okta

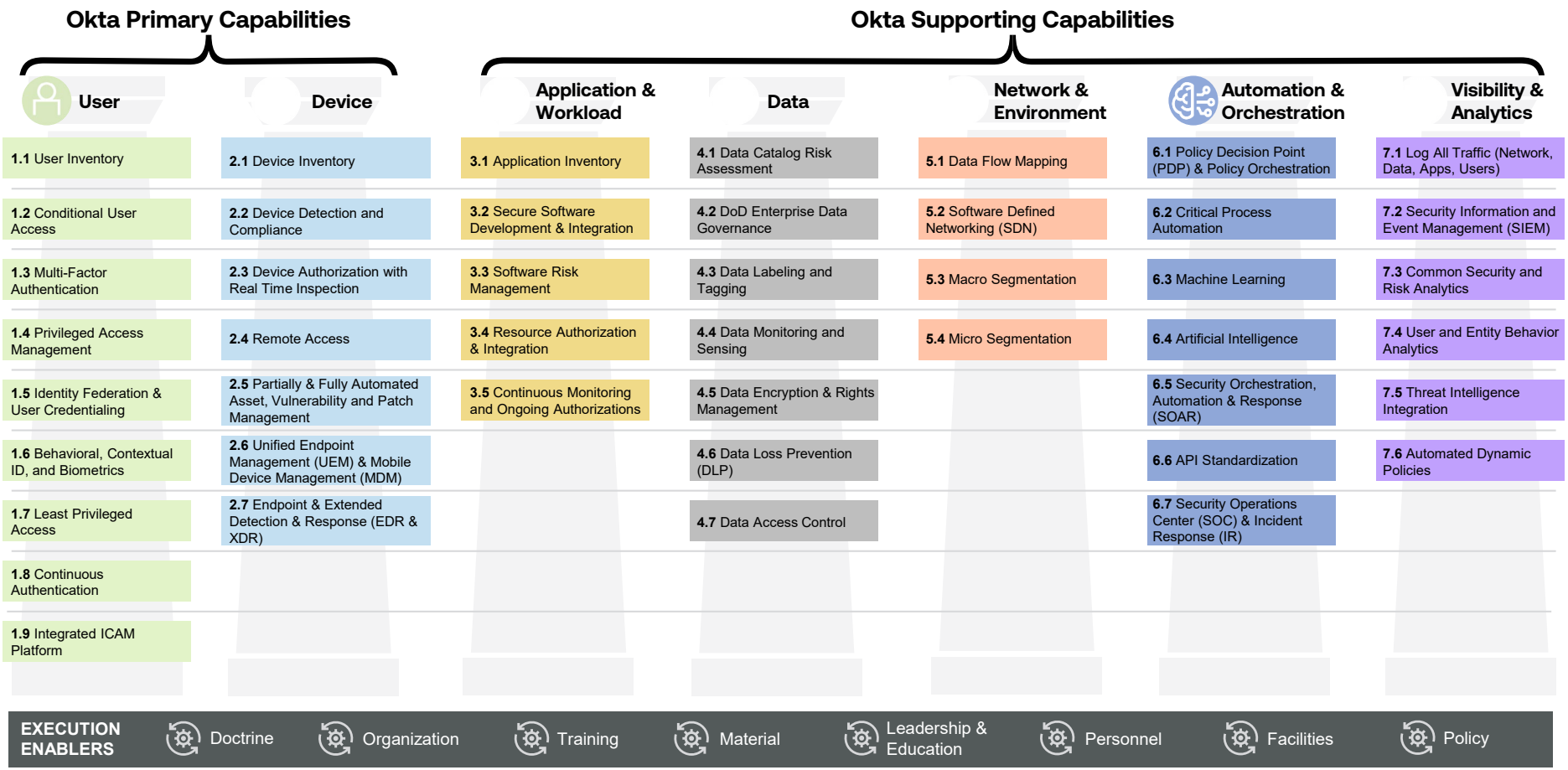
How Okta can help meet the DoD Zero Trust Capability Execution Roadmap

Identity is a common thread that binds the *U.S. Department of Defense (DoD) Zero Trust Reference Architecture*, the *DoD Enterprise Identity, Credential, and Access Management (ICAM) Strategy*, and the *National Security Agency (NSA) Embracing a Zero Trust Security Model*. Use this document to discover a breakdown of how adopting Okta, the leading independent Identity provider, can help your organization meet specific DoD Zero Trust capabilities. This document will map Okta capabilities to the DoD Zero Trust pillars, as defined in the DoD Zero Trust Capability Execution Roadmap (COA 1).

Overview

The DoD has already made significant technology investments to get to where it is today. The Department requires a vendor-neutral approach that complements existing solutions and facilitates a seamless journey to managing Identity in multi-cloud environments. Okta for US Military can help. Okta's Impact Level 4 (IL4) authorized[1] Identity platform is designed specifically for the DoD and approved mission partners and can support Identity and access management into IL5 applications. It can integrate with existing cloud and legacy infrastructure to support enterprise-wide Identity management, security, and modernization at scale. Our pre-built integration with 7,000 applications includes modern DoD apps with IL4 and IL5 authorizations (such as AWS, Box, CrowdStrike, O365, Salesforce, ServiceNow, VMware, Zoom, Palo Alto Networks, Splunk, and Zscaler).

[1] The Okta service currently has a conditional provisional authority to operate at Impact Level 4 (IL4) and service IL5 environments.



V1.0 as of 10/04/2022

Source: [DoD Zero Trust Capability Execution Roadmap (COA 1)]

Okta for US Military meets the User and Device requirements of DoD Zero Trust strategies, and it supports the other pillars with its open API framework, application ecosystem, and trust frameworks for easy integration with other Zero Trust vendors.

See the below table for information on key Zero Trust impact and outcomes, as well as details around how Okta helps customers meet these capabilities.

okta

Pillar 1: User

Capability	Capability Description	Capability Outcome	Impact to ZT	Okta Alignment
1.1 User Inventory	Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software, and services that have local users are all part of the inventory and highlighted.	System owners have control (visibility and administrative rights) of all authorized and authenticated users on the network.	Users not on the authorized user list will be denied access by policy.	Okta Universal Directory (UD) controls sprawl of user attributes and entitlements, helping organizations structure and manage identities from a single control pane. Okta developed scalable people and group management features, as well as advanced search capabilities, and no-code automation rules to manage user groups from multiple sources in UD, providing greater flexibility in administering user identities as organizations take on external identities such as customers, partners, and contractors. Privileged users can be managed by group membership or by a separate Identity - depending on customer requirements.
1.2 Conditional User Access	Through maturity levels, Conditional Access works to create a dynamic level of access for users in the environment. This starts with traditional role-based access controls across a federate ICAM, expands to application-focused roles and ultimately utilizes enterprise attributes to provide dynamic access rules.	Eventually, organizations control user, device, and non-user entity DAAS access through dynamically changing user risk profiles and fine-grained access control to include the use of user risk assessments.	Users not known to the system and users who present an unacceptable degree of risk will be denied access with greater accuracy.	Okta is an immensely customizable Identity platform with flexible authentication options based on your security environment and digital policy rules: Role Based Access Control (RBAC) or Attribute Based Access Control (ABAC) for defining application access. Further, dynamic access rules can be enacted based on continually assessed contextual factors such as where the user is geographically, suitability of their access, or what device they are using. For managed devices, Okta partners with Endpoint Detection and Response (EDR) vendors, like CrowdStrike, to combine at least one device-level signal alongside Identity information to provide important device assurance.
1.3 Multi-Factor Authentication (MFA)	This capability initially focuses on developing an organization-focused MFA provider and Identity Provider to enable the centralization of users. Retirement of local and/or built-in accounts and groups is a critical piece to this capability. At the later maturity levels, alternative and flexible MFA tokens can be used to provide access for standard and external users.	DoD organizations require users and non-user entities to authenticate using at least two of the following three attributes: knowledge (user ID/password), possession (CAC/token), or something you are (inherence, e.g., iris/fingerprints), in order to access DAAS.	Users not presenting multiple forms of authentication will be denied access to DAAS system and resources.	Okta embeds Zero Trust, phishing-resistant authentication into mission systems. Okta supports CAC or CAC alternatives, including existing third-party authenticators deployed within your extended workforce (e.g., YubiKeys, PIV cards, Generic OTP tokens, Google Authenticator, Duo MFA, FIDO2, and others) for consistent MFA interface across every application, custom, or COTS. Smart Card Authentication (per App PIV) is a way to use PIV/CAC to safeguard the most critical resources or for specific groups, while allowing lower assurance factors for less sensitive apps and persons. All factors listed are managed in Okta as one or more of the following factor types: Knowledge, possession, or biometric (inherited from device platform biometrics). Okta Adaptive MFA is an additional layer of security designed to consider user behavioral patterns and a number of contexts when evaluating login attempts: device, location, network, application, and user and group.

Pillar 1: User (continued)

Capability	Capability Description	Capability Outcome	Impact to ZT	Okta Alignment
1.4 Privileged Access Management (PAM)	The capability focuses on removal of permanent administrator/elevated privileges by first creating a Privileged Account Management (PAM) system and migrating privileged users to it. The capability is then expanded upon by using automation with privilege escalation approvals and feeding analytics into the system for anomaly detection.	DoD organizations control, monitor, secure, and audit privileged identities (e.g., through password vaulting, JIT/JEA with PAWS) across their IT environments.	Critical assets and applications secured, controlled, monitored, and managed through limits on admin access.	Okta MFA hardens access to critical applications, like the CyberArk Privileged Account Security Solution, with a full range of step-up authentication factors based on device, user, or location attributes.
1.5 Identity Federation & User Credentialing	The initial scope of this capability focuses on standardizing the Identity Lifecycle Management (ILM) processes and integrating with the standard organizational IDP/IDM solution. Once completed, the capability shifts to establishing an Enterprise ILM process/solution either through a single solution or Identity federation.	DoD organizations manually issue, manage, and revoke credentials bound to DoD person, device, and NPE identities. Identity information is developed and shared across entities and trust domains, providing "single sign-on" convenience and efficiencies to identified (authenticated and authorized) users and devices.	Visibility and accuracy of user authentication information is increased, to include DoD users and users managed by other agencies. Users lacking sufficient credentials are denied access according to established policies.	Okta provides insight into unclassified or internet-connected Identity use cases for the DoD through Lifecycle Management (LCM) tools needed for a consolidated and centralized virtual directory. Okta strengthens your security policies with automation of joiners/movers/leavers lifecycle transactions based on triggers from Active Directory, LDAP sources, and modern HR systems. Okta supports industry-standard protocols (SAML, OIDC, WS-Fed, SCIM) when federating with major vendor-offered and government-backed IDPs. Additionally, Okta has extensive SDKs that allow for integration of legacy and custom apps into Okta. Okta also streamlines integration of multiple Okta orgs/tenants through Okta Org2org integration capability. Okta leverages CAC/DoD PKI to safeguard the most critical resources or for specific user groups, while allowing lower assurance factors for less sensitive apps and persons. Okta also supports non-cardholders and federated identities as needed.
1.6 Behavioral Contextual ID, and Biometrics	Utilizing the Enterprise IDP, user and entity behavioral analytics (UEBA) are enabled with basic user attributes. Once completed this is expanded into Organizational specific attributes using Organizational IDPs as available. Finally, UEBA are integrated with the PAM and JIT/JEA systems to better detect anomalous and malicious activities.	DoD organizations utilize behavioral, contextual, and biometric telemetry to enhance risk-based authentication and access controls.	Behavioral, contextual, and biometric telemetry enhances MFA.	Okta provides Just-in-Time, Zero Trust contextual decisions on user access permissions and activity logs. When an end user logs in, Okta builds a risk profile and rates authentication requests as Low/Medium/High based on user, device, and network context. Based on the rating, Okta can deny or terminate access, and require additional authentication factors. Okta supports integration with enterprise SIEM/SOAR/UEBA tools that allow for log streaming into said tools. This allows for a full end-to-end orchestrated security.

Pillar 1: User (continued)

Capability	Capability Description	Capability Outcome	Impact to ZT	Okta Alignment
1.7 Least Privileged Access	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities. DoD Application Owners identify the necessary roles and attributes for standard and privileged user access. Privileged access for all DoD organization DAAS is audited and removed when unneeded.	DoD organizations govern access to DAAS using the absolute minimum access required to perform routine, legitimate tasks or activities.	Users on the network only have access to the DAAS for which they are authorized and authenticated over a specific timeframe.	Okta helps DoD Application Owners find patterns and high-value indicators at scale by correlating Identity data with that of other security and network systems. Okta's Identity and Access Management (IAM) system provides flexible policies so DoD Application Owners can set their unique authentication policy, which may vary by user groups or regions to enable scalable and manageable segmentation of permissions. Okta's LCM capabilities can be configured to terminate access for users when no longer necessary.
1.8 Continuous Authentication	The DoD organizations and overall enterprise will methodically move towards continuous attribute-based authentication. Initially, the capability focuses on standardizing legacy single authentication to an organizationally approved IDP with users and groups. The second stages adds in rule-based (time) authentication and ultimately matures to Continuous Authentication based on the application/software activities and privileges requested.	DoD organizations continuously authenticate and authorize users' access to DAAS within and across sessions using MFA.	Users not continuously presenting multiple forms of authentication will be denied access to DAAS system and resources.	Okta allows for granting access via Group or Attribute-based rules. These rules can be configured in Okta to automatically give/revoke access based on changes to user groups/attributes. As a cloud-native, modern enterprise IDP, Okta directly integrates with market-leading EDR platforms for device signaling and offers session-level access to technologies like Single Sign-On (SSO), to enable continuous authentication. Okta is also leading the development of industry open standards to process risk signals in near real-time.
1.9 Integrated ICAM Platform	DoD organizations and overall enterprise employ enterprise-level Identity management and public key infrastructure (PKI) systems to track user, administrator and NPE identities across the network and ensure access is limited to only those who have the need and the right to know. Organizations can verify they need and have the right to access via credential management systems, Identity governance and administration tools, and an access management tool. PKI systems can be federated but must either trust a central root certificate authority (CA) and/or cross-sign standardized organizational CAs.	DoD organizations employ enterprise-level Identity management systems to track user and NPE identities across the network and ensure access is limited to only those who have the need and the right to know; organizations can verify they need and have the right to access via credential management systems, Identity governance and administration tools, and an access management tool.	Identities of users and NPE are centrally managed to ensure authorized and authenticated access to DAAS resources across platforms.	Okta supports the full management of person and non-person identities (e.g., API accounts) in a common Identity-as-a-Service (IDaaS) platform. Okta seamlessly works with many authentication schemas, including issued DoD PKI credentials for CAC, Purebred-credentialed end-user devices, NPE-credentialed infrastructure, and internal less-than-medium assurance PKI solutions to govern access management to resources. Okta can enroll other MFA factors for additional security of accounts. Okta supports Role Based Access Control (RBAC) or Attribute Based Access Control (ABAC) for defining application access. Further, dynamic access rules can be enacted based on continually-assessed factors such as where the user is geographically, suitability of their access, or what device they are using.

okta

Pillar 2: Device

Capability	Capability Description	Capability Outcome	Impact to ZT	Okta Alignment
2.1 Device Inventory	DoD organizations establish and maintain an approved inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection. Device attributes will include technical details such as the PKI (802.1x) machine certificate, device object, patch/vulnerability status, and others to enable successor activities.	DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection.	By default policy, devices will be denied network access; the only devices permitted access to the network shall be known, authorized, and listed in the device inventory.	Okta Verify supports enhanced user authentication and authorization through device visibility. This includes context of managed device status through EDR/EMM integrations, but without replacing device management capabilities for corp/government-owned devices and managed bring your own device (BYOD) that enable deeper management control and visibility. Okta provides greater device inventory visibility than traditional device management because of the visibility it has on user access via unmanaged devices of platform status (e.g., device, OS, disk encryption, jailbreak/root detection). When using Okta Verify, devices can be tied to individual users as registered devices, regardless of management status, which provides additional control options for authentication policies. Okta augments EDR/EMM solutions for government managed devices.
2.2 Device Detection and Compliance	DoD organizations employ asset management systems for user devices to maintain and report on IT and Cybersecurity compliance. Managed devices (enterprise and mobile) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C).	DoD organizations employ asset management systems for user devices to maintain and report on IT compliance. Any device (including mobile, IoT, managed, and unmanaged) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C).	Any device attempting to connect to the network will be detected; only those devices that are compliant (e.g., anti-virus is up to date, approved configuration) will receive access to requested DAAS.	Device visibility data from Okta Verify can be evaluated through authentication policies to enforce compliance/assurance. Okta augments existing C2C capabilities that support 802.1X network authentication by providing authentication services.
2.3 Device Authorization with Real Time Inspection	DoD Organizations conduct foundational and extended device tooling (NextGen AV, AppControl, File Integrity Monitoring (FIM), etc.) integration to better understand the risk posture. Organizational PKI systems are integrated to expand the existing Enterprise PKI to devices as well. Lastly, Entity Activity Monitoring is also integrated to identify anomalous activities.	DoD organizations establish processes (e.g., Enterprise PKI) and utilize tools to identify any device (including unmanaged devices, infrastructure devices, and endpoint devices) attempting to access the network, and make a determination if the device should be authorized to access the network. Maturation of this capability monitoring and detection of this activity on endpoints and IT infrastructure in real time.	Components can use policies to deny devices by default and explicitly allow access to DAAS resources only by devices that meet mandated configuration standards. Security threats identified are remediated faster through continuous activity inspection enables faster remediation of security threats.	Through integrations with EDR/EMM solutions, Okta can provide the control point to allow/disallow real-time authentication to applications based on compliance/security policy of a user/device from the EDR/EMM.

Pillar 5: Network and Environment

Capability	Capability Description	Capability Outcome	Impact to ZT	Okta Alignment
5.4 Micro Segmentation	DoD organizations define and document network segmentation based on Identity and/or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly, where possible, organizations will utilize host-level process micro segmentation.	DoD organizations define and document network segmentation based on Identity and/or application access in their virtualized cloud environments.	Network segmentation enabled by narrower and specific segmentation in a virtualized environment via Identity and/or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes.	Okta provides user and authentication management to network/environment segmentation capabilities. Okta provides access management for API accounts with custom scopes to segment machine access/permissions.

Pillar 7: Visibility and Analytics

Capability	Capability Description	Capability Outcome	Impact to ZT	Okta Alignment
7.1 Log All Traffic (Network, Data, Apps, Users)	DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format, and rules/analytics are developed as needed.	DoD organizations collect and process all logs, including network, data, application, device, and user logs, and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or SOC.	Foundational to the development of automated hunt and incident response playbooks.	Okta logs authentication transactions for users and machine APIs. These transactions contain information pertaining to user/device/network/application/risk context. Okta offers two routes to integrate with best-of-breed SIEM solutions to ingest Okta's log data: through APIs and with out-of-the-box application integrations, allowing for aggregation of authentication and application access information with the rest of the logging data from the security stack.

To learn more about how Okta can help your organization meet Zero Trust requirements and modern ICAM adoption, contact us at federal@okta.com.