook.com/redhatinc
linkedin.com/company/red-hat
twitter.com/RedHatNews
youtube.com/user/RedHatVideos