Using Okta to Protect IL4 Data

okta

Index

Overview

Okta is the industry leader in identity and access management, enabling organizations to accelerate the secure adoption of their web-based applications, both in the cloud and on premises. Okta delivers a complete solution that addresses the needs of IT, end users, business leaders, and developers; no customization is required. By adopting the Okta service, organizations dramatically improve the security and ease of managing their applications, including Software as a Service (SaaS), Platform as a Service (PaaS), and other on-prem and cloud-based applications. IT benefits by using one central place for policy-based management that governs which users get access to the mission-critical applications and data that power core business processes, regardless of their location. End users benefit by using their Okta single sign-on homepage to simplify their life and reduce the security risks caused by "password fatigue," and developers benefit through the use of an easy-to-implement, hardened identity platform, enabling them to focus on delivering feature sets, not building user management. With Okta, there is no longer a need for users to resort to the typical tricks for memorizing passwords—obvious or reused passwords, writing passwords down on Post-it notes, or saving them in Excel files on their laptops.

Using industry-standard technologies such as SAML, OpenID, OAuth2, and WS-Fed, Okta is designed to provide the benefits of strong, centralized authentication without 3rd party exposure to downstream data. Customers regularly use Okta to protect Personally Identifiable Information (PII), Payment Card Industry (PCI), credit cardholder data environments (CDE), Healthcare and Life Science data such as electronic Protected Health Information (ePHI), Financial data, and more, while staying out of scope for the associated regulations. This reduces cost and increases technology organization to be more flexible, ultimately creating a better user experience.

In 2017, Okta obtained a FedRAMP Moderate Authorization, enabling Federal customers to use the Okta service for unclassified workloads which includes DoD Impact Level 2. Okta provides identity services for multiple agencies, including the Department of Justice, Center for Medicare and Medicaid Services (part of Health and Human Services), Surface Transportation Board, and the Federal Communications Commission. Okta is also integrated as part of other cloud services currently FedRAMP Authorized. As Department of Defense agencies continue to migrate workloads to the cloud, there is a greater need for centralized identity management. In this document, we will discuss methods that can be used to reduce the risk of using Okta to protect DoD workloads up to Impact Level 4.

Secure Architecture

Okta is implemented as the identity layer in your application, where it performs authentication and authorization, passing a token to the application with an identity assertion. It is the responsibility of the application to correctly assign and manage privilege to the user based on this token. With this model and approach, Okta does not have access to any sensitive data stored within the application, and can be separated from this data.

Authentication is typically performed using one of the SAML 2.0, OAuth, or OpenID Connect standards, where an authentication token is generated and signed using a pre-shared certificate configured by the system administrators. This token is passed over a TLS 1.2 connection through the end-user's browser (UserAgent), which creates a separation between Okta and the data in the downstream application.

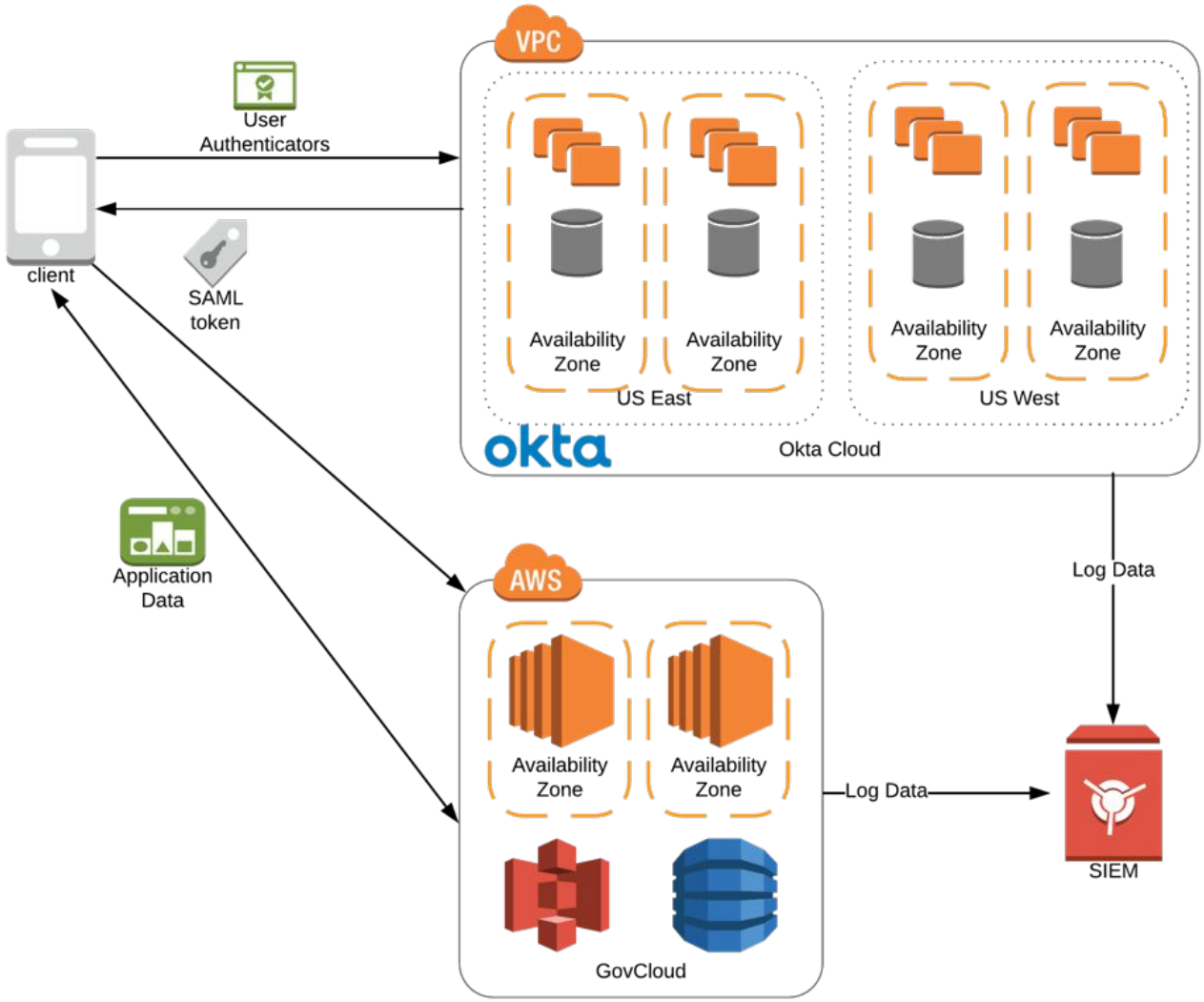

Figure 1: Okta as Enterprise SSO Identity Provider

Okta may also be connected to a directory system such as Active Directory or LDAP in order to extend the organization's identity into the cloud. Okta's AD agent is designed with security in mind; in a typical deployment, no firewall changes are needed to integrate on-premises directories. The Okta agent may be installed on any domain member server, installation on a domain controller is not required. This allows the customer to maintain full control over the permissions the Okta Agent operates under, and can filter and control what attributes are shared with Okta. Data is always encrypted while at rest and in transit.

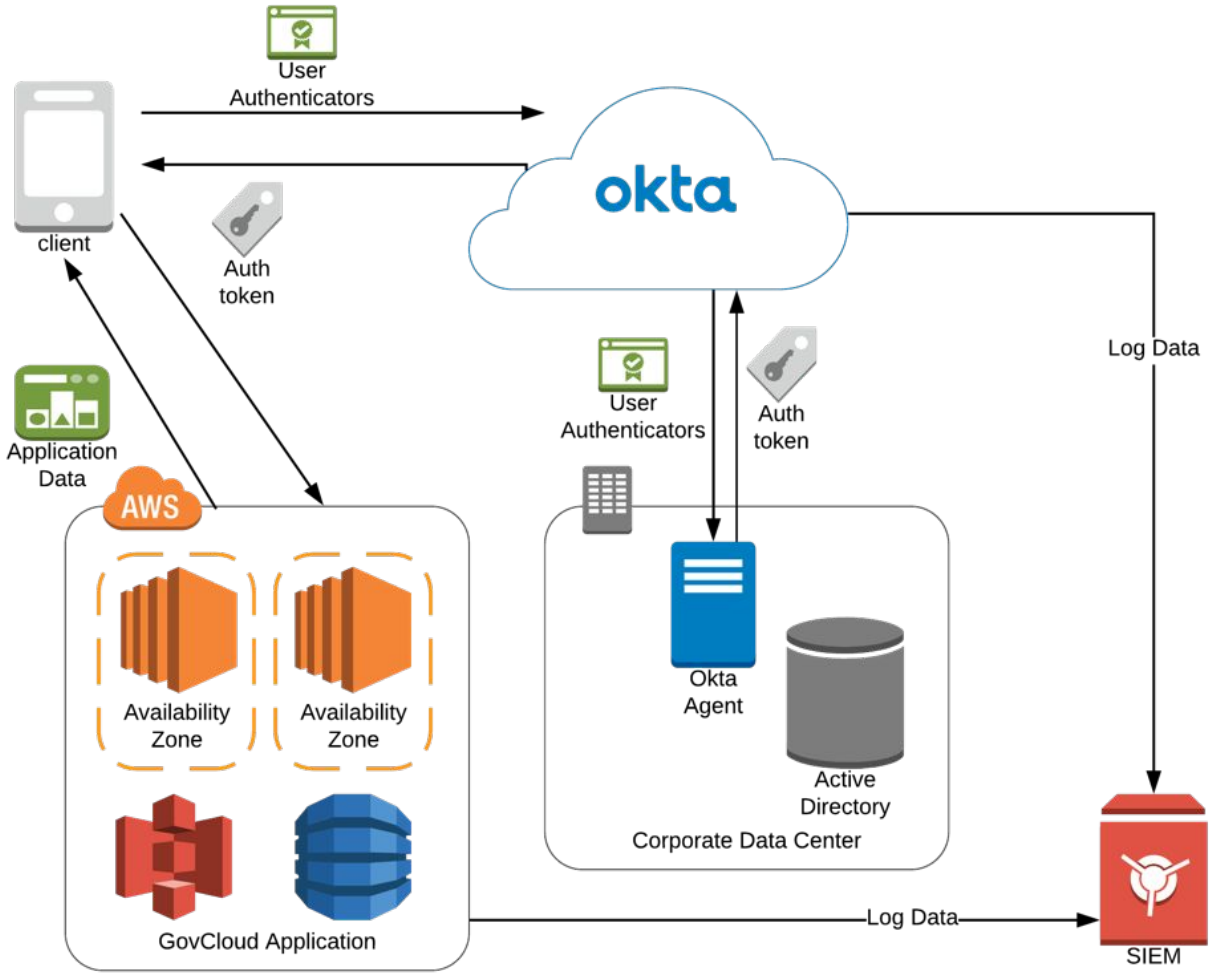

Figure 2: Okta Integrated with Active Directory

Because in both use cases, Okta passes only an authentication token back to the client, Okta is not exposed to sensitive data maintained in the protected application. Okta only handles authenticator information, and steps out of the way. Detailed Log information can be fed in near real-time to your SIEM tool for aggregation and reporting with a feed from your downstream application to identify and protect against internal threats.

IL4 and IL5 Control Mapping

The FedRAMP Moderate Authorization level contains 325 controls that align with Impact Level 2 requirements. In order to support Controlled Unclassified Information (IL4), the DoD has added 38 additional controls to the FedRAMP Moderate baseline, and 48 additional controls to achieve the IL5 baseline. Okta has reviewed these controls and provided responses in the Control Enhancement Workbook, in Appendix A.

Of the additional controls, 18 are the Customer's responsibility, or are shared between Okta and the Customer, and 4 are Not Applicable. The remaining controls can be reduced in risk by implementing Okta as an Interconnected System and ensuring that log data is fed to an appropriate SIEM, managed by the customer. This ability to link and correlate log feeds provides detection and response capabilities to any anomalies in the authentication process.

Customers may also choose to implement Okta with FIPS-validated authentication credentials, further reducing the perceived risk associated with Okta. This includes using Okta Verify, PIV or CAC cards, or authentication tokens such as Symantec VIP. Okta's Adaptive Multi-factor Authentication (Adaptive MFA) product enables the use of costly high-strength authenticators where they are required, while allowing organizations to use lower-cost authenticators where they can be supported. This helps to eliminate "authentication fatigue", providing a better user experience without impacting security.

Protection of PII and PHI

The Okta service was built on the foundation of strong protections for user Personally Identifiable Information. This is evident in our security controls, our ISO 27018 certification, and our commitment to international privacy regulations such as the EU GDPR. With respect to US Government data, Okta provides the protections required for both Personally Identifiable Information (PII), and Protected Health Information (PHI). All data is encrypted both at rest and in transit. Additionally, Okta uses organization-level encryption to protect sensitive data, such as authentication credentials and certificates. This organization-level encryption uses Amazon KMS, a FIPS 140-2 L2 hardware encryption module to protect a key that is unique to each customer tenant. This protects against cross-tenant attacks, and provides a log of all accesses to customer authentication data. More details about Okta's layered security approach can be found in Okta's Security Technical Whitepaper, also available at http://bit.ly/okta-security-technical-whitepaper.

Risk Scoring of PII

Okta performed a Privacy Impact Assessment as part of the FedRAMP authorization process. This risk assessment identified the following PII and components (From SSP Attachment 4 – Okta IDaaS PTA PIA v1.2):

Components	Does this function collect or store PII?	Type of PII	Reason for Collection of PII	Safeguards
Web Application	Yes	Name / Address / Phone Number / Email Address	Registering and using the Okta Services / Populate Services with Customer Data	Username and Password / SSL (TLS) Encryption
Database	Yes	Name / Address / Phone Number / Email Address	Registering and using the Okta Services / Populate Services with Customer Data	Username and Password / SSH VPN / SSL (TLS) Encryption

Table 1: Risk Scoring of PII

At a minimum, Users must provide an Email address to use the Okta service. In many cases users may also provide a First Name and Last Name for personalization, and a cell phone number in order to receive multi-factor authentication tokens. The customer may choose to include other PII about the users as required for the usage of downstream systems. This additional information may impact the Privacy Impact of the application.

In reviewing the Confidentiality Impact Levels from NIST SP800-122, Okta has determined the application poses Moderate risk to PII:

NIST SP 800-122 Factors	Score	Description
Identifiability	Moderate	Okta retains at least First Name, Last Name, Email address. These fields together may uniquely identify an individual. Okta does not maintain biometric, Social Security Numbers, or other highly-identifiable data.
Quantity of PII	Moderate	As an Identity and Access Management service, Okta will contain a substantial amount of data.
Data Field Sensitivity	Moderate	The data fields retained by Okta may be used for phishing or other identity-related attacks, but do not include data such as Social Security Number, which would be used for identity theft.
Obligation to Protect Confidentiality	Low / Moderate	Most use cases would retain a Low Obligation score, however, Okta may be used to protect PHI, which would increase the score to Moderate.
Access to and Location of PII	Moderate	PII stored by Okta is accessible by a limited number of people based on role. Data is accessed by Okta-managed systems over secure communications channels outside of Okta physical locations. Remote access is not permitted from personal devices, nor is export onto removable drives.
Context of Use	Low	Only PII required for the use of the service is collected. It is the customer's responsibility to ensure that users are notified of the collection and use.

Table 2: NIST SP800-122 Risk Factors

Risk Scoring of PHI

There are a minimal number of use cases where Okta may store or process Protected Health Information. The most common case is where Okta is used to authenticate users into a health portal, where the assignment of a downstream application may indicate a medical condition or diagnosis. If Okta is used to authenticate users into an application that contains PHI, but where the existence of the application does not indicate a medical condition, then the Okta service is not subject to HIPAA regulation. The most common use case is when Okta is used as a hospital employee portal, and one of the assigned applications is an Electronic Health Records application such as Epic, or another application that contains PHI.

When Okta is used in a method that puts it in scope for PHI, the risk associated is Moderate, as determined in the PII risk assessment.

Conclusion

Okta has been designed from the ground up to safely store and process an individual's most sensitive data – their identity, while being segmented as much as possible from the business's most sensitive data. With the implementation of log aggregation and monitoring, appropriate multi-factor tokens, and configuration of authenticator strength controls such as session timeout, the additional risks of implementing Okta can be mitigated. In exchange, the ability to deploy a risk-based authentication strategy and enforce strong authenticators where they are required reduces the risk of identity-related breaches while providing users with a better experience.

Appendix A:

Control Enhancement Workbook

SP 800-53r4 FedRAMP+ for FedRAMP

Cont./Enh. ID	Moderate Baseline				Responsibility			
	Lvl 4	Lvl 5	Name	Description	Okta	Customer	N/A	Description
AC-06 (07)	✓	✓	Least Privilege | Review Of User Privileges	The organization: (a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.		✓		As tested in control AC-02, Okta reviews access to privileged data at least quarterly. The number of Okta employees with privileged access to customer data is extremely limited (less than 30), making any role changes visible, and reducing the likelihood that an employee would retain privileged access after a change in role. It is the customer's responsibility to perform reviews of their user privileges.
AC-06 (08)	✓	✓	Least Privilege | Privilege Levels For Code Execution	The information system prevents [Assignment: organization-defined software] from executing at higher privilege levels than users executing the software.			✓	Okta does not offer users the ability to execute code on the Okta platform.
AC-17 (06)	✓	✓	Remote Access | Protection Of Information	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.		✓		Information about remote access is managed as Company Confidential and maintained on corporate resources. All remote access is protected using strong authentication and physically separate multifactor tokens. As such, disclosure or identification of the remote access endpoints does not increase the likelihood of a security incident.
AC-18 (03)	✓	✓	Wireless Access | Disable Wireless Networking	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.			✓	Okta is hosted within Amazon Web Services. Wireless networks are technically and administratively prohibited from AWS facilities.
AC-23	✓	✓	Data Mining Protection	Control: The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.	✓	✓		Okta implements default landing pages and non-specific error messages to protect against customer and user enumeration techniques. Okta offers customers the ability to deploy account lockout restrictions on failed password attempts to protect against password or identifier brute-force attacks. It is the customer's responsibility to configure these protections.
AT-03 (02)	✓	✓	Security Training | Physical Security Controls	The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.		✓		It is the customer's responsibility to educate users on physical security protections. All customer data is maintained in Okta's production environment within AWS. Okta inherits all physical protection controls from AWS.
AT-03 (04)	✓	✓	Security Training | Suspicious Communications And Anomalous System Behavior	The organization provides training to its personnel on [Assignment: organization-defined indicators of malicious code] to recognize suspicious communications and anomalous behavior in organizational information systems.	✓	✓		As tested in control AT-02, Okta provides training to all employees on identification and reporting of anomalous behavior, instead of delivering this training at the role level. ALI activities within the Okta IDaaS product are exposed as part of our Events API, and can be imported into the customer's SIEM for correlation, monitoring, and alerting. As each customer has unique use cases and patterns, it is the customer's responsibility to perform training on suspicious code or anomalous behavior.

Cont./Enh. ID	Moderate Baseline				Responsibility			
	Lvl 4	Lvl 5	Name	Description	Okta	Customer	N/A	Description
AU-04 (01)	✓	✓	Audit Storage Capacity | Transfer To Alternate Storage	The information system off-loads audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited.	✓	✓		As tested in control AU-9, Okta exports data from the system being audited immediately onto a log aggregation server, and into folders with no user write access. Okta provides the ability to export audit records in near-real-time via our Events API. It is the customer's responsibility to configure a target location for this log stream.
AU-06 (04)	✓	✓	Audit Review, Analysis, And Reporting | Central Review And Analysis	The information system provides the capability to centrally review and analyze audit records from multiple components within the system.	✓	✓		As described in control AU-06 (01), Okta imports all log data into a Splunk-based SIEM for aggregation, correlation, reporting, and alerting. This allows for central review an analysis of log data. Okta provides an administrative review dashboard, and a near-real-time stream of log data. It is the customer's responsibility to configure a target location for this log stream.
AU-06 (10)	✓	✓	Audit Review, Analysis, And Reporting | Audit Level Adjustment	The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.		✓		It is the customer's responsibility to review and respond to the log data provided by Okta. Log review cadence and reporting is determined by the customer.
AU-12 (01)	✓	✓	Audit Generation | System-Wide / Time-Correlated Audit Trail	The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time- correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].	✓	✓		As tested in control AU-08, Okta uses the same NIST-approved time sources as the source for all logs This ensures that the time correlation in the audit trail is within tolerance. It is the customer's responsibility to also utilize NIST-approved time sources.
CA-03 (01)		✓	System Interconnections | Unclassified National Security System Connections	The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].		✓		As a VPC-based solution in AWS, all outbound connections from Okta are required to use our network gateway. Additional network routing protections may be put in place by the customer through the use of an AWS DirectConnect connection. The customer is responsible for protection of their endpoints, including defining protections for connection to external networks. Customer data is not stored or processed on Okta endpoints, placing them out of scope.
CM-03 (04)	✓	✓	Configuration Change Control | Security Representative	The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element].		✓		All changes to the Okta application go through the change management process as defined in the Okta-PP_005_CM_Policies_Procedures document. This includes security review and approval for high risk changes. The customer is responsible for maintaining changes and updates to their Okta org, and the accompanying change management.
CM-03 (06)	✓	✓	Configuration Change Control | Cryptography Management	The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management.	✓			All changes to the Okta application go through the change management process as defined in the Okta-PP_005_CM_Policies_Procedures document, including Cryptographic libraries and configurations for the Okta IDaaS service.
CM-04 (01)	✓	✓	Security Impact Analysis | Separate Test Environments	The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	✓			As described and tested in control CM-3, Okta tests all builds in a preview environment before releasing to the IDaaS product. This environment includes security and vulnerability scanning, and participation in Okta's public bug bounty program

Cont./Enh. ID	Moderate Baseline				Responsibility			
	Lvl 4	Lvl 5	Name	Description	Okta	Customer	N/A	Description
CM-05 (06)	✓	✓	Access Restrictions For Change | Limit Library Privileges	The organization limits privileges to change software resident within software libraries.	✓			All changes to the Okta application go through the change management process as defined in the Okta-PP_005_CM_Policies_Procedures document. This includes all libraries that make up the Okta service whether internally supported or obtained from a third party (OSS Software)
IA-02 (09)	✓	✓	Identification And Authentication | Network Access To Non-Privileged Accounts - Replay Resistant	The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.	✓			All authentications into the Okta IDaaS by Okta employees is considered to be privileged access, and is tested under control IA-08 (02). It is the customer's responsibility to manage their non-privileged user authentications. As tested in control IA-08 (02), all user authentications are performed over HTTPS, which includes anti-replay mechanisms. Furthermore, Okta also supports many multi-factor authentication solutions such as standards-based Okta Verify or Okta Verify with Push, RSA SecurID, Symantec VIP, Google Authenticator, and others.
IA-05 (13)	✓	✓	Authenticator Management | Expiration Of Cached Authenticators	The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].	✓			Okta employees are unable to use cached authenticators for access into the production environment. User authenticators are only cached when using Okta in Delegated Authentication mode, and there is a failure with the connection to the Okta Agent behind the customer's firewall. Cached authenticators are valid for up to 5 days. Administrators may disable accounts through the Okta Admin panel or API, invalidating the cache. If users are managed with Okta-mastered authentication, no credential caching is available.
IR-04 (03)	✓	✓	Incident Handling | Continuity Of Operations	The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions.	✓			Okta identifies incidents that may affect the availability of the Okta IDaaS, and maintains a Business Continuity Plan to define actions necessary to ensure continuation of mission-critical functions. The business continuity plan is provided as part of Okta's SSP, in document SSP_Attachment_05-Okta IT Contingency Plan.
IR-04 (04)	✓	✓	Incident Handling | Information Correlation	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	✓	✓		Okta tracks all incidents and suspicious events in a centralized ticket tracking system, allowing for metrics and reporting to be performed against this data. All log and activity information is provided to the customer in a near-real-time format, for incorporation into their SEIM and incident reporting and tracking systems.
IR-04 (06)	✓	✓	Incident Handling | Insider Threats - Specific Capabilities	The organization implements incident handling capability for insider threats.	✓			As tested in control AU-02, Okta logs all required information to detect and respond to insider threats within the production environment
IR-04 (07)	✓	✓	Incident Handling | Insider Threats - Intra-Organization Coordination	The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization].	✓			As tested in control IR-04, Okta's security team handles incident response, responding to both internal and external threat actors.
IR-04 (08)	✓	✓	Incident Handling | Correlation With External Organizations	The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross- organization perspective on incident awareness and more effective incident responses.	✓			Okta participates in information sharing programs with federal and private sector organizations in order to increase our visibility to threat sources.

Cont./Enh. ID	Moderate Baseline				Responsibility			
	Lvl 4	Lvl 5	Name	Description	Okta	Customer	N/A	Description
IR-05 (01)	✓	✓	Incident Monitoring | Automated Tracking / Data Collection / Analysis	The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	✓			As tested in control IR-04 (01), Okta uses automated mechanisms to collect, analyze, and track incident information.
IR-06 (02)	✓	✓	Incident Reporting | Vulnerabilities Related To Incidents	The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles].	✓			As tested in control IR-06, Okta reports system vulnerabilities to US-CERT
MA-04 (03)	✓	✓	Nonlocal Maintenance | Comparable Security / Sanitization	The organization:(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.	✓			All maintenance is performed over a VPN using approved and monitored ports, protocols, and services, as tested in control MA-04
MA-04 (06)	✓	✓	Nonlocal Maintenance | Cryptographic Protection	The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.	✓			Maintenance is performed over the OpenSSL VPN as described in Okta's SSP. This is an AES-based VPN protected using RSA 2048 bit certificates and multifactor authentication.
PE-03 (01)	✓	✓	Physical Access Control | Information System Access	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the information system].	✓			Okta inherits physical protections from Amazon Web Services. All customer data is encrypted at rest and in transit, reducing the risk posed by physical threats.
PL-08 (01)		✓	Information Security Architecture | Defense-In-Depth	The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security safeguards] to [Assignment: organization-defined locations and architectural layers]; and (b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.	✓			Okta has a strong defense-in-depth strategy as defined in Okta's SSP.
PS-04 (01)		✓	Personnel Termination | Post-Employment Requirements	The organization: (a) Notifies terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and (b) Requires terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.	✓			As tested in control PS-04, Okta reminds terminated employees of their confidentiality agreements. Only Okta employees with a business need have access to customer data, and there are fewer than 30 employees with privileged access to customer data. All access is logged. There are no functions by which an employee can bulk export or exfiltrate customer data.
PS-06 (03)		✓	Access Agreements | Post-Employment Requirements	The organization: (a) Notifies individuals of applicable, legally binding post-employment requirements for protection of organizational information; and (b) Requires individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.	✓			As tested in control PS-04, Okta reminds terminated employees of their confidentiality agreements. Only Okta employees with a business need have access to customer data, and there are fewer than 30 employees with privileged access to customer data. All access is logged. There are no functions by which an employee can bulk export or exfiltrate customer data.

Cont./Enh. ID	Moderate Baseline				Responsibility			
	Lvl 4	Lvl 5	Name	Description	Okta	Customer	N/A	Description
SA-04 (07)		✓	Acquisition Process | Niap-Approved Protection Profiles	The organization: (a) Limits the use of commercially provided information assurance (IA) and IA-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and (b) Requires, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated.	✓			Okta uses FIPS-compliant algorithms, but does not use only FIPS-validated encryption modules. This is noted as a risk on our POAM, and Okta is working with AWS, our infrastructure vendor on a solution.
SA-12	✓	✓	Supply Chain Protection	Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	✓			As tested in control PS-04, Okta reminds terminated employees of their confidentiality agreements. Only Okta employees with a business need have access to customer data, and there are fewer than 30 employees with privileged access to customer data. All access is logged. There are no functions by which an employee can bulk export or exfiltrate customer data.
SA-19	✓	✓	Component Authenticity	Control: The organization: a. Develops and implements anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the information system; and b. Reports counterfeit information system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].	✓			Okta maintains alerting systems to detect unauthorized systems starting in the production environment. Okta's use of AWS Security Groups and the configuration management database prevent any unauthorized system from communicating with systems that store or process customer data, reducing the risk of counterfeit systems.
SC-07 (10)	✓	✓	Boundary Protection | Prevent Unauthorized Exfiltration	The organization prevents the unauthorized exfiltration of information across managed interfaces.		✓		Okta is a web-based service, all connections are performed over HTTPS UI or API. It is the customer's responsibility to configure and maintain any connections to external sources.
SC-07 (11)		✓	Boundary Protection | Restrict Incoming Communications Traffic	The information system only allows incoming communications from [Assignment: organization- defined authorized sources] routed to [Assignment: organization-defined authorized destinations].		✓		Okta is a web-based service, all connections are performed over HTTPS UI or API. It is the customer's responsibility to configure and maintain any connections to external sources
SC-08 (02)		✓	Transmission Confidentiality And Integrity | Pre / Post Transmission Handling	The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.	✓			Okta enforces encryption in transit, at rest, and associates all decryption of customer data with a unique session identifier. Okta can work with the customer on any specific protection requirements for transmission through an AWS DirectConnect channel.
SC-23 (01)	✓	✓	Session Authenticity | Invalidate Session Identifiers At Logout	The information system invalidates session identifiers upon user logout or other session termination.		✓		Okta enables customers to configure session timeout and termination actions. It is the customer's responsibility to configure this as required for their environment.
SC-23 (03)	✓	✓	Session Authenticity | Unique Session Identifiers With Randomization	The information system generates a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognizes only session identifiers that are system-generated.	✓			Okta uses at least 128 bits of randomness for the session identifier.
SC-23 (05)		✓	Session Authenticity | Allowed Certificate Authorities	The information system only allows the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.		✓		Okta is designed to allow customer-managed "Bring Your Own Certificate" capabilities, enabling the customer to require authentication assertions to be signed using customer-defined certificate authorities. More detail can be found at: https://developer.okta.com/docs/how-to/byo_saml.html

Cont./Enh. ID	Moderate Baseline				Responsibility			
	Lvl 4	Lvl 5	Name	Description	Okta	Customer	N/A	Description
SI-02 (06)	✓	✓	Flaw Remediation | Removal Of Previous Versions Of Software / Firmware	The organization removes [Assignment: organization-defined software and firmware components] after updated versions have been installed.	✓			As tested in control CM-06, Okta hardens systems using CIS benchmarks, including removing unnecessary software components.
SI-03 (10)		✓	Malicious Code Protection | Malicious Code Analysis	The organization: (a) Employs [Assignment: organization-defined tools and techniques] to analyze the characteristics and behavior of malicious code; and (b) Incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes.	✓			Okta has a strict change management process that includes peer review of all code, static and dynamic code testing, and vulnerability management process including feedback. There are no known methods by which end-users can run arbitrary code on the Okta platform.
SI-04 (12)	✓	✓	Information System Monitoring | Automated Alerts	The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined activities that trigger alerts].	✓	✓		All activities that occur within the customer org are logged and provided in a near-real-time format that can be imported into the customer's SEIM for logging and alerting.
SI-04 (19)	✓	✓	Information System Monitoring | Individuals Posing Greater Risk	The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.	✓			All user activities are logged, regardless of the role of the user.
SI-04 (20)	✓	✓	Information System Monitoring | Privileged User	The organization implements [Assignment: organization-defined additional monitoring] of privileged users.	✓			Privileged user monitoring is described in control AU-2 of Okta's SSP. Access to customer data is limited to only customer support and technical operations team members with a business need. All administrative actions and access to customer data is logged.
SI-04 (22)	✓	✓	Information System Monitoring | Unauthorized Network Services	The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection (one or more): audits; alerts [Assignment: organization-defined personnel or roles]].	✓			The Okta production environment uses AWS Security Groups attached to system configurations to block network traffic to any unapproved network service using a default deny-all rule. This protects customer data from access by an unapproved network service.
SI-10 (03)	✓	✓	Information Input Validation | Predictable Behavior	The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	✓			Okta performs input validation and has removed all sensitive information from error messages as required in FedRAMP Moderate controls SI-10 and SI-11.
DoD SRG 5.1.4		✓		Requirement for usage of Level 5 for unclassified National Security Systems.		✓		It is the customer's responsibility to accurately select an appropriate cloud service offering.
DoD SRG 5.1.5	✓	✓	CNSSI 1253 Privacy Overlay		✓			Okta is identified as a Moderate Risk system for PII and PHI