Okta Security

Technical White Paper

okta

Index

Introduction

Businesses are trusting us with their applications and their data, and that is a great responsibility. Our team is passionate about their work and is excited about the opportunity to play a central role in our customers' security programs.

We continuously invest, innovate and partner with industry leaders to harden our platform and protect our customers. While we have put years of effort into building the security program described in this document, we also understand that this is only the start.

We look forward to continuing on the security journey with you.

– Yassir Abousselham, Okta Chief Security Officer

Identity and Access Management and Information Security are mission-critical functions in modern organizations. Our customers trust Okta to safely connect people to technology. That trust requires a service that is highly available and secure.

As an Okta customer, you benefit from a service designed, built, maintained, and monitored to meet the rigorous Confidentiality, Integrity, and Availability requirements of the most security-sensitive organizations and industries.

This document provides an introduction to Okta's approach to managing security throughout the following chapters:

- **Okta and Service Security**
  Provides an overview of Okta, the Okta Identity Cloud Platform, the Okta's approach to security, and the shared security model.
- **Okta Security Controls**
  Lists some of the major security controls implemented and leveraged by Okta to safeguard your data and to maintain the service's confidentiality, integrity, and availability.
- **Compliance**
  Lists the security certifications achieved by Okta's Identity Cloud Platform and how Okta can help you achieve security certifications and comply with specific industry regulations.
- **Learn More**
  Provides additional resources about Okta security and how you can strengthen your security posture by leveraging the Okta Identity Cloud Platform.

Okta and Service Security

> Okta has demonstrated, not just to us, but to industry analysts and security experts that they take security very seriously, and that it’s a service that we’ll be able to trust.

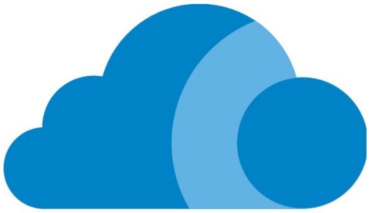
– Den Jones, Senior Manager IT Services

Adobe

https://www.okta.com/customers/adobe-systems/

About Okta

Okta is the market-leading Identity Cloud provider. Our independent platform securely connects the right people to the right technologies at the right times.



The Okta Identity Cloud

The Okta Identity Cloud is the Identity as a Service (IDaaS) platform built and maintained by Okta. As a true cloud-native service—100% born and built in the cloud, Okta provides key benefits:

- It's globally available, 100% multi-tenant, stateless, and redundant.
- It's regularly updated with security enhancements and new features.
- It has zero planned downtime, since we update the platform on-the-fly and don't schedule downtime for maintenance.
- It drastically reduces operational tasks and setup and maintenance costs.
- It's subscription-based and cost-flexible.

The benefits above are rarely found in on-premise software, managed cloud services, or at vendors that ported legacy on-premises software to the cloud.

The Identity Cloud Platform features include both Workforce and Customer Identity products.

Workforce Identity

Workforce Identity products are geared toward IT and security leaders. At a very high level, they simplify the way people connect to enterprise technology, while increasing efficiency and helping keep IT environments secure. These solutions include:

Universal Directory
Customize, organize and manage any set of user attributes from multiple identity sources with this flexible, cloud-based user store.

Single Sign-On
Free your people from the chains of multiple passwords. A single set of credentials gives them access to enterprise apps in the cloud, on-prem and on mobile devices.

Lifecycle Management
Automate user onboarding and offboarding by ensuring seamless communication between directories such as Active Directory and LDAP, and cloud applications such as Workday, SuccessFactors, Office 365 and RingCentral.

Adaptive Multi-Factor Authentication
Secure your apps and VPN with a robust policy framework, a comprehensive set of modern verification factors, and adaptive, risk-based authentication that integrates with all of your apps and infrastructure.

With Workforce Identity, IT enjoys 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.

Employees benefit from a single sign-on home page that simplifies their lives and reduces security risks caused by “password fatigue.” With Okta, they no longer resort to risky practices for memorizing passwords—for example, by choosing obvious or reused passwords, writing passwords down on Post-it notes, or saving them in Excel files on their laptops.

Customer Identity

Customer Identity products allow you to embed Okta as the identity layer of your apps or customize Okta in order to:

Deliver Customizable User Experience

Leverage Okta APIs and widgets to create fully-branded login flows or end-user portals. You can even use our APIs to build a custom admin experience where customers or division managers can manage their users.

Extend Okta to Any Use Case

Solve any complex identity integration, data or automation challenge by taking advantage of Okta's broad APIs. Run scripts to modify user data, automatically integrate apps or integrate with custom workflows.

Leverage the Best-in-Class Customer IAM (CIAM) Solution

Free your developers to focus on the customer experience and leave identity to Okta. Leverage Okta as an "identity API" for all your app dev projects, with Okta handling authentication, authorization and user management.

Customer Identity products provide programmatic access to the Okta Identity Cloud, enabling your developers to build great user experiences and extend Okta in any way you can imagine. By powering customer identity for your digital business, we can solve your most complex enterprise architecture challenges.

Enterprises that adopt the Okta service dramatically improve the security and experience for users interacting with their applications—whether they be employees, contractors or customers, using a cloud service, on-premise application, VPN, firewall, custom app, etc.

Okta’s Approach to Security

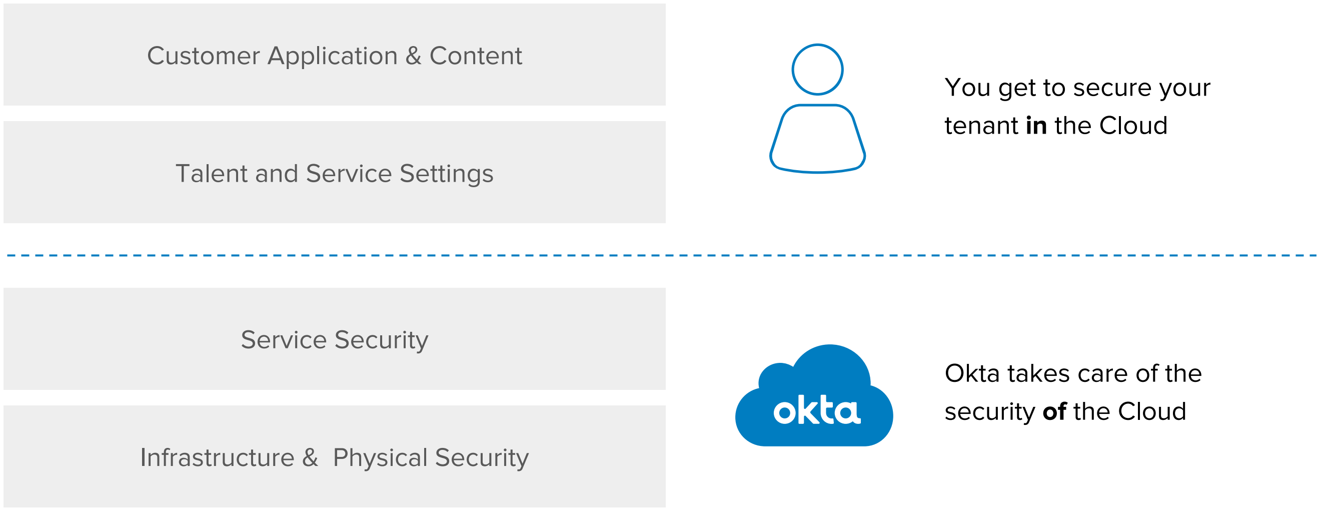
The Okta Identity Cloud is designed, built, maintained, monitored, and regularly updated with security in mind.

To deliver our service with consistent confidentiality, integrity and availability to every customer—regardless of their industry, size, products used, etc., Okta operates under a shared security responsibility model.

Shared Security Responsibility Model

The shared security responsibility model is a framework adopted by many cloud providers—including Amazon AWS, Microsoft, and Salesforce—to identify the distinct security responsibilities of the customer and the cloud provider. In this model:

- Okta is responsible for the security of the cloud.
- You are responsible for the security *in* the cloud based on your company's information security requirements.



Customer Application & Content

Talent and Service Settings

You get to secure your tenant **in** the Cloud

Service Security

Infrastructure & Physical Security

Okta takes care of the security **of** the Cloud

Okta’s shared security responsibility model

Okta's Responsibility: Security of the Cloud

Okta is responsible for the security "of" the Okta Identity Cloud Platform underlying infrastructure. Okta is also responsible for providing features you can subscribe to in order to secure what you host in Okta.

The section below on Okta Security Controls lists some of the major controls we've implemented and leveraged to ensure the security of the cloud.

Your Responsibility: Security in the Cloud

Our customers are responsible for securing what they host "in" Okta. This includes, for example, granting the correct permissions to your users, disabling accounts when employees are terminated, enforcing multi-factor authentication, properly configuring and monitoring the authentication policies required to protect your data, reviewing activity data in the system log to ensure users are following your policies, and monitoring your Okta tenants for attacks, such as password spraying, phishing, etc.

In our To Learn More section, you can find resources that will help you fulfill your responsibilities using Okta.

Okta Security Controls

> Okta plays a role in all three of my initiatives: Cyber security, business productivity, and best of breed. It fits all three, so it’s a perfect match.

– *Gus Shahin, CIO*

flex

https://www.okta.com/customers/flex/

Introduction

As a cloud provider, Okta is responsible for the security “of” the Okta Identity Cloud Platform including our service's underlying infrastructure.

Some of the major security controls we use to secure our cloud service infrastructure include:

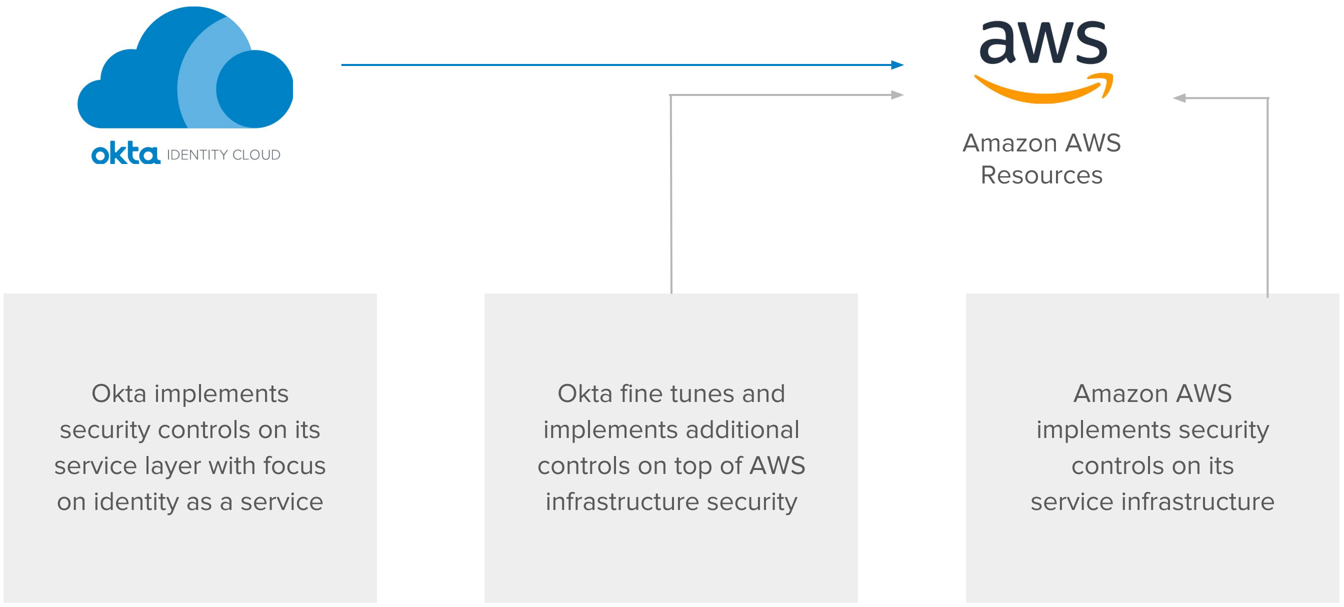
- Infrastructure/Physical Security
- Personnel Security
- Software Development Security
- Service-Level Security
- Security and Penetration Tests

Infrastructure/Physical Security

The Okta technical team has deep experience in developing and operating market-leading cloud services. Okta drew on that experience to select an infrastructure provider that can scale and support Okta’s security and availability requirements.

Amazon AWS is that partner. Amazon runs one of the largest cloud platform services and has significant expertise in building, operating and maintaining the worldwide infrastructure required to power that business. Since early 2006, AWS has provided companies of all sizes with a platform that powers business applications of tremendous scale.

Okta leverages this infrastructure and adds security controls on top of Amazon AWS:



Okta implements security controls on its service layer with focus on identity as a service

Okta fine tunes and implements additional controls on top of AWS infrastructure security

Amazon AWS implements security controls on its service infrastructure

Okta delivers identity as a service and extended security capabilities on top of AWS

- We run our workloads on Amazon AWS.
- We leverage the AWS infrastructure and native security.
- We fine-tune and configure additional security controls in AWS with security in mind.
- In addition, we implement additional security controls on our service layer, focused on Identity-as-a-Service needs. This allows us to deliver a secure and reliable service.

Infrastructure security—operated collectively by Okta and Amazon AWS as described in the next sections—starts with physical security, extends through the computer, network and storage layers of the service, and is complemented by well-defined security and access policies with ongoing audit and certification by third parties.

Physical Security

Okta leverages AWS' physical security for access to its physical servers and implements physical security controls in our own offices. This security strategy aims to preserve the confidentiality, integrity and availability of our services from physical threats.

Data Centers

AWS data centers are housed in nondescript facilities, where physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems and other electronic means. Authorized staff use multi-factor authentication mechanisms to access data centers, and all physical access by employees is logged and audited routinely.

Data center access and information is only provided to employees and contractors who have a legitimate business need for such privileges, and when an employee no longer requires these privileges, their access is immediately revoked—even if they continue to be an Amazon employee. All visitors and contractors are required to present identification before being signed in and continuously escorted by staff.

Okta Offices

Okta also applies physical security controls in its own offices. These measures include, among others:

- Access control and audit trail for employees and visitors
- Video monitoring of all entrance and exit points
- Delimited security perimeters with additional security for places such as storage rooms, power and AC rooms, and loading areas
- 24/7/365 security personnel on premises
- Employee awareness training
- Periodic testing of physical security controls

Compute Security

Okta customizes its AWS Elastic Cloud Compute (EC2) instances and its Virtual Private Cloud (VPC) infrastructure to ensure security is maintained on multiple levels:

- The virtual instance operating system or guest OS
- The firewall and signed API calls

We also maintain secure isolation at the instance level, and leverage AWS' Availability Zones to improve service availability.

Instance Level Security

Multi-factor authentication is required for administrative access to host operating systems for instance management. These administrative hosts' systems are specifically designed, built, configured and hardened to protect the management plane of the cloud. Okta logs and audis all such access. AWS has no access rights to our guest OS environments, which are locked down and completely controlled by Okta administrators.

Okta has also configured the firewall to enable only those ports required for our application—all other ports are disabled. In addition, only our front-end application components are Internet accessible. All other access to the Okta production infrastructure requires a VPN connection.

Fault Separation to Improve Reliability

Okta improves reliability by leveraging Amazon features to place instances within multiple geographic regions, as well as across multiple Availability Zones. Each Availability Zone is designed with fault separation and physically separated across typical metropolitan regions (each on different floodplains and in seismically stable areas). The Amazon Data Center controls page describes several fault separation controls implemented for AWS' Availability Zones.

Data Security (Data-at-Rest Security)

Okta makes multiple investments to ensure our customers' data is secure and available. As detailed in the Service-Level Security section below, customer data, and access to it, is isolated at the customer level within Okta's data layer. Physically, that data is stored using the AWS Elastic Block Storage (EBS) service. To meet Okta's one-hour recovery point objective, database snapshots of EBS volumes are taken regularly and stored in AWS' S3 storage service. Access to S3, even within AWS, requires encryption, providing additional insurance that the data is also transferred securely.

Within AWS S3, we restrict access at both the bucket and object level, and only permit authenticated access by the bucket and/or object creator—Okta. Any request to access data must be authenticated using an HMAC-SHA1 signature of the request using the user's private key. Further, we control authenticated users' permissions with an access control list (ACL) that independently determines read/write permissions at the bucket and object level. We log and audit all access.

Network Security (Data-in-Transit Security)

The AWS network provides protection against traditional network security issues, including:

- **Distributed denial of service (DDoS) attacks**
  AWS network infrastructure leverages proprietary DDoS mitigation techniques developed as a result of running the world's largest online retailer. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.

- **Man in the middle (MITM) attacks**
  Amazon EC2 virtual machines (VMs) automatically generate new SSH host certificates on first boot and log them into the instance's console. Okta leverages secure APIs to access the host certificates before logging into an instance for the first time.

- **IP spoofing**
  Amazon EC2 VMs running the Okta service cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure does not permit an instance to send traffic with a source IP or MAC address other than its own.

- **Port scanning**
  Unauthorized port scans of EC2 customers are a violation of the Amazon EC2 Acceptable Use Policy (AUP). Violations of the AUP are taken seriously, and every reported violation is investigated. When unauthorized port scanning is detected, it is stopped and blocked. Port scans of Amazon EC2 instances are ineffective because, by default, all inbound ports on Amazon EC2 instances are closed.

- **Packet sniffing by other tenants**
  It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. Even two virtual instances that are located on the same physical host cannot listen to each other's traffic. Attacks such as a address resolution protocol (ARP) cache poisoning do not work within Amazon EC2.

Okta complements AWS network security with specific security controls for its service. These security controls are described in detail on the section Service-Level Security.

Availability and Performance Monitoring

We monitor each server in the Okta environment for machine health metrics twice per minute to track availability. These metrics include standard items such as network connectivity, CPU utilization, memory utilization, storage utilization, service status and key file integrity. Failures generate alerts that are pushed to our operations staff through prioritized channels.

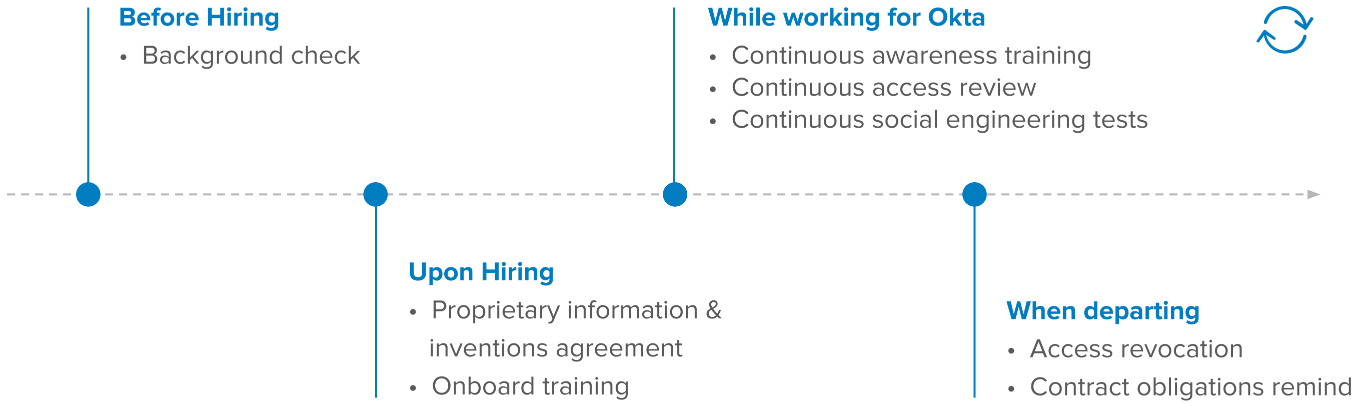
Okta also collects trending data for per-server and per-service performance metrics, such as network latency, database query latency and storage responsiveness. We track this performance for end-to-end scenarios across the application as a whole. Okta assigns health thresholds to each of these metrics, and uses the same alerting mechanism as for our machine-level availability monitoring described above. We use additional instrumentation in our runtime environment to collect metrics internal to the application.

Okta not only invests in internal monitoring, but also publishes real-time and historical data on our public monitoring and alerting system at **trust.okta.com**. To learn more about this, see the Service-Level Security section of this document.

Personnel Security

Security starts with the people Okta employs. We implement security controls for employees and contractors before, during and after their tenure at Okta.

Secure Personnel Practices



Before Hiring
- Background check

Upon Hiring
- Proprietary information & inventions agreement
- Onboard training

While working for Okta
- Continuous awareness training
- Continuous access review
- Continuous social engineering tests

When departing
- Access revocation
- Contract obligations remind

Okta's ongoing personnel security controls

Before Hiring

Before hiring, all employees and contractors **undergo background checks** where permitted by law.   The background check reviews both criminal and financial background indicators and includes a credit check for senior finance positions.

All new hire references, both requested and non-requested, are carefully scrutinized. Employees and contractors are made aware of their responsibilities, plus operational and security policies, as well as repercussions for failure to adhere to said responsibilities and policies.

Our SOC 2 Type II audit report provides third-party attestation regarding the efficacy of Okta's background check procedures and policies. This document is available for review under NDA.

Upon Hiring

Upon hiring, all employees and contractors go through an onboarding process that includes:

- **Signing a Proprietary Information & Inventions Agreement (PIIA).**
  The PIIA states the confidentiality obligations as an Okta employee or contractor.

- **Completing the employment onboard and security awareness training**. This training helps new hires understand their security responsibilities as an Okta employee or contractor, as the case may be.

Our SOC 2 Type II audit report provides third-party attestation regarding the efficacy of Okta's background check procedures and policies. This document is available for review under NDA.

While Working for Okta

Security awareness training is an ongoing educational process throughout employment with Okta that helps employees and contractors understand their responsibilities over data protection.

In addition, Okta's security team performs progressive social engineering tests and awareness campaigns to build security into the culture of the company.

When Departing Okta

- All Okta employees and contractors are reminded of their confidentiality obligations upon leaving.
- Their user accounts, passwords, hardware, and badges are revoked within a strict time frame.

Least Privilege Access Policy

Okta requires that all access to its infrastructure, application, and data be controlled based on business and operational requirements. Following the principles of segregation of duties and least privilege, code changes and maintenance are split between multiple teams. The operations team is responsible for maintaining the production environment, including code deploys, while the engineering team develops features and code in development and test environments only. This ensures multiple employees are required to deploy any code into production. In all cases, administrative access is based on the concept of least privilege; users are limited to the minimum set of privileges required to perform their required job functions.

Software Development Security

The Okta Software Development Lifecycle is designed with precautions to reduce security risks during code development while delivering software functionality.

Okta's application development follows rigorous processes and adheres to much of the Open Web Application Security Project's CLASP (Comprehensive, Lightweight Application Security Process) concepts. Feature requests, bugs, and code enhancements are triaged and processed for threat modeling and risk analysis. Developed code is peer- and security-reviewed prior to final commit and quality assurance ("QA") validation. All developed code must have unit test code developed for test release as well. Okta's QA team performs automated testing to validate all unit, regression, performance, and stress tests, as well as web and mobile application penetration testing.

For optimal results, the software development security controls are implemented before and during the software development.

Development Practices

Okta continuously trains its developers on secure development practices. In addition to the standard security personnel practices, developers have:

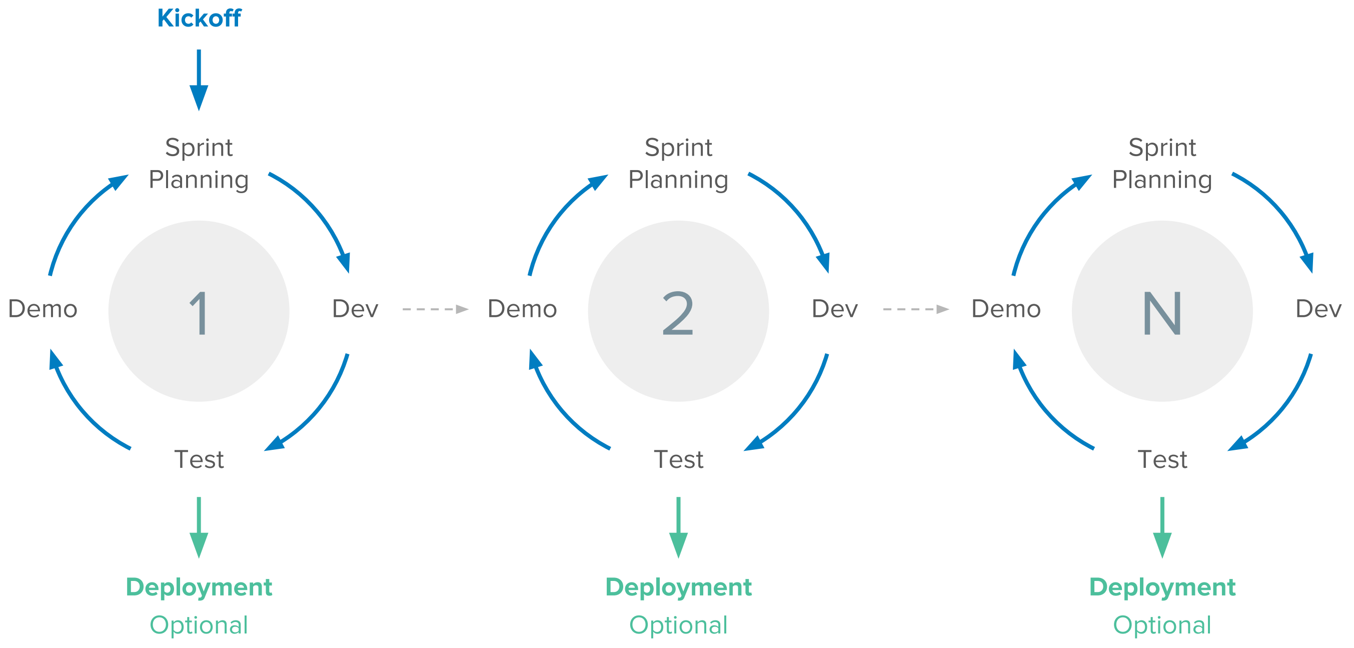
- An onboarding training required for all new engineers. Training sessions enable new Okta developers to learn and practice Application Security.
- A quarterly technical training provided by the security team. Training is also recorded and available for viewing to engineers that are unavailable to attend in person. Training includes learning about security vulnerabilities and prevention of exploiting vulnerabilities in the application.

The continuous training helps to ensure developers will provide adequate protection for the various types of potential attacks are identified, such as:

- Malformed input
- SQL injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Other Open Web Application Security Project Top 10 threats (OWASP's Top 10)

Software Development Lifecycle

The Okta software development lifecycle uses an iterative approach to development by leveraging the Agile/Scrum framework:



Agile/Scrum iterative software development lifecycle

The iterative approach concentrates on producing frequent new versions of the software in incremental, short cycles. The process loops round with each of the stages being carried out many times in small iterations (in the Agile method these are called “Sprints”).

This results in small incremental releases with each release building on previous functionality. Each release is thoroughly tested to ensure software quality is maintained.

In Agile, development testing is performed in the same iteration as programming.

Because testing is done in every iteration—which develops a small piece of the software—users can frequently use those new pieces of software and validate the value.

Okta incorporates security into various stages within the Software Development Lifecycle.

Business Prioritization & Planning

During this phase, Product and Engineering Management plan and set priorities on new service features, components, or functionalities. The business requirements may specify:

- The value of the information involved
- The criticality of the new service and the information it holds
- The legal, regulatory and contractual environment the system must operate within

If any potential security impact is identified, Product Management and Engineering will engage with the Security team to identify the security and compliance requirements that the new feature/component/service will adhere to in order to hold and process information.

The security requirements are carried out through the feature design, development, testing, deployment, and maintenance.

System Design

During the design phase, the solution must present the appropriate security controls to address the security and compliance requirements set during the planning.

Development

During the development phase, a secure development environment is provided for each developer. This includes the physical laptop configuration from IT and the Development coding environment. Depending on the coding environment, languages, databases, tools and other components selected, the appropriate guidelines for secure coding and configuration are adopted.

When a developer is ready to merge the code into an integration branch, they are responsible for getting a code review. Other developers assess the code for compliance, security, performance, and logical correctness. If there is security impact, the Security team is included in the unit test process.

In addition, the Security team perform its independent assessment of upcoming code releases to determine features requiring focused reviews. Based on risk, the reviews range from automated code analysis to deep manual code reviews and penetration tests.

Tests

During the lifecycle of a software application, many different forms of testing will be carried out, including unit, functional and security tests.

The testing process includes over 60,000 tests including:

- Continuous Integration (CI) for building, testing and deploying new code
- Instrumented tests in different environments and browsers
- Unit and Functional tests
- Mandatory Peer Review for all changes
- Quarterly Security Reviews

In addition, we only use protected test data (no customer data).

Release

Each week following the code freeze, a job runs to compile the code of the next release in pre-production environments. Each candidate release promoted is auto-tested using a proxy scanner. The scanner profile tests for specific threats such as OWASP-specific attacks. The job also includes running an antivirus scan for all artifacts.

The results are compiled in a report reviewed by the Security team, who have the authority to block the release until the issue is resolved.

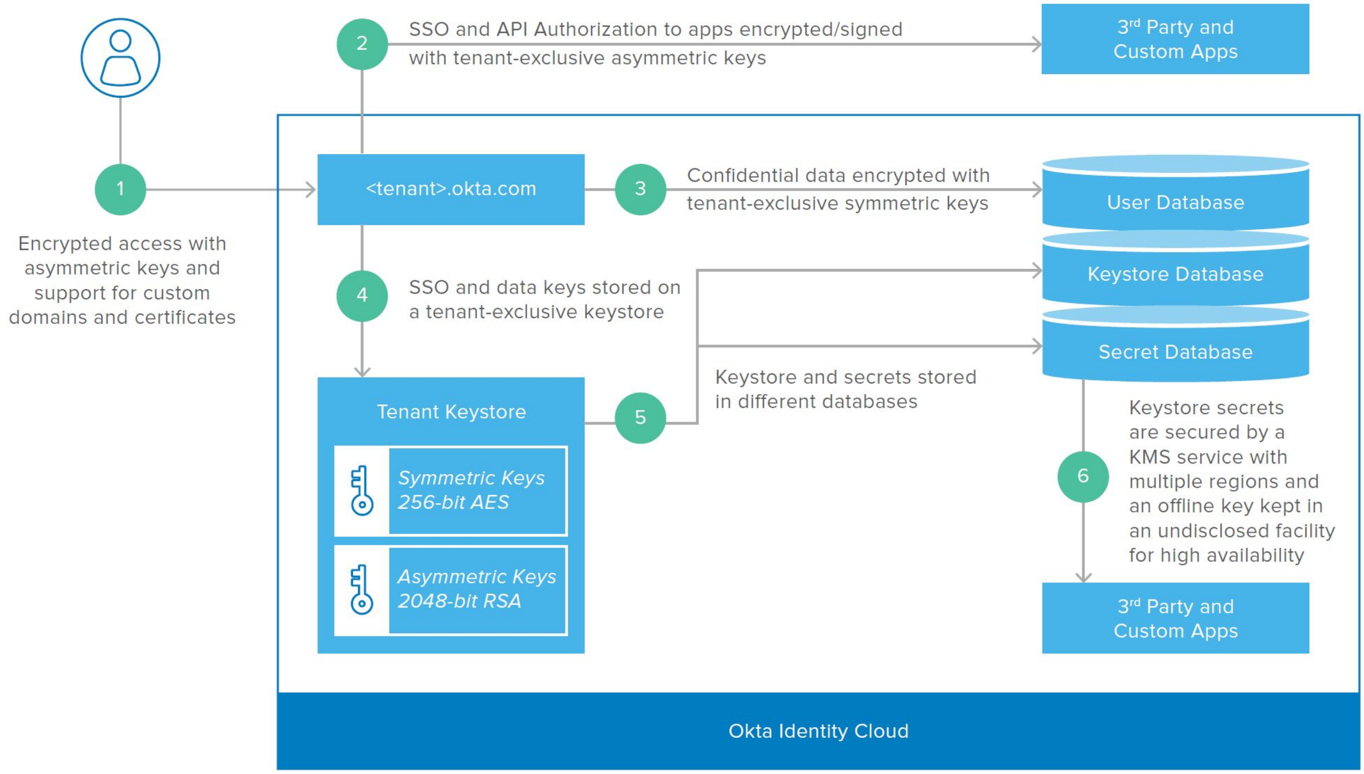
Service-Level Security

This section presents some of the controls implemented by Okta at the service level to secure the platform. The Service-Level security controls are divided in the following areas:

- Okta's Encryption Architecture
- Tenant Data Security
- Tenant Network Segregation and Security
- Tenant Performance Segregation
- Tenant Feature Set Segregation
- Web Application Security
- Service-Level Availability and Performance Monitoring

Okta's Encryption Architecture

Okta uses a multi-layer encryption architecture to protect data at rest and over the wire:



2
SSO and API Authorization to apps encrypted/signed with tenant-exclusive asymmetric keys
3rd Party and Custom Apps
1
Encrypted access with asymmetric keys and support for custom domains and certificates
<tenant>.okta.com
3
Confidential data encrypted with tenant-exclusive symmetric keys
User Database
Keystore Database
Secret Database
4
SSO and data keys stored on a tenant-exclusive keystore
Tenant Keystore
Symmetric Keys 256-bit AES
Asymmetric Keys 2048-bit RSA
5
Keystore and secrets stored in different databases
6
Keystore secrets are secured by a KMS service with multiple regions and an offline key kept in an undisclosed facility for high availability
3rd Party and Custom Apps
Okta Identity Cloud

Okta's encryption architecture and layers

The architecture provides encryption in multiple layers:

1

Users' access to Okta

Okta encrypts the communication between its service and users using HTTPS with strong encryption algorithms and keys (2048-bit RSA) and allows tenants to customize their experience and bring their unique domains and certificates.

Security Benefits

- Confidential data is encrypted in transport
- The connection uses strong encryption algorithms such as TLSv1.2
- Customers can bring their own certificates

2

Access to Single Sign-On Apps and API Authorization

Okta uses asymmetric encryption to sign and encrypt SAML and WS-Fed Single Sign-On assertions and to sign OpenID Connect and OAuth API tokens. The keys used on SSO and API authorization are 2048-bit RSA and exclusive per tenant. In addition, Okta allows you to import your own keys for SAML assertions and OAuth token signatures.

Security Benefits

- Supports signing and encrypting Single Sign-On assertions
- Use of tenant-exclusive 2048-bit RSA keys for encryption and signing
- Tenant exclusive asymmetric keys mitigates SSO risk if a single org is compromised
- Tenants can change the asymmetric keys for the SSO and API Authorization to 3rd party apps

3

Tenant data at rest

Okta encrypts the tenant's confidential data in the database. The encryption is performed using symmetric encryption 256-bit AES with exclusive keys per tenant.

Security Benefits

- Confidential data is encrypted
- Signs and encrypts SAML and WS-Federation assertions using strong keys
- Tenant exclusive symmetric keys ensures data segregation

4

Tenant keys at rest

All the tenant-exclusive keys are stored in a tenant exclusive keystore. The keystore can be accessed only with a tenant-exclusive master key. The unique tenant keystore mitigates damage if a single tenant is compromised.

Security Benefits

- Okta segregates not only the data and assertions, but also the keys used by tenant
- The keystore supports storing multiple tenant-exclusive keys, that can be used for different purposes
- Tenant keys are only cached in memory for a short time and never stored on disk

5

Keystore storage and segregation

The tenant-exclusive keystores and their respective master keys are stored in different databases

Security Benefits

- The storage separation helps protect the keystore confidentiality

6

Master key encryption

The tenant-exclusive master keys are encrypted in three different ways to achieve the highest level of availability and business continuity.

First, the tenant-exclusive master key is encrypted using a KMS—a Federal Information Processing Standards (FIPS) 140-2 Level 2 Hardware Encryption Module—service. The KMS encrypts and decrypts the tenant-exclusive master keys using strong keys (4096-bit RSA) that never leave the KMS.

Second, the tenant-exclusive master key is encrypted using a second KMS service for high availability purposes. The access to both KMSs are tightly controlled to a minimal set of services and users, and all access is tracked in an immutable log that cannot be modified or deleted.

Finally, the tenant-exclusive master key is encrypted with a public key to provide the safest recovery mechanism for business continuity. The backup key, used only if all KMS services fail, is stored in a secured location and requires two Okta employees to access. This ensures that no single person can decrypt customer data without leaving a detailed audit trail.

Security Benefits

- No single person can decrypt customer data without a detailed audit trail and security response
- Master keys are easily rotated
- Immutable logs of key use are maintained
- High availability is preserved
- Business continuity is preserved

In addition to the security layers, Okta implements additional measures:

- The service allows you to change the asymmetric keys for the user access to Okta and also for the SSO and API Authorization to 3rd party apps
- Tenant keys are only cached in memory for a short time and never stored on disk

Tenant Data Security

In addition to Okta's Encryption Architecture, Okta implements the following security controls to protect customer's data.

Tenant Data Segregation

Okta leverages encryption to segregate customer data. The logical data segregation is applied to the data storage using symmetric encryption, over the wire using asymmetric encryption, and to the key storage using segregated databases and KMS.

Confidential Data Encryption

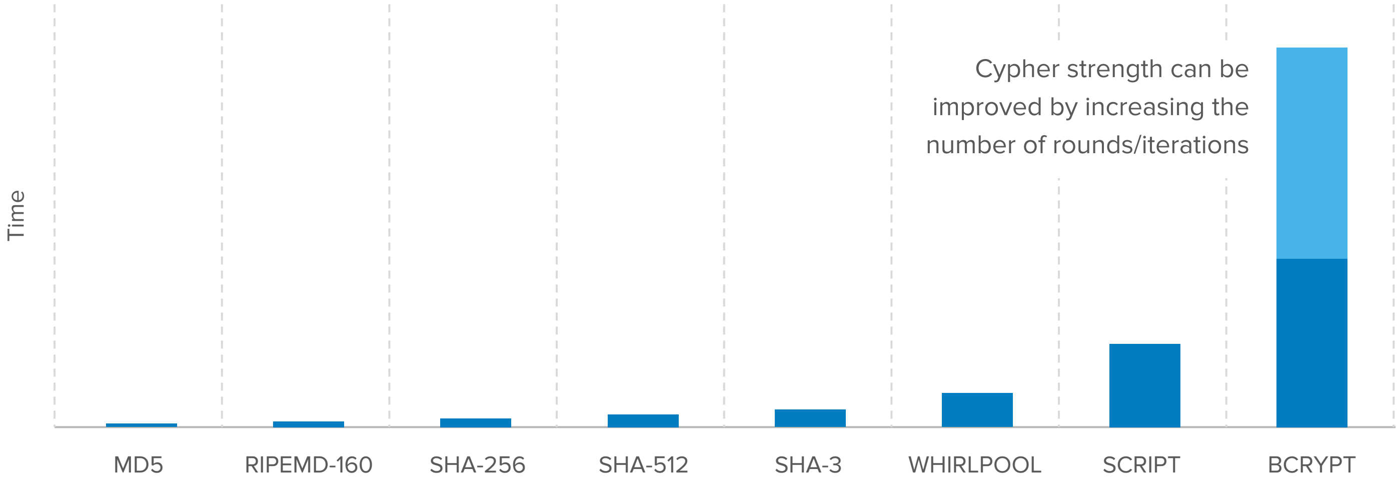
In some cases, customers wish to store confidential Personally Identifiable Information within their Universal Directory to provision into downstream applications. Okta admins can choose the specific attributes they wish to encrypt via Universal Directory. This information is encrypted using symmetric keys exclusive to their tenant and is not searchable within the Okta admin console. In addition to the data encryption, Okta uses a security framework that isolates the tenant data during its access.

Password Encryption

Okta also applies special controls for securing user passwords. Users can authenticate to Okta with a password in one of two ways:

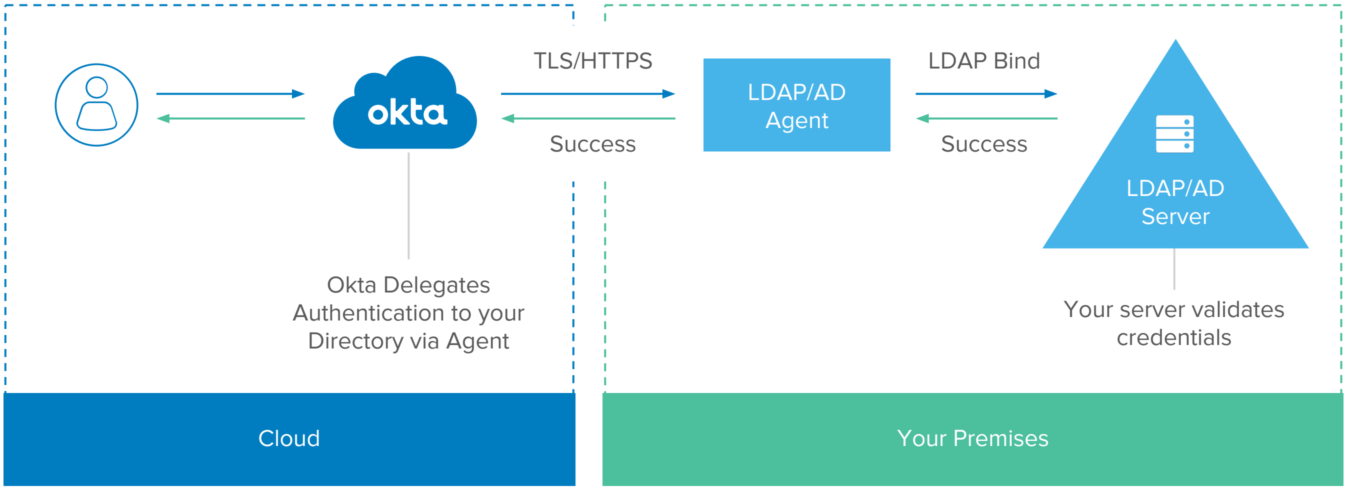
- Local Okta password
- Delegated authentication

When users authenticate to Okta with a local Okta password, credentials are stored in the Okta cloud. Okta uses salted bcrypt with a high number of rounds to protect the Okta passwords. Unlike other hashing algorithms designed for speed and thus susceptible to rainbow table or brute-force attacks, bcrypt is very slow and an adaptive function, meaning its hash function can be made more expensive and thus slower as computing power increases. In short, bcrypt can keep up with Moore's Law.



Cipher strength on popular hashing algorithms

When users authenticate to Okta with AD or LDAP server credentials, credentials are maintained within the customer's directory. This model of authentication is called delegated authentication. Users enter AD or LDAP server credentials at the Okta sign-in page, and Okta delegates the authentication to AD or LDAP for validation. When delegated authentication is configured, the password policy from AD or LDAP is enforced instead of the Okta password policy.


okta
TLS/HTTPS
Success
LDAP/AD Agent
LDAP Bind
Success
LDAP/AD Server
Okta Delegates Authentication to your Directory via Agent
Your server validates credentials
Cloud
Your Premises

How Okta can delegate authentication to external directories

Okta strongly recommends configuring and enforcing Multi-Factor Authentication (MFA) to further strengthen the login to Okta. Okta supports different MFA factors and adaptive policies. The section To Learn More provides more information about the MFA capabilities provided by Okta.

Tenant Network Segregation and Security

Okta implements the following controls to protect customer's data traffic:

Network Separation

Customers have exclusive sub-domains for access and with administrative tasks:

- Access sub-domain

```
https://{customername}.okta.com
```

- System Administration sub-domain

```
https://{customername}-admin.okta.com
```

The use of independent sub-domains:

- Enables customization of the Okta login and error pages, which provides a consistent look and feel, and it helps mitigate phishing attacks
- Enables separation of network rules (whitelisting/blacklisting), CORS/Redirect rules, SSO assertion issuers, and rate-limiting
- Enables cookie uniqueness so each tenant sub-domain is issued a unique cookie that restricts access to that sub-domain

Custom Domains and Certificates

In addition, depending on your subscription, Okta allows you to bring your own url domains, e-mail senders, and HTTPS certificates. You can use these features for a complete domain name isolation and to use certificates issued by a Certificate Authority of your choice.

Session Context Validation

Okta developed logic that validates requests based on the user's "context." The context is a function of two unique identifiers and a session cookie. This prevents cookie hijacking and replay.

Tenant Performance Segregation

Okta implements rate limits to help insulate tenant performance issues. Each tenant has a rate limit for API calls that comfortably satisfies the usage for most of our customers. The API limit is reset every minute. Anytime a tenant reaches an API limit, Okta returns the HTTP error 429—Too Many Requests until the rate limit is reset (up to a minute). Okta keeps different API limits per API endpoints. So, even if you reach an API limit in one API, you don't compromise the other functions within the service. In addition to that, you can request Okta Support to temporarily raise your API limits in specific situations, such as cutover to production or in seasonal events.

The section To Learn More provides links to the rate limiting documentation and procedures.

Tenant Feature Set Segregation

Okta supports multiple customers with different business needs and priorities. Each customer adopts new features at a different pace based on their security requirements and the business value a feature will deliver. Okta supports feature segregation so each customer can determine the best time to enable a feature in their tenant.

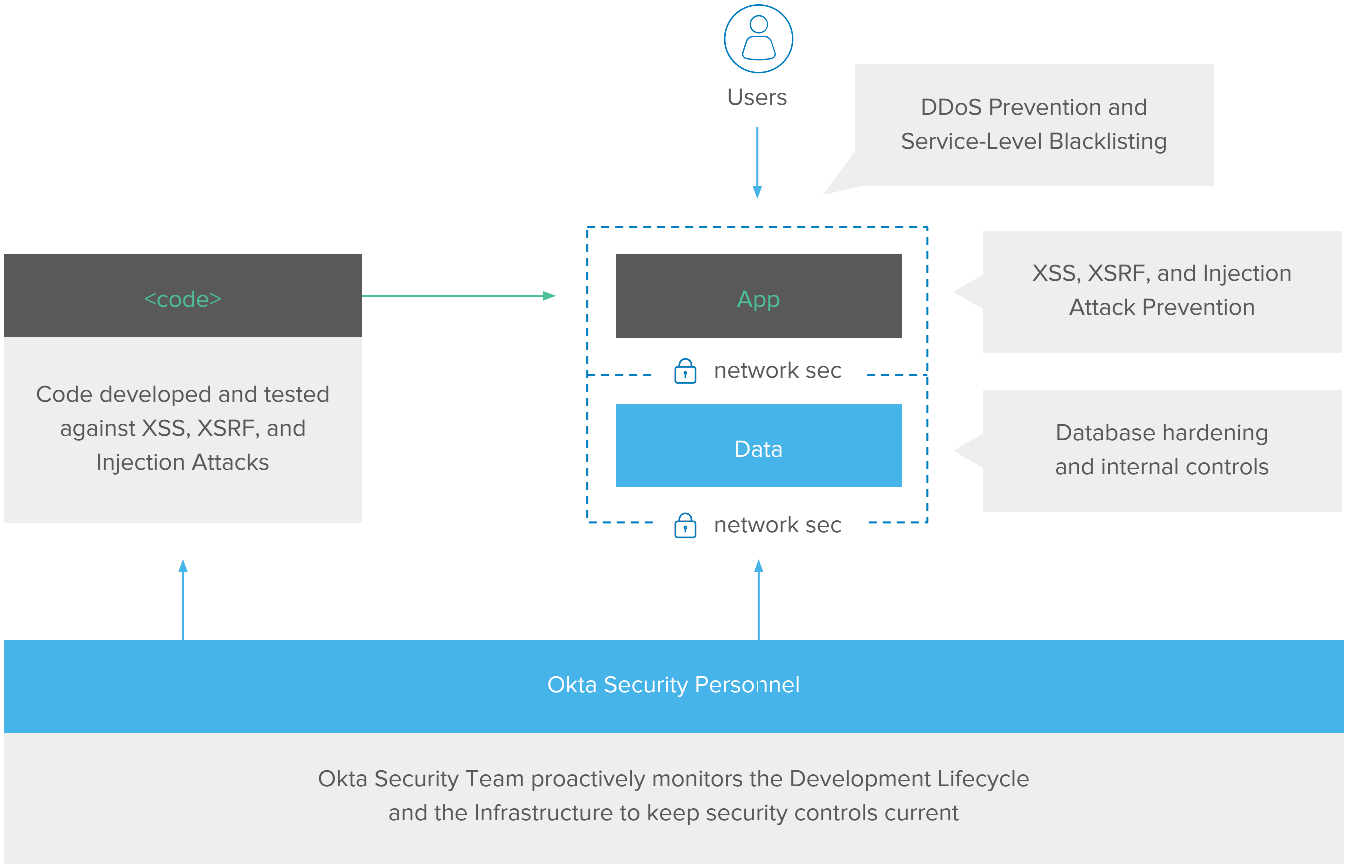
Okta currently have three kinds of feature flags.

- The **Beta** flag is available only on Okta Preview ([orgname].oktapreview.com). Features with beta flag are usually enabled for customers subscribed to the Okta Beta program.
- The **Early Access (EA)** flag is available on both Okta Preview and Production environments. Features with the EA flag can be enabled either via support or by using the Feature Manager.
- The **General Availability (GA)** flag is available and turned on by default on both Okta Preview and Production environments.

If you have further questions specific to your tenant and requests for enabling specific flags, contact your support representative.

Web Application Security Controls

Okta implements web application security controls in the entire software lifecycle, runtime operations, and monitoring:


Users
DDoS Prevention and Service-Level Blacklisting
<code>
Code developed and tested against XSS, XSRF, and Injection Attacks
App
network sec
Data
network sec
XSS, XSRF, and Injection Attack Prevention
Database hardening and internal controls
Okta Security Personnel
Okta Security Team proactively monitors the Development Lifecycle and the Infrastructure to keep security controls current

Okta's shared security responsibility model

Code

To learn more about how Okta implements web application security during the software design, development, test, and deploy, visit the Software Development Security section.

Access to Okta

Okta implements IP blacklisting and other security controls to mitigate the risk of Distributed Denial of Service (DDoS) attacks at the global router level. In addition to the controls implemented by Okta at the global level, the service allows you to implement your own IP blacklisting rules.

Application and Database Controls During Runtime

Okta implements controls at the application level during runtime to mitigate the risk of application attacks such as cross-site scripting (XSS), cross-site request forgery (XSRF), and injection attacks. Controls include, for example, cross-origin resource sharing (CORS) validation, trusted origin validation, and session context validation.

To mitigate XSS risk, Okta validates that all input from the user conforms to the appropriate data type format (e.g., dates are in a date format), do not contain scriptable HTML tags, and are stripped of any potential tags before rendering. In addition, all HTML output is encoded to ensure that the browser does not process any scripts.

To mitigate XSRF risk, Okta validates that all POSTed requests come from a page generated by Okta, based on a standard technique widely used as a best practice in the industry. In this approach, the server generates a secure token. The secure token is embedded into the page, such that it is included

as a parameter to POSTs from that page. The token is specific to a user session, and it is hashed with a secret known only to the server. A server-side interceptor checks incoming POSTs for the expected request parameter containing this token and ensures that the token is both present and matches the session to which it is being posted.

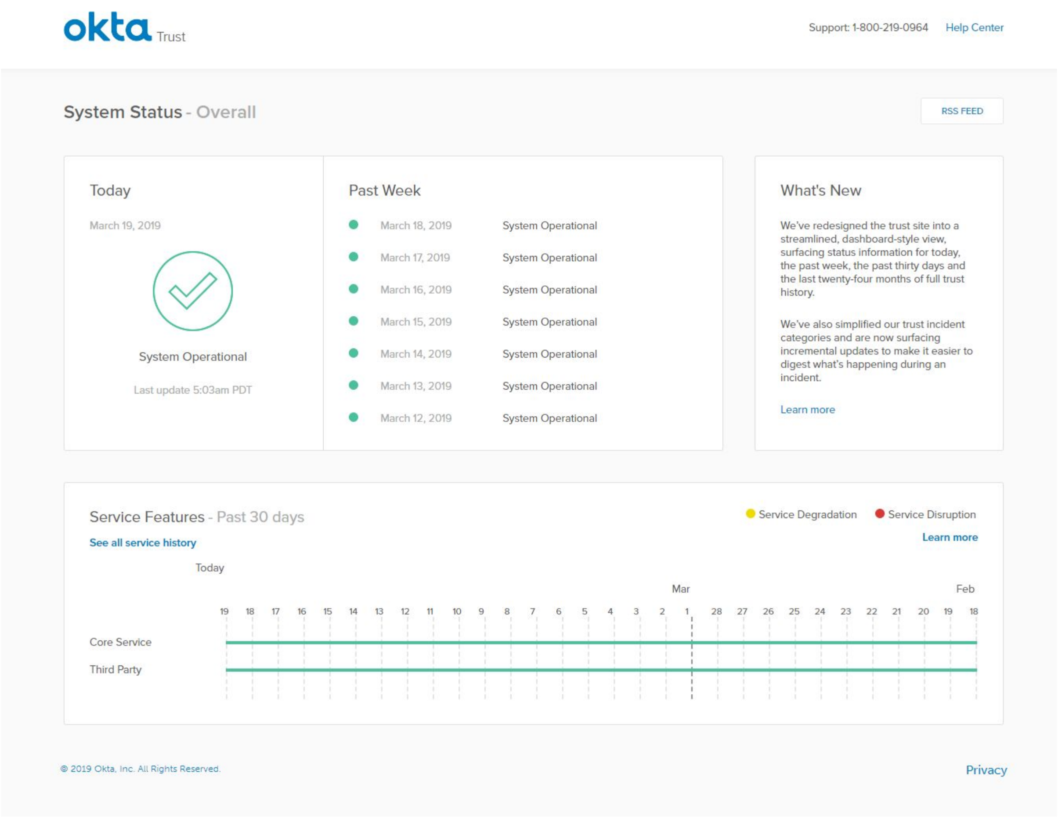
Okta mitigates the risk of injection attacks by limiting and validating data inputs, and by implementing frameworks for database persistence with bind variables on SQL queries. A bind variable is a placeholder in an SQL command for a value that is supplied at runtime by the application. Using parameters or parameter markers to hold values is more secure than concatenating the values into a string that is then executed as part of a query.

Okta Security Personnel

The Okta Security Personnel proactively monitors the development lifecycle and the infrastructure to keep security controls current. The security personnel work on each stage is described on the Software Development Security and the Security and Penetration Tests sections.

Service-Level Availability and Performance Monitoring

Okta is committed to trust and transparency. In addition to the monitoring at the infrastructure level, Okta implements a transparent monitoring, communication, and an incident response system via the **Okta Trust Site** (trust.okta.com).



okta Trust

Support: 1-800-219-0964 Help Center

System Status - Overall

RSS FEED

Today

March 19, 2019

System Operational

Last update 5:03am PDT

Past Week

●	March 18, 2019	System Operational
●	March 17, 2019	System Operational
●	March 16, 2019	System Operational
●	March 15, 2019	System Operational
●	March 14, 2019	System Operational
●	March 13, 2019	System Operational
●	March 12, 2019	System Operational

What's New

We've redesigned the trust site into a streamlined, dashboard-style view, surfacing status information for today, the past week, the past thirty days and the last twenty-four months of full trust history.

We've also simplified our trust incident categories and are now surfacing incremental updates to make it easier to digest what's happening during an incident.

Learn more

Service Features - Past 30 days

See all service history

● Service Degradation ● Service Disruption

Learn more

© 2019 Okta, Inc. All Rights Reserved.

Privacy

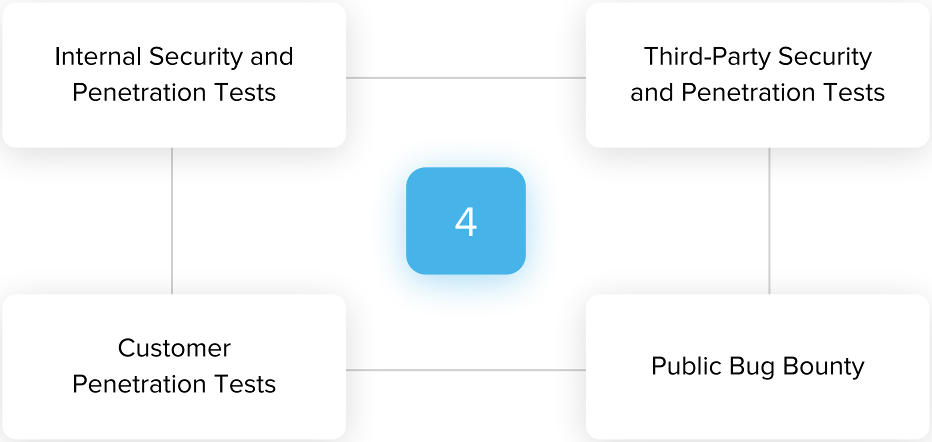
Okta Trust Site

Okta Trust Site

The Okta Trust Site provides you real-time information about Okta and third-party service availability and flexibility in receiving updates during an incident. Status information is provided in an easy-to-read dashboard-style design, providing consolidated incident categories for clarity, updated with detailed incident information as it happens, and fast access to root cause analysis reports.

Security and Penetration Tests

As part of its security strategy, Okta supports four different security and penetration testing programs:


Internal Security and Penetration Tests
Third-Party Security and Penetration Tests
4
Customer Penetration Tests
Public Bug Bounty

Okta's security and penetration test programs

Okta's Security and Penetration Test programs

- **Internal security and penetration tests**
  As a continuous effort, Okta's internal security "Red Team" regularly test the Okta service security against the latest security threats.
- **Third-party security and penetration tests**
  Okta hires third-party security research firms to perform gray-box penetration tests on the Okta service at least annually. The assessments are organized so that the research firm has complete access to the Okta source code and dedicated Okta instances for testing analysis and vulnerability exploit creation.
- **Public bug bounty program**
  Okta uses leading public platforms for managing its ongoing public bug bounty program. The public bug bounty program supports any person who wants to perform an external penetration test on Okta. Security vulnerabilities are triaged and validated, and the researchers are rewarded with cash proportional to the severity of their findings. For more information about the public program, visit: https://www.okta.com/bugbounty.
- **Customer penetration tests**
  Okta will work with customers so they can perform their own penetration testing on an Okta preview instance.

All these programs are complementary to each other and ensure that Okta is in a continuous state of security testing and posture improvement.

Compliance

> Okta helps us be HIPAA compliant…largely because we don't have to go in and manage and maintain the identity of our customers.

– *Rish Tandon, Chief Technology Officer*

heal

https://www.okta.com/customers/heal/

Introduction

We understand that identity is mission critical, and our customers depend on Okta to manage and protect access to applications and data. That trust requires us to:

- Ensure our service is certified to the most recognized certifications and regulations and
- Help our customers meet security certifications and regulations from their industries

Okta Service Certifications

Okta's compliance program is built upon industry-standard certifications and authorizations.

As the compliance and regulatory environment is always changing, a current list can be found at https://www.okta.com/security:

ISO 27001:2013

Okta has achieved ISO 27001:2013 Certification, attesting to the commitment of Okta's leadership to a secure service for our customers.
Okta's ISO 27001:2013 Certification is available here.

ISO 27018:2014

Okta has achieved ISO 27018:2014 Certification, attesting to the commitment of Okta's leadership to secure personally identifiable information (PII) in the cloud.
To learn more about ISO 27018:2014, click here.

SOC 2 Type II Certification

As part of its commitment to security, Okta has used the AICPA SOC 2 Type II process—formerly known as SAS 70 Type II—to successfully certify the operational and security processes of its service and the company. Current customers can request results through their Customer Success Manager or Account Executive
Prospects can request the results here.

Cloud Security Alliance Security, Trust, & Assurance Registry (CSA STAR)

We have achieved the Cloud Security Alliance (CSA) Security, Trust, & Assurance Registry (STAR) Level 2 Attestation.

To learn more about CSA STAR, click here.

To view Okta's CSA Attestation, click here.

FedRAMP—Authority to Operate (ATO)

Okta has an official authorized status with the Federal Risk and Authorization Management Program (FedRAMP) Moderate authority to operate (ATO).

To learn more about FedRAMP, click here.

To view Okta's FedRAMP certification, click here.

How Okta Helps You Meet Compliance Requirements

In addition to its own certifications above, the Okta Identity Cloud helps customers adhere to the following regulations and certifications:

HIPAA

To better serve the highly-regulated and security-conscious healthcare industry, we've established a HIPAA Compliant Service instance.

To learn more about how HIPAA and our compliance instance, click here.

PCI-DSS 3.2

Since Okta MFA qualifies as a PCI-compliant multi-factor according to the current PCI-DSS requirements, many customers use Okta as a supporting system for their PCI compliance. Okta has a PCI Attestation of Compliance.

For more information, click here.

Sarbanes Oxley (SOX)

Okta is an excellent tool for ensuring SOX controls are in place and generating evidence for auditors. By using Okta to enforce password complexity requirements and providing SSO into in-scope financial applications, your IT team has a unified control for authentication and application provisioning and deprovisioning.

GDPR

Identity and Access Management using a product such as Okta can provide a strong foundation for GDPR compliance and can help reduce your risk. You can learn more and download Okta’s GDPR-compliant DPA at https://www.okta.com/gdpr.

NYDFS

Okta’s IAM solutions can help you comply with the access and requirements specified in NYFDS while also providing a strong security foundation.

Resources

I’m really impressed with Okta’s responsiveness. Within an hour or two, we always get a response to acknowledge that a request has gone through. And the technicians we’ve worked with on some of the trickier problems, they own the problem, and they’ll work right through to completion. That’s an important thing for us as well. And there’s follow-up.

– *Grant Holton Picard, Enterprise Architect*

OXFAM

https://www.okta.com/customers/oxfam/

Security Documentation

- Be certified to the most recognized certifications and regulations
  https://help.okta.com/en/prod/Content/Topics/Security/Security_at_Okta.htm

Okta Solution Briefs

- Protect Against Data Breaches
  https://www.okta.com/resources/whitepaper/protect-against-data-breaches
- Creating a Secure, Seamless Customer Experience
  https://www.okta.com/resources/whitepaper/secure-customer-experience/
- Secure Access to AWS for Suppliers and Partners
  https://www.okta.com/resources/whitepaper/solution-brief-secure-access-to-aws-for-suppliers-and-partners/
- Reduce IT Friction—Automate the Identity Lifecycle to Streamline IT Operations
  https://www.okta.com/resources/whitepaper/okta-solution-briefs-reduce-it-friction/
- Modernize Enterprise IT
  https://www.okta.com/resources/whitepaper/modernize-enterprise-it/
- Building a 100% Cloud and Mobile IT Infrastructure
  https://www.okta.com/resources/whitepaper/solution-brief-build-100-cloud-mobile-infrastructure/
- Increasing Agility for Mergers and Acquisitions
  https://www.okta.com/resources/whitepaper/increasing-ma-agility/

Okta Security and Availability

- Zero Trust with Okta: A Modern Approach to Secure Access from Anywhere
  https://www.okta.com/resources/whitepaper/zero-trust-with-okta-modern-approach-to-secure-access
- Not All Cloud Services Are Built Alike—Okta's High Availability Architecture
  https://www.okta.com/resources/whitepaper/not-all-cloud-services-are-built-alike
- Scaling Okta to 10 Billion Users
  https://www.okta.com/resources/whitepaper/scaling-okta-to-10-billion-users
- Okta Privacy Policy
  https://customer.okta.com/privacy

Universal Directory and Lifecycle Management

- Okta Lifecycle Management Vision and Overview
  https://www.okta.com/resources/whitepaper/okta-lifecycle-management-vision-and-overview/

- Okta Directory Integration—An Architecture Overview
  https://www.okta.com/resources/whitepaper/ad-architecture/

- HR-Driven IT Provisioning
  https://www.okta.com/resources/whitepaper/olm-technical-whitepaper-hr-driven-it-provisioning

- How Identity Orchestration Transforms Service Delivery and Automation
  https://www.okta.com/resources/whitepaper/how-identity-orchestration-transforms-service-delivery-and-automation/

Multi-Factor Authentication

- Moving Beyond User Name & Password—Okta Adaptive MFA White Paper
  https://www.okta.com/resources/whitepaper/adaptive-mfa/

- Security Built to Work Outside the Perimeter
  https://www.okta.com/resources/whitepaper/security-built-to-work-outside-the-perimeter

- 7 Things to Consider Before Making the Switch to MFA
  https://www.okta.com/resources/whitepaper/7-things-to-consider-mfa

- Multi-Factor Authentication Deployment Guide
  https://www.okta.com/resources/whitepaper/multi-factor-authentication-deployment-guide

- Securing VPN with Multi-Factor Authentication
  https://www.okta.com/resources/whitepaper/securing-vpn-with-multi-factor-authentication

SSO and Integrations

- How Okta Integrates Applications—An Architectural Overview
  https://www.okta.com/resources/whitepaper/how-okta-integrates-applications-architectural-overview

- User Identity and Access Management: A Bridge to Government IT Modernization
  https://www.okta.com/resources/whitepaper/user-identity-and-access-management-government-it-modernization/

- 6 Reasons Microsoft Customers Choose Okta for Identity
  https://www.okta.com/resources/whitepaper/six-reasons-microsoft-customers-choose-okta-for-identity

- Automate Security Incident Response with Okta
  https://www.okta.com/resources/whitepaper/okta-security-infrastructure-to-automate-incident-response

- Four Myths About Credential Phishing You Can't Ignore
  https://www.okta.com/resources/whitepaper/four-myths-about-credential-phishing-you-cant-ignore

Compliance and Regulation

- What Finance Institutions Need to Know About the NYDFS Cybersecurity Regulations
  https://www.okta.com/resources/whitepaper/need-to-know-nydfs

- Meeting the Latest NIST Guidelines with Okta
  https://www.okta.com/resources/whitepaper/meeting-the-latest-nist-guidelines-with-okta

- How to Meet NYDFS Mandates with Identity & Access Management
  https://www.okta.com/resources/whitepaper/how-to-meet-nydfs-mandates-with-iam

- Preparing Your Organization for the GDPR: What You Need to Know
  https://www.okta.com/resources/whitepaper/preparing-for-gdpr

Books and Publications

- API Security: A guide to building and securing APIs from the developer team at Okta
  https://developer.okta.com/books/api-security/

- OAuth 2.0 Simplified: A guide to building OAuth 2.0 Servers
  https://www.amazon.com/dp/1387130102/ref=cm_sw_r_cp_ep_dp_WOSgBbEG187V4
  https://www.oauth.com

Third-Party Resources

- Introduction to AWS Security
  https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf

Conclusion

Okta considers Identity a critical component of any organization's technology stack. As such, it requires the highest levels of confidentiality, integrity, and availability. Our team is constantly working to stay steps ahead of threat actors, securing the Okta service for the benefit of every one of our customers.

We believe this document, along with the Shared Security Responsibility Model provides a good view into the security controls offered by Okta, while raising awareness of your responsibilities to protect your people and information.

It's my greatest privilege to lead security for a company that is at the center of the security strategy of its customers. The responsibility of protecting Okta and our customers is constantly at the forefront of our thoughts at Okta.

Threats are changing, as are the tools used to mitigate attacks. To be effective, today's organizations need a multi-layered approach to designing security and should partner with technology vendors that are continuously improving their security capabilities. We are proud to be one of those vendors and seek to put our expertise at the service of our customers so that they can focus on advancing their business.

Yassir Abousselham

Chief Security Officer, Okta