okta
The World's
Identity Company

Table of Contents

Disclaimer

Okta's response herein may contain proprietary information, trade secrets, and confidential pricing and financial data ("Proprietary Information"), and therefore may be exempt from further disclosure, in whole or in part, under the Freedom of Information Act (5 U.S.C. § 552(b)(4)) and the Trade Secrets Act (18 U.S.C. § 1905), or any Public Disclosure Law. Further, the information and data contained in Okta's response shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate Okta's products and services, or to learn more about the identity and access management marketplace generally. Okta's response shall not be incorporated in whole or in part into any resultant award, and any of Okta's Proprietary Information incorporated into such an award shall not be disclosed publicly.

Okta pricing provided in this response is conditional upon the purchaser's understanding and acceptance of Okta's enterprise cloud subscription service and the core principles of the one-to-many business model which are reflected in Okta's MSA and associated documentation. Okta's Service is provided on a single code line and runs on the same operational infrastructure using the same security and support operations for all of Okta's customers. The Okta Service relies on the standardization of Okta's operations and Okta does not agree to individual customer's security or support policies that do not accurately reflect Okta's security controls and single back-end support model.

100 First St.
San Francisco, CA 94105
888-722-7871

GLCLOUD 15

Dear Public Sector Clients

Okta's solution delivers a set of extensible building blocks, exposed through APIs and protocols, with amazing user experiences for operators of the identity ecosystem. Our platform solves for any use case without having to compromise in the balance of customer convenience, privacy, and security. Okta was designed from the ground up to deliver a modern identity and access management platform that meets customer requirements while avoiding common pitfalls that hinder performance and limit customer value, as outlined in the following table.

Okta	Traditional Identity Platforms
+ Cloud native with 99.99% availability + Rapid time to value + Customizable and extensible + Modern workflow orchestration + Breadth of pre-built integrations + Integrated security and attack protection + Modular building blocks support all use cases + No-, low-, and pro-code options for a developer and operator-friendly experiences + Upfront cost + Identity expertise (Gartner Magic Quadrant leader for nine consecutive years)	- Legacy - On premise - Slow deployment timelines - IT workflows - Prescriptive - Single-use-case point solutions - No and low code only - Lacks developer support - Unpredictable cost - Increased complexity

Please don't hesitate to contact me with any questions or to schedule a meeting.

Sincerely, Heidi Holdsworth – Okta Public Sector Account Executive

okta
The World's Identity Company

Executive Summary

Modernising Identity for the Public Sector

Public Sector organisations today face the dual challenge of maintaining secure digital services while managing the rising costs of legacy IT infrastructure. By adopting a modern Identity framework, organisations can move away from expensive manual processes, reduce technical debt, and ensure a secure environment for a hybrid workforce.

Strategic Value of a Modern Identity Fabric

- Vendor Neutrality: A neutral integration layer allows for seamless access across diverse environments, including Microsoft, AWS, Google Workspace, and on-premises applications.
- Operational Efficiency: Automating the Joiner-Mover-Leaver (JML) process reduces administrative overhead and eliminates the compliance risks associated with manual provisioning.
- Reduced Total Cost of Ownership (TCO): Moving from custom scripts to no-code/low-code automation can lead to a 90% reduction in time spent maintaining brittle code.
- Rapid Time to Value (TTV): Real-time identity provisioning ensures "Day One Access" to critical tools, improving the onboarding experience for staff, clinicians, and students.

Sector-Specific solution examples:

Healthcare (NHS)

- Reducing Clinician Friction: Address "login fatigue" by enabling seamless access to vital tools like Foundry and centralising access to NHS England applications
- Cross-Trust Collaboration: Facilitate secure and efficient access for clinicians working across multiple Trusts

Higher Education

- AI Security: Gain the visibility needed to discover and assess the risks associated with the rapid influx of AI agents into student and staff workflows.
- Legacy Modernisation: Retire unsupported "home-grown" identity hubs and custom scripting in favour of a single, future-proof Identity Hub.

Centra/Local Government

- Managing Legacy Debt: Lower maintenance costs by retiring outdated identity systems that create excessive workloads for IT and HR teams.
- Secure Hybrid Working: Provide a single, secure entry point for staff to access digital services regardless of their physical location.

NGOs and Non-Profits

- Secure Collaboration: Enable volunteers and affiliates to collaborate seamlessly without compromising enterprise-grade security.
- Mission-Focused Productivity: Automate routine IT tasks, such as password resets, to allow resources to stay focused on the organisation's mission.

Identity Security Posture Management (ISPM)

- Beyond access management, ISPM provides a comprehensive, risk-based analysis of an organisation's entire identity landscape—both human and non-human—in a single pane of glass.
- Non-Human Identity (NHI) Governance: Automatically inventory and secure service accounts, API keys, and AI agents that often bypass traditional security controls.
- Continuous Compliance Validation: Map security posture against frameworks like NIST and PCI-DSS to identify and remediate misconfigurations before they are exploited.
- Automated Risk Mitigation: Trigger automated workflows to enforce security hygiene, such as forcing MFA enrolment for overprivileged accounts

Strategic Contacts for Public Sector Transformation

Education, Local Government & NGOs: Heidi Holdsworth (heidi.holdsworth@okta.com)

NHS, Local Government & NGOs: Sotiris Kalli (sotiris.kalli@okta.com)

Central Government: Finn Turley (finn.turley@okta.com)

Why Okta, Inc.

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. With flexibility and neutrality at the core of our Okta Platform and Auth0 Platform, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and thousands of pre-built integrations. We're building a world where Identity belongs to you.

2009	19,300+	20	6,000+	9 years
Founded	**Customers**	**Global Offices**	**Employees**	**Gartner MQ Leader**

Okta's fully managed software-as-a-service solution is delivered as a multi-tenant service built from the ground up. Customers benefit from regular product updates, 99.99% availability with zero planned downtime, pre-built UIs, and comprehensive documentation that streamlines time-to-value for our customers. These are some of the reasons why Okta continues to be a leader in both Gartner's Access Management Magic Quadrant and Forrester's Identity as a Service Wave as well as Gartner's Customers' Choice in Access Management.

Intentionally Neutral

We design easy-to-integrate solutions ***that free everyone to safely use any technology*** regardless of platform, device, or location.

Universally Trusted

The world's most trusted brands ***trust*** Okta to provide ***the right people access to the right things at the right time.***

Relentlessly Committed

We're ***100% committed to advancing and innovating Identity***—no distractions, no other priorities.

Learn why the world's leading brands trust Okta for authentication, authorization, and more at Okta.

Okta Platform

The core of every successful modern enterprise is a robust, flexible, and secure identity and access management (IAM) platform. For the UK Public Sector this means a solution that not only meets today's technical requirements but also provides the agility to adapt to future challenges without compromise. The Okta Identity Cloud is designed precisely for this purpose, providing a transparent, vendor-neutral platform that simplifies your digital landscape while reinforcing your security posture.

A Single, Unified Identity Platform

- Okta's cloud-native architecture is built to centralize and simplify your entire identity ecosystem. Instead of managing disparate user stores and on-premises infrastructure, Okta's **Universal Directory** consolidates all your identities—from Active Directory and LDAP to custom user stores—into a single point of control. This unified approach eliminates complexity, improves operational efficiency, and ensures a consistent, secure experience for every user.

Unmatched Integration and Extensibility

- Integration is a cornerstone of our platform. With the **Okta Integration Network (OIN)**, you gain access to a catalog of over 8,000 pre-built integrations for the most common enterprise applications, including Workday, Office 365, Salesforce, and ServiceNow. This extensive network, coupled with our support for industry-standard protocols like SAML, SCIM, and OAuth 2.0, ensures rapid deployment and seamless integration into your existing application landscape. For custom applications, our comprehensive APIs and SDKs provide the building blocks for rapid development and full control.

Enterprise-Grade Security and Compliance

- Security and compliance are not add-ons; they are built into the fabric of the Okta Identity Cloud. Our platform offers inherent high availability, scalability, and security with a guaranteed 99.99% uptime. Our commitment to robust security is backed by industry-standard certifications and authorizations, including **SOC 2 Type II**, **ISO 27001**, and **FedRAMP Moderate & High**, providing you with the peace of mind that your mission-critical information is protected.

By partnering with Okta, you are choosing a strategic identity solution that delivers a faster time to value, reduces total cost of ownership, and provides a future-proof foundation for your business.

Conclusion

Okta is eager to earn your business and to work with you to elevate and modernize your identity and access management with the implementation of our comprehensive, extensible, and secure identity solution. Our commitment to helping you achieve and exceed your identity goals, coupled with our market-leading product as well as our identity expertise, will start your organization on a path to success. We look forward to working with you during the final steps of the vendor evaluation and selection process, and ultimately, we hope to support you as your long-term strategic partner in identity. ￼

Information and Product Overviews

Okta Industry Recognition

In 2009, Okta launched the world's first cloud-based identity and access management system, marking the birth of an industry that is now known as Identity and Access Management as a Service (IDaaS). Over time, Okta added a host of new products and features that further established identity as the modern security perimeter for Workforce Identity. In 2021, Okta acquired Auth0 to enhance its customer identity offerings and continue building an identity cloud that is broad enough for every use case, adaptable so developers can build on top of it, integrated into customers' technology stacks, and trusted with the highest standards for security, reliability, and scalability.

Today, Okta is the identity standard, with the most complete identity and access management offerings in the industry, trusted by over 19,300 organizations to solve some of their most intractable security problems (www.okta.com/customers).

Gartner recognized Okta as a Leader in the Magic Quadrant™ for Access Management, November 2025.

Gartner defines access management (AM) as tools that include authentication, authorization, single sign-on (SSO) and adaptive access capabilities for modern standards-based web applications, classic web applications and APIs.

This is the nine year in a row that Okta has been recognized as a Leader in the Magic Quadrant™ for Access Management.

**Gartner, Magic Quadrant for Access Management, Brian Guthrie, Nathan Harris, Yemi Davies, Steve Wessels, 11 November 2025.*

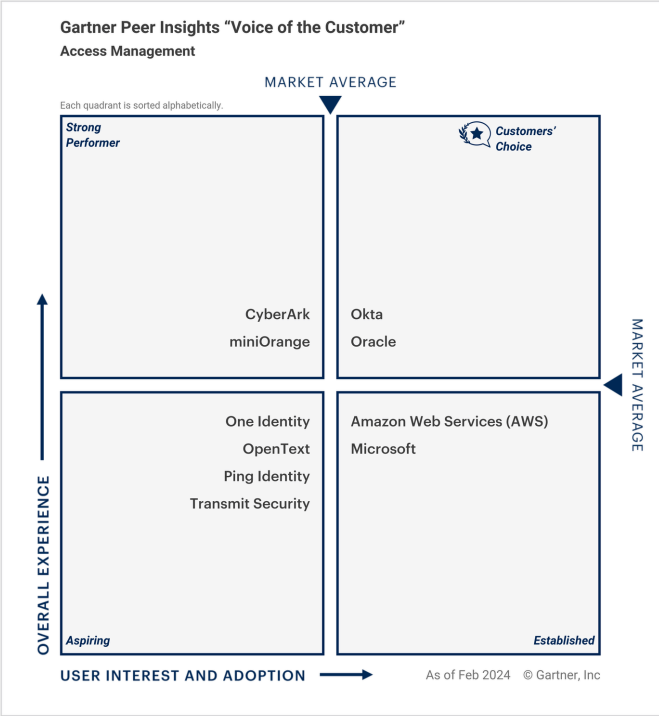
For additional information and to download the report, please see: Okta named a Leader in Gartner® Magic Quadrant™ for Access Management for the 9th year in a row

Okta Recognized as a 2024 Gartner® Peer Insights™ Customers' Choice in Access Management

Okta is the only vendor to be recognized as a Customers' Choice for Access Management 6x in a row:

94% of reviewers said they would recommend Okta

Okta's impact on its enterprise customers and developers are well-expressed in these reviews:



- "The gold standard in Identity Management, Okta is an amazing platform."
  - IT leader in Healthcare and Biotech Industry (March 2024)
- "Best access management tool to enable secured logins for the users"
  - HR in Software industry (October 2023)

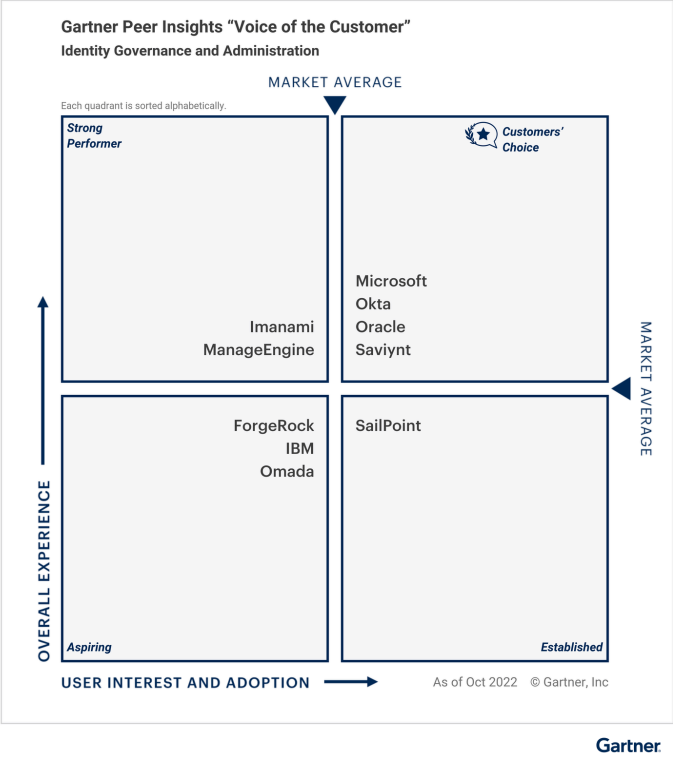
Source: Gartner Peer Insights 'Voice of the Customer': Access Management, April, 2024

For additional information and to download the report, please see: [Okta Recognized as a Gartner® Peer Insights™ Customers' Choice for Access Management]

Okta Recognized as a Gartner® Peer Insights™ Customers' Choice for IGA

Here's a snapshot of what Okta's customers shared with Gartner in the latest "Voice of the Customer" report:

- 92% of reviewers said they would recommend Okta, the highest willingness to recommend score among Customers' Choice vendors
- Okta received the highest Support Experience ratings among Customers' Choice vendors



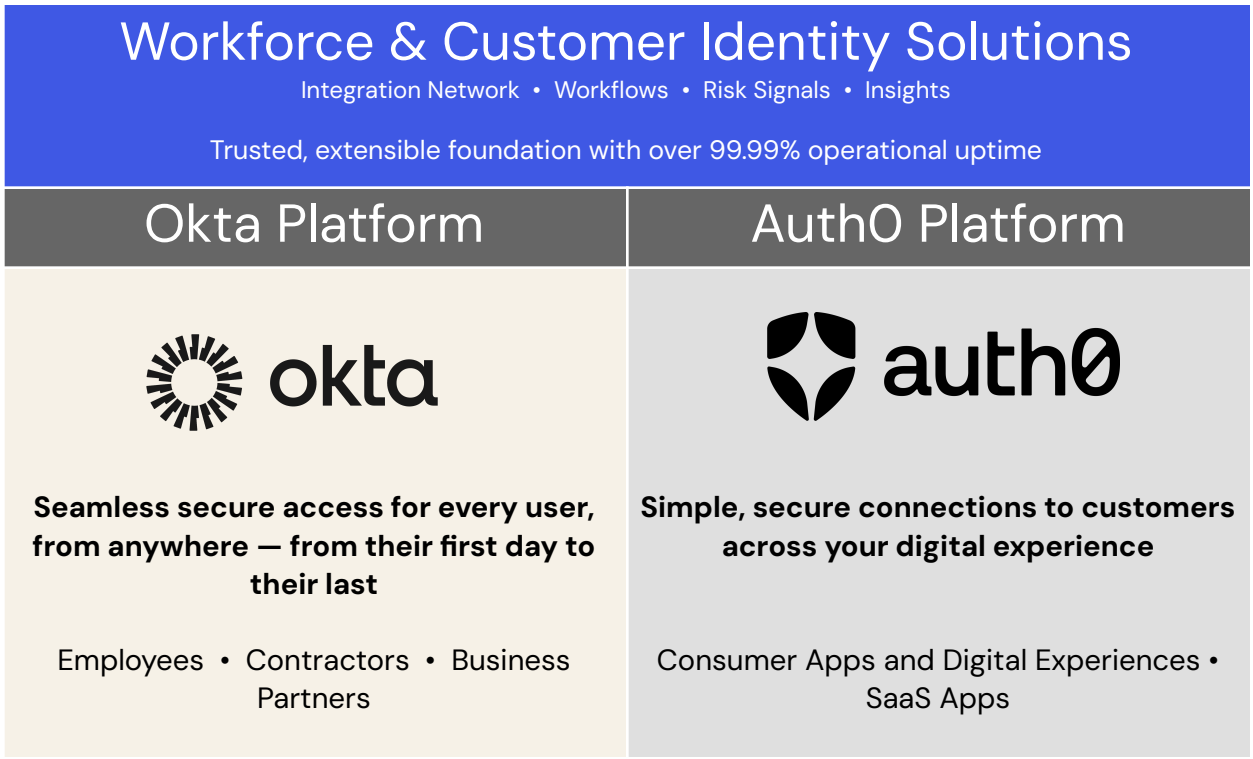
In our customers' own words:

- "Okta Just Makes Life Easy…Can't go wrong with Okta. This has really simplified and streamlined the way we operate internally within our applications…" - Sales Manager, Software (July 2022)
- "A Comprehensive Identity Management Solution" - Software Engineer, Media (January 2022)

Source: Gartner Peer Insights 'Voice of the Customer': Identity Governance and Administration, December 28, 2022

For additional information and to download the report, please see: [Okta Recognized as a Gartner® Peer Insights™ Customers' Choice for IGA]

Our Products



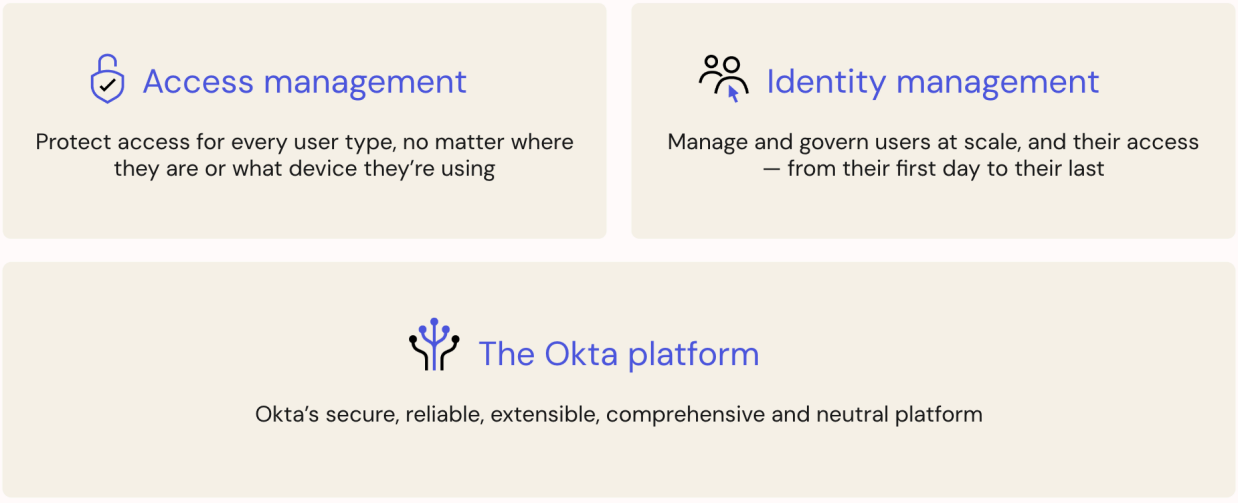
Okta consists of the Okta Platform and Auth0 Platform. It is a one-stop solution that's comprehensive and customizable for all your evolving needs. Enable your organization to handle any workforce or customer identity use case while enhancing your security:

- **Okta is Cloud-based.** Okta is built from the ground up on cloud technologies and frameworks to deliver a scalable multi-tenant SaaS with regular upgrades and updates.
- **Okta is Universal.** Okta is an independent platform with support for a wide range of open standards, including OAuth, OIDC, SAML, WS Fed, AD/LDAP. Customers benefit from the Okta Integration Network, a catalog of 8,000+ pre-built application integrations, and the Auth0 Marketplace, which developers can leverage to quickly find and install third-party applications.
- **Okta is Reliable.** Okta provides all customers with 99.99% availability to the service with zero planned downtime and zero maintenance windows.
- **Okta is Easy.** Okta's solutions can be rapidly deployed, easily configured, and centrally administered, resulting in very fast time-to-value without the need for protracted services engagements.
- **Okta is Secure.** Okta's compliance program is built upon industry-standard certifications and authorizations. See https://trust.okta.com/compliance

Okta Platform

The Okta platform provides a broad set of functionalities to address the user management, single sign-on, governance, and reporting needs for your employee, customer, and partners, including:

- Flexible cloud identity meta-directory
- Automated user registration and management
- Automated provisioning and deprovisioning
- Single sign-on to any cloud or web application
- Adaptive multi-factor authentication
- Identity governance and administration
- Integration with 3rd-Party Portals
- Integration with SharePoint, AWS, Microsoft, G Suite, and many others
- Integration with existing identity and access management solutions



Okta Platform

The Okta Platform is built on a set of modular Platform Services, which can be combined to build new features and tailored experiences faster. Platform Services are available in Okta's packaged products, APIs, and SDKs.

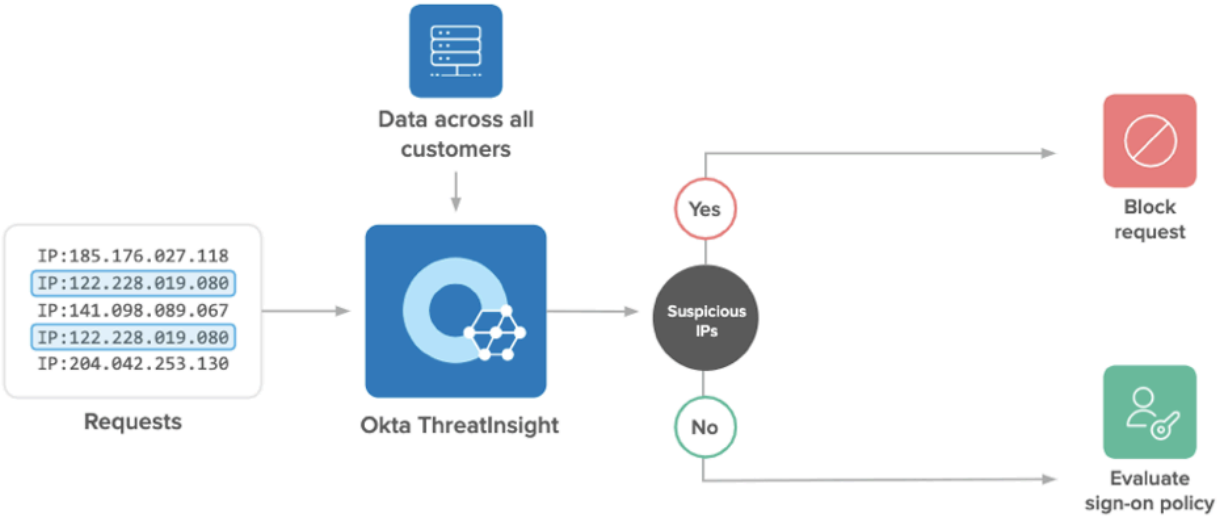
Each of these core Platform Services serves a distinct purpose:

- **Okta Identity Engine:** runs a customizable, extensible sequence of steps to deliver authentication, authorization, and registration flows based on context.
- **Okta Directories:** stores users and attributes, making Okta Universal Directory and User Management products more flexible and scalable.
- **Okta Integrations:** offers tools, templates, and frameworks that make it easy for partners and customers to build integrations and publish them to the Okta Integration Network.
- **Okta Insights:** aggregates, analyzes, and disseminates Okta data to be used across systems. Insights-powered features — ThreatInsight, HealthInsight, and UserInsight — leverage data to increase overall security posture by blocking malicious IP addresses, offering personalized recommendations for security policies and settings, and alerting end-users of suspicious account activity.
- **Okta Workflows:** automates complex identity-centric business processes, all without code.
- **Okta Devices:** collects device identity and context to inform access decisions and enhance user experience, powering key features including Okta FastPass, Limited Access, Device Visibility, and Remote Sign-out.

Okta Platform Services are not only designed to be broadly accessible within Okta product features but can be combined to create entirely new capabilities. For example, the Okta FastPass feature leverages Okta Devices, Okta Directories, and Okta Identity Engine to deliver an entirely new passwordless experience. Some key platform services and features include:

ThreatInsight

Okta offers service level threat protection via Okta ThreatInsight. ThreatInsight captures IP addresses accessing Okta across all customers and checks for IPs that are causing password spray and brute force attacks. These IPs are marked as suspicious and put into the ThreatInsight pool, giving admins the option to block or audit access from those IP addresses in their own org. ThreatInsight is evaluated pre-authentication to prevent user lockout.



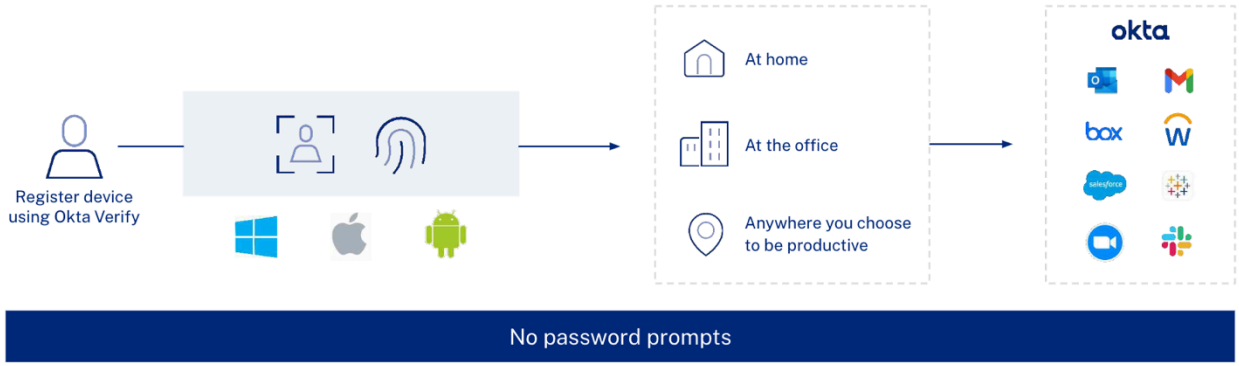
Workflows

Okta Workflows is a no-code automation platform that enables admins to modernize ever-more-sophisticated identity-centric processes without leaning on developers. Workflows can be used to augment Lifecycle Management and provide custom logic for organization-specific use cases. It provides a graphical drag-and-drop interface that combines triggers, logic, and time-based actions to build powerful "if-this-then-that" flows. As a result, anyone can easily stitch together app-specific provisioning and deprovisioning tasks.

FastPass

Okta FastPass is a Zero Trust authenticator designed for defence in depth to mitigate the impact of phishing attacks, session theft, and unauthorized local activity. Enabling secure, device-based access is a challenge for many organizations, especially with the influx of new device types across mobile and desktop platforms. Okta FastPass enables passwordless authentication to any SAML, OIDC, or WS-Fed app on any device and from any location. Utilize Okta FastPass to minimize end user friction when accessing corporate resources, while still enforcing Okta's adaptive policy checks. This reduces the probability of data breaches that can occur from compromised credentials.

Once a device is registered, the user is not prompted for a username or password when they try to log into their Okta apps. The passwordless experience is controlled by the Okta sign-on policy and app sign-on policy configured by the admin.



Okta FastPass enables the following key benefits:

- **Passwordless authentication** from any device, location, or network to any Okta-managed app
- **Works with any device management tool**, with no dependency on AD or specific enterprise mobility management (EMM)/mobile device management (MDM) software.
- **Combine Okta FastPass with device-level biometrics** to avoid additional prompts when accessing Okta-managed apps.
- **Option to combine Device Trust with Okta FastPass** so passwordless login is only available on managed, compliant devices.

Devices register with Universal Directory through the Okta Verify app. After the one-time registration (regardless of where the user is located), the user has passwordless access to all resources in Okta, including the Okta End-User Dashboard, native mobile apps, SP-initiated browser access, and desktop thin clients that support modern authentication.

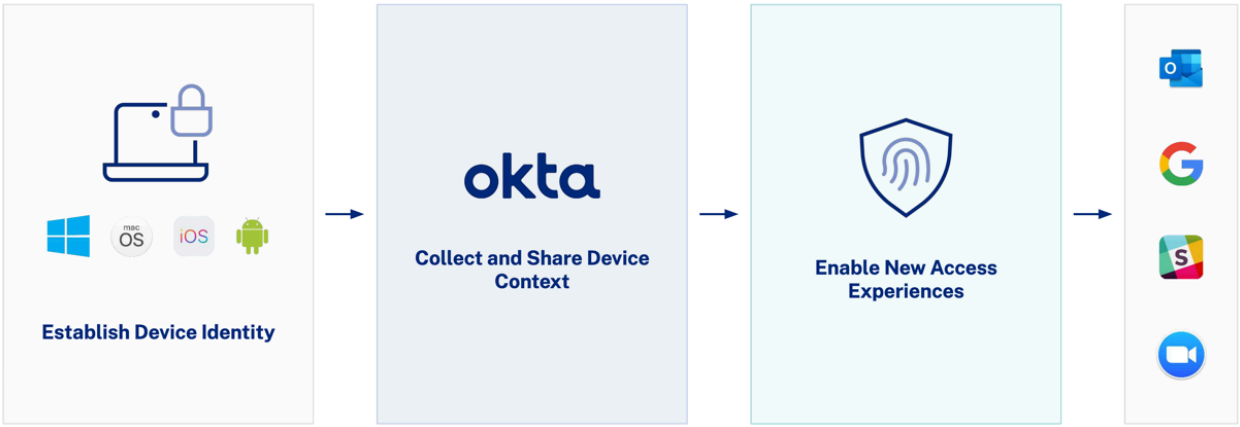
Okta FastPass is compatible with Windows, iOS, Android, and macOS and works on any device: managed or not managed, AD-joined or not AD-joined. It does not require devices to be on an office network. Older desktop single sign-on (SSO) features in Okta require Active Directory (AD), but Okta FastPass has no requirements for AD, other user-directories, or specific end-point management tools.

Device Context

Device Context provides maximum visibility into the devices that access Okta and enables contextual access decisions to Okta-managed apps. Combined with App-level Policies and assurance levels, Device Context is an enabler of secure, passwordless experiences.

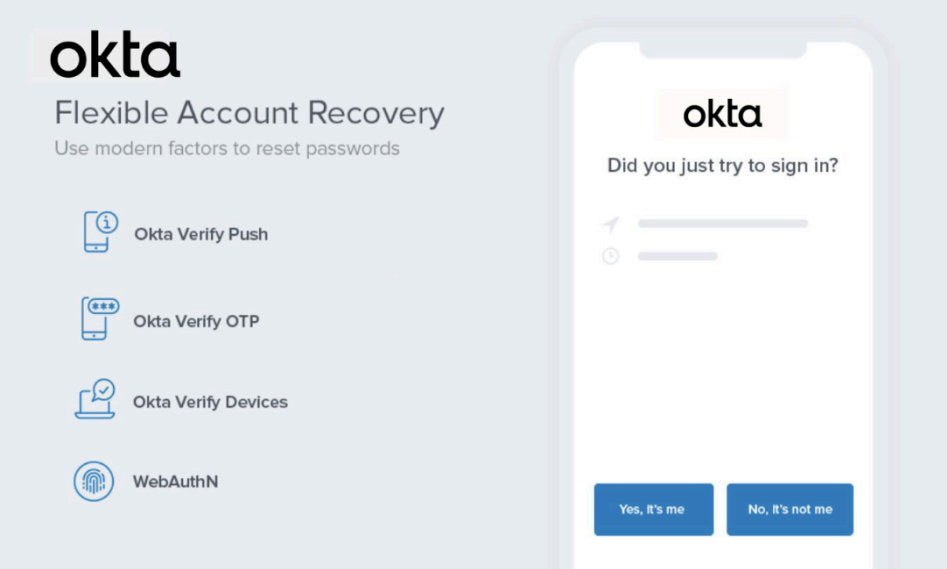
Admins have better access control, with the ability to:

- View the status of all devices associated with a user in Universal Directory, including whether they are managed by EMM, EDR Signals, or registered by Okta through the Okta Verify app
- Suspend or deactivate devices
- Remotely log a user out of active Okta sessions across individual devices
- Create policies based on Device Trust and security posture information ingested from 3rd parties (EDRs such as Carbon Black, Tanium, etc.)
- Control in-app actions based on managed vs unmanaged device state



Flexible Account Recovery

Okta's flexible account recovery feature allows users to self-service reset their password with modern authenticators such as WebAuthn biometrics and Okta Verify Push in addition to email or phone (SMS, voice call). If admins require step up authentication, end users can use any enrolled authenticator. This improves the end user access experience, strengthens security posture, and decreases IT Help desk tickets.



Okta Platform Products

The products within the Okta Platform are built on top of the platform services to enable organizations to securely embrace the rise of cloud and mobile, move away from traditional perimeter-focused approaches to security, and focus resources on enabling access for all users regardless of their location, device, or network.

- Single Sign-on
- Multi-factor Authentication
- Universal Directory
- Lifecycle Management
- Workflows
- Access Governance
- API Access Management
- Access Gateway
- Privileged Access Management
- Identity Security Posture Management
- Identity Threat Protection

The following sections expand on each of the Okta Platform's products.

Single Sign-on

Okta Single Sign-on is part of a complete identity and access management solution for organizations adopting and building for cloud and mobile who need to contain costs, fulfill user productivity targets, and avoid security risks. Unlike legacy Federation and Access Management systems, Okta Single Sign-on is a lightweight, easy-to-deploy solution that securely connects your employees, contractors, and customers across any of their devices to all their cloud and on-premises applications.

Capabilities

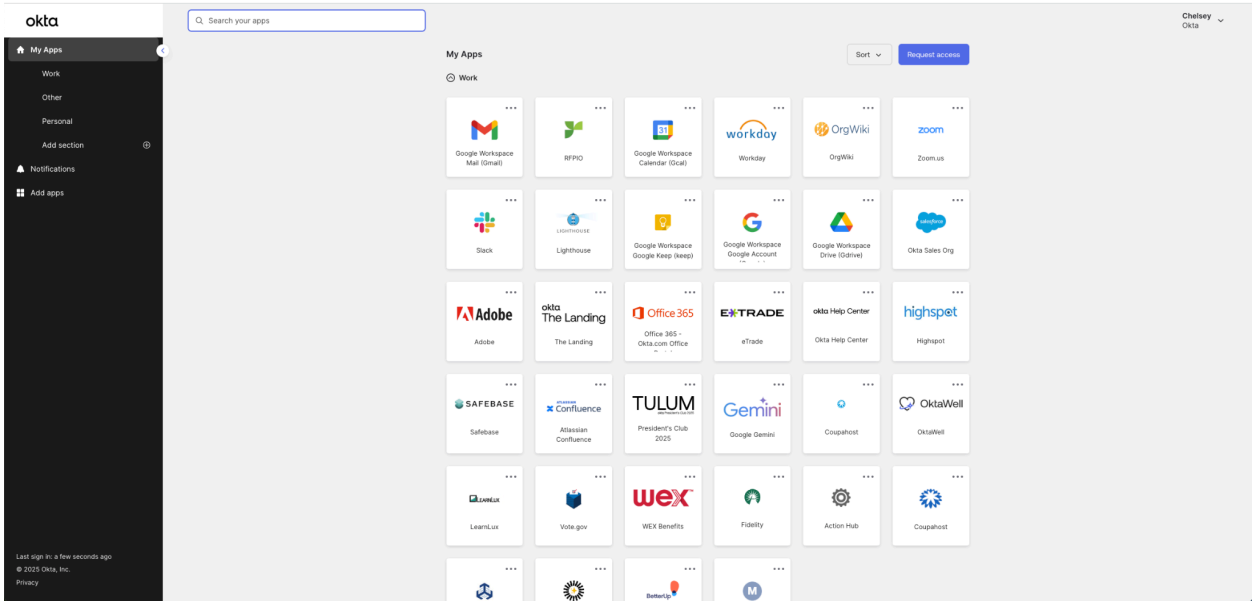
- **Integrated Access Management.** Reliable integration for SSO to all your web and mobile apps, with a full featured federation engine that supports all modern protocols and flexible access policy.
- **Customizable User Experience.** One user-friendly portal for end-users to access all their applications, tailored to each of their devices and fully customizable to their workflow.
- **Secure Directory with Integration.** Securely store user credentials with support for custom attributes and delegated authentication to AD/LDAP across multiple domains with self-service AD/LDAP password reset with Universal Directory.
- **Real-Time Security Reporting.** Sophisticated search of real- time system log, with geolocation tracking and integration with 3rd party SIEMs.

Benefits

- **Remove Barriers to Growth Within Your Organization.** As organizations grow, one of the biggest IT challenges they face is how to best secure their environment. Individual employees, contractors, and customers all have their own permissions and security needs. It can be tough for one helpdesk administrator to manage all of these moving parts.
- **Decrease Costs While Increasing Efficiency.** Okta reduces on-prem infrastructure and custom development by embracing cloud and mobile while increasing efficiencies by automating manual provisioning and reducing helpdesk calls.
- **Strengthen Security and Compliance With the right SSO solution.** companies can rest knowing that the right people have the right level of access. Even more, users can safely access all of their apps with a single password, from any device.

Okta provides end users with a common user dashboard which is dynamically rendered upon login and is based on the user access rights. The user is presented with all the application icons upon login. The icons are movable items and can be placed in additional tabs on the dashboard for easier management. Okta administrators can add additional

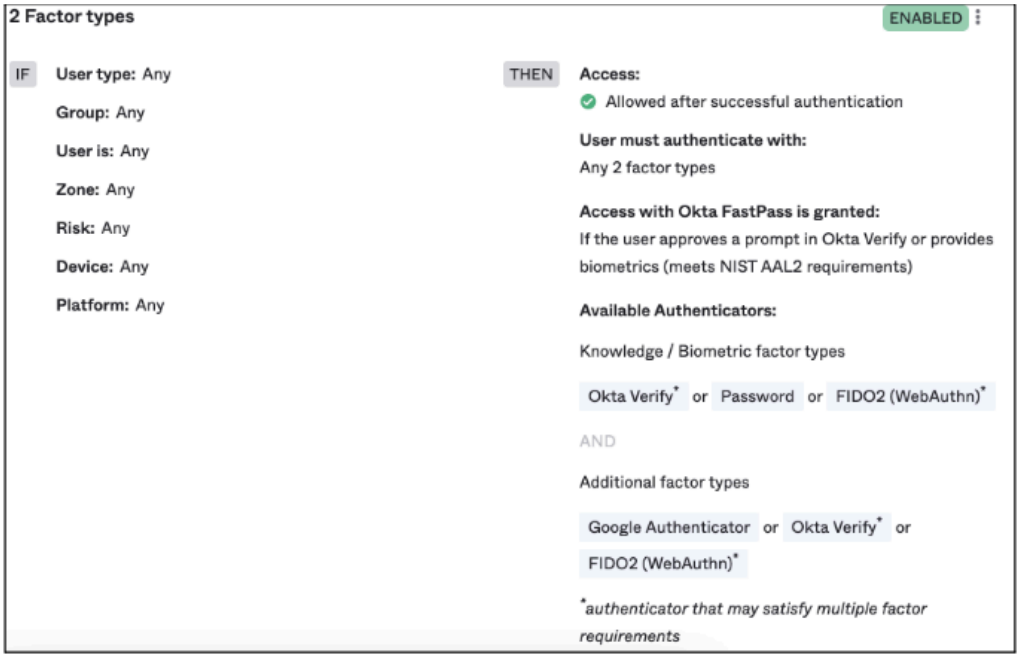
notes and make the applications accessible when/if accessed on the corporate network. The icons can be configured, and the look and feel of the UI can be changed.



Application-level Sign-on Policies

Okta enables the creation of dynamic sign-on policies tailored for different applications based on user behavior, risk level, and context. App-level policies allow organizations to model security outcomes for application access based on industry-accepted digital identity best practices (outlined by NIST and other security standards). App-level policies enforce end-user authentication in the context of the requested application, maximizing flexibility in developing security policies tailored to your organization's landscape.

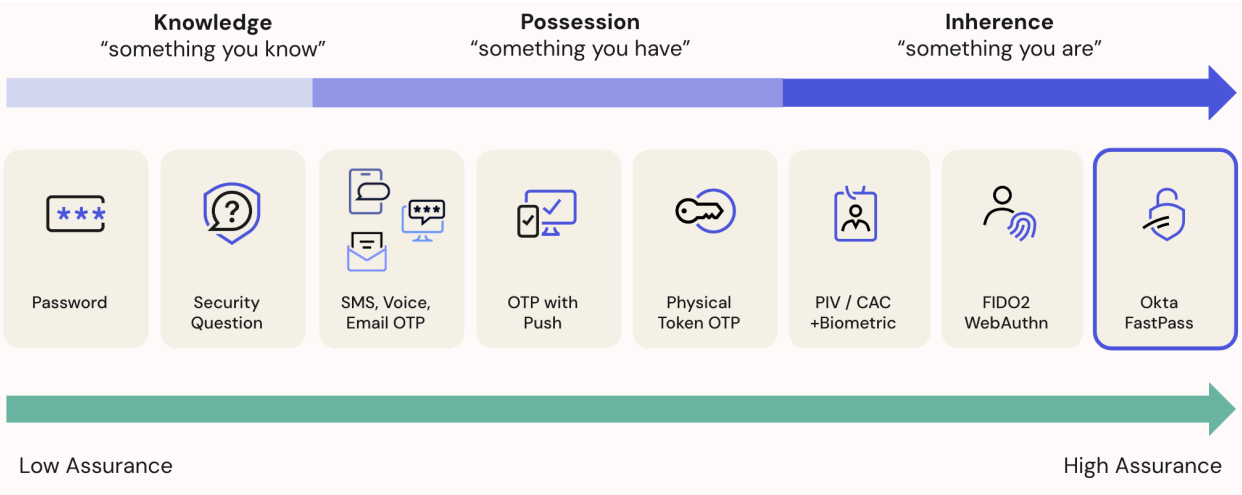
This helps manage who can sign in and how a user is allowed to sign in to Okta, including whether they are challenged for MFA and how long they are allowed to remain signed in before re-authenticating. For example, organizations may want to enforce more stringent assurance requirements for access to a sensitive app, but relax those requirements if there is high confidence the access request is legitimate given the user's past behavior and current context.



Multi-factor Authentication

Okta provides multi-factor authentication (MFA) as a core feature of the identity management service. Okta built all functionality with the same focus on flexibility, security, and ease of use that we apply to all other aspects of our product and comes bundled with the Okta solution. No third-party products are required.

Okta's MFA solution supports a range of authenticators to suit your business needs, assurance levels and overall security risks.



Okta's MFA solution is designed to manage the entire lifecycle of a user's MFA flow including registration, on-boarding, deployment, and factor reset. Admins can assign MFA to users

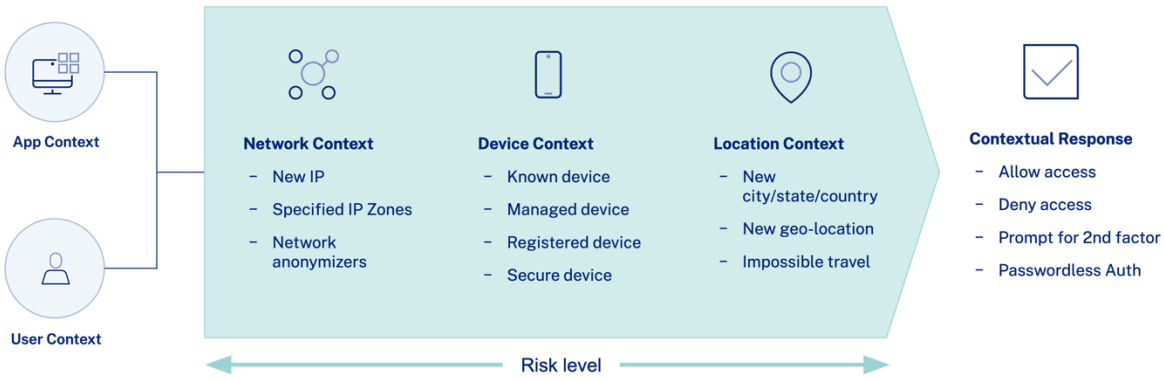
based on group membership or application access. Okta offers a range of native authenticators but can also work with existing 3rd party authenticators deployed with your end-users (e.g., YubiKeys, PIV cards, Generic OTP tokens, Google Authenticator, Duo MFA, and others).

Adaptive Multi-factor Authentication

Okta's Adaptive Multi-factor Authentication is an additional layer of security designed to consider user behavioral patterns and context when evaluating login attempts. Okta's Adaptive Multi-factor Authentication leverages a number of contexts including

- Device Context
- Location Context
- Network
- Application Context
- User and Group

Each context represents a family of signals such as IP address, Country, Device ID, etc. to understand a user's typical login patterns. Admins can build smart adaptive authentication policies and request for MFA step-up authentication only when a user deviates from normal login patterns.



Adaptive MFA addresses common pain points in deploying a multi-factor solution with the following capabilities:

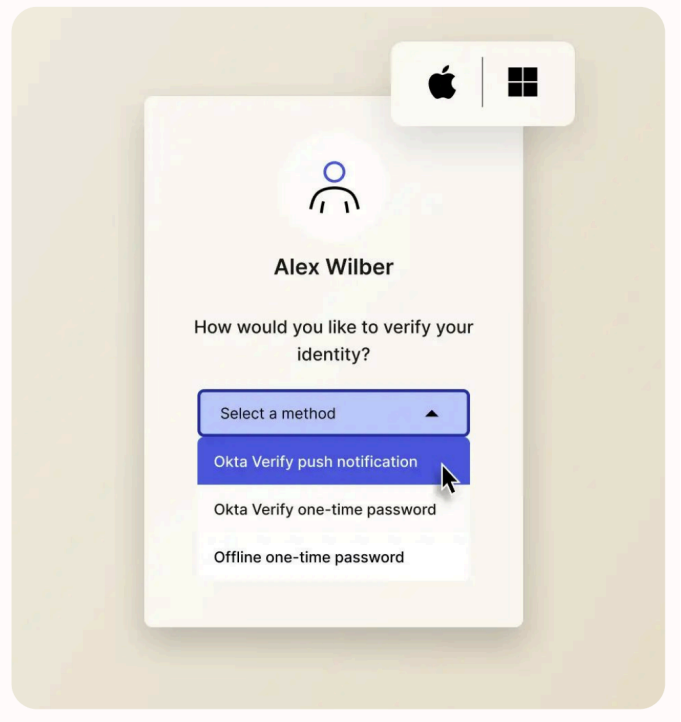
- **A flexible solution for all user types.** Whether you need to enforce MFA and adaptive policies for your own employees, suppliers, contractors, customers or consumers, Okta has you covered. Policies can be applied to any web or native mobile app—you can even use Okta as the auth provider for your custom-built apps.
- **Dynamic response based on login context.** Multi-factor authentication isn't great when all you can enforce is a basic "yes" or "no." Okta enforces step-up

authentication when it makes sense based on historical context on the user paired with their device, location and IP and many more login characteristics.

- **Make passwords less significant.** Even with reasonable password policies in place, users still tend to be the weakest link in the chain. Give your end users a simple login experience while staying secure by using strong auth authenticators like Okta Verify, biometrics, and FIDO2.0 tokens to replace passwords.

Device Access

Okta Device Access extends IAM capabilities across desktops and laptops, increasing your org's security posture and protecting you from phishing attacks. Local device data is protected by the same Identity Provider that protects access to data and applications in the cloud.



Users access sensitive information by signing in to their computers with their authenticated Okta credentials from anywhere, even without an internet connection. Okta Device Access secures devices, simplifies the single sign-on experience, and streamlines access to devices and apps. Organizations can meet compliance needs and equip employees to work productively. Okta Device Access currently includes two critical capabilities: Desktop MFA and Desktop Password Sync

Desktop MFA

Enforce MFA on top of passwords when end users login to their managed Windows (Active Directory (AD) or Azure AD joined) or macOS (local) desktops/laptops. Windows virtual machines and servers are also supported.

Features:

- Choice of possession factors: Okta Verify push, Okta Verify one-time password, YubiKey (OTP)
- Intuitive user experience for device login and factor enrollment

- End users can login with or without access to the internet
- Configure a policy and target it for certain users and groups
- Deploy through an existing device management tool (e.g., MDM, GPO)

Desktop Password Sync

Sign in to your macOS account with your Okta password by syncing passwords. Also, auto-enroll end users into Okta Verify and FastPass to provide secure and passwordless access to all their apps. Desktop Password Sync for macOS takes advantage of Apple's Platform SSO extension for macOS and improves upon it.

Features:

- Synchronize passwords to eliminate a local macOS account password to remember
- Enforce a secure IdP password policy for devices
- Streamlined onboarding flow that auto-enrolls users in FastPass
- Passwordless login to apps via FastPass, a high assurance authenticator

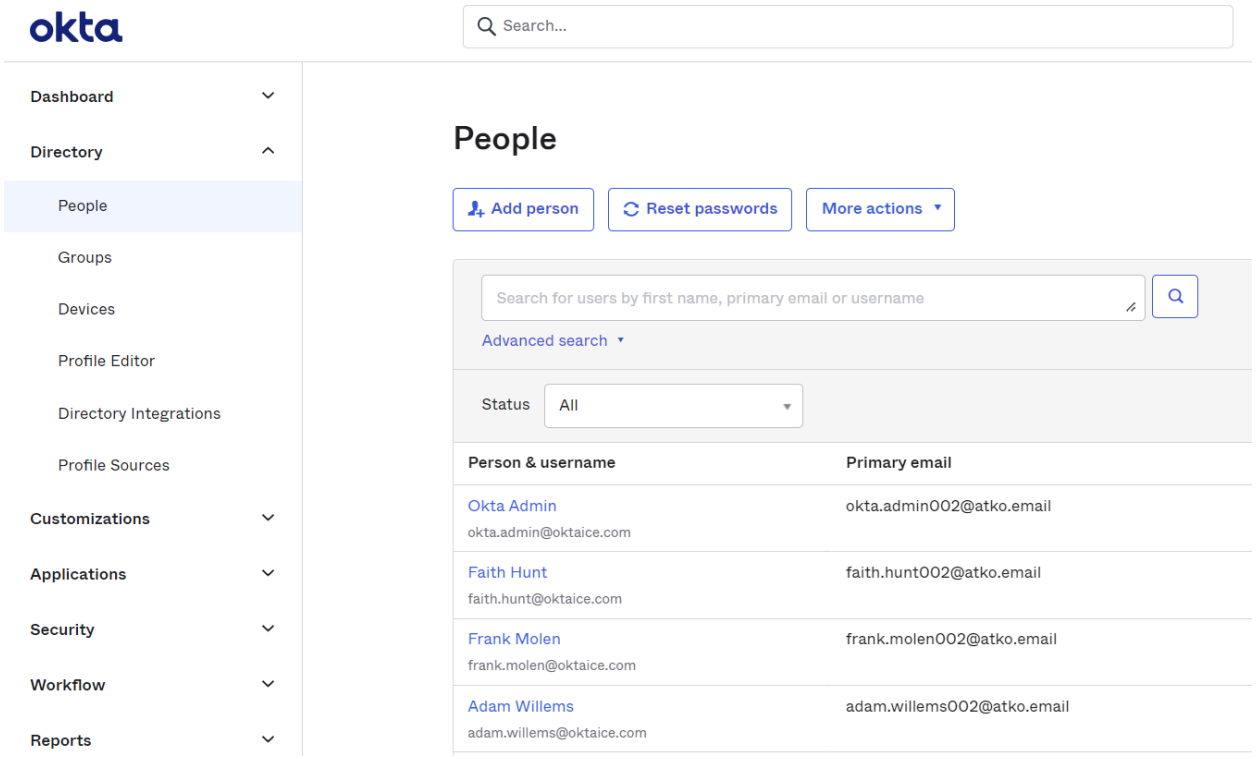
Universal Directory

Okta's Universal Directory (UD) provides organizations with a central identity management plane and cloud source of truth. UD offers one place to manage all users, groups and devices, sourced in Okta or from any number of sources. Organizations can store an unlimited number of users and attributes from applications and sources like AD or HR systems. Any type of attribute is supported, including linked objects, sensitive attributes, and pre-defined lists. This user information can be securely leveraged by apps in the Okta Integration Network catalog, over LDAP or via API.

UD allows information across disparate user directories or "As-A-Source" (such as Salesforce, Workday, Bamboo or CSV) applications to be synchronized to Okta. UD allows Okta to map different fields that are part of different directories or user stores into a single, consistent, detailed view of user identities and attributes. This capability allows Okta to support configurations where multiple directory or application types are deployed.

In UD, organizations can store, map, and transform Okta and application attributes to automatically manage users' attributes between the Okta and application users' attributes

where user management is available. Then in the application profile mapping, you can map between applications the various user or application attributes. Attributes stored within the Okta Cloud Directory can also be included in SAML assertions or API calls for the purposes of provisioning.



Directory Integration

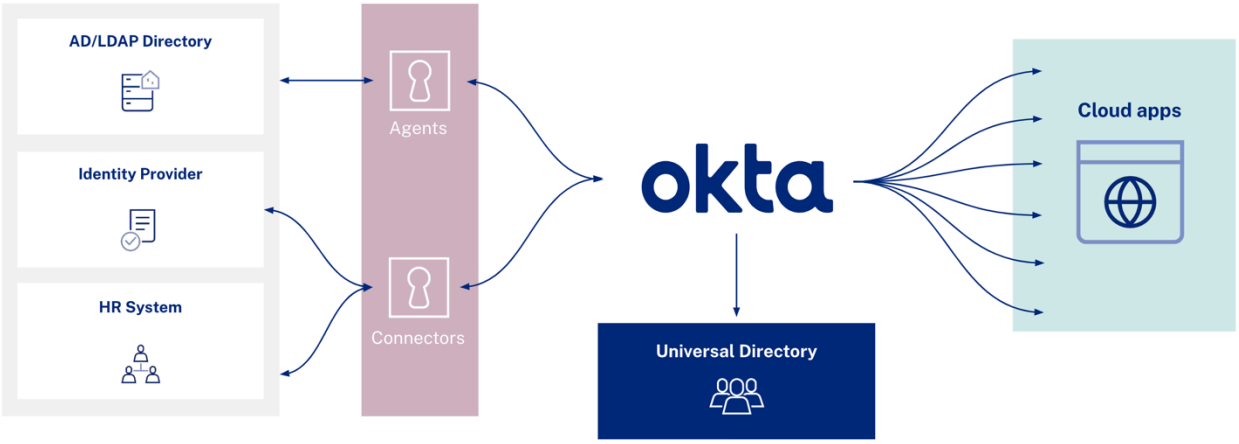
Organizations continue to shift their focus from legacy on-premises applications to newer cloud-based services. The newer cloud services offer enormous benefits, both in expanded capabilities and in lower overall cost. One of the biggest obstacles in this path is managing user identities in a way that is consistent with users' and administrators' experience and expectations.

Okta offers a complete and easy-to-use directory integration solution for cloud and on-premises web applications. Okta provides user authentication, user provisioning and de-provisioning, and detailed analytics and reporting of application usage, for both cloud applications and on-premises web applications. A key component of this service is Okta's directory integration capability, which is very easy to set up and is architected for high availability. In addition, Okta maintains the integrations for you, with thousands of applications supported in Okta's Integration Network (OIN).

Okta's robust cloud-based directory service (Universal Directory) enables organizations to integrate with multiple identity stores simultaneously including, but not limited to

- Microsoft Active Directory
- V3 compliant LDAP directories
- and third-party human resources management systems (HRMS) solutions (e.g. Workday, PeopleSoft, etc.).

Okta's flexible architecture can take the feeds from multiple sources and directories and can correlate the user identities to provide a 360-degree view of a single individual regardless of the origin of the identity. You can then create policies based on various different elements to grant them access as birthright access or based on a specific attribute/group membership to specific application or sets of applications.



Okta also supports the concept of Okta-sourced accounts where an identity originates in Okta Universal Directory (and is not sourced from an existing identity repository). This allows organizations to support disparate user segments which are typically stored in disparate identity stores. Once the identities are in Okta's Universal Directory, Okta can leverage group and attribute information (from the originating identity store) or assign Okta groups based on the user's identity attributes (Okta group membership rules).

Okta Identity Governance

Okta Identity Governance (OIG) is a unified Identity and Access Management (IAM) and governance solution that simplifies access fulfillment and entitlement management across the entire identity lifecycle. It helps governance, risk, and compliance teams improve their security posture and mitigate modern risks.

OIG is comprised of three core products that work together to provide a holistic solution:

- **Okta Lifecycle Management (LCM):** Automates user provisioning and de-provisioning, ensuring that access is granted, updated, or revoked automatically as employees join, move, or leave the company. This prevents orphaned accounts and reduces the organization's attack surface. LCM works with HR systems, Active Directory, and LDAP to maintain a single, accurate source of identity data.
- **Okta Workflows:** Provides a no-code platform for automating complex and unique identity governance processes. Using simple "if-this-then-that" logic, pre-built connectors, and API access, you can create custom solutions without writing a single line of code.
- **Okta Access Governance (OAG):** A central component of OIG that provides centralized control over access management. OAG ensures the right people have the right access to the right resources at the right time.

Key Features of Okta Access Governance

- **Access Request:** Users can easily request access to applications and resources through a self-service portal. Requests are automatically routed for approval, and access is provisioned efficiently.
- **Access Certification:** Streamline audit campaigns to periodically review user access to critical resources. This prevents "access creep," enforces the principle of least privilege, and provides a clear audit trail.
- **Entitlement Management:** Discover, manage, and assign granular entitlements using attribute-based access control (ABAC) policies. This ensures consistent enforcement of least privilege across an employee's lifecycle.
- **Disconnected Applications:** Import entitlements from applications without native integrations, enabling them to be included in certification campaigns and Separation of Duties (SoD) rules.
- **Separation of Duties (SoD):** Proactively prevent toxic combinations of access, detect them as they arise, and use reporting and certification campaigns to mitigate their impact.
- **Out-of-the-Box Reporting:** Generate comprehensive reports for audit and compliance demands. Access governance data is retained for three years, simplifying thorough audits.

Unlike traditional Identity Governance and Administration (IGA) solutions that often rely on complex and costly custom integrations, Okta's unified approach to identity, access, and governance delivers a holistic improvement to an organization's security posture and operational efficiency. For instance, by integrating Okta with existing HR systems and directories, organizations can centrally manage access. Furthermore, OIG enables proactive security measures: if Okta detects unusual activity via ThreatInsight or a lifecycle status

change, automated certification campaigns can be triggered to immediately review and potentially suspend access to sensitive resources.

Okta Identity Governance vs Legacy IGA

OIG distinguishes itself from traditional IGA vendors through several key aspects:

1. **Unified Identity Platform**
    - Comprehensive Identity Governance: Okta's governance capabilities are built on the proven foundation of Lifecycle Management (LCM), which has been trusted by thousands of organizations for over a decade to automate provisioning, deprovisioning, and access management at scale. Okta Identity Governance (OIG) builds on that success with modern capabilities—like access requests, certifications, entitlement management, policy enforcement, and Separation of Duties (SoD)—all delivered natively within the Okta platform. The result is a unified, easy-to-deploy solution that accelerates time-to-value without the complexity of legacy IGA tools.
    - Flexible Workflow Orchestration: A no-code, integrated approach to automating identity workflows across the entire lifecycle—before, during, and after access is granted. Okta Workflows, included with OIG, empowers organizations to drive powerful, enterprise-wide security outcomes, such as enforcing Zero Standing Privilege, adapting quickly to M&A activity, and ensuring consistent access policies. Built into the Okta platform, orchestration eliminates the need for point solutions or professional services.
    - Extensive Integration Ecosystem: Okta Identity Governance (OIG) is built on the industry's most extensive integration ecosystem—spanning infrastructure (IaaS and on-prem servers), applications (SaaS and on-prem), and APIs (public and private). This deep integration fabric ensures every identity—human or non-human—is governable from a single platform. By eliminating identity silos, OIG enables consistent policy enforcement, comprehensive access visibility, and true end-to-end security across your entire environment.
2. **Focus on Agility and Time-to-Value:**
    - Faster Deployment and Implementation: Being a SaaS solution, OIG typically offers faster deployment times compared to traditional on-premises IGA systems that require significant infrastructure setup and configuration. With 800+ SCIM Integrations spanning SaaS and On-prem applications, customers can get up and running, integrating applications within days, as opposed to months.

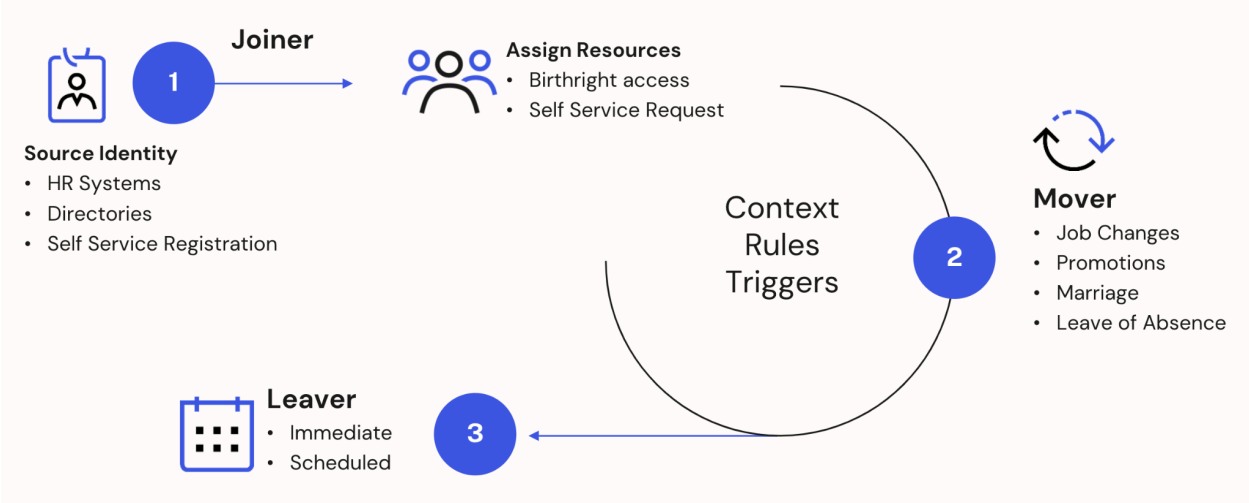
- No-Code/Low-Code Automation: Okta Workflows, a core component of OIG, enables the automation of complex identity processes without requiring extensive coding. This empowers a wider range of users to build and manage governance workflows, increasing agility and reducing reliance on specialized developers. Traditional IGA often requires significant custom coding for process automation.
- Extensive Pre-built Integrations: Okta boasts a vast library of 800+ pre-built connectors (OIN - Okta Integration Network) for various applications and systems, simplifying integration and reducing the need for custom development including both Cloud and On-Prem integrations that are out of the box. More than 400+ applications are Entitlement aware by default - which is the broadest set of integrations offered by any governance vendor in the market

3. **Enhanced Security Posture:**
    - Enforce Least Privileged with Real-time Risk Detection and Response: Integration with other Okta security features like Okta Identity Threat Protection and Okta ThreatInsight allows OIG to leverage real-time risk signals. For example, unusual login activity detected from a third party solution, like Crowdstroke can trigger automated access certification reviews or immediate suspension of access, providing a more proactive security approach. Traditional IGA often operates in a more reactive, periodic review cycle.
    - Attribute-Based Access Control (ABAC): OIG's Entitlement Management capabilities heavily leverage ABAC policies, enabling fine-grained access control based on user and resource attributes. This allows for more dynamic and context-aware access decisions compared to traditional role-based access control (RBAC) prevalent in many legacy IGA systems.
4. **Cost Efficiency:**
    - SaaS Model Benefits: The subscription-based SaaS model of OIG can offer more predictable costs compared to the significant upfront investment and ongoing maintenance associated with traditional IGA software.
    - Streamlined Operations: Automation through Workflows and easier integrations can lead to reduced administrative overhead and improved IT efficiency, contributing to cost savings.
    - SaaS License Optimization: OIG can help organizations gain better visibility into application usage and identify inactive licenses, leading to potential cost savings in SaaS subscriptions.

In summary, OIG differentiates itself by offering a modern, unified, agile, and security-focused approach to identity governance, leveraging the benefits of the cloud and tight integration with a comprehensive identity platform. This contrasts with traditional IGA vendors that often provide complex, on-premises-centric solutions with longer deployment times and greater reliance on custom integrations and coding.

Lifecycle Management

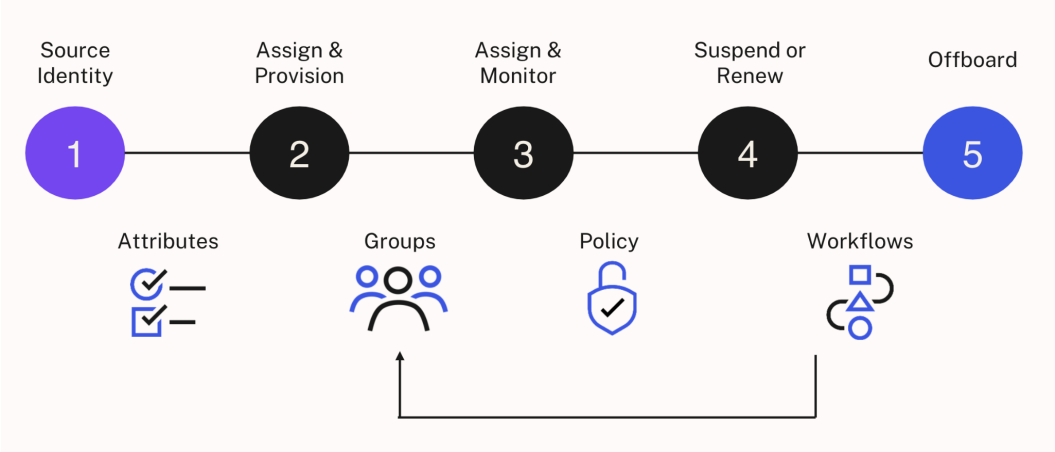
Efficient identity lifecycle management is the absolute foundation to IT. It drives who has access to what—everything else proceeds from there. VPN access, MFA policy, BYOD policy, and application access entitlements all depend on the foundation of user lifecycle management. To achieve full adoption of provisioning, organizations have to solve lifecycle management.



Okta Lifecycle Management is a cloud-based identity lifecycle automation product that increases IT processes efficiency and streamlines access decisions. Unlike traditional IGA systems, Okta Lifecycle Management is integrated, has built-in best practices for automation, frictionless and intuitive user experience, and extensibility to any application on any device. Okta Lifecycle Management has extensible pre-integrated provisioning to applications, a directory that is built for integration, a lifecycle orchestration engine with workflows and policies, and access governance reporting.

Okta Lifecycle Management centralizes and automates lifecycle management across all apps on-premises and in the cloud. Users and their devices get instant access to the applications they need, for not a minute longer than they need, while the IT team saves significant management costs.

Lifecycle Management collects all information about a user, including their job title, the groups they belong to, which devices they own, and more from AD, HR, CRM, or ERP systems. Most importantly, the directory is lifecycle aware—a user can be staged, activated, suspended, deactivated, and deleted, based on lifecycle state change events. IT teams can create a self-service flow that sends an app access request directly to the application business owner, like a Sales Director managing Salesforce, who has the best idea of what access level is appropriate. The ticket never touches the IT helpdesk.



Lifecycle Management Benefits

- **Automates Access Decisions and Prevents Errors.** New employees get secure access on day one, employees who leave lose access immediately.
- **Automate Account Creation and Changes.** Save an average of 30 minutes of IT admin time, on average, per provisioning request.
- **Maintain One Source of Truth for Users, Groups, and Devices.** Eliminates additional user stores. Enables users to be sourced in different sources (e.g. HR systems – see graphic below).
- **Prevent Errors in User Access Rights.** Avoid unnecessary costs of preparing for audits and unforeseen security breaches.

Okta provides the following capabilities for identity lifecycle management:

- **Pre-Integrated Provisioning:** Okta supports over 500 pre-integrated applications for provisioning and deprovisioning. Real-time user provisioning can be triggered by HR systems or applications including Workday, UltiPro, BambooHR, SuccessFactors, G Suite and Netsuite. Okta integrates with Active Directory or LDAP to allow rich management of profiles, groups and roles. It automatically detects different users' attributes in different applications, along with application entitlements. With Okta

API, SDKs and SCIM, you can further customize and automate provisioning for custom applications.

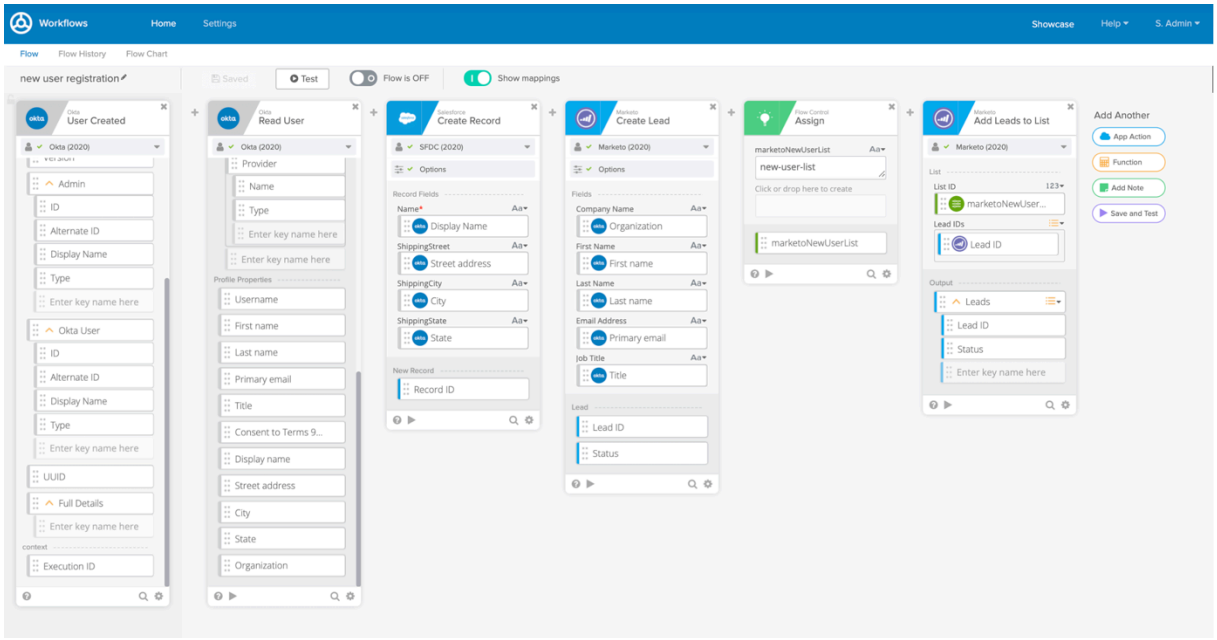
- **Universal Directory:** Okta provides an extensible, customizable directory for users, groups and devices The Meta-Directory features smart group rules to automatically group users based on attributes. It allows custom attribute mapping and transformation and can sync identities from multiple authoritative integration sources such as AD, LDAP, HR System, and systems that support OIDC and SAML.
- **Prescriptive Lifecycle Orchestration:** The lifecycle engine allows provision app access and provisioning tied to lifecycle states. It can centrally manage entitlements, accounts and groups based on rules and policies. IT workflows automate lifecycle-related tasks such as access request, deprovisioning, and user imports with conditions & actions structure. Integration to ITSM ticketing and orchestration engines are also available via API.

Workflows

Okta Workflows is a no-code automation and orchestration platform that enables admins to modernize ever-more-sophisticated identity-centric processes without leaning on developers. Workflows can be used to augment Lifecycle Management and provide custom logic for organization-specific use cases. It provides a graphical drag-and-drop interface that combines triggers, logic, and time-based actions to build powerful “if-this-then-that” flows. As a result, anyone can easily stitch together app-specific provisioning and deprovisioning tasks.

For instance, with Okta Workflows, you can leverage Okta’s library of pre-built connectors for apps like Box, Slack, Salesforce, and more (or connect via public APIs) to tailor processes with deeper actions that meet your precise requirements. With out-of-the-box functions for flow control, branching, and data manipulation, Okta offers the power of code without code, and it is finally possible to orchestrate identity tasks that were previously just too hard to automate. By having this capability built-in to your identity architecture, your team will increase agility and decrease costs, all while facilitating constant business change and improving your company’s security posture.

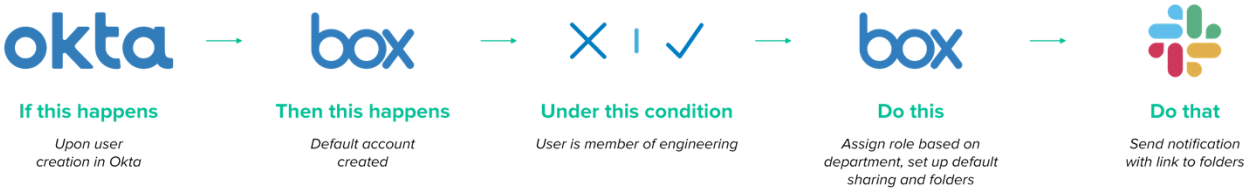
Okta Workflows' graphical interface makes automating business processes - like deprovisioning a user and transferring their files - quite simple. Use our library of connectors that includes Box, Slack, Salesforce, and more, or call APIs to customize your workflow.



Sample Workflows

Here are some examples that might be relevant to your organization of what you can do with Okta Workflows:

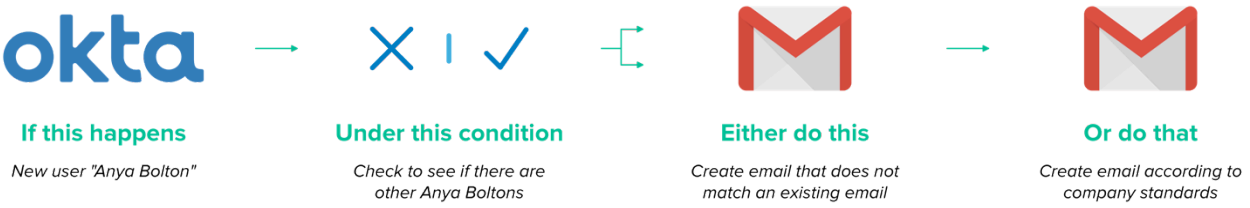
- **Granular actions during onboarding and offboarding** - Add user roles and permissions during account creation or convert licenses from paid to free after account deactivation.
- **Enhance provisioning** - Create a personal Box folder for a newly provisioned employee and add them to Slack rooms relevant to their role and function.
- **Deepen deprovisioning** - Transfer a deprovisioned employee's Box files and Salesforce contacts to a manager.
- **Nudge the right people to act** -Notify managers, IT, or app owners after an account is deprovisioned or if an error occurs, so they can take further action.



- Define identity processes based on time and context - Grant provisional access, pause processes, or make actions dependent on specific attributes, such as role or team membership.

- **Allow conditional access** - Only grant access after checking a third-party system to see if a user has the correct set of permissions.
- **Give granular permissions** - Revoke access to core business applications and files, while maintaining access to other services, like payroll information.
- **Grant time-bound access** - If a user is inactive for 30 days, send an email warning. If there's no activity within 24 hours, deactivate the account.

- **Resolve identity creation conflicts** - Catch and fix conflicts during identity creation, such as duplicate usernames or emails.
- **Clean up messiness during account creation** -Create unique identities and resolve user attribute conflicts during creation and import processes.
- **Simplify email address creation at scale** - Automatically create valid email addresses for users with identical names and strip unsupported characters, like accents.



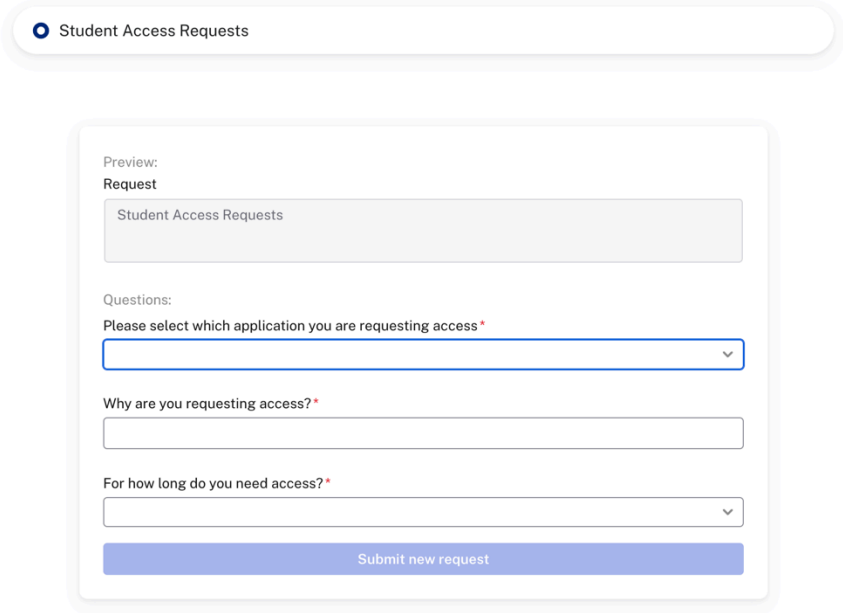
- **Distill and share important data quickly** - Automatically create tables based on changes in user lifecycle states, and then share them across your organization on a regular schedule.
- **Send critical data to the right team** - Automatically create a table of deactivated contractors and email it to the compliance team on the first of every month.
- **Regularly call out to a third-party system** -Get a weekly report of all users who have not signed into Salesforce in the last month.

Access Governance

Okta's Access Governance solution simplifies access management tasks so administrators can make sure the right people have access to the right resources when they need them. Access Governance includes three key features: Access Request, Access Certification, and Governance Reports.

Access Request

Okta Identity Governance automates and simplifies the access request process by enabling users to request access to applications or roles using Okta's self-service Access Request Portal or through integrated productivity applications, such as Slack and Microsoft Teams. User requests are automatically routed to one or more approvers for action.



Unlike many traditional IGA solutions, organization Okta administrators have full control over their Access Request configuration. Okta's Access Request Portal, accessible through the Admin Console, includes a user-friendly, no-code interface for administrators to configure access request flows. For example, users can be required to specify an access timeframe and/or provide a justification message for approvers. Administrators can also configure self-service request flows based on the resource and various levels of approvals as well as trigger actions such as sending notifications to different approvers/access requestors or creating a Jira/ServiceNow ticket for additional visibility.

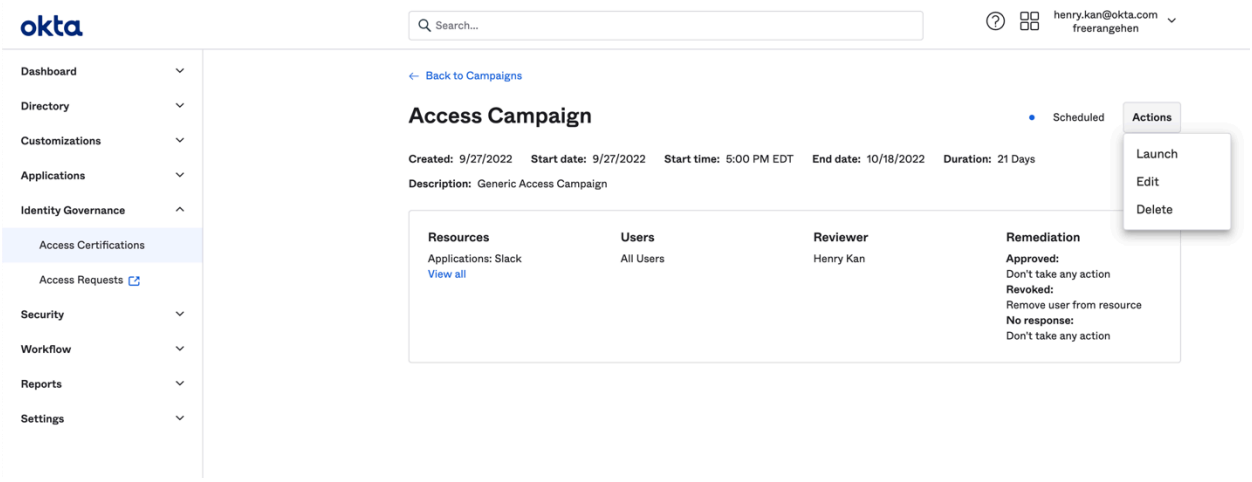
Okta's access request functionality can be integrated with productivity tools such as Slack and Microsoft Teams to support the same access request/review/approval workflow in a simplified, consolidated manner.

Access Certification

Okta's Identity Governance solution (OIG) includes a robust access certification capability that enables organizations to create audit campaigns to review users' access to resources and approve or revoke access automatically when required. Okta supports both scheduled and ad hoc certification campaigns that can include one or many applications/resources or one/many Okta groups. This means you can also run certifications at the role level through Okta's certification functionality.

The configuration UI is designed to be intuitive, enabling non-technical administrators to manage campaigns. Through the Admin Console, administrators can:

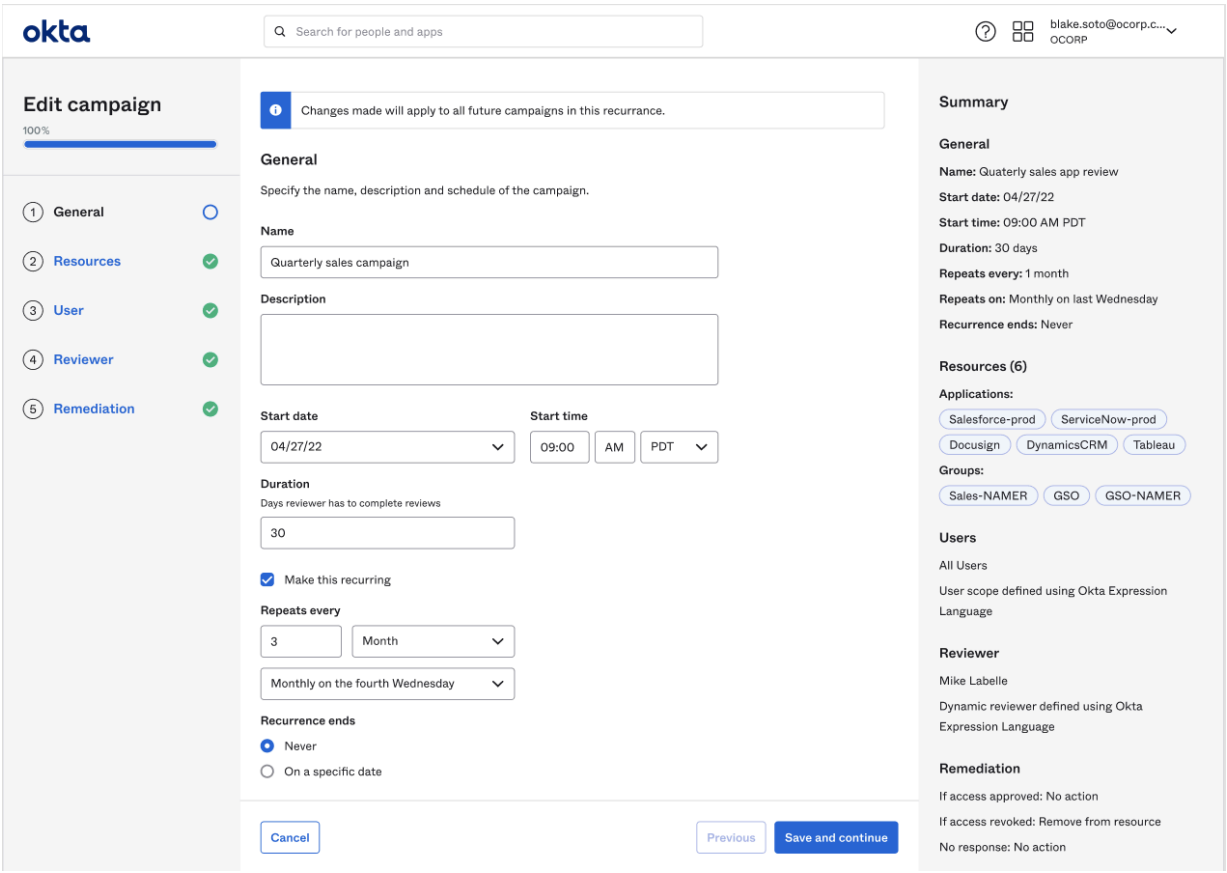
- Set user exclusion criteria; assign a static/dynamic and a fallback reviewer to remediate any potential issues with the certification campaign
- Configure additional scoping for users and reviewers using Okta Expression Language (e.g., all users assigned to those resources or filtered users using their job title, department, or any other user profile attribute)
- Preview the certification campaign before launching it
- Schedule certification notifications for assignments, reminders, and campaign end activities



The certification remediation workflow can remove access to a resource or group and automatically trigger other operations, including customized Workflows to meet more complex remediation requirements. Workflows can also be called following the start or finish of certification campaigns due to Okta's tight integration between the two modules. Administrators can also view previously closed campaigns and generate custom reports based on the campaign as the certification results are stored directly in the Okta Identity Cloud.

For each campaign, administrators can specify the:

- Start date, duration, and recurrence of the campaign
- Resources (apps or groups) that should be included or excluded in the review
- Users or teams that should be included in the campaign
- Reviewers who should review the access for each user and resource
- Revocation actions taken for remediation attempts



Governance Reports

Enhanced governance reports provided through Okta Identity Governance include:

Entitlements and Access Reports (User App Access, Group Membership, User Accounts, Past Access Requests): comprehensive auditor views of access requests and certifications. Organizations can:

- Monitor the activity and security of the organization
- Manage user access and assignment to resources
- Validate user account status
- Review high level activity on completed Access Request tickets

Access Certification Campaigns Reports (Past Campaign Summary, Past Campaign Details): attestation reports to audit the history, outcome, details, and past access requests within an organization. Organizations can:

- Obtain a high-level overview of past certification campaigns, including their duration and resources included
- See details of past resource access requests and campaigns, including users involved and remediation status
- Meet audit and compliance requirements for attestation campaigns

Application Access Audit Reports (Current Assignments, Recent Unassignments): provide audit history at the application level as opposed to the user level. This report can be used to view current assignments to a specific application(s) or recent unassignments.

Deprovision Details Report: detailed audit information on date, user, application, and resolution of deprovisioning activity

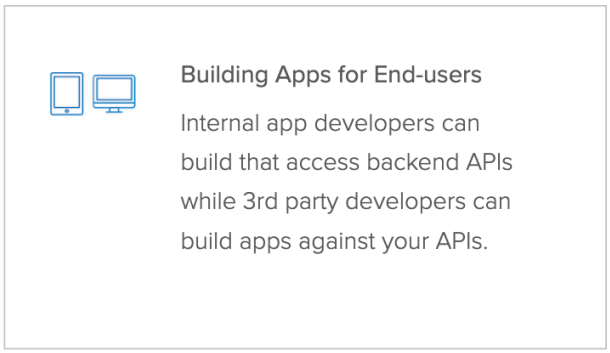
API Access Management

Custom apps are increasingly modern with an API backend. Secure enterprise data and enable developers to focus on the user experience. Centralizing the management of your APIs makes it easier for others to consume your API resources. Using Okta's OAuth-as-a-Service feature, API Access Management, provides many benefits:

- **Create one or more Custom Authorization Servers, hosted on Okta.** Custom Authorization Servers make it easier to manage sets of API access for multiple client apps across many customer types.
- **Create custom scopes and claims.** Map your claims to the profiles in your user directory.
- **Tokens are passed instead of credentials.** In addition, the JWT tokens carry payloads for user context.
- **Stay protected with security standards compliance.**
- **Manage API access with rules.** Specifying the conditions under which actions are taken gives you precise and confident control over your APIs.
- **Control complex business requirements with polices and rules.** You control the ordering and relationships.
- **Let Okta do the work of consuming standards changes to provide more or better services.**

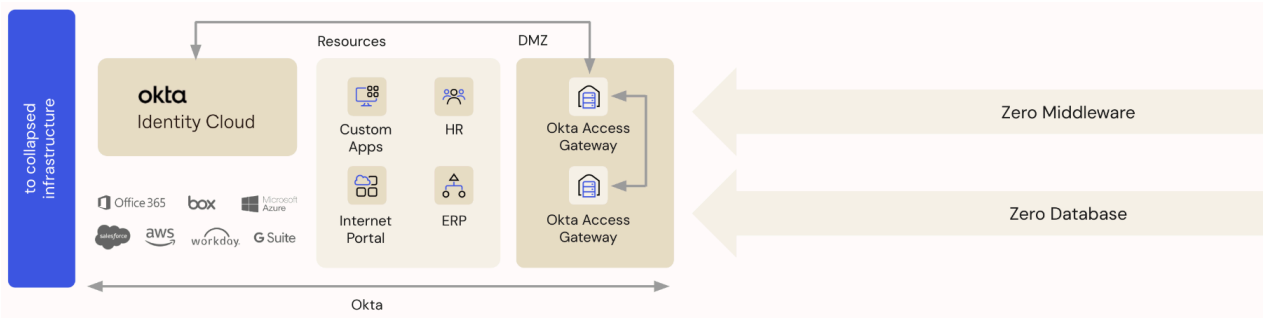
Okta API Access Management provides identity-driven authorization for any app or service, with user-friendly and centralized administration across all your APIs.

- **OAuth 2.0 API Authorization**
    - Complete standard-compliant support for OAuth 2.0
    - Proven compatibility with 3rd party API management solutions
    - Designed for modern web and mobile applications, and service-to-service scenarios
- **Flexible Identity-Driven Policy Engine for Any Type of User or Service**
    - Flexible policies that define access based on user profile, groups, network, client, and consent
    - Instant access revocation or updates to user permissions based on user profile and status



Access Gateway

With Okta Access Gateway (OAG), organizations can secure access to their on-prem apps and protect their hybrid cloud infrastructure – all without changing how existing apps work today. Okta Access Gateway enables access to on-prem and cloud apps with a single login, delivering a delightful and consistent access experience for all applications – SSO from Office 365 to eBusiness Suite, from cloud to ground.

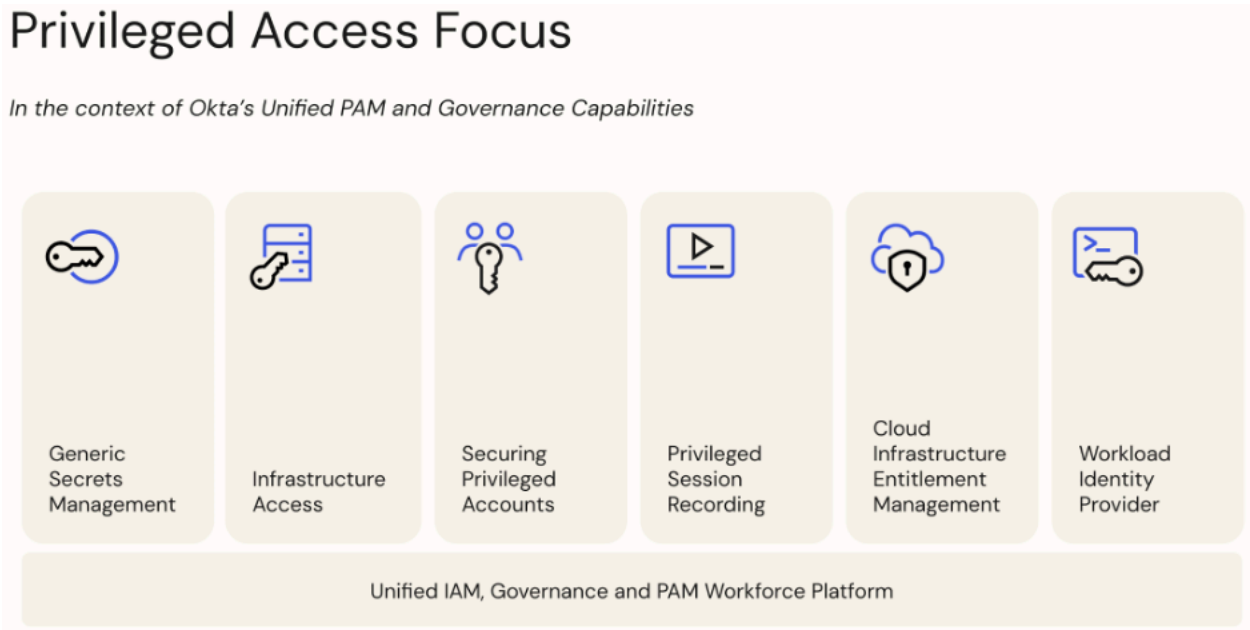


By leveraging Access Gateway, your organization's on-prem applications benefit fully from all the improvements that come from the Okta Cloud, including on-Prem Access with Adaptive MFA. Organizations can:

- Protect on-premises applications with a variety of authentication factors across usability and assurance levels.
- Implement adaptive policies and deny risk access while and rewarding users with a passwordless experience.
- Authorize Access with Granular Policies: with Okta Access Gateway, you can Authorize access based on application URLs, users, groups, and network information.
- Leverage a single identity provider to manage access policies across on-prem and cloud resources centrally.

Privileged Access Management

Okta Privileged Access (OPA) empowers teams to gain visibility, meet compliance requirements, and enforce zero standing privileges with just-in-time access for critical cloud, hybrid, and on-prem infrastructure. Unlike traditional PAM solutions, Okta Privileged Access is cloud-architected and fully integrated with Okta's unified workforce identity solution, giving organizations core IAM and governance capabilities in a single platform. This solution helps organizations maintain least privilege without relying on fragmented experiences across disparate tools.



With centralized access management, OPA provides passwordless, zero-trust access to on-prem and cloud infrastructure. It ensures critical roles can access what they need just-in-time and delivers security for an organization's most-privileged credentials —including those for local administrator accounts — with a modern cloud vault under management by Okta.

OPA automates access controls to empower ops teams to focus on infrastructure and software, not Identity and Access Management (IAM). Integrated with governance (IGA), OPA provides usability, including access requests via popular messaging tools like Slack and MS Teams. It helps maintain compliance by ensuring all shared account access is attributable individually and provides comprehensive privileged session reporting.

Some of the key features and benefits of Okta's PAM solution include:

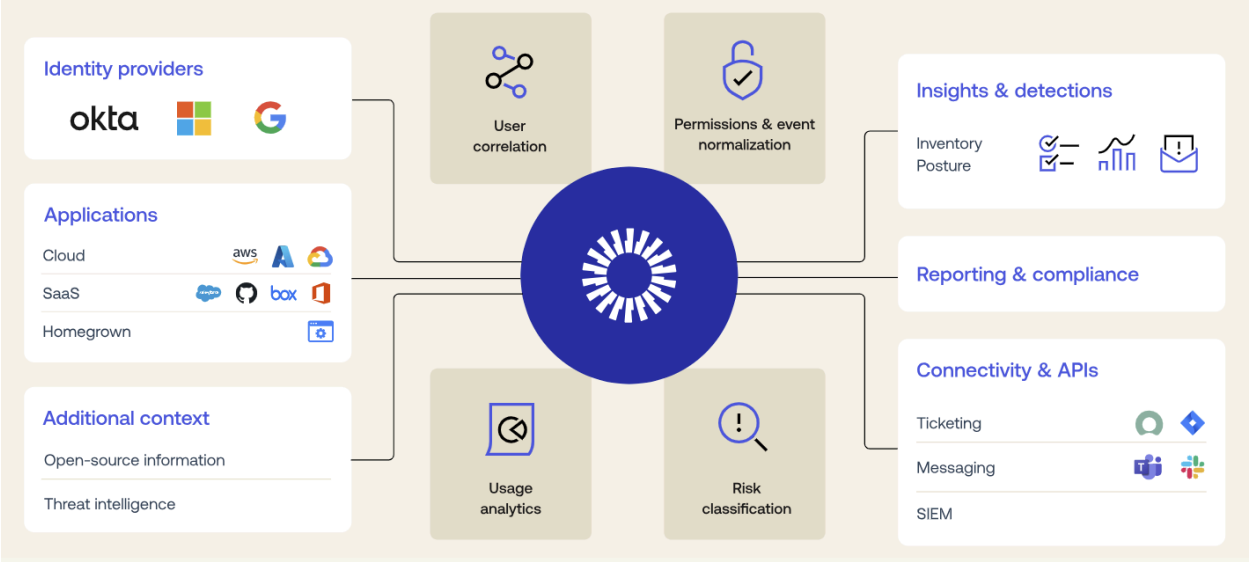
- **Converge on a single identity solution:** Eliminate disparate systems for Identity Access Management, Privileged Access Management, and Identity Governance & Administration.
- **Discover & vault passwords:** Secure, store, rotate, and manage access to privileged account passwords.
- **Maintain least privilege for highly privileged resources:** Lock down access and determine the appropriate level of privilege for important resources from one easy-to-use interface.
- **Integrated governance:** Create request types and approval workflows for privileged resources in Okta Access Requests.

- **Built-in admin separation of duties:** New Roles provide separation between users who need to administer resources, those that configure access to privileged resources, and non-administrators who can only see the resources they have access to.
- **Granular control with policies:** Define requirements for when a Request and Approval is needed before access is granted.
- **Reporting:** Privileged Access events are integrated with the Okta System Log to tie privileged access back to an individual Okta user.
- **Easy integration:** Reduce friction between security teams and developers by making it easy for developers to onboard resources and securely access privileged resources without disrupting their workflows.

Identity Security Posture Management

Okta Identity Security Posture Management (ISPM) helps customers take control of identity and access sprawl in their organization by uncovering hidden risks, prioritizing critical threats, and guiding remediation. It is a "one- stop-shop" for identifying identity risk and prioritizing it, with unparalleled contextualization capabilities that link all user accounts to their required privileges, activities, and stage in the employee lifecycle to mitigate threats and ensure compliance.

Okta's customers report that 75% of critical identity issues were resolved within several weeks following a quick deployment.



Okta ISPM allows organizations to proactively reduce their identity attack surface and improve the security of the organization:

- Uncover hidden threats and misconfiguration across identity providers, SaaS, and Cloud infrastructure (IaaS).
- Discover and prioritize vulnerabilities like MFA bypass, overprovisioned users with elevated accumulated permissions, and improper offboarding. See Supported detections.
- Enable ongoing risk-based monitoring against security, IAM, and compliance standards (such as NIST, CIS, ISO, SOX, and PCI-DSS).
- Gain actionable security insights to drive quick remediation.
- Get ongoing, continuous analysis of your identity security exposure within minutes

Identity Threat Protection

Identity Threat Protection (ITP) with Okta AI is a continuous identity threat solution designed to protect organizations from identity-based attacks, such as phishing, session hijacking, and credential stuffing. ITP combines existing identity security solutions like ThreatInsight, Behavior Detection, and risk-based authentication to provide comprehensive protection throughout the entire user session.

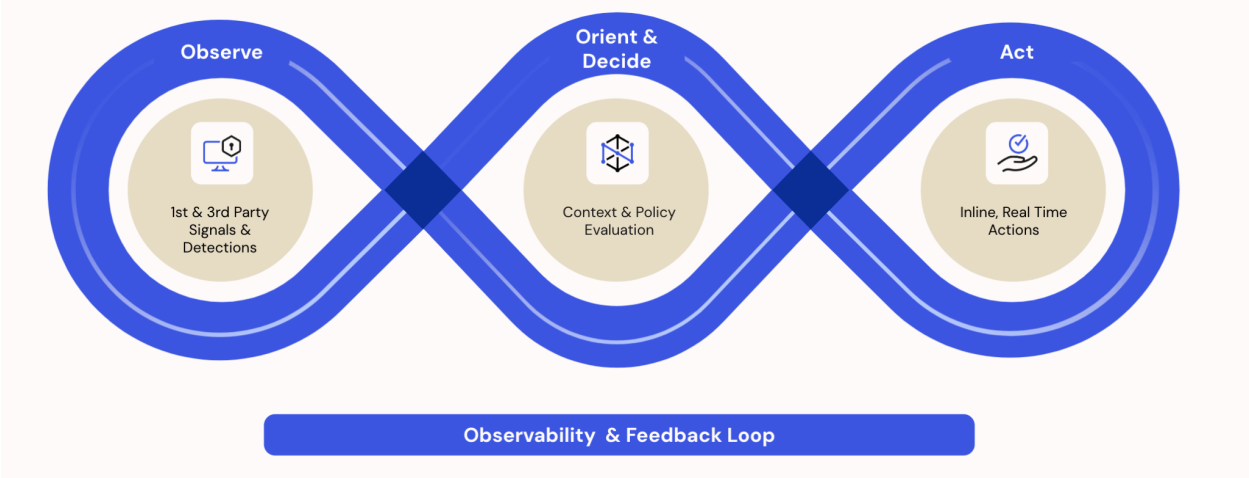
Unlike traditional security measures that only evaluate identity threats during sign-in, ITP continuously monitors users' sessions, risk levels, and behaviors in real time. It evaluates factors such as network zones, devices, and changes in user behavior. When potential threats are detected, automated mitigation actions, such as terminating sessions or prompting for multi-factor authentication (MFA), are triggered.

ITP integrates with Okta Verify and other endpoint detection systems to gather additional security signals, ensuring real-time threat detection. The Shared Signals Framework (SSF) allows organizations to configure integrations with third-party security event providers to receive even more risk data, enhancing protection.

Key features include session protection, automated threat remediation, and universal logout, which allows administrators to immediately terminate sessions across all supported

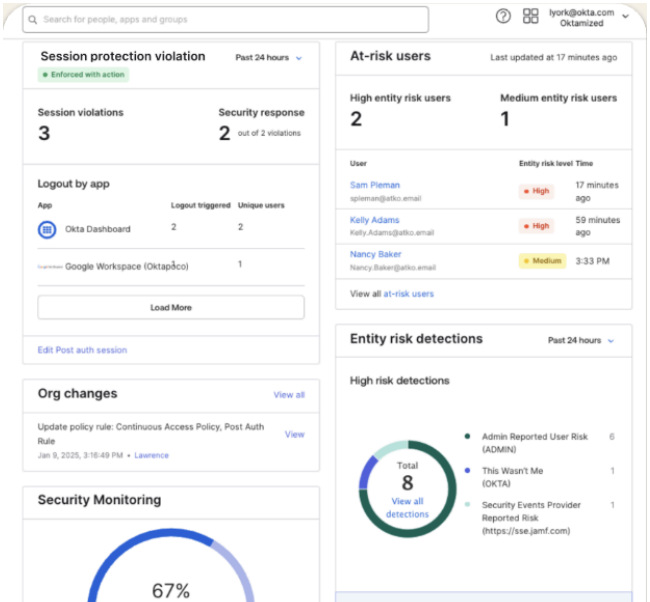
apps and devices. The system also provides detailed monitoring and reporting tools, giving organizations insights into their security posture and potential risks.

By using a Zero Trust approach, ITP ensures that user sessions are continuously evaluated, and risks are proactively addressed, significantly enhancing the security of your organization.



ITP will provide your organisation with these important security features:

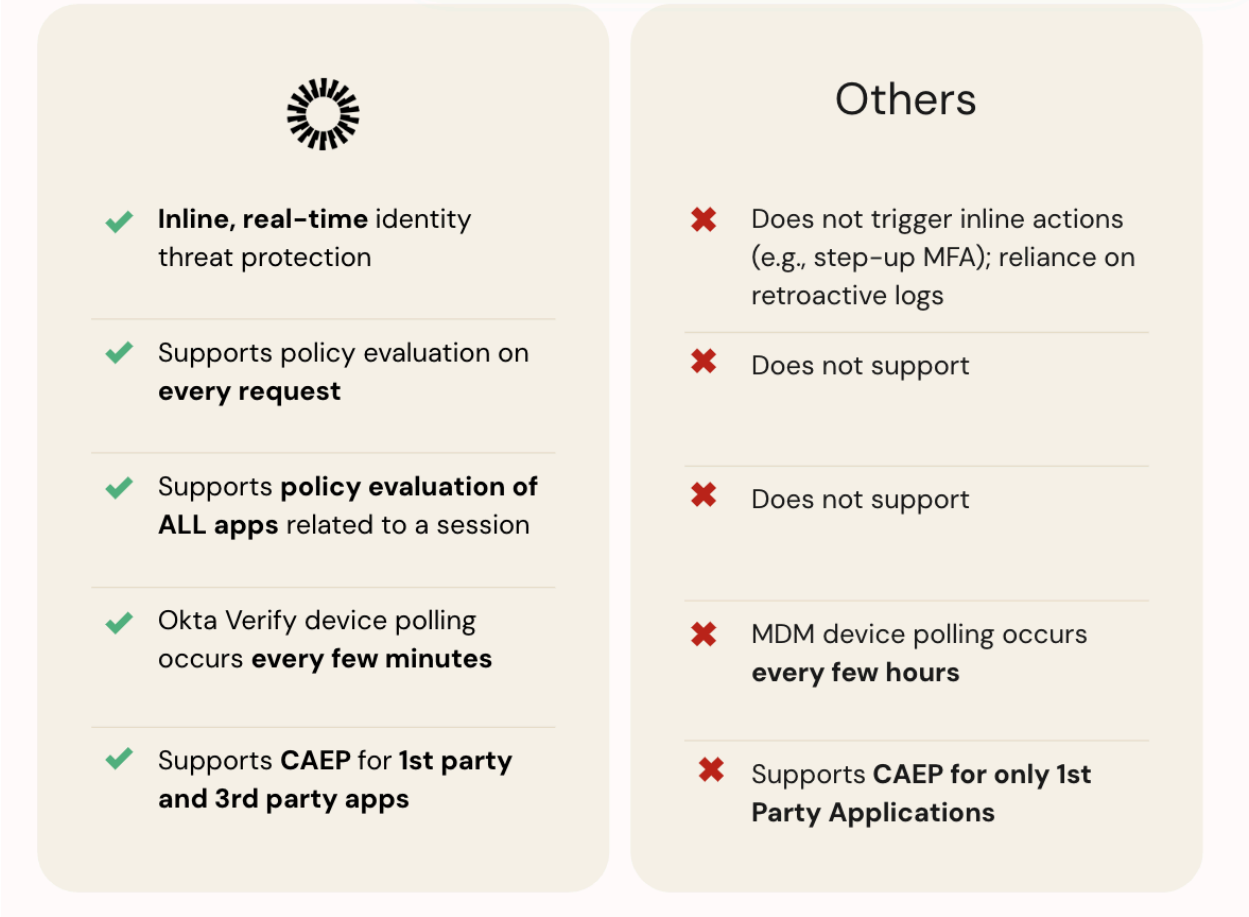
- **Post auth session and risk evaluation:** ITP continuously evaluates your global session, authentication, and entity risk policies to identify risks that occur during an active session, and not just when users sign in. The Shared Signals Framework (SSF) enables continuous access monitoring even when the user isn't interacting with Okta.
- **Diverse risk signals:** ITP evaluates risk signals that Okta identifies and signals that your security providers identify. Orgs can analyze risk signals from multiple sources to increase their protection against identity threats. By using security providers, you can choose the best options for your unique security needs.
- **Automated threat remediation:** ITP continuously assesses policy criteria to drive actions like terminating a session or prompting users for MFA. It can also initiate flexible Workflows to impose read-only access based on changes in identity, device context, or entity risk, or launch an incident



management process to quarantine the user, device, or app.

- **Universal Logout:** You can instantly terminate sessions across all supported apps and devices, ensuring comprehensive security during threats or employee lifecycle management.
- **User risk insights:** Dashboard widgets, entity risk levels, and reports allow you to view your org's overall security landscape at a glance.

Now that we've seen how Identity Threat Protection works, let's look at what sets Okta apart:

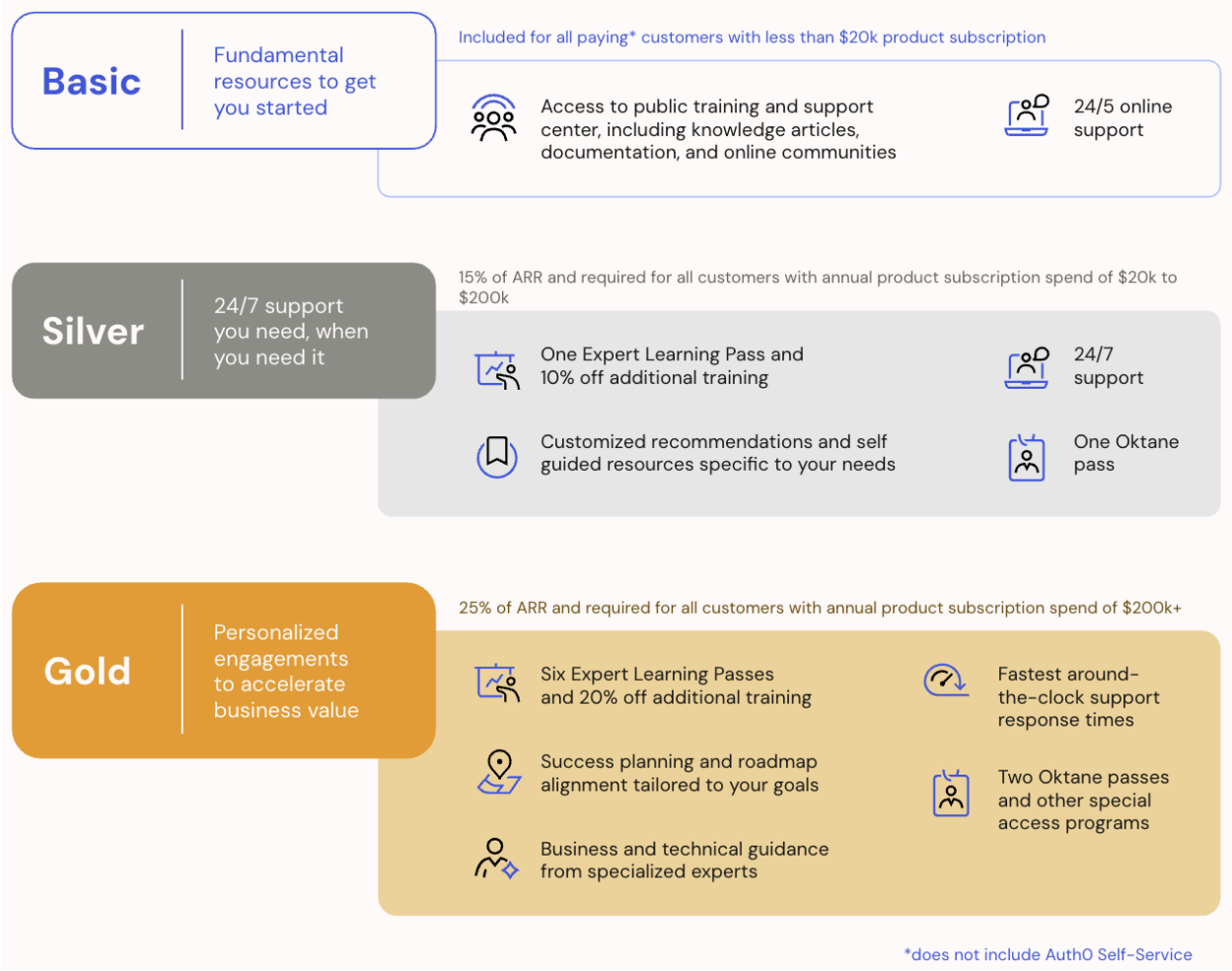


Learn more: https://help.okta.com/oie/en-us/content/topics/itp/overview.htm

Customer Success and Implementation Services

Customer Success

Okta has a complete customer support structure in place that includes 24x7x365 options, a 99.99% guaranteed uptime SLA, phone and online support. Our packages include Basic, Silver, and Gold. Additional information about Okta's support packages can be found here: https://www.okta.com/services/success-and-support/



Implementation Services

Okta's Professional Services team comprises experienced consultants with many years of IAM background. A team of consultants will be assigned to guide you through planning, configuration, testing & implementation. For larger or complex implementations, Okta Professional Services offers our customers Identity Enablement & Advisory Services, to proactively mitigate operational & functional program risk. On-demand training videos, live instructor-led webinars, and other knowledge assets are available at no charge for all customers through the Okta Community. Hands-on lab courses are available for an extra fee.

It is worth noting that because Okta is a fully cloud service, our implementation fees are typically a fraction of the other vendors in the Leaders category of the Magic Quadrant. Our business is software driven and we aim to deliver as much functionality out of the box as possible, limiting the requirement for heavy customization.

Okta also has a large network of certified deployment partners. These companies range in size from small regional firms through the largest technology consulting firms in the world. All certified partners have made significant investments in training their people on how to successfully deploy Okta.

Okta provides ongoing professional services including:

- **Consultative services** to assist customers with strategic direction, reference architecture, and subject matter expertise on security, identity, risk, compliance, and IT service management.
- **Implementation services** available to assist customer plan, configure and deploy the Okta service.
- **Identity Enablement & Advisory Services** to assist our customers in optimizing their Identity Investment by showing how technology capabilities enable their organizational objectives with a multi-year, actionable, decision-centric roadmap.
- **Major tasks** such as user deployment, application configuration, application integration, Active Directory integration.

Social and Environmental Responsibility

We believe Okta has a long-term responsibility to maximize benefits to our society, the environment, and all of our stakeholders, including our employees, customers, and communities. We take that responsibility seriously, and we'll lead Okta with the conviction that how we build the future is as important as what we build.

In May 2020, we launched our Sustainability & Responsible Technology Program. Our sustainability efforts are led by our executive leadership team and are reviewed by the Nominating and Corporate Governance Committee of our Board of Directors.

Our commitment to integrating ethical practices and sustainable operations into our business model, creating value for both stakeholders and society, is comprehensively detailed in Okta's Sustainability Fact Sheet. This report highlights our achievements and commitments in several key areas:

- **Protecting Customers:** Okta maintains robust security through significant investments, infrastructure hardening, and adherence to various industry certifications (ISO/IEC 27001, SOC 1 Type II, SOC 2 Type II, SOC 3, FedRAMP, PCI DSS, BSI-C5, ENS High, HDX, IRAP, TISAX) and data privacy regulations. Ethical business practices are reinforced through company policies and our Code of Conduct.
- **Investing in People:** Talent, Connection, and Community is a core philosophy integrated into operational practices and employee programs, with transparent data provided. Okta signed the #EqualPayCA pledge and achieved 78% employee engagement favorability in FY2025.
- **Workforce training and development**: Okta aims to empower employees and foster a culture that focuses on engagement, performance, recognition, and development. In FY2025, Okta employees completed nearly 55,000 hours of training.
- **Environmental Training**: Okta provides employees with annual sustainability updates and training through company-wide all-hands meetings, internal education opportunities, and webinars during the annual Earth Week celebration. Okta helps customers meet their climate goals; Okta's own emission-reduction efforts (like energy efficiency and renewable energy) directly reduce their customers' Scope 3 (value chain) emissions.
- **Supporting Communities:** Okta announced a partnership with CodePath to create an open-source cybersecurity lab. This lab aims to train 3,000 students annually using simulated, real-world scenarios for identifying and addressing cyber threats. Okta funded the launch of Canada's first university-based cybersecurity clinic at Toronto Metropolitan University. This clinic will offer free cybersecurity services to

nonprofits and provide students with vital hands-on experience. For more information, see the Okta for Good Impact Report.

- **Health, Safety, and Wellbeing:** Okta ensures a safe working environment and offers inclusive benefits including gender-neutral parental leave, global family-forming benefits, and mental health support.
- **Human Rights**: Okta established our Responsible AI Principles and shared our approach to Responsible AI Innovation. We launched a human rights webpage sharing our commitment and related policies. Okta conducted human rights due diligence through a supply chain risk assessment.
- **Committing to Sustainability:** In FY2025, Okta launched its first Environmental Policy, showcasing our commitment to the environment. Okta aims for 100% renewable energy and has validated science-based targets (SBTs) to reduce GHG emissions by 67% (Scope 1 & 2) and 42% (Scope 3 business travel/commuting) by FY2030.
- **EcoVadis- Third party certification**: Okta scored 60 on the EcoVadis Sustainability Assessment and achieved the "Committed" badge.. EcoVadis analyzes a supplier's sustainability performance into a standardized, credible, and globally recognized metric. Okta's EcoVadis scorecard can be requested within the EcoVadis portal.

More info can be found here: https://www.okta.com/responsibility/