OKTA SECURITY

Technical White Paper

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

info@okta.com
1-888-722-7871

TABLE OF CONTENTS

INTRODUCTION

The shift to the cloud is changing how companies think about their IT infrastructure and what they must do to manage it. In the 1980s and 1990s, business applications and data were largely confined within and protected by a local area network (LAN). Securing enterprise information technology at the time consisted of building a castle (the company) with high walls, a deep moat (the firewall), and two points of access to applications: through the front gate (physically walking in the door) or through a secret tunnel such as a virtual private network (VPN). That was it.

The 2000s introduced a significant change. IT transformed from applications and data residing within the castle or firewall to services subscribed to and accessed from the cloud. As a result, the LAN of the 1990s is giving way to the cloud services network of today. Unlike a LAN, a cloud services network powers a federated collection of on-demand services, which are provided by a variety of vendors for a set of highly distributed users.

The on-demand applications and services that comprise a cloud services network enable companies to rapidly deploy powerful capabilities to a broad set of users at very low costs. However, they also introduce challenges associated with securing and controlling users and access, simplifying adoption and scaling of these applications, and providing insight into utilization to ensure the business is optimizing its cloud investments.

Okta is the market-leading on-demand identity and access management service that enables enterprises to accelerate the secure adoption of their web-based applications, both in the cloud and behind the firewall. Okta delivers a complete solution that addresses the needs of IT, end users, and business leaders; no customization is required. The service offers:

- *Secure, single sign-on for end users, giving them one place to access the cloud applications they need, whenever and wherever they need them*
- *Comprehensive user management integrated with Active Directory (AD), including user provisioning and de-provisioning, enabling IT to accelerate the move to the cloud*
- *Cross-application analytics spanning usage, utilization, and cost that provide IT with the insight needed to optimize its cloud investments and address its compliance needs*

By adopting the Okta service, enterprises dramatically improve the security and ease of managing their Software as a Service (SaaS) 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.

End users benefit by using their Okta single sign-on homepage to simplify their life and reduce the security risks caused by "password fatigue." 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.

OKTA’S FOCUS ON SECURITY AND RELIABILITY

When setting out to build a company that offers an on-demand identity management service, Okta placed security and reliability front and center. Okta understands that the set of functionality it provides for user authentication, password and access management, integration with on-premises user directories, and cross-application usage analysis requires that the service be both highly available and secure.

Okta's approach to ensuring security and reliability is comprehensive. It spans its hiring practices, the architecture and development of the software that powers Okta, and the data center strategies and operations that enable the company to deliver a world-class service.

Secure Personnel Practices

Security starts with the people Okta employs. Background checks are performed on all employee candidates. Okta checks financial and criminal records over the past seven years. Additionally, employees, contractors, and third-party users must confirm in writing that they understand their roles and responsibilities regarding information security as part of their employment or vendor contract.

Security awareness training is an ongoing educational process throughout employment with Okta. Security responsibilities are renewed throughout an employee's tenure to ensure that employees and contractors understand their responsibilities, and are suitable for their roles. Okta's security team performs progressive social engineering tests and awareness campaigns to build security into the culture of the company. Okta's developers are trained annually on secure coding practices as well as secure code review techniques. Upon their departure, terminated employees are reminded of their confidentiality obligations and their user accounts, and passwords are immediately revoked.

Secure Platform Development

The Okta software platform is built to provide both a secure and reliable foundation for a broad set of functionality that helps customers scale and manage their cloud applications. This includes ensuring that all communications with Okta are secure and verified, that access to and control of the Okta service can be securely delegated across an organization, and that customer data is protected. Okta's audited Security Development Lifecycle practices mitigate the occurrence of web application security flaws, such as those described by the Open Web Application Security Project's Top 10. Additionally, Okta works with independent external security researchers to regularly validate the security of its design and service implementation.

Secure Access to Okta

All access to, and communication with, the Okta service is over an HTTPS connection. Okta has fully deprecated the SSLv3 protocol, and whenever possible TLS1.2 is negotiated with client browsers (this depends on the end user's OS and browser versions).

Customers are provisioned to and log into their own unique sub-domain (e.g., https://{customername}.okta.com leveraging the Hibernate ORM framework). Administrative functions are separated through an additional sub-domain: https://{customername}.okta-admin.com. These sub-domains enable customization of the Okta service to ensure customer-specific identification.

- *Login page customization: Customers select a theme and import their logo. This provides a consistent look and feel, and it helps mitigate phishing attacks.*

- *Unique cookie: Each customer's sub-domain is issued a unique cookie that restricts access to that sub-domain.*

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.

Robust, Extensible Permissions Model

The Okta platform supports an underlying permissions model designed to flexibly enable granular control of access to and administrative rights for the individual capabilities of the Okta service.

The model is very straightforward. A *resource* is something within the Okta system that is protected. Resource types include things such as applications and organizations. A *permission* is an action that can be taken on a resource. Activities such as READ, WRITE, and DELETE are examples of permissions. Finally, a *role* is a grouping of permissions that can be applied to one or more resources.

Okta currently supports several administrator roles:

- *Super administrators create Okta users and assign application administrator privileges to any application (including Okta).*

- *Organization administrators create and edit Okta users, manage password resets, and edit Okta customization settings (theme, logo, etc.).*

- *Application administrators create and edit instances of one or more assigned applications and manage users for those applications.*

- *User administrators perform user-related functions (view, activate/deactivate, edit, reset passwords, and create); this role can be scoped to control only certain groups of users.*

- *Mobile administrators create and configure mobile policies, Okta Mobility Management (OMM) wifi settings, device management, and Okta SSO/MFA policies.*

The permissions model is designed with enough underlying flexibility that it can easily be extended to add more roles with different permissions and eventually custom roles.

Secure Customer Data

Okta has taken several steps to secure customer data. For all queries, gets, and bulk updates, the Okta service returns or updates only validated data. Data is validated for each requestor in the context of the customer sub-domain (https://customername.okta.com).

All Okta system responses to a request are subject to any access restrictions in place for that customer and their Okta-registered users. This user/customer relationship is revalidated on every request, ensuring that all data is viewed only by authorized users within the customer's sub-domain.

Preventing Web Application Attacks

Core to the security of the underlying Okta platform is the ability to prevent cross-site scripting (XSS), cross-site request forgery (XSRF), and SQL injection attacks.

To prevent XSS, Okta validates that all input from the user conforms to the appropriate data type format (e.g., dates are in a date format), does not contain scriptable HTML tags, and is 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 prevent XSRF, 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.

SQL injection is a basic attack used to either gain unauthorized access to a database or retrieve information directly from the database. It occurs when an application program accepts arbitrary SQL from an untrusted source (think "end user"), blindly adds it to the application's SQL, and executes it. It's akin to an operating system taking a couple of lines of C code from a user, compiling it on the fly, and executing it in the operating system kernel. Okta avoids this by always using bind variables within 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.

Third-Party Penetration Testing

As part of its security strategy, Okta annually hires third-party security research firms to perform gray-box penetration tests on the Okta service. 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.

Okta uses BugCrowd, a platform that manages bug bounty programs. The program maintains a rotating population of 20 individually selected independent security researchers who perform external penetration testing of their own instances of Okta. Security vulnerabilities are triaged and validated by BugCrowd, and the researchers are rewarded with cash proportional to the severity of their findings.

Finally, for customers with their own in-house security research expertise, Okta will work with its team to perform its own penetration testing on an Okta test instance. All three of these programs, in addition to Okta's internal attack security researchers, ensure that Okta is in a continuous state of security testing.

Key Management Service

Okta uses a highly secure key management service to protect an org's sensitive data. The architecture comprises several key components, each with its own unique security mechanisms.

Part 1: Customer Key Stores

When Okta creates an org for a new customer, it automatically generates two unique sets of keys:

- *2048-bit RSA public / private key pair*
- *256-bit symmetric key*

The public/private key pair is used for SAML transactions, while the symmetric key is used to encrypt a customer's sensitive data (e.g., Facebook password, Okta API tokens, and sensitive attributes) at rest. Both sets of keys are stored in a key store that Okta encrypts with a unique org master key. For example, Org1's key store is encrypted with Org1's master key, whereas Org2's key store is encrypted with Org2's master key.

Security Benefits:

- *Sensitive customer data is encrypted*
- *Unique org master keys mitigate damage if a single org is compromised*

Part 2: Org Master Keys

Org master keys are themselves encrypted with a master key stored within Amazon's Key Management Service (KMS). Org master keys are encrypted by multiple master key providers (multiple KMS and an RSA offline public key, stored within a secured facility with dual keys) for redundancy.

Security Benefits:

- *Data is encrypted in layers*
- *Org master keys are themselves encrypted*
- *Redundant master keys (online and offline) ensure availability*

Part 3: Okta App

The Okta App needs the decrypted org master keys to decrypt org key stores. To decrypt the org master keys, Okta uses Amazon's KMS. The Okta application server authenticates to KMS via an Amazon Web Services (AWS) role and sends the encrypted org master key. KMS decrypts the org master key and returns it to Okta. Okta temporarily caches the decrypted key in memory, decrypts the key store, and subsequently shreds the key in memory.

Security benefits:

- *Multiple layers of encryption are used*
- *Each org key store is protected by a unique org master key*
- *Amazon KMS's master key protects the unique org master keys*
- *Decrypted org master key is cached in memory (not stored on disk)*

Part 4: KMS

KMS is a Federal Information Processing Standards (FIPS) 140-2 Level 2 Hardware Encryption Module operated by Amazon as a managed service. It provides key creation, rotation, and usage policies. As described above, KMS contains the master keys that encrypt and decrypt the org master keys. In this manner, the KMS master keys never leave KMS. Access to the KMS is 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. The backup key, used only if all KMS services fail, is stored in a secured, off-site facility that requires two or more 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 has direct access to KMS master keys*
- *Master keys are easily rotated*
- *Logs of key use are maintained (AWS CloudTrail and Splunk)*

HOW OKTA ENHANCES SECURITY

The Okta Password

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 cloud. Customers place considerable trust in Okta to protect the credentials that could yield the "keys to the kingdom." Therefore, Okta uses Bcrypt with a high number of iterations to protect the Okta password. Unlike other hashing algorithms designed for speed and thus susceptible to rainbow table or brute-force attacks, Bcrypt is very slow. Bcrypt is 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.

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 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 strongly recommends configuring multifactor authentication (MFA) to further strengthen the login to Okta. Okta provides integrated support for many MFA options. See the section entitled Multifactor Authentication/Strong Authentication.

Directory Integration

For many organizations, AD is the core repository of users and the associated credentials used to govern access to network and application resources. Okta integrates with AD to extend this capability to cloud-based applications and enables:

- *Automated import of users from AD to Okta, with adjustable frequency*
- *Automatic provisioning and de-provisioning of access to applications and Okta, based on changes in AD and security group membership*
- *Authentication against AD with the user's AD credentials to grant access to Okta*

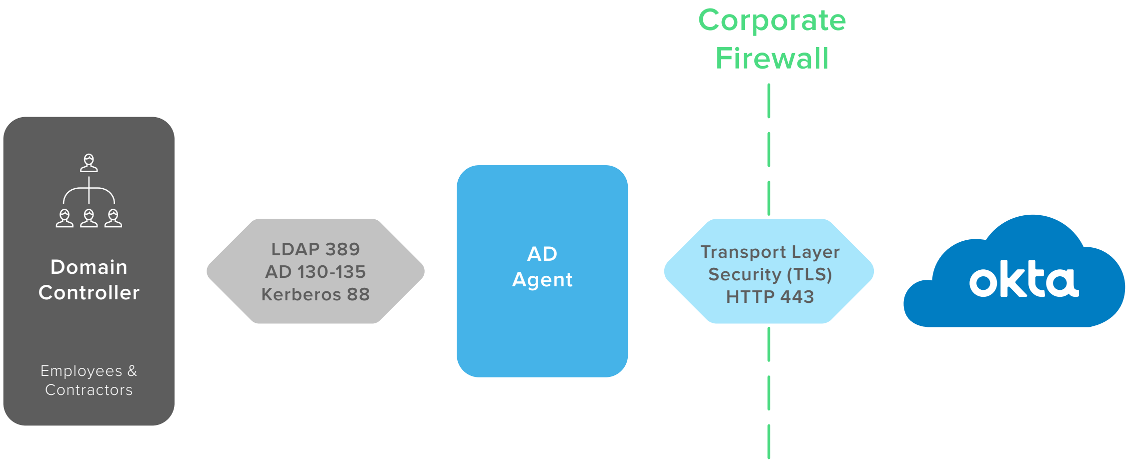
Okta's AD agent is designed with security in mind; in a typical deployment, no firewall changes are needed to integrate on-premises directories. The Okta agent may be installed on any domain member server—installation on a domain controller is not required. Domain membership is a requirement; this allows Okta to communicate with the domain controller to perform authentication and provisioning activities.

Installation must be performed by an Okta administrator but not necessarily a domain administrator. The Okta AD agent only requires elevated rights if password management is required. In that case, the Okta AD agent service must run as a service account with "modify user attribute" permissions. Full domain administrator privileges are not required.

During installation, the Okta agent registers itself with the Okta core service via an OAuth-based exchange. The installation admin authenticates to Okta using his or her own Okta admin credentials and issues the agent an API key. The API key gets automatically deleted if the agent is not used within 30 days; each use resets the API key's life to 30 days.

Once registered, the Okta AD agent communicates with the Okta service as follows:

The Okta agent communicates outbound through the corporate firewall via an HTTP request over port 443 to the Okta core service. This allows the agent and the Okta core service to mutually authenticate and establish a transport layer security (TLS) channel without requiring an inbound "hole" in the corporate firewall. TLS channels are encrypted using asynchronous keys, a process that protects data in transit from unauthorized interception and disclosure.



The AD agent enables delegated authentication and user provisioning from AD to Okta and vice versa. Note that this architecture applies to the Okta LDAP agent and Okta RADIUS agent as well.

Provision and De-provision Users (SaaS Apps)

Okta automates user management—also known as user provisioning—to connected applications that support and allow it. This feature set will create, update, and delete user accounts in applications based on rules and driven by attributes and group memberships. This improves security for organizations in a number of ways:

- *Creating accounts based on attributes from an authoritative source removes the element of human error. An IT admin who manually creates accounts can misspell fields, misunderstand instructions, or lack the necessary information to perform that task correctly. This could lead to end users getting unauthorized access to resources that should be protected.*

- *Automatically updating accounts with fresh attributes also assures security. For example, if an employee leaves one team and joins another, his or her permissions will most likely change as well. Okta will automatically update those attributes and reassign applications as needed. In a manual scenario, the end user may accumulate permissions over time, since access will not be changed.*

- *Deleting an end user or admin that has left the organization is critical. Okta will automatically de-provision accounts in connected applications so that even if the user remembers his or her password, there is no account to log into and confidential assets are protected. The manual equivalent is not only time-consuming—which reduces the likelihood that an IT admin will complete it punctually—but also rife with opportunities to make mistakes.*

Streamlining identity provisioning processes with Okta will ensure that end users have the right access to the right resources at the right time.

Single Sign-On

Okta can perform single sign-on (SSO) to web apps in two ways: secure web authentication (SWA) and federation.

Okta Secure Web Authentication (SWA)

SWA is Okta terminology for password vaulting. In an SWA configuration, a user enters a username and password for an app (e.g., Facebook), and Okta stores the credentials. When the user subsequently accesses the app, Okta posts the stored credentials to the app's login form, automatically signing in the user. As described in the Key Management Service section, app passwords and other sensitive data are encrypted with a customer-specific symmetric key before they are stored. SWA is typically used for SaaS applications that do not provide support for federated single sign-on. Because Okta recognizes an app's login form, SWA provides excellent protection against phishing attacks; a malicious login form will not "look the same" to Okta, and the user's credentials will be safe.

Federation

If an application offers federated SSO, Okta recommends using it over SWA. Most leading SaaS vendors support the Security Assertion Markup Language (SAML) or WS-Federation standards. Okta supports both standards and acts as the identity provider (IdP) to facilitate secure user authentication to various service providers (SPs).

When a new customer signs up for their Okta service, an instance of Okta is created for that customer. This is referred to as an "org." During org creation, Okta automatically generates an org-specific x.509 certificate and corresponding private key (details in the Key Management Service section). Customer admins can then easily download the public certificate to configure federated SSO to an app.

To configure SAML-based SSO, the Okta administrator typically does the following:

- *Logs into the target application, such as Salesforce, Google Apps, or Office 365*
- *Uploads the public key generated by Okta*
- *Identifies Okta as the issuer of the key, generally by copying over the Okta issuer token*
- *Provides any required data dictating how user IDs are exchanged in the authentication process*

When a user attempts to access an SP that has been configured for federated SSO, Okta validates the user and uses the private key to generate an SAML assertion response that includes the relevant information. The SP validates the SAML response, understands the assertion, and extracts the user information. The user is then allowed access to the application, without his/her application-specific password ever being stored within Okta or used during the authentication process.

Multifactor Authentication/Strong Authentication

Multifactor authentication (MFA) is designed to protect against the range of attacks that rely on stealing user credentials. Organizations can use a variety of techniques, but they all work by requiring the user to provide something in addition to their primary password—something the user is, has, or knows—before they can be authenticated to the protected service. With MFA in place, even if users' passwords are stolen, their accounts are safe from unauthorized access.

Okta offers a comprehensive MFA solution—running entirely in the cloud—that keeps users safe without getting in their way. Okta provides several convenient methods as detailed in the following table. As an open platform, Okta also supports third-party factors.

SMS

Okta offers a text message option that delivers a one-time password (OTP) code via text message to any SMS-enabled phone. Like the other MFA options, it is built into the service; no additional third-party services are required.

Verify

Okta Verify is a mobile app that generates authentication codes on a rotating basis, which users can use to provide secondary verification in Okta. Because the apps are preregistered with the Okta service, the attacker would have to possess the user's phone to know the code. This method does not require a messaging plan or a connection to the Internet.

Verify with Push

Okta Verify with Push is the easiest way to provide second-factor authentication. Okta will send a notification to a user's smart phone or tablet, and a single tap will provide the proof of ownership that Okta needs to allow or deny access to an application. If a user receives an unexpected authentication request, he/she can simply deny it and prevent any invalid access.

Third Party

Okta also supports third-party factors, including Duo Security, RSA, Symantec VIP, Yubikey, and more.

Okta knows that user adoption is critical to the success of any IT initiative, so balancing security with a non-disruptive user experience is critical. Okta employs authentication intelligently by assessing the risk associated with an authentication event and prompting only when needed. Okta allows admins to configure policies to prompt users based on authentication metadata, including IP address, location, device, application, group membership, and more. This capability can flexibly enforce MFA for authentication requests that deviate from expected patterns, denying malicious requests and permitting legitimate ones.

Delegated Administration

Okta supports delegated administration use cases through an administrator role called user administrator. The role comprises permissions that allow limited user-related tasks, such as create users, deactivate users, reset passwords, etc. Unlike other Okta administrator roles, whose permissions broadly apply to all users, the new user administrator role can be scoped to select Okta groups of users. This provides more granular administrative control.

Okta has several other administrator roles: super, organization, application, mobile, and read only. Users with those administrator roles can view and generally perform actions on all users, depending on the role. However, organizations might wish to 1) choose the users whom an administrator controls and 2) restrict the actions that an administrator can perform on users.

The ability to limit the scope of control is required for delegated administration use cases. Delegated administration allows an organization to spread administrative duties and, more importantly, segregate duties so that no administrator has too much control.

Encrypted User Attributes

While all customer data is protected when stored in Okta's Universal Directory (UD), Okta recognizes that you may need to maintain even more sensitive data, such as Social Security numbers or private information. To support this, Okta admins can choose the specific attributes they wish to encrypt. The org-specific symmetric key (described in the Key Management Service section) then encrypts the selected attributes, protecting them with the same security that saved logins and passwords have.

HOW OKTA STAYS SECURE

The Okta technical team has deep experience in developing and operating market-leading on-demand services such as Salesforce.com, SuccessFactors, and Rearden Commerce. Okta drew on that experience to conduct a comprehensive evaluation of infrastructure providers to select the right partner to complement its secure software development and enable it to accelerate the introduction of a highly secure and reliable service that easily scales as the needs of Okta's customers grow.

AWS is that partner. Amazon runs one of the world's largest networks of websites, serving millions of customers every month and executing millions of transactions for their customers and sellers. Over time, they have developed 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, including NASDAQ, Lawson, Adobe, Netflix, SAP, Virgin Atlantic, ESPN, Intuit, Siemens, and Tibco, with an infrastructure platform that powers business applications of tremendous scale.

Together, Okta and AWS have a comprehensive approach to ensure security and reliability of the Okta service. It starts with the physical data center, extends through the computer, network, and storage layers of the service, and is complemented by well-defined access policies and ongoing audit and certification by third parties.

ISO 27001:2013 Certification

ISO 27001 is an internationally recognized best practices framework for information security management. Okta has developed its internal policies and procedures with these best practices in mind, and the ISO 27001:2013 certification demonstrates that information security is ingrained in everything it does. Okta's ISO Certification can be verified online by its auditor, Brightline.

ISO 27001
CERTIFIED
BY BRIGHTLINE

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. The detailed results of this stringent certification process are available upon request under a nondisclosure agreement. Simply email security@okta.com.

AICPA
SERVICE ORGANIZATIONS
SOC

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

The CSA STAR is a powerful program that provides security assurance to enterprises leveraging cloud applications. The STAR leverages key principles of transparency, rigorous auditing, and overlaying data security standards (https://cloudsecurityalliance.org/star/). As the only IDaaS service to achieve a STAR Level 2 Attestation, Okta continues to lead the industry in protection of customer data. The STAR Attestation can be viewed at https://cloudsecurityalliance.org/star-registrant/okta-inc.

Physical Security

AWS data centers are housed in nondescript facilities. 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 must pass two-factor authentication a minimum of two times to access data center floors, and all physical access by employees is logged and audited routinely. When an employee no longer has a business need for these privileges, their access is immediately revoked, even if they continue to be an employee of Amazon.

Data center access and information is only provided to employees and contractors who have a legitimate business need for such privileges. All visitors and contractors are required to present identification and are signed in and continuously escorted by staff.

Network 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 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 generally 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 ARP cache poisoning do not work within Amazon EC2.

Compute Security and Reliability

Okta customizes its AWS EC2 instances to ensure security is maintained on multiple levels: the operating system (OS) of the host system, the virtual instance operating system or guest OS, the firewall, and signed API calls. Secure isolation is also maintained at the instance level, and Okta leverages AWS's Availability Zones to improve reliability.

Instance Level Security

Administrative access to the host operating systems for instance management requires the use of multifactor authentication. The administrative hosts' systems are specifically designed, built, configured, and hardened to protect the management plane of the cloud. All such access is logged and audited. Guest OS environments are also locked down and completely controlled by Okta administrators. AWS has no access rights to the guest OS.

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

All Okta calls to AWS to launch and terminate instances, change firewall parameters, and perform other functions are signed by Okta's secret access key. This secret access key is a 40-character sequence unique to Okta that is used to both generate and confirm digital signatures associated with any API call.

Fault Separation to Improve Reliability

Okta takes advantage of EC2's ability to place instances within multiple geographic regions as well as across multiple Availability Zones. Each Availability Zone is designed with fault separation. Availability Zones are physically separated within a typical metropolitan region on different flood plains in seismically stable areas. In addition to discrete uninterruptible power source (UPS) and on-site backup generation facilities, they are each fed through different grids from independent utilities to further reduce single points of failure. They are all redundantly connected to multiple tier-1 transit providers.

Data Security and Reliability

Multiple investments are also made to ensure customer data is secure and reliable. As detailed in the platform section of this document, 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 the EBS volumes are taken regularly and stored in AWS's S3 storage service. Access to S3, even within AWS, must be through SSL, providing additional insurance that the data is also transferred securely.

Within Amazon S3, Okta restricts access at both the bucket and object level and only permits 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, an authenticated user's permission is controlled by an access control list (ACL) that independently determines read/write permissions at the bucket and object level. All access is logged and audited.

Comprehensive Availability and Performance Monitoring

Each server in the Okta environment is monitored 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 the operations staff through email and SMS.

Okta also collects trending data for per-server and per-service performance metrics such as network latency, database query latency, and storage responsiveness. Performance is tracked for end-to-end scenarios across the application as a whole. These monitors all have health thresholds assigned and use the same alerting mechanism as the machine-level availability monitoring described above. Additional instrumentation in the runtime environment is also used to collect metrics internal to the application.

External to the service is a best-of-breed solution that Okta uses, with facilities for full transactional monitoring, benchmarking, SLA reporting, and alert escalation.

Least Privilege Access Policy

Okta requires that all access to its infrastructure, application, and data be controlled based on business and security requirements. Following the principles of segregation and least privilege, service 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. Software development teams cannot access the production system directly. 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 functions.

CONCLUSION

In the introduction, traditional IT infrastructure was compared to a castle, with high, strong walls and controlled entry points. But castles were difficult to scale—even the largest ones could not protect an entire village. The challenges faced by today's IT are no different—even the largest LAN cannot protect all of an organization's data. It's time to expand past the network perimeter and protect the data itself.

Okta's on-demand identity management service enables companies to address these challenges head-on by being designed from the ground up as a scalable, secure, multi-tenant service that protects your data through centralized access control.

The Okta team understands the need for its service to be both highly available and secure, and every aspect of the organization reflects this. From its hiring practices to the software it develops and the operational environment in which it runs, Okta understands that it is Always On.

Okta enables enterprise administrators to increase security above what is available through traditional on-premises technologies. By offering strong password management capabilities, account management capabilities, easy-to-deploy multifactor authentication, and encrypted attributes, the enterprise is now able to put strong controls on high-value data while balancing the ease-of-access users demand.

Okta is a leader in third-party certifications, physical and network security architecture, and reliability, so customers need not worry about putting authentication data in the cloud. Okta is trusted by organizations of all sizes and in all industries. Contact your sales representative to find out how Okta can make you more agile, more available, and more secure.

okta

www.okta.com