okta

NIST Zero Trust 800-207 Mapping for Okta

Identity as the Foundation for Zero Trust

The

right people

have the

right level of access

to the

right resources

in the

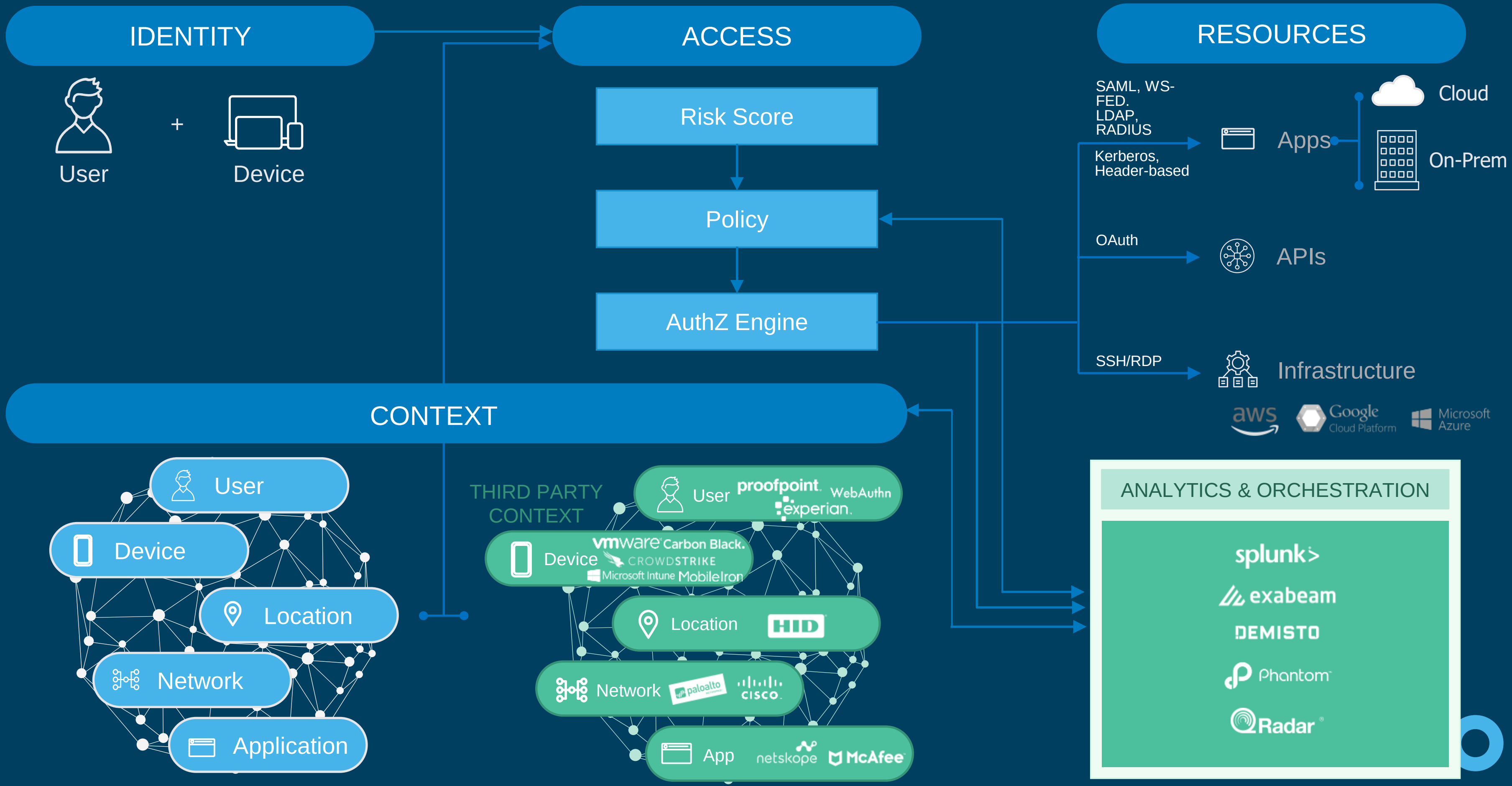
right context

that is

assessed continuously

Least Friction Possible

Zero Trust Reference Architecture



IDENTITY

User + Device

ACCESS

Risk Score

Policy

AuthZ Engine

RESOURCES

SAML, WS-FED. LDAP, RADIUS

Kerberos, Header-based

Apps

Cloud

On-Prem

OAuth

APIs

SSH/RDP

Infrastructure

aws Google Cloud Platform Microsoft Azure

CONTEXT

User

Device

Location

Network

Application

THIRD PARTY CONTEXT

User proofpoint. WebAuthn experian.

Device vmware Carbon Black. CROWDSTRIKE Microsoft Intune MobileIron

Location HID

Network paloalto cisco

App netskope McAfee

ANALYTICS & ORCHESTRATION

splunk>

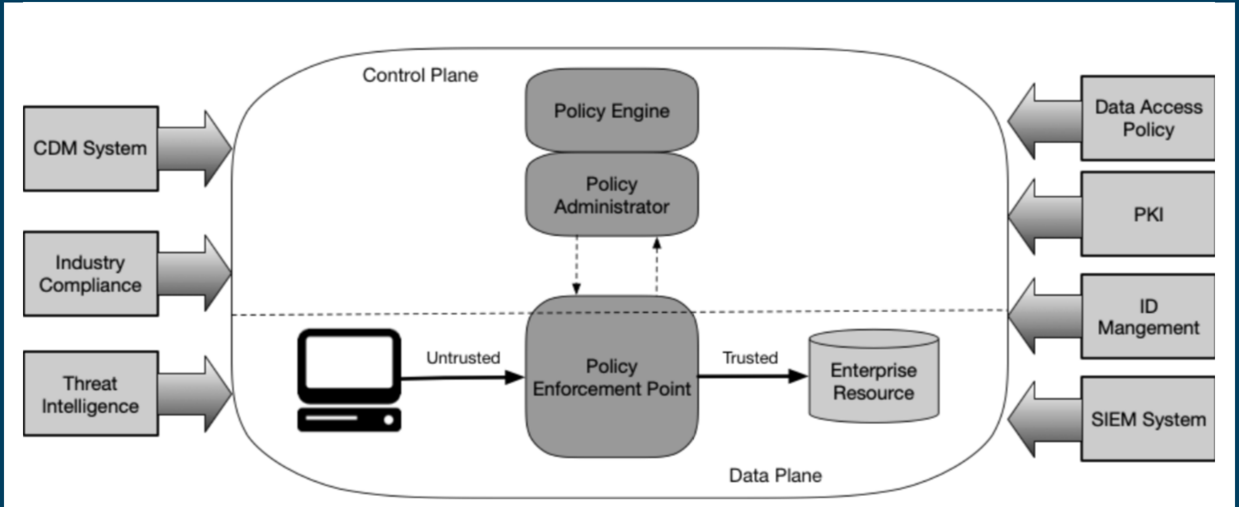
exabeam

DEMISTO

Phantom

Radar

Okta Mapping to NIST 800-207 Guidance



Okta as Policy Enforcement Point

- Okta as IdP is directly an PEP that enforces access to the application
- Okta as IdP to SP of App model (where go to app first) supported and enforcement occur at app
- Okta as IdP of OIDC redirect supported and ID token at app is enforced by app

Okta as Policy Administrator

- Okta provides direct and delegated admin to policies for zero trust access
- Okta API Server and Authentication policy issues tokens and cookies for OIDC/OAuth2 and/or SAML access
- Okta Access Gateway translates to app where legacy protocols required

Okta as Policy Engine

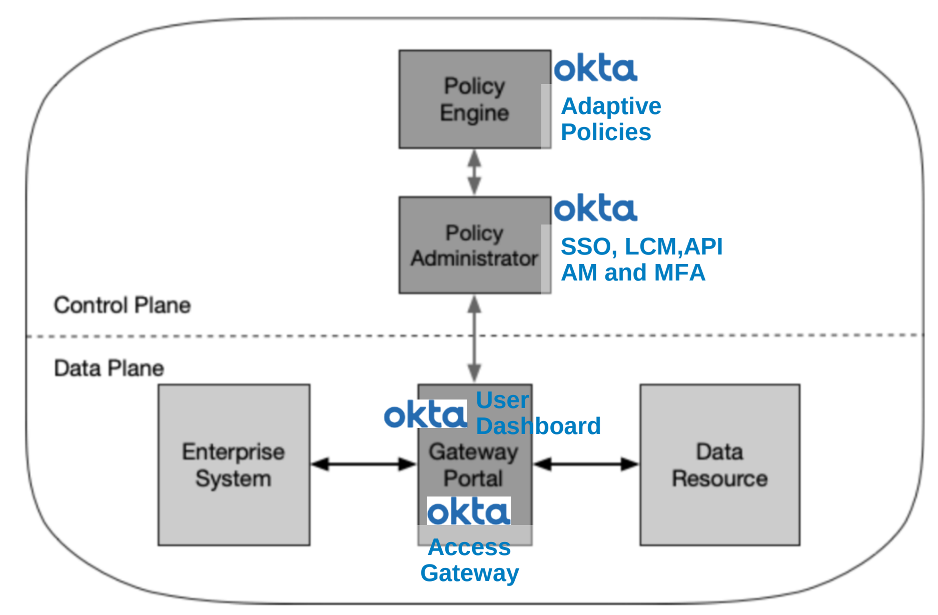
- Okta provides Policy Engine execution through Adaptive Policies and API Policies
- Okta API Server determines scopes and claims.
- Okta Adaptive Policy implements ZTA Trust Algorithm (TA)

Okta NIST 800-207 Resource Model Deployment

Deployment models (though are not direct application access model) as described in 3.1.1 and 3.1.2 can be supported with Okta partners such as Palo Alto, ZScaler and CASBs or with Okta Advanced Server Access.

Okta out of box focus is on direct application access model that does not depend on agents on clients. To this end the out of box deployment model is the Resource Portal-Based Deployment model.

Sample on right is from Figure 5 page 11 and overlaid are the Okta components fulfilling that capability.

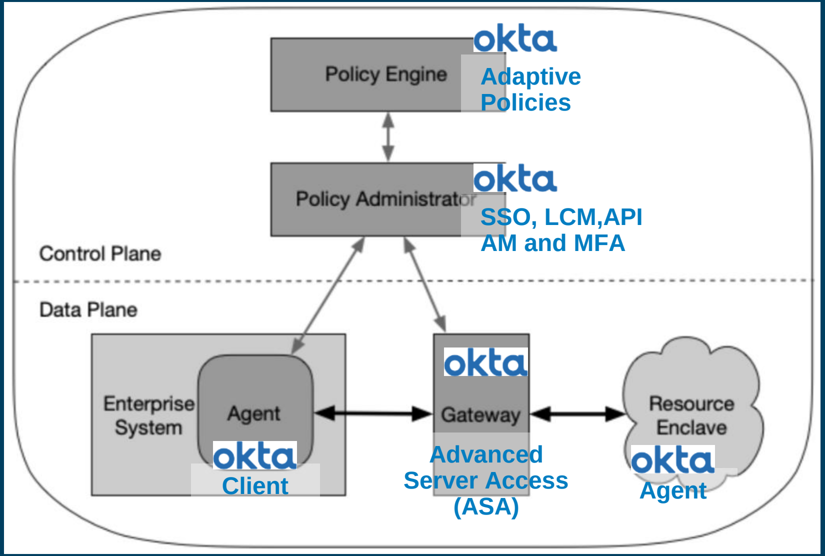


Okta NIST 800-207 Microperimeter Deployment

Okta does support 3.1.2 using Okta Advanced Server Access for purposes of accessing server resources.

Okta provides identity functions from Okta Identity Cloud for PE and PA and uses Okta Advanced Server Access for PEP function access to server resources.

Sample on right is from Figure 4 page 10 and overlaid are the Okta components fulfilling that capability.

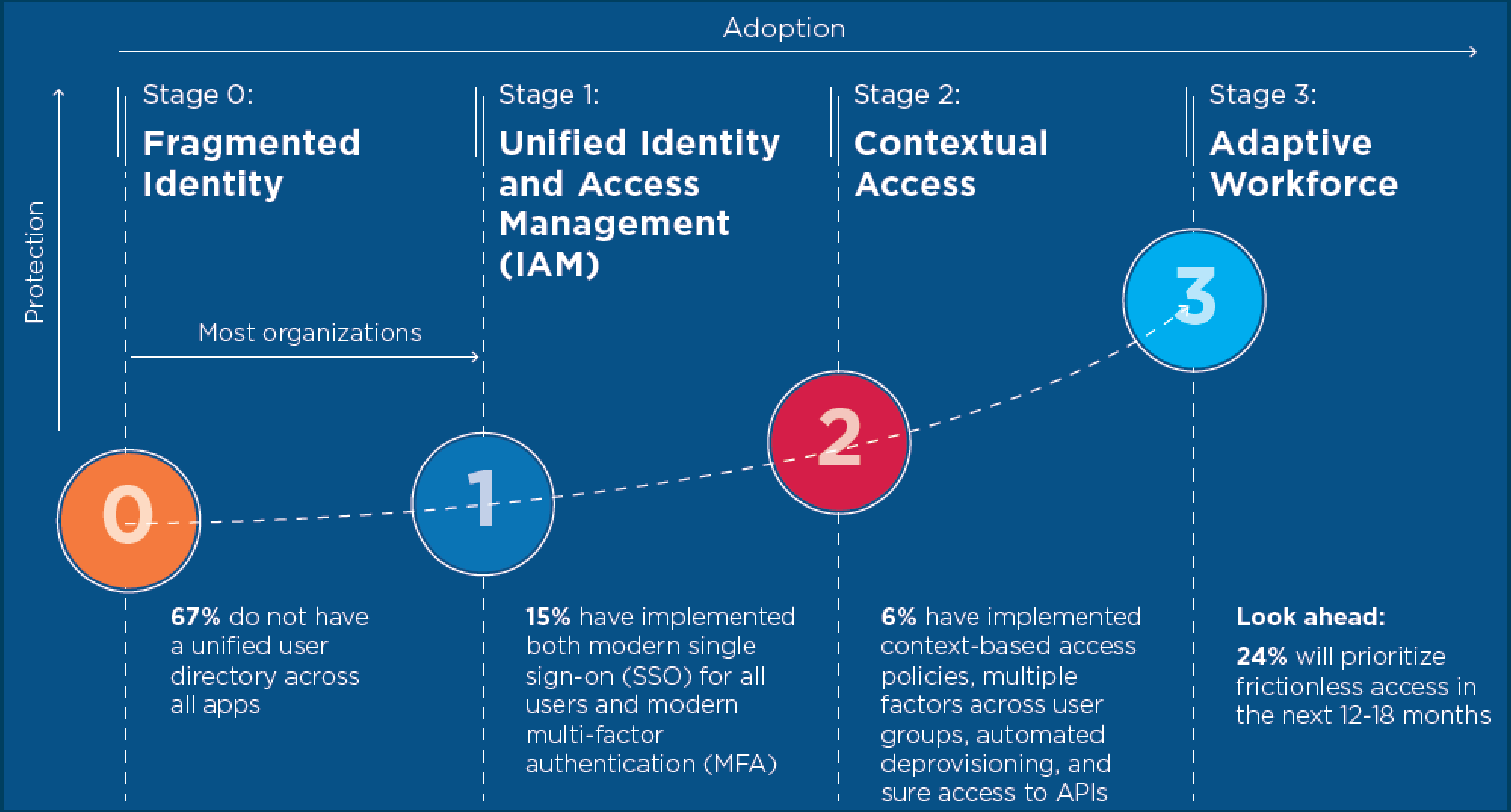


Q + A

okta

Thank You

Data Insights into Federal Adoption



Stage 0:

Fragmented Identity

67% do not have a unified user directory across all apps

Stage 1:

Unified Identity and Access Management (IAM)

15% have implemented both modern single sign-on (SSO) for all users and modern multi-factor authentication (MFA)

Stage 2:

Contextual Access

6% have implemented context-based access policies, multiple factors across user groups, automated deprovisioning, and sure access to APIs

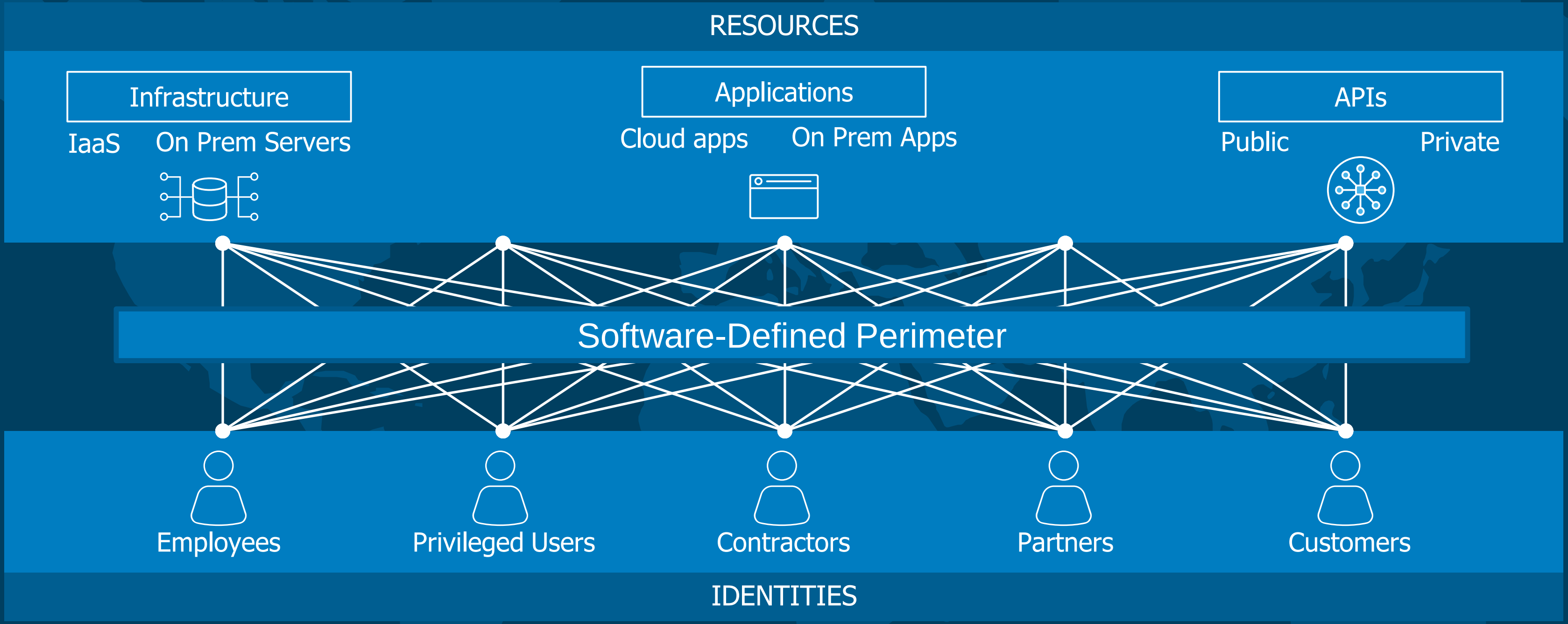
Stage 3:

Adaptive Workforce

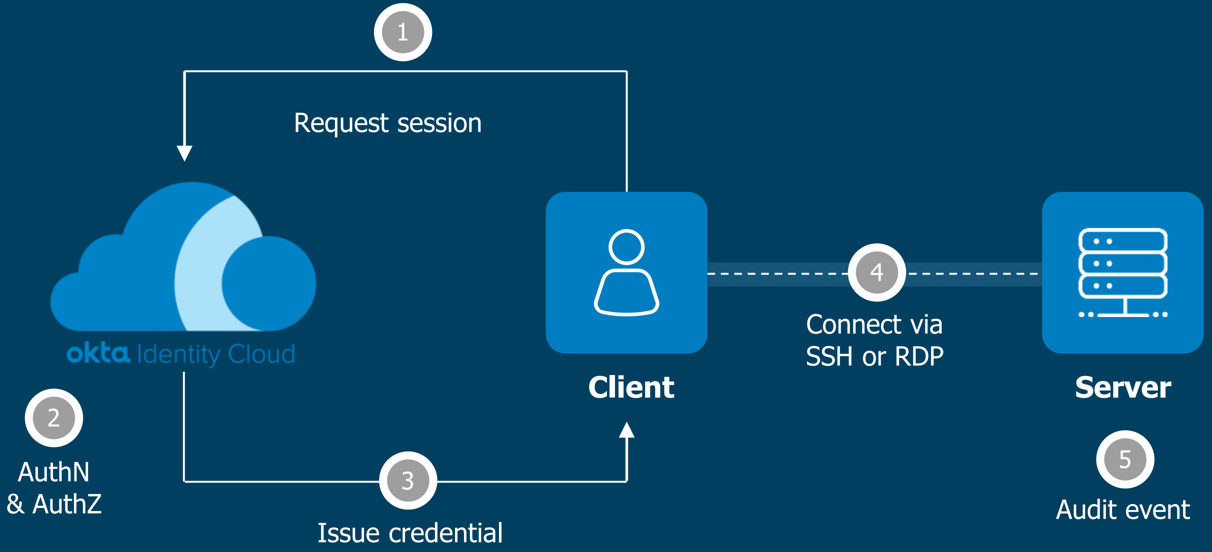
Look ahead:

24% will prioritize frictionless access in the next 12-18 months

Cloud, Mobile Have Dissolved the Network Perimeter



Advanced Server Access – Zero Trust for Infrastructure



Eliminates the use of static credentials by minting short-lived, tightly scoped client certificates for every independent request only once fully authenticated and authorized