Indian Health Service

Identity Management and IHS Authentication as a Service Supporting Zero Trust

KATHRYN LEWIS, OIT, SAILPOINT

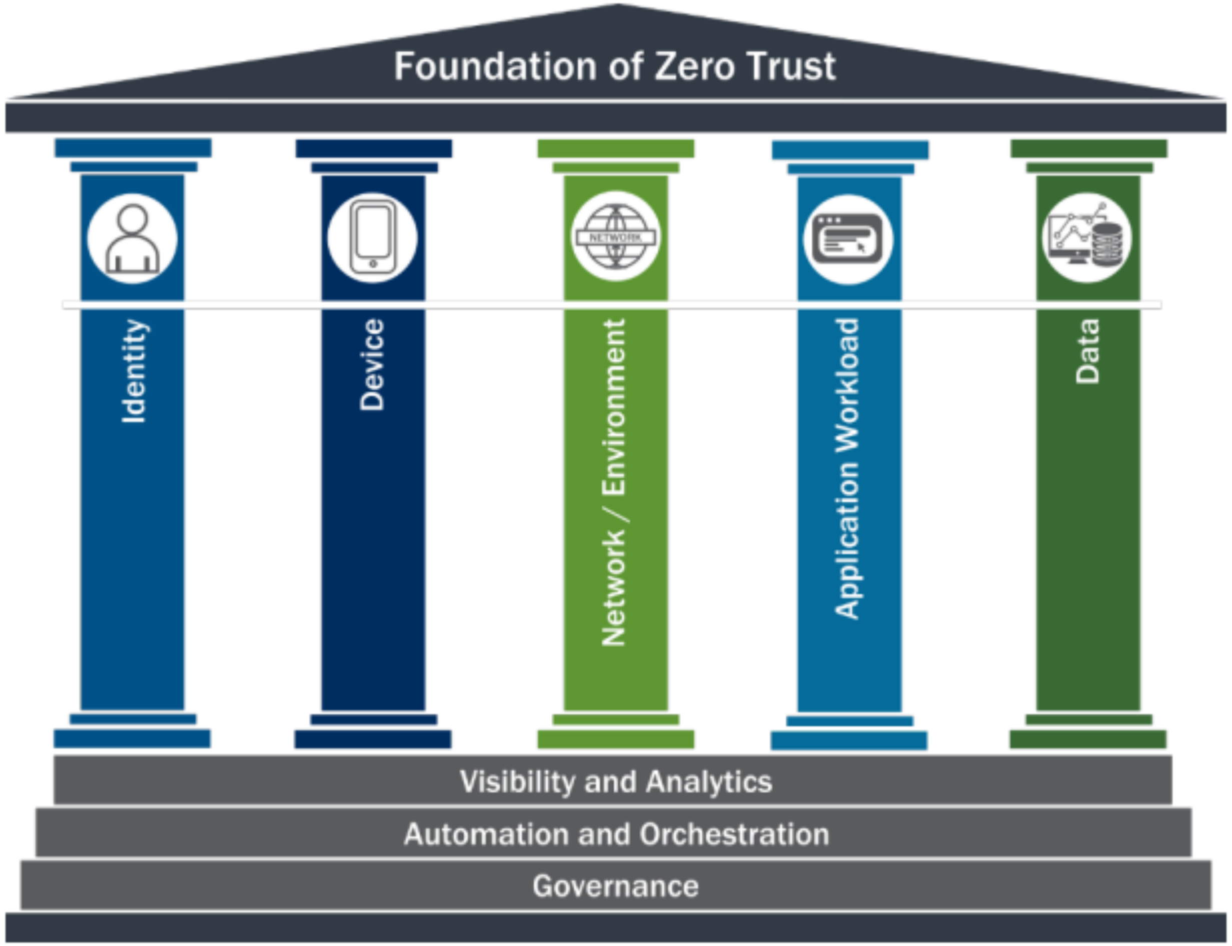
RAY GARZA, OIT, OKTA

08/23/2023

Agenda

- Zero Trust and the 5 CISA Pillars
- Zero Trust Identity Overview
- What is IHS Identity Access Management in support of Zero Trust?
- HHS/IHS IAM Policy References
- Identity Types and Onboarding
- Identity Audit and Certifications
- IHS Identity Goals & Roadmap
- IAM Future State Goals?
- Okta Overview
- Questions

CISA Five Pillars of Zero Trust



Pillar 1 – Zero Trust Identity Overview

Executive Order M-22-09 mandates that all federal agencies implement Zero Trust principles. The Executive Order defines an identity as an attribute or set of attributes that uniquely describe an agency user or entity. Agencies should ensure and enforce that the right users and entities have the right access to the right resources at the right time.

Identity: An identity refers to an attribute or set of attributes that uniquely describe an agency user or entity. This includes applying the following practices and controls:

1. Employ centralized identity management systems for agency users that can be integrated into applications and common platforms. COMPLETED
2. Require users to use a phishing-resistant method to access agency-hosted accounts. PARTIALLY COMPLETED
3. Public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication. IN PROGRESS
4. Remove password policies that require special characters and regular password rotation from all systems.
5. Agency authorization systems should work to incorporate at least one device-level signal alongside identity information about the authenticated user.

What is Identity Access Management in support of Zero Trust?

- Identity and Access Management (IAM), what is it and why is it important? In summary, Identity and Access Management is a structured set of business processes, policies, and technological solutions that allow an organization to manage digital identities efficiently and securely.

- This includes the consolidation of specific Identity information from authoritative sources such as Human Resources or the HSPD-12 Office for the use of Personal Identification and Verification (PIV) cards as well as the process for identity proofing to ensure that the right users obtain the right access at the right time in support of the IHS Mission. This creates a “Master User Record” for each user.

- Each authorized manager can access an application known as an IAM SailPoint identity vault and authorize the identity activation, view a users identity information and confirm what systems, applications, and databases that users are authorized to access on a network. This allows managers and IT security staff to also periodically certify a users assigned access based on a user’s role in the organization to and quickly remove access to multiple systems when they exit the organization. All part of the lifecycle management capabilities from within SailPoint IAM.

- IAM for IHS also includes an access request process using the ServiceNow Service Catalog for all team members managed by their authorized Identity Manager. Access is requested, verified, approved and either automatically added or assigned to the local IT fulfiller staff to complete the access provisioning to health IT systems and other local system in use across IHS.

HHS/IHS IAM Policy References

- Homeland Security Presidential Directive 12 (HSPD-12), “Policy for a Common Identification Standard for Federal Employees and Contractors,”
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards 201 (FIPS 201-3), Personal Identity Verification (PIV) of Federal Employees and Contractors, dated January, 2022
- National Institute of Standards and Technology (NIST) Special Publication (SP) for Digital Identity Guidelines, 800-63-4. These guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government information systems over networks. They define technical requirements in each of in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.
- HHS HSPD-12 Implementation Policy for the Use of the Personal Identity Verification (PIV) Card for Strong Authentication and OMB M-19-17
- IHM 10-7 Identity Authentication Policy (Final)
- IHM 10-2 Access Control Policy (DRAFT pending approvals)

Identity Types and Onboarding

There are two primary identity types currently managed using SailPoint IAM within IHS:

- Users with an HHSID: This includes all Federal employees and contractors. The digital identity is preauthorized based on identity information collected from other authoritative sources such as the Human Resource (HR) office (EHCM, EVD, BIIS related data), from the IHS Active Directory, from the Smart Card Management system (SCMS) and training completion from the Information System Security Awareness (ISSA) training system. These users are pre-created in a disabled state based on these identity sources and authorized/activated based on the managers approval.
- For non-employees or users working less than 120 days and who do not receive an HHSID, we have created an alternate unique ID (AF#) which will require each authorized manager to confirm the users identity within the IAM system as part of creating a new D1 user account. Every user is required to have completed the mandatory yearly ISSA training and validated within SailPoint.
- All Managers will perform the majority of these team identity management functions using SailPoint IAM

SailPoint IAM Yearly Certifications

What are Identity Certifications and Why is it required?

- Federal security regulations require all IAM Access Managers to conduct annual team member access reviews and to certify the continued access for every team member once a year or more often as necessary. With that managers can make administrative changes during the certification if there are discrepancies. This annual access review is essential to ensure that users not only maintain the access needed to do their jobs but are also compliant with the mandatory ISSA training requirements. This includes the determination for revoking specific access and privileges in alignment with users role and duties. This process of reviewing and certifying access is known as Access certifications or an IT access review.

- These requirements apply to ALL identity types (Employees, Contractors and Affiliates).

- As it can be seen, Identity and Access Management and the authorized access to critical IT systems, is a vital component of an organization's security posture. As we move forward into the next generation of business automation and Health IT modernizaton, both on-premise and in the cloud, solid Identity and Access business practices and associated technologies will help significantly ensure a more efficient and secure computing environment in support of patient care access and the security of patient data.

Identity Future State Goals

- **Vision: To align business requirements to authorized identity policies and access to IHS IT managed systems**

- **Goals:**
  - **Increase Identity Management Visibility for all Roles, Entitlements and Authorizations**
  - **Increase Identity Data Automation for standard access and authorization processes**
  - **95% Completions of Identity Certifications and Audit Campaigns for all Roles and Entitlements**
  - **Optimization of all identity processes to ensure the agility and timeliness of the right user access provided at the right time and for the right reasons**
  - **To improve the lifecycle management, rules, activation and deactivation practices**
  - **To expand on user application entitlements and roles to accurately reflect system level access**
  - **Evolve toward a Zero Trust Architecture (ZTA) for all aspects of Identity management**

IHS IAM Goals & Roadmap

Items highlighted in **blue** are completed activities
Items highlighted in **green** are activities in progress
Items highlighted in **black** are future activities
Yellow highlights indicate items that directly involve all IAM Managers

Goal 1

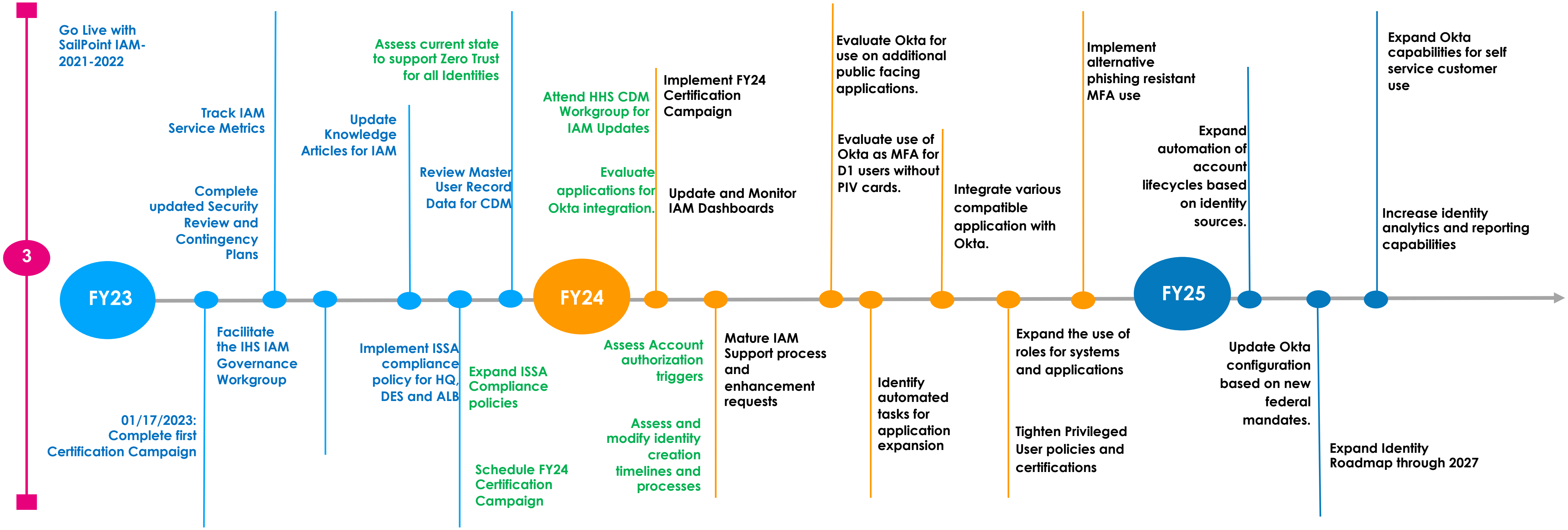
Increase Identity Management Visibility for all Roles, Entitlements and Authorizations

Goal 2

Increase Identity Data Automation for standard access and authorization processes

Goal 3

95% Completions of Identity Certifications and Audit Campaigns for all Roles and Entitlements



Go Live with SailPoint IAM- 2021-2022

01/17/2023: Complete first Certification Campaign

Facilitate the IHS IAM Governance Workgroup

Track IAM Service Metrics

Complete updated Security Review and Contingency Plans

Update Knowledge Articles for IAM

Implement ISSA compliance policy for HQ, DES and ALB

Review Master User Record Data for CDM

Expand ISSA Compliance policies

Schedule FY24 Certification Campaign

Assess current state to support Zero Trust for all Identities

Attend HHS CDM Workgroup for IAM Updates

Evaluate applications for Okta integration.

Assess Account authorization triggers

Assess and modify identity creation timelines and processes

Implement FY24 Certification Campaign

Update and Monitor IAM Dashboards

Mature IAM Support process and enhancement requests

Evaluate Okta for use on additional public facing applications.

Evaluate use of Okta as MFA for D1 users without PIV cards.

Identify automated tasks for application expansion

Integrate various compatible application with Okta.

Expand the use of roles for systems and applications

Tighten Privileged User policies and certifications

Implement alternative phishing resistant MFA use

Expand automation of account lifecycles based on identity sources.

Update Okta configuration based on new federal mandates.

Expand Identity Roadmap through 2027

Expand Okta capabilities for self service customer use

Increase identity analytics and reporting capabilities

What is Okta?

1. Okta is a cloud-based identity and access management (IAM) platform.
2. It provides a centralized solution for managing user authentication, authorization, and security across various applications and services.
3. Okta offers single sign-on (SSO) functionality, allowing users to log in to multiple applications with a single set of credentials.
4. It supports multi-factor authentication (MFA), adding an extra layer of security to user logins.
5. Okta enables administrators to manage user access and permissions to different resources and applications.
6. It offers integration capabilities, allowing organizations to connect Okta with various software and services, such as HR systems and cloud applications.
7. Okta provides robust security features, including user provisioning, password policies, session management, and Zero Trust architecture.
8. The platform offers comprehensive reporting and auditing capabilities, helping organizations monitor and track user activities.
9. Okta supports identity federation, allowing users to access applications and services using their existing credentials from other identity providers.
10. It can be used by businesses of all sizes and across various industries to enhance security, streamline user management, and improve user experience.

Okta AaaS Benefits

1. Okta provides a seamless implementation of multi-factor authentication (MFA), which adds an extra layer of security to user logins by requiring multiple factors such as passwords, SMS codes, or biometrics.

2. With Okta, organizations can enforce strong authentication policies and easily configure MFA for various applications and resources, reducing the risk of unauthorized access.

3. Okta integrates with popular MFA methods, such as SMS, email, voice call, authenticator apps, and hardware tokens, allowing organizations to choose the most suitable option for their environment.

4. Okta's MFA capabilities enhance the security of a zero-trust environment by adding an additional authentication step for every access attempt, reducing the risk of compromised credentials leading to unauthorized access.

5. Okta's adaptive MFA can dynamically assess risk factors such as device trust, IP reputation, and user behavior, prompting for additional authentication when suspicious activity is detected, ensuring a higher level of security in a zero-trust environment.

6. Okta's MFA solution is easy to manage and administer, with centralized control and policy enforcement, enabling organizations to streamline the implementation of MFA across their environment.

7. Okta's MFA capabilities support various use cases, including remote workforce, partner/vendor access, and customer authentication, making it a versatile solution for organizations in different industries and environments.

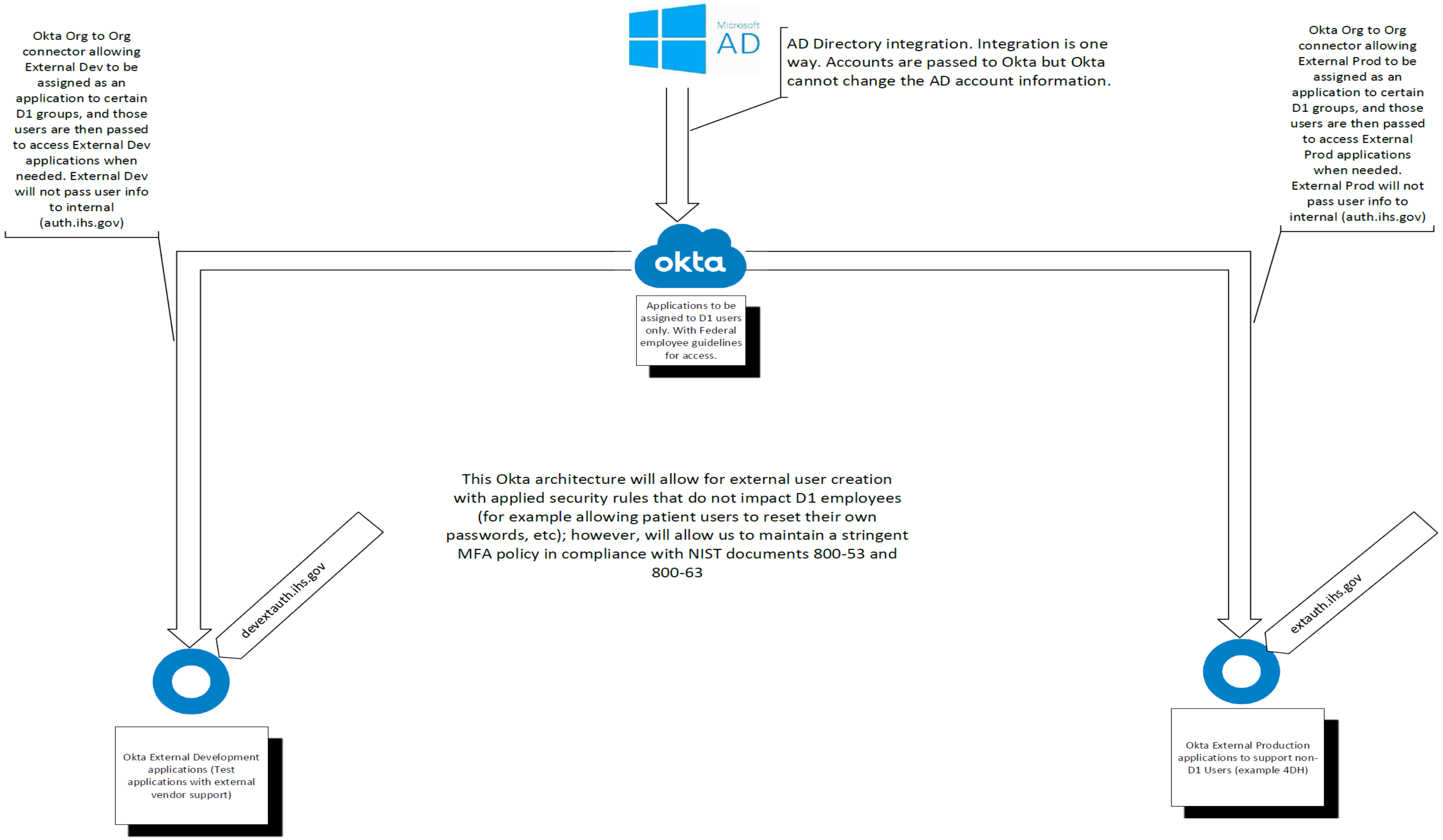
8. Okta's MFA can be seamlessly integrated with other Okta features like single sign-on (SSO) and user lifecycle management, providing a comprehensive identity and access management solution for organizations adopting zero-trust principles.

9. By incorporating Okta's MFA into a zero-trust environment, organizations can strengthen their security posture, reduce the risk of data breaches, and ensure that only authorized users with trusted devices gain access to critical resources and applications.

Okta High-Level Architecture (Preview and Prod)

1. Okta Preview -> Development and testing for internal and POC/POV implementations.
2. Okta Production ->Direct Access to IHS/(D1) users (internal employees)
3. Okta External Development -> External facing Okta that allows for testing and POV/POC development when outside accounts are needed for testing/development (i.e. Third party apps, external patient test accounts). Specific passed IHS accounts can have access and passed via Okta Production validation.
4. Okta External Production -> External Facing Okta that allows external users access to applications (i.e. 4DH). Specific passed IHS accounts can have access and passed via Okta Production validation.

Okta High-Level Architecture (Preview and Prod)



Okta Org to Org connector allowing External Dev to be assigned as an application to certain D1 groups, and those users are then passed to access External Dev applications when needed. External Dev will not pass user info to internal (auth.ihs.gov)

AD Directory integration. Integration is one way. Accounts are passed to Okta but Okta cannot change the AD account information.

Okta Org to Org connector allowing External Prod to be assigned as an application to certain D1 groups, and those users are then passed to access External Prod applications when needed. External Prod will not pass user info to internal (auth.ihs.gov)

Applications to be assigned to D1 users only. With Federal employee guidelines for access.

This Okta architecture will allow for external user creation with applied security rules that do not impact D1 employees (for example allowing patient users to reset their own passwords, etc); however, will allow us to maintain a stringent MFA policy in compliance with NIST documents 800-53 and 800-63

Okta External Development applications (Test applications with external vendor support)

Okta External Production applications to support non-D1 Users (example 4DH)

Okta Integration Questionnaire

Can be accessed via Service Now “Service Catalog->Active Directory Services->Okta Application Integration Request”

Okta Application Integration Request - Service Portal (servicenowservices.com)

1. What is the name of the application?
2. What is the background of the application?
3. Who is the business owner?
4. Who manages the application?
5. Is the application in production already?
6. Who are the supported end users?
7. What is the number of active users/accounts within the system?
8. Does the application reside on the internal network?
9. Is the application customer-developed or commercial off-the-shelf?
10. Does the application support any of the following authentication/sign in methods?
    1. OpenID Connect or SAML 2.0
    2. Neither

Current Application Integrations

1. Cisco Call Manager
2. Proofpoint
3. Tenable.io and Tenable.sc
4. 4DH (in Development/Test) -4DH Prod is in process
5. Crowdstrike (prod and Test/Dev)
6. Splunk
7. PRTG Network Monitor

Okta Future State Internal to IHS

1. Okta will continue to establish Zero trust capabilities to its applications.
2. 4DH Prod will be migrating to Okta’s external facing tenant to allow for patient login.
3. External users will be set to “self-reset” their passwords.
4. NIST guidance on 800-63v4 and 800-217 (PIV card guidance) will be evaluated and applied (if necessary) to strengthen our security posture and start moving to a Zero trust architecture.
5. Okta will work to apply these security standards while maintaining a user-friendly environment.

Okta Future State

1. Okta and zero trust will continue to evolve and play a crucial role in securing digital environments against emerging threats and complexities.

2. Okta is likely to enhance its integration capabilities with other zero-trust components, such as network access control (NAC), secure web gateways (SWG), and cloud security posture management (CSPM) solutions, to provide a comprehensive zero-trust framework.

3. Okta may incorporate advanced technologies like artificial intelligence (AI) and machine learning (ML) to strengthen its adaptive authentication and risk assessment capabilities within a zero-trust model.

4. Okta might expand its identity and access management (IAM) offerings to cover more aspects of the zero-trust architecture, including micro-segmentation, data protection, and endpoint security, enabling organizations to build end-to-end zero-trust ecosystems.

5. As the adoption of zero-trust principles grows, Okta is likely to introduce industry-specific solutions and compliance frameworks tailored to the unique requirements of various sectors, such as healthcare, finance, and government.

6. Okta may focus on simplifying the implementation and management of zero-trust principles, offering more intuitive interfaces, automated workflows, and pre-configured policies to streamline the adoption process for organizations.

7. Okta will likely continue to invest in research and development to address emerging threats and vulnerabilities, ensuring that its solutions remain at the forefront of zero-trust security practices.

8. Okta's zero-trust capabilities may extend beyond traditional IT infrastructure to encompass emerging technologies such as Internet of Things (IoT), cloud-native applications, and edge computing, providing a unified approach to security in complex, distributed environments.

9. Okta's future advancements in zero trust are likely to prioritize user experience, focusing on frictionless authentication methods, context-aware access controls, and intelligent risk-based decision-making to balance security and usability effectively.

10. As the digital landscape evolves, Okta's collaboration with industry partners, standardization bodies, and security communities will contribute to shaping the future of zero trust, promoting interoperability, best practices, and continuous innovation in securing digital identities and data.

Compliance References

Current State

1. NIST 800-53
2. NIST 800-63v3
3. NIST Best Practices for Privileged User PIV Authentication
4. Memorandum M-22-09 Zero Trust Strategy
5. Okta for Healthcare/Okta Compliant Service for ePHI compliance

Future State

1. NIST 800-63v4 (draft)
2. NIST 800-217 (draft)

Questions?

Kathryn.Lewis@ihs.gov
Ray.Garza@ihs.gov
Stephen.Freeman@ihs.gov