Welcome to Okta in U.S. DOD/IC

DISA Technical Exchange Meeting
Nov 15, 2023

Brandon Iske
Principle Solution Architect
brandon.iske@okta.com

Tyler Briley
DoD Sr. Systems Engineer, Okta

Agenda

01 Okta Introduction and Overview

02 Demonstration

03 Q & A

okta

Identity as a Service

Complete control of Authentication and Authorization

Employees & contractors

Community Members

Non-Person Entities

okta Identity Platform

Infrastructure *(Cloud/On-Prem)*

Applications *(Cloud/On-Prem)*

APIs *(Public/Private)*

- Access Gateway
- Single Sign-On
- Adaptive MFA
- Lifecycle Management
- API Access Management
- Seamless Integrations
- Universal Directory
- Advanced Server Access

Built for global scale and reliability

>99.99%
Uptime

10+ Billion
monthly auths

Platform innovations

- Zero planned downtime
- Self-healing nodes
- Granular rate limiting
- Redundant SaaS, PaaS, and IaaS

okta

Okta's investments in supporting the Federal Government

	Okta for Government Moderate	Okta for Government High	Okta for US Military
Okta Cell(s)	OK5/OK10	OG1	OM1
Domains	okta.com	okta-gov.com	okta.mil
Authorizations	• FedRAMP Moderate • DISA IL2 (via reciprocity) • HIPAA	FedRAMP High	DOD IL4 Provisional Authorization
Infrastructure	AWS US East / US West	AWS GovCloud East / West	• AWS GovCloud East / West • Internet and NIPRNet Accessible
Eligibility & Other Notes	• U.S. government customers (federal, state, local, tribal, territorial, Federally Funded Research and Development Centers (FFRDCs) or lab entities) • U.S. government contractors and CSPs leveraging Okta's FedRAMP Moderate ATO • U.S. government contractors and CSPs using Okta for the fulfilment of a U.S. government contract • Entities that must meet specific U.S. government regulations and requirements (banking, healthcare, financial services, etc.)	• U.S. government customers (federal, state, local, tribal, territorial, Federally Funded Research and Development Centers (FFRDCs) or lab entities) • U.S. government contractors, subcontractors, and cloud service providers leveraging Okta's FedRAMP High ATO • U.S. government contractors and subcontractors using Okta for the fulfilment of a U.S. government contract	• Exclusively DoD-authorized users. • DoD CAP; DoD IP's and Domain Names. • Provisional authorization permits Okta to be used as an Identity provider for DoD authorized **IL5 environments.** • Bound by same security and compliance constraints as a DoD owned cloud operated by a Contractor. • All traffic monitored by Okta and DISA • RMF and Continuous Monitoring performed by okta and reported to DoD Monthly. • Previous restriction removed: users no longer need to seek a DoD CIO Exception to Policy to use okta.

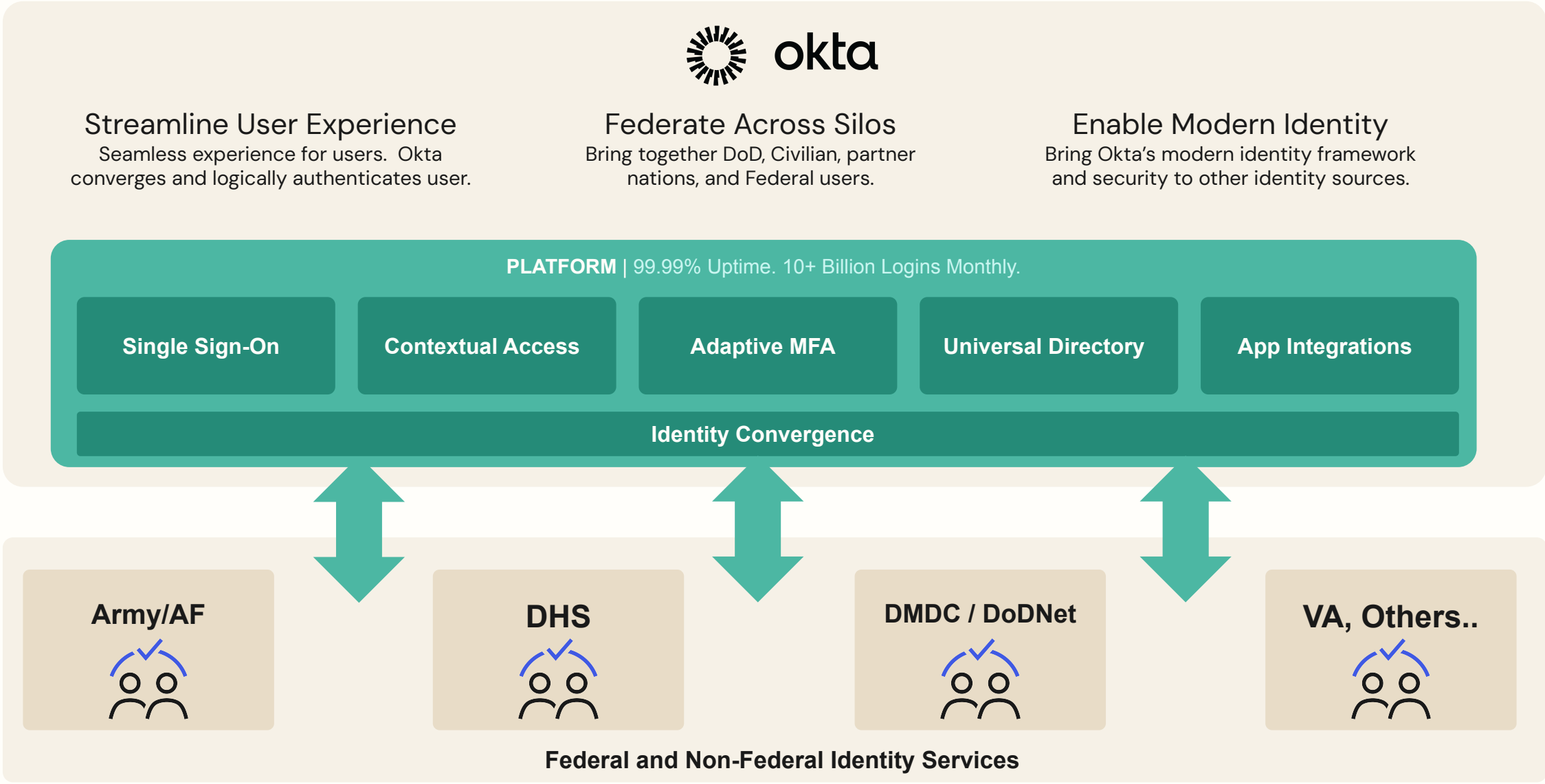
okta

okta

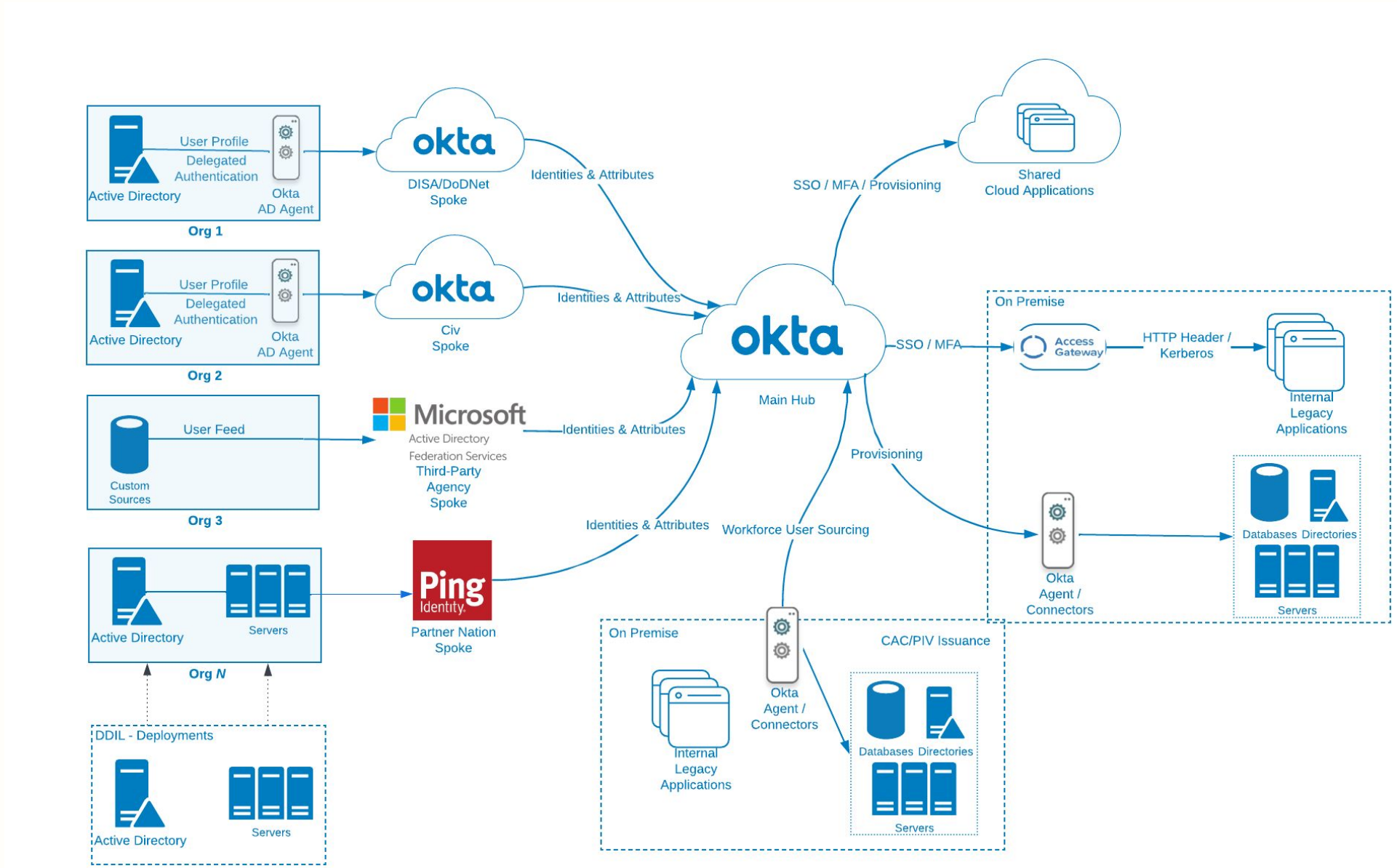
Okta Connect Everything

Identity Broker

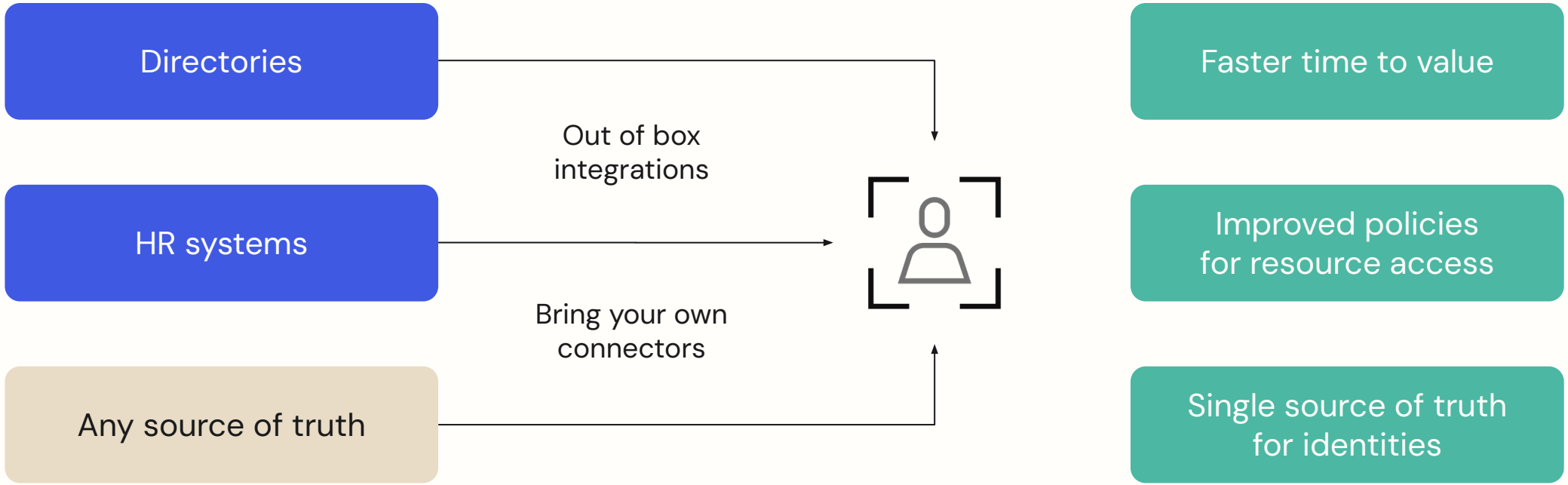
Converge identity and attribute data in and out of the DoD.



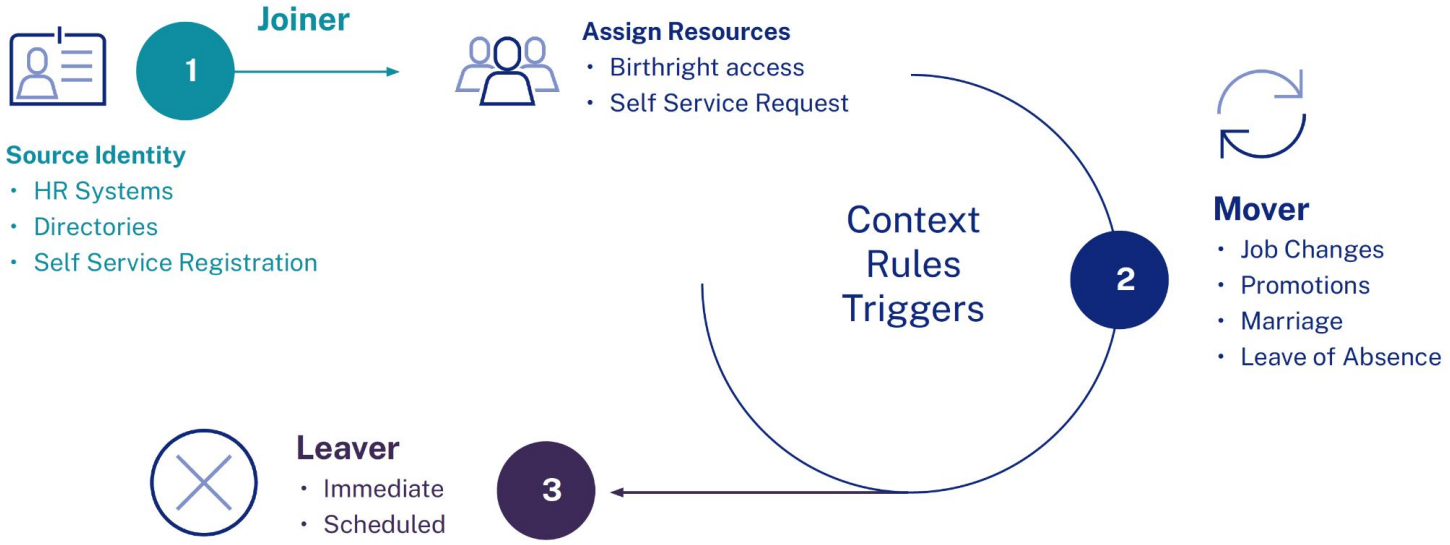
Notional Cloud Native Federation Hub Diagram



Import Identities from **ANY** source of truth



Dynamic Conditional Access



Okta's conditional access simplifies the administration of groups. Creating **Lifecycle Management Rules** that allow you to automatically populate provision application access based on rules that you define.

Okta's rules allow for deep integration into the application. Not just allowing access but **provisioning accounts to downstream applications.**

Conditional access rules can be based on:

- **Attribute-based rules attributes**
- **Group-based rules**
- **Attribute and Group-based rules**

Okta's agnostic support for authenticators

Utilize the right authenticator for the right assurance

Security Question	SMS, Voice, Email	One Time Password	Push Notification	Okta FastPass	FIDO2/Webauthn	Certificate (PIV/CAC)
Pros • Provides baseline security at a low cost • Users are familiar with process.	**Pros** • Easy to use, low cost as many users have their own mobile devices and access to email	**Pros** • Easy to use, low cost as many users have their own mobile devices and access to email	**Pros** • Stronger Phishing resistance • Easy to use	**Pros** • Phishing resistant • Support for on-device biometrics • Cryptographic functions, hardware backed by TPM • Passwordless • Device Posture Evaluation • Phishing resistant onboarding of a second device	**Pros** • Phishing resistant • Support for on-device biometrics • Cryptographic functions, hardware backed by TPM • Passwordless	**Pros** • Phishing resistant • Issued by DoD and well known/high assurance credential • Passwordless
Cons • Lowest security assurance • Subject to social engineering and users forgetting their answers.	**Cons** • Relies on phone/Internet service provider for security and subject to social engineering. • Usually requires using a personal device • Personal email inboxes are usually not secured	**Cons** • subject to social engineering and phishing. • Usually requires using a personal device or physical token • Physical Tokens have deployment and provisioning costs • Most tokens do not require biometrics • Okta Verify App Installation Required	**Cons** • Okta Verify requires a smartphone • Cost of deploying smartphones • Or-complexity of requiring personal devices • Okta Verify App Installation Required	**Cons** • Not applicable for shared device use cases • Okta Verify App Installation Required	**Cons** • Hardware to procure and manage lifecycle	**Cons** • Complex to issue and manage • Form factor challenges • Minimal self-service • No Device Signaling information

Okta Verify Product

okta

Phishing Resistant Authenticators at Okta

	FIDO2 WebAuthn			Okta FastPass	Smart Card
	Security Keys (e.g Yubikeys)	Platform Authenticator (Single-device)	Passkeys (Multi-device)		
Phishing Resistant	✓	✓	✓	✓ deployment dependent	✓
Hardware Protected (TPM/Secure Enclave)	✓	✓ system dependent	✗	✓ system dependent	✓
Authenticator Bound	✓	✓	✗	✓	✓
Browser / OS Support	✓	✓	Platform dependent	✓	Limited mobile support
Self Service Enroll & Recovery	✓	✓	✓	✓	✗
Deployability	Additional Hardware	✓	✓	✓	Additional Hardware
Device Context	✗	✗	✗	✓	✗

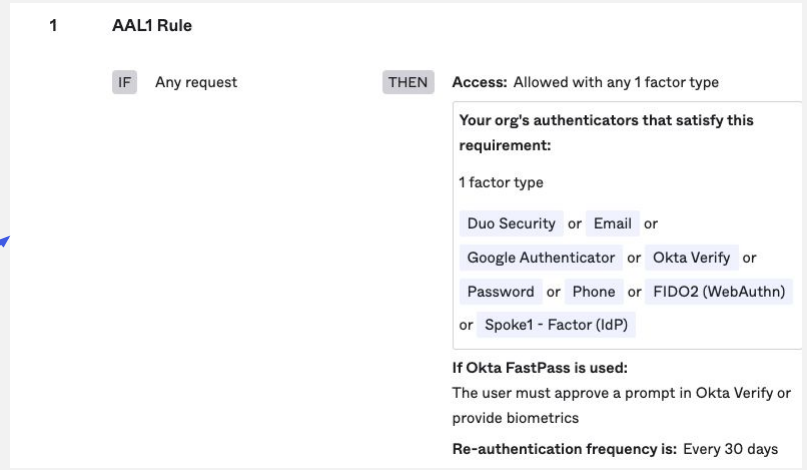
okta

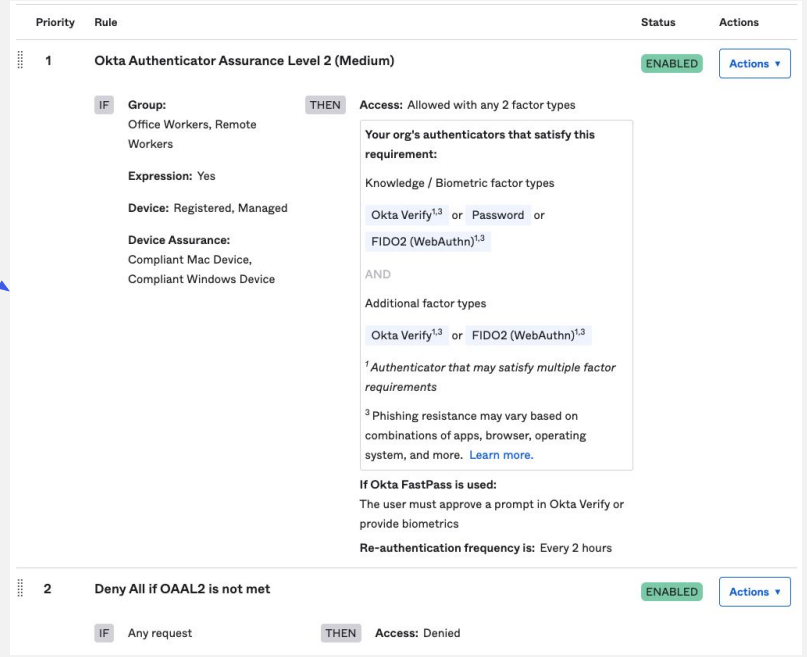
Risk-Determined Classification

Classify apps based on their risk profile io determine requirements related to MFA frequency and assurance strength.

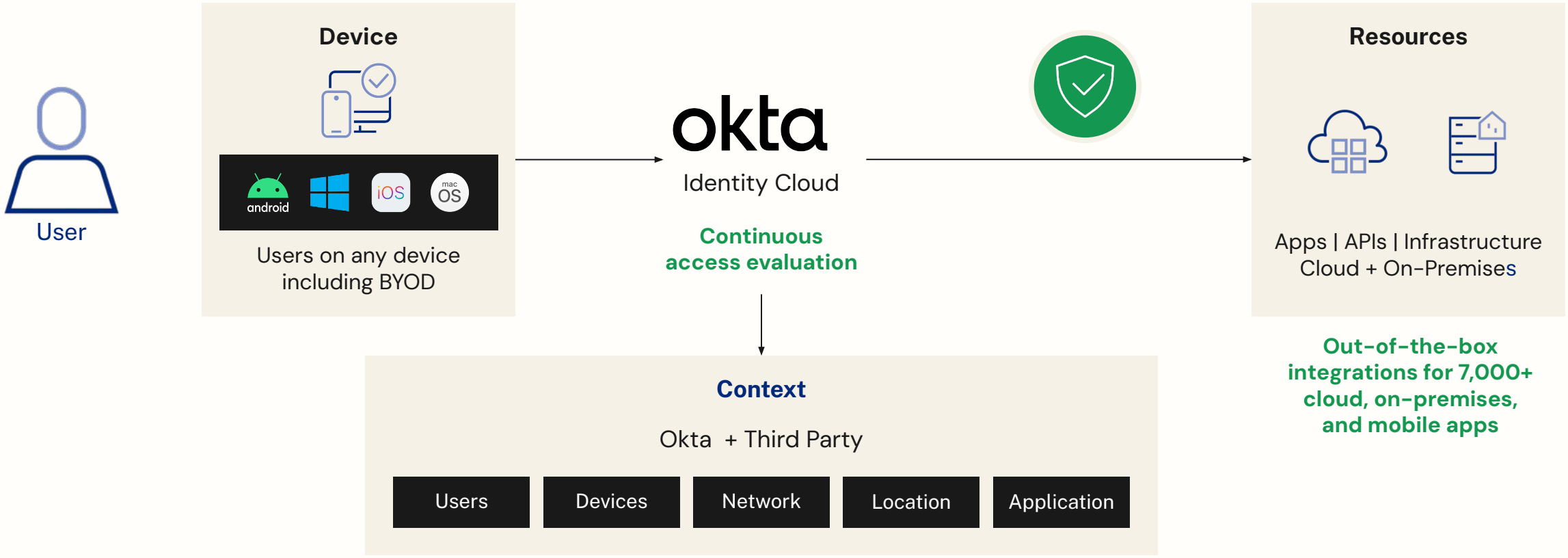
NIST SP 800-63-3 (section 6.2) provides a sample decision tree on categorising apps. Group applications by risk to simplify policy creation (e.g. AAL1, AAL2, AAL3).

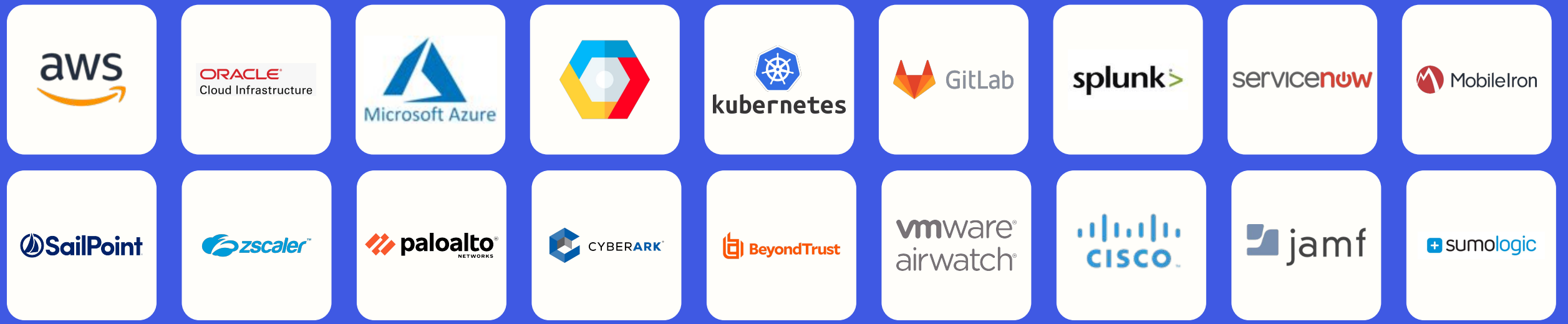
Policies are configured in the Okta Admin Console at **Security > Authentication Policies**





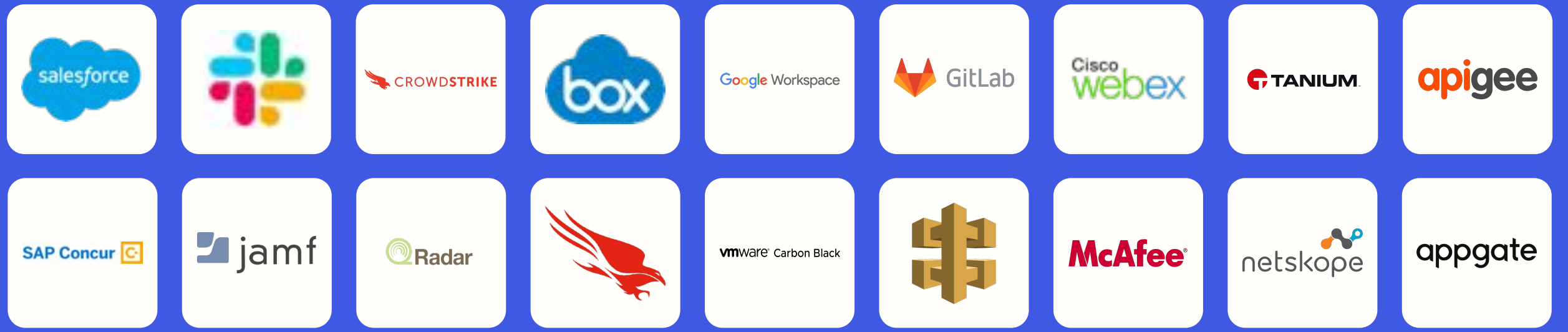
Zero Trust-based Decision Flow



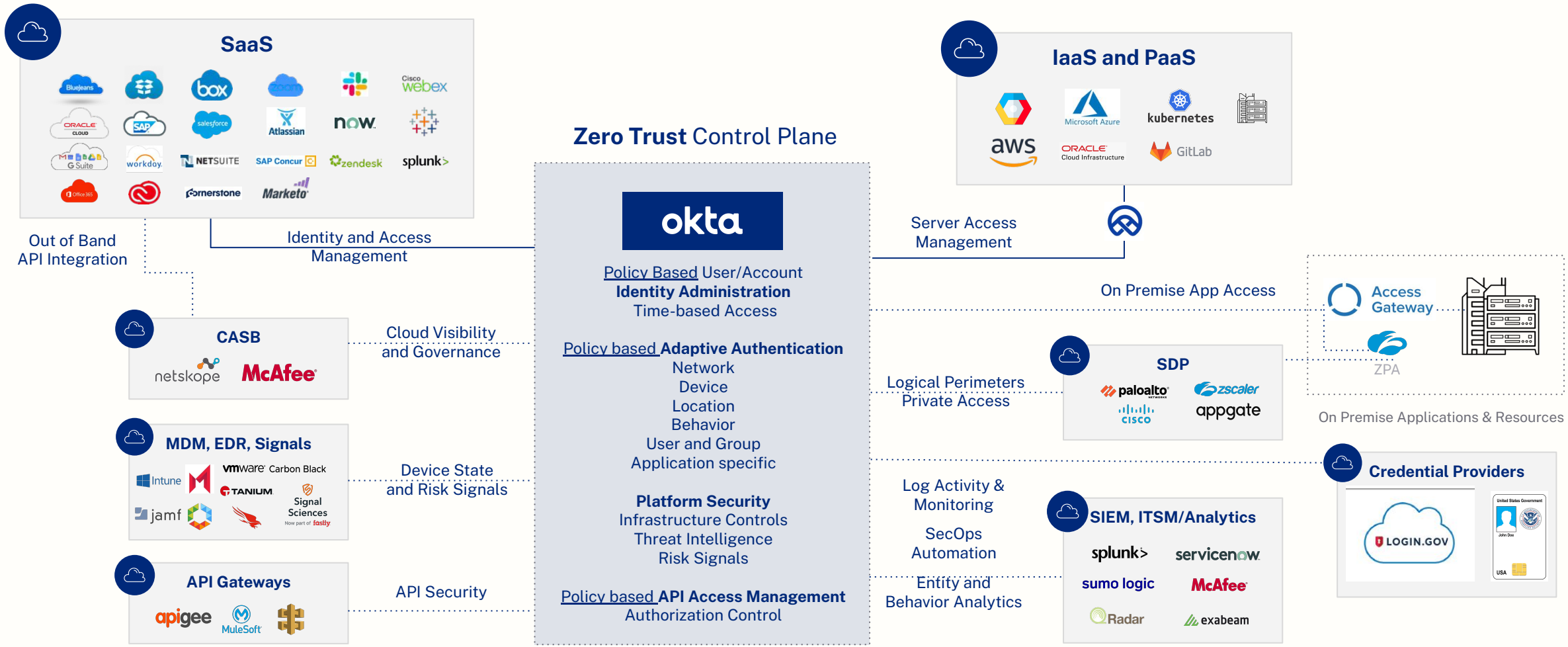


7,000+ Okta Integration Network

Broadest and deepest catalog of pre-built integrations • Extensible across legacy and cloud • DevSecOps friendly



ZT Reference Architecture



User friendly Okta Dashboard

Unified MFA experience across all factors

Zero Trust Best of Breed coordination

Pre-built integrations (Okta Integration Network)

External User use case (beneficiaries/dependents)

Delegated auth to local directory/AD (SSO)

Control API access and integrate with API gateways

Flexible architecture through multi-tenancy and hub-and-spoke integration

Demonstration

okta

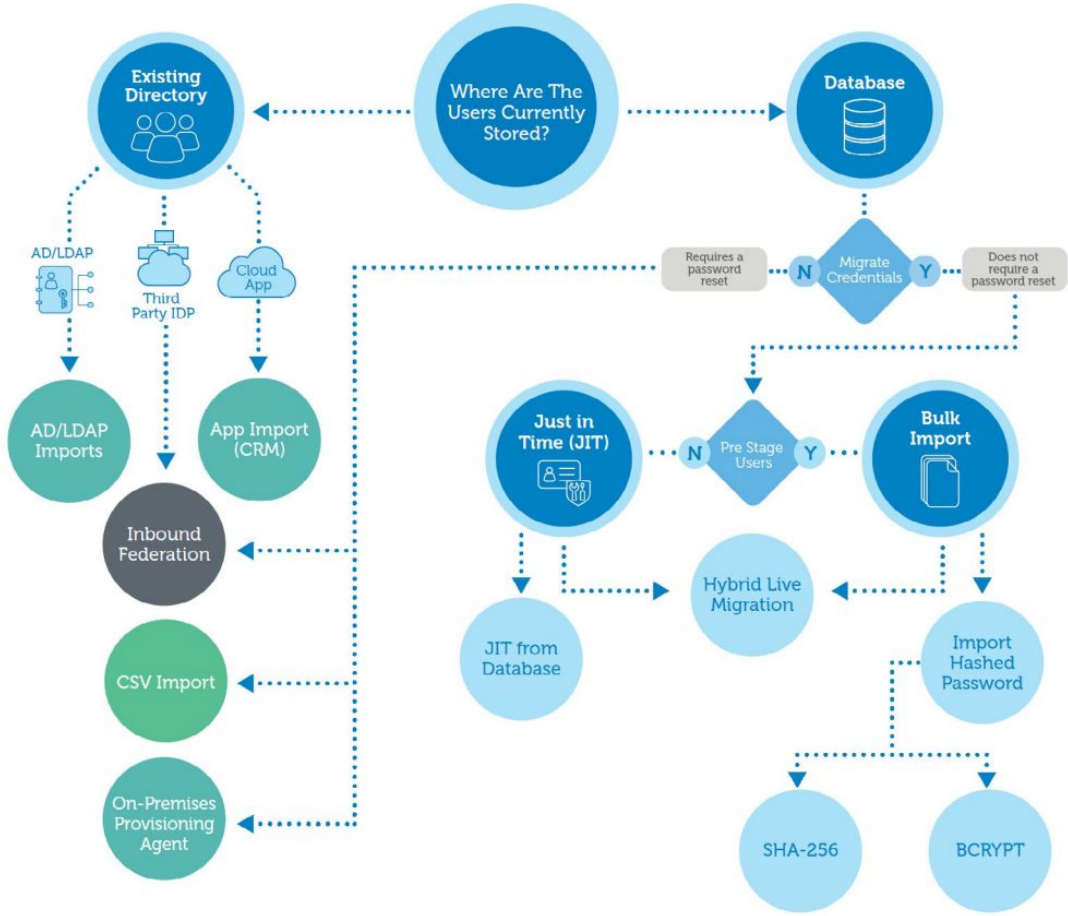
What is an Okta Org?

- An Okta Org represents a single customer population
  - Similar to a Domain or Tenant in other technologies
  - Contains Users, Groups, Applications, and Devices
  - Can be federated to other Orgs or IdPs
  - Applications can sync existing accounts with an Org
- Considerations to use multiple Okta Orgs:
  - Users need to exist in multiple populations
  - Data geographic residency
  - Separate compliance per population
  - Separation of customer data
  - Custom apps per population
  - Complexity of delegated permissions/administration
  - Complex Okta portal/login branding / sub-brands

Okta as an IdP - User Sourcing

-How would Okta perform the Identity Provider function?

- The Universal Directory is the user/attribute store the acts as the primary IDaaS service provided by Okta
- Setup AD Agent sync to ECUF or an IDSS sourced AD-LDS directory



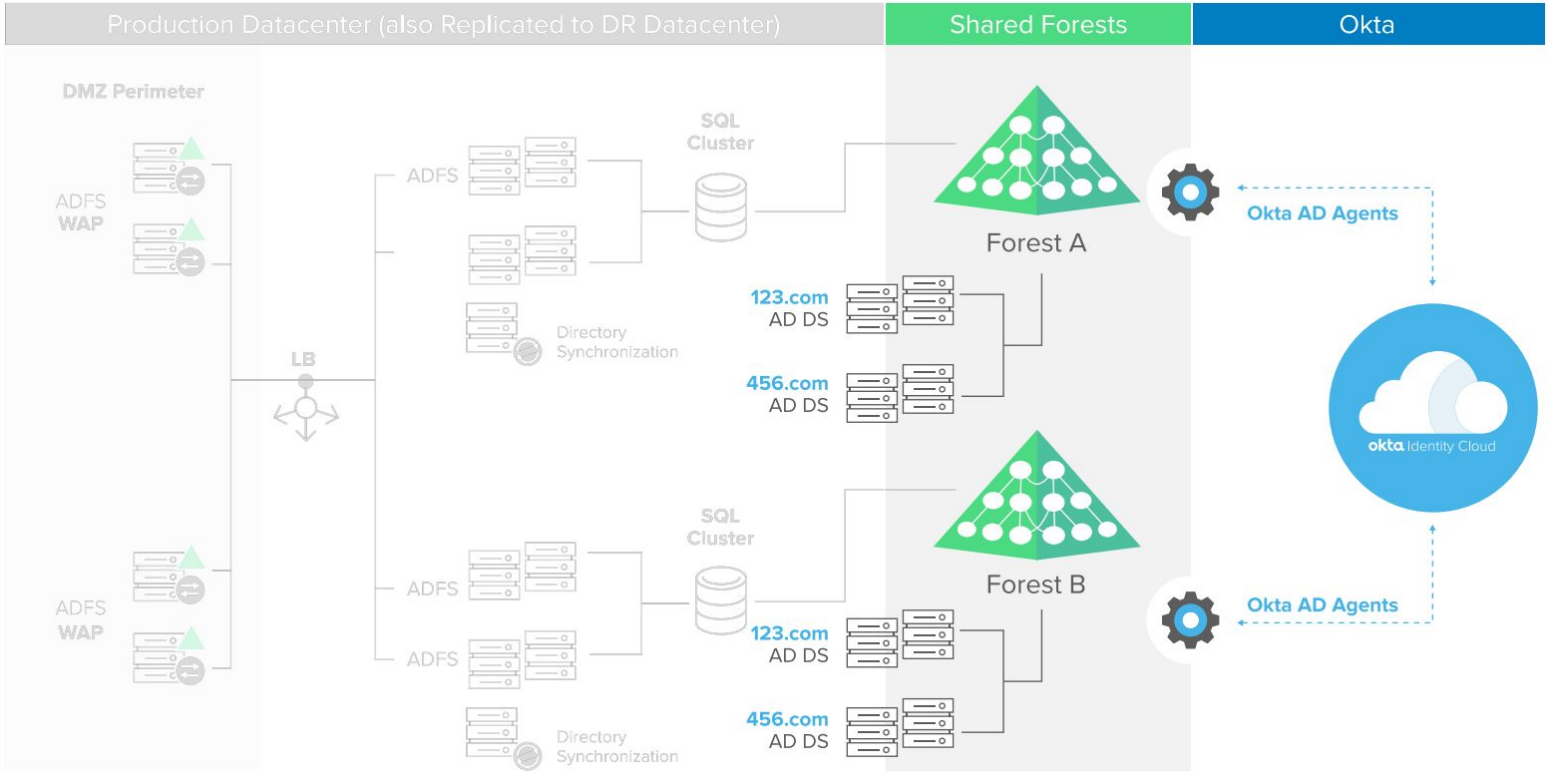
Source: https://www.okta.com/sites/default/files/2021-02/WPR_Okta-User-Migration-Guide.pdf

okta

Okta as an IdP - Add MFA to GFUD

-How would Okta perform the Identity Provider function?

- Use Okta as an MFA provider to GFUD/ADFS
- Install Okta ADFS Plugin on GFUD/ADFS farm
- Adjust Client Secret across farm per help article



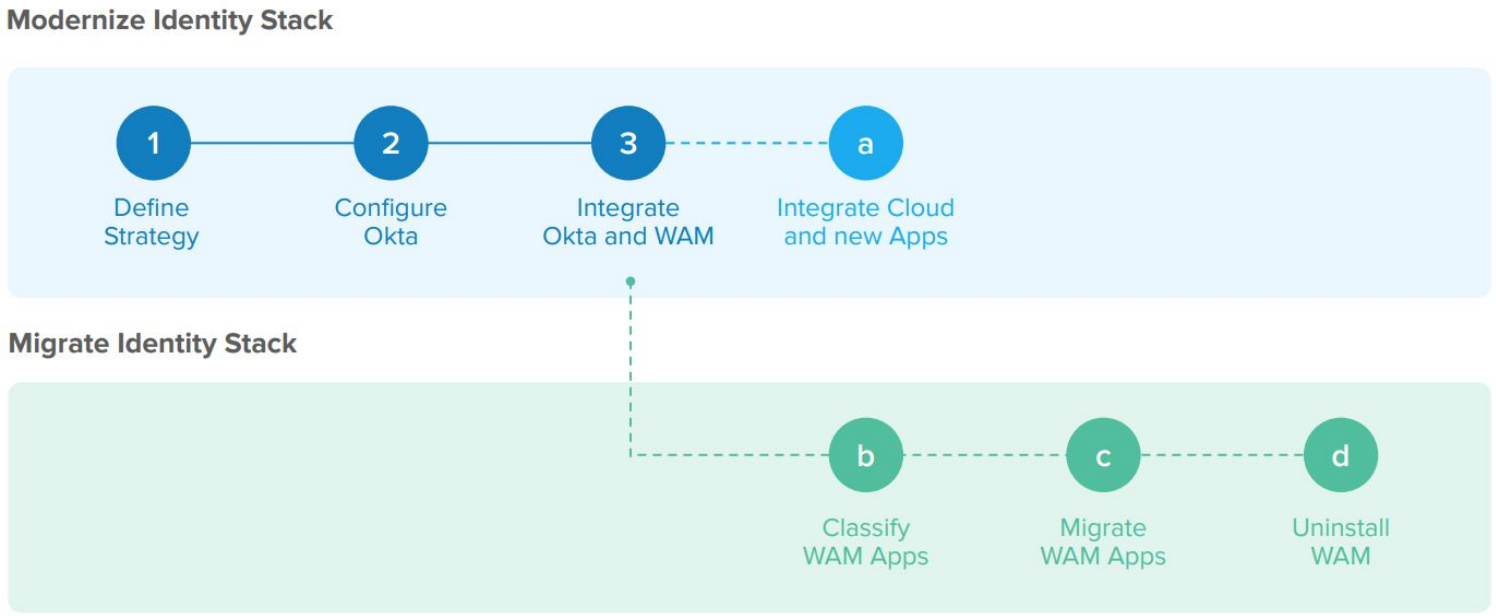
Sources: https://www.okta.com/resources/whitepaper/wam-modernization-and-migration-guide/
https://www.okta.com/resources/whitepaper/the-benefits-of-migrating-from-adfs-to-okta/
https://help.okta.com/en-us/Content/Topics/integrations/adfs-okta-int-farm.htm

okta

Okta as an IdP - Transition Off ADFS

-How would Okta perform the Identity Provider function?

- IdP authentication services can be configured:
  - Natively in Okta via SAML and OIDC for integration into downstream applications or
  - As inbound federation configured to accept GFUD authentication from existing IdPs into Okta



Okta Implementation Phases across different scenarios.

Source: https://www.okta.com/resources/whitepaper/wam-modernization-and-migration-guide/
https://www.okta.com/resources/whitepaper/the-benefits-of-migrating-from-adfs-to-okta/

okta

Okta capabilities for Automated Account Prov (AAP)

Okta supporting AAP:

- The Okta UD can be used to synchronize between multiple applications and external directories to provide a single user access.
- Existing applications that support account provisioning via SCIM can be integrated with UD and our Lifecycle Mana the creation, management, and decommissioning of accounts.
- OIN
- An external workflow could be integrated to Okta via API to provide equivalent DD2875 requests near term

What Okta IDaaS provides and/or aligns with c functions (Tier I-III support)

An admin role assignment consists of the following components (at the Okta Org level):

- Admin: The user or the user group that you need to grant admin permissions to.
- Role: A set of permissions that you constrain an admin to. There are two types of roles standard and custom. You can create a maximum of 100 roles for an org. Currently, permissions are limited to managing user, group, and app activity, as well as running profile source imports.
- Resource set: A collection of resources. You can create a maximum of 10,000 resource sets and assign a maximum of 1,000 resources for each resource set. Currently, only user groups and apps in your org are considered as resources

Standard Roles:

- Super Admin
- Org Admin
- Group Admin
- App Admin
- Read-Only Admin
- Mobile Admin
- Help Desk Admin
- Report Admin
- API Access Management Admin
- Group Membership Admin

Appendix - Okta capability descriptions.

Okta Verify	Okta's native desktop and mobile application, supporting Microsoft Windows, Apple MacOS, Apple iOS and Google Android.
Okta FastPass	A native desktop and mobile application that runs on the same platforms as Okta Verify. FastPass is a cryptographic authenticator that enables secure password-less authentication to minimize end user friction when accessing corporate resources, while still enforcing Okta's adaptive policy checks.
Adaptive Multi-factor authentication (aMFA)	Adaptive MFA provides an additional layer of security for access control, which gives Okta customers the ability to create contextual access policies that assess risk factors such as device, network, location, travel, IP, and other context at each step of the authentication process.
Single Sign-On	Okta creates a seamless user experience by providing single sign-on to all the web and mobile applications users need to access. Users log in once and can then launch each application without having to re-enter credentials. Okta utilizes identity federation via the most common industry protocols, including SAML 2.0, OAuth 2, OIDC, etc.
Integration with Applications	Okta comes with pre-integrated applications that customers can select to allow their users to access them through the Okta Integration Network, either in their enterprise or in a cloud.
Universal Directory (UD)	Many companies have multiple identity sources with different types of users, such as contractors, partners, and customers. Okta Universal Directory provides a single view across all these groups with AD and LDAP directory integrations and out-of-the-box connections with HR systems, CSV files, and third-party IdPs. Customers can choose to authenticate these users against their own user store (e.g., Active Directory or LDAP) or they can use Okta as the user store.
Okta API integration	Customers can also integrate their own applications with Okta API. For Okta IDaaS GHC, customers are responsible for ensuring they allow their users to connect only to authorized applications, whether on-premises or in the cloud.
Okta Sign In Widget (SIW)	The out of the box end user experience that our customers can deploy in an Okta hosted environment. SIW provides configurable user registration, sign in and recovery experience. Customers can also configure policies that manage user access and security when they access various applications. The user flows can be branded according to customers' brand.
Okta SDKs	Allows customers to build their own identity experience using Okta as a back end. SDKs abstract the complexity of Okta platform for server-side web, front end web and mobile application development. SDKs are available in several programming languages and are accompanied by sample applications.
Okta's prebuilt monitoring, logging, and reporting tools	Makes it easy to analyze security posture, user access events, lifecycle management transitions, security risks and other identity-related data. These logs and signals can be ingested into various SIEM solutions for additional analysis.
Okta's Admin Dashboard	Provides central administration and provisioning of users and the applications they can access. User management is bidirectional, so accounts can be created inside applications and imported into Okta, or account information can be added to Okta and then pushed to the corresponding applications.
App analytics	Analyze usage and utilization, as well as logs that can be ingested into a customer's SIEM solution for monitoring

okta

Thank you!

Contact Information:

Ken Parrotte
571-246-3891
ken.parrotte@okta.com

Tyler Briley
tyler.briley@okta.com

Available Resources:

https://www.okta.com/resources/datasheet-factor-assurance/

https://www.okta.com/resources/whitepaper-deploying-modern-identity-for-national-security/

okta