A Comprehensive Guide for Your Workforce Identity Maturity Journey

An extensive roadmap for raising productivity, increasing efficiency, and strengthening security through Identity

Table of contents

Introduction: Identity Enables Business Priorities

While previously regarded as only a utility service managing usernames and passwords, Identity has become both a necessity for, and an enabler of, any modern business.

In the context of organizations, a mature workforce Identity infrastructure:

- Enables employees, contractors, and business partners to work from anywhere with seamless and secure access to critical tools and resources;
- Strengthens the organization's overall security posture;
- Provides a convenient user experience that frees up time and energy to focus on growth, innovation, and other priorities;
- Enables the organization to scale and improves its agility;
- Increases operational efficiencies and decreases administrative burdens; and
- Supports governance, risk management, and compliance (GRC) initiatives by meeting the stringent Identity requirements included within many regulations, standards, and frameworks.

Securing Identity is a foundational element of a strong security posture — one that can help combat abuse from insider threats and intruders abusing stolen credentials.

In their 2022 Trends in Securing Digital Identities report, based on a survey of more than 500 IAM or security professionals, the Identity Defined Security Alliance (of which Okta is a member) revealed that:

- 84% of respondents said their company experienced an Identity-related breach in the previous year;
- 78% cited direct business impacts resulting from a breach; and
- 64% indicated that effectively managing and securing digital Identities is either the top security priority (16%) or a top-3 priority (48%).

The Identity management and access control imperative

Today's organizations require a holistic, integrated approach to Identity management. One that not only allows governance to play a crucial and connected role with access management, but that also helps to strengthen security posture, mitigate modern risks, improve efficiency, and even enhance overall productivity.

Learn how Okta can help

Modernizing Workforce Identity

The maturation journey from basic functions to an optimized Identity infrastructure is rarely straight or narrow, and it can be difficult to know where to start — and where you're going.

Based upon lessons learned from the most successful practices across thousands of Okta customers, and observations of different patterns these customers exhibit, Okta's Workforce Identity Maturity Model aims to empower organizations to:

- Assess the relative state of their Workforce Identity posture;
- Identify and implement new capabilities that will aid in the organization's maturation; and
- Measure the impact and outcomes of Identity initiatives as they progress along the maturation journey.

Estimate the potential IT and security savings of a workforce Identity solution

Determine your savings

Assessing workforce Identity maturity and evaluating success

The first step on the workforce Identity maturation journey is to conduct a thorough and realistic assessment of your company's existing approach, including key capabilities and challenges. To enable this evaluation, we recommend considering five critical categories: agility, experience, security, reliability, and strategy, described in Table 1.

And as you journey through the four stages of maturity, it's important to think about how your organization is investing in key business outcomes. By consistently measuring key performance indicators (KPIs), such as the ones presented in Table 1, you'll be able to show progress and secure additional organizational buy-in.

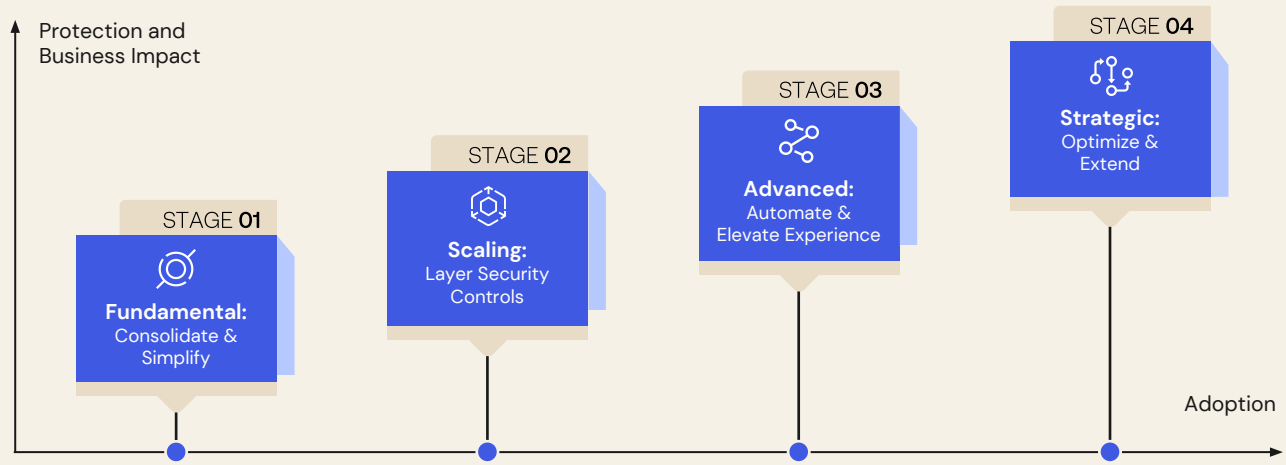

Table 1: To enable evaluation of Workforce Identity initiatives, we recommend a category-based approach

Category	Description	Key Metrics for Evaluating Identity Success
Agility	**Ability to develop, deploy, and manage Identity-related services and flows** (e.g., modern IAM access across the tech stack, fast implementation and adoption of new applications, centralized administration console, efficient lifecycle management, etc.)	• IT FTE hours dedicated to Identity administration and support • Time to adopt and deploy applications • Cost or time spent maintaining Identity infrastructure • Help Desk tickets related to access issues or requests for applications
Experience	**Ability to deliver effective, desirable, and convenient experiences to end-users** (e.g., seamless remote access, use of 'birthright' applications on day 1, self-service options for requesters and reviewers, etc.)	• Employee satisfaction scores • Time spent logging in or responding to step-up authentication prompts • Time spent waiting for access to new applications, or being onboarded
Security & Governance	**Ability to proactively and effectively mitigate and remediate security risk and incidents and support regulatory compliance** (e.g., enabling secure access and governance across the whole workforce, implementation of Zero Trust practices, contextual insight and intelligence, etc.)	• Number of Identity-related security issues • Time to detect and respond to Identity-related security issues • Time spent on audit, and compliance related reporting • Employee adoption of advanced authentication
Reliability	**Ability to provide a resilient, high-performing, and future-ready Identity service at any scale** (e.g., avoidance of outages, dynamic scaling, etc.)	• Average frequency and duration of unplanned downtime per month • Number of performance incidents that impact workforce productivity
Strategy	**Ability to plan and deliver holistically, intelligently, and with a focus on innovation** (e.g., organization-wide strategy, alignment with business needs, sufficient funding to execute, quantified measurements, etc.)	• Annual investment in Identity-related technologies • Term of fully-funded Identity program • Identity service ROI and TCO

STAGE 1

Fundamental: Consolidate and Simplify

Start looking at Identity as an interconnected and foundational system, rather than a collection of discrete utilities and functions

Organizations at the beginning of their workforce Identity journey are typified by disconnected, ad hoc solutions that were implemented to address specific issues — but which had the unintended consequence of expanding the threat surface and contributing to directory sprawl.

In many cases, these solutions have limited or cumbersome integrations with each other or other systems, and require considerable manual effort on the part of administrators.

Recognizing that managing applications and users is a time-consuming undertaking that distracts from other initiatives, and that the organization is vulnerable to Identity-based attacks, stakeholders are motivated to make a meaningful start on the Identity maturation journey.

Advanced capabilities that streamline success

Operational Efficiency: Support organizations for M&A and divestitures through a flexible universal directory.

Security: Secure a wide-range of modern and legacy access points with multi-factor authentication (MFA) including RADIUS, LDAP.

Governance: Align to FIPs requirements; Leverage a Universal Directory that will allow you to have a single source of truth for all of your Identities.

Problems to Solve

Specific issues that characterize the Fundamental stage include:

- **Fragmented user Identities:** Organizations are attempting to consolidate Identity sources (e.g., the result of introducing cloud resources, of merger and acquisition activities, of homegrown solutions, etc.), as logging into multiple tools with different credential requirements is both frustrating and time consuming for end-users. Any use of Single Sign-On (SSO) at this stage is sporadic and disparate.

- **On-premises Identity infrastructure costs:** Workforce Identities are managed on premises, with high maintenance and management costs and a dependence upon specialized expertise.

- **Password reliance:** Many applications, systems, and other resources rely on username-and-password credential pairs, providing the illusion of security while actually heightening risk and harming the user experience.

- **Limited federation:** The use of tools without modern federation limits each user's ability to access multiple applications with one single set of credentials, negatively affecting productivity while contributing to password sprawl and its associated risks.

- **No policy-based enforcement:** A lack of sufficient access conditions increases risk, as intruders or insider threats can access resources and systems.

- **Fragmented security posture and limited visibility:** An incomplete approach to security creates gaps that increase risk; at the same time, security is not yet an executive or board-level issue, and internal cyber and Identity expertise are both limited, creating additional challenges to establishing a mature Identity and security posture — as a consequence, security remains reactive and compliance is aspirational.

- **Hybrid IT infrastructures highlight Identity issues:** Hybrid infrastructure exacerbates all of the above problems and legacy Identity solutions fall short to effectively address those for a variety of reasons, such as limited support for open standards, inability to scale, a lack of out-of-the-box integrations, and more.

Actions, Business Benefits, and Security Outcomes

Actions at the Fundamental stage orient around consolidating Identity (and the tools that power it), integrating Identity systems with each other and with the wider IT stack, and implementing necessary security and governance controls.

Collectively, these activities will improve productivity by reducing friction for users, strengthen the organization's security posture, and reduce the amount of manual effort required both for day-to-day Identity activities (e.g., making and approving access requests) and for occasional large projects (e.g., a merger or acquisition).

Table 2: Stage 1 actions, business benefits, and security outcomes

Category	Actions to Take	Business Benefits & Security Outcomes
Agility	• Consolidate and synchronize user repositories across legacy directories and systems of record (e.g., using a unified, modern user directory) • Introduce a basic Identity management system for user and policy management	• Reduction in IT time spent maintaining and synchronizing user stores • Reduction in IT time spent managing user/group access • Faster time to value from M&A activity through quicker integration of users
Experience	• Deploy basic SSO and end-user authentication • Implement simple self-service functions (password recovery, etc.)	• Improvement in workforce productivity due to faster application adoption and access
Security & Governance	• Install an authorization server compliant with modern standards • Establish basic MFA and organizational unit-based access policies that reflect user group needs and network zones	• Strengthened security posture via workforce MFA adoption • Reduction in account lockout resulting from malicious attacks
Reliability	• Adopt a basic high-availability (HA) architecture (e.g., with failover, disaster recovery capabilities, SLA standards, etc.)	• Increased system uptime and availability • Reduction in workforce time spent locked out of applications and unable to access business-critical accounts
Strategy	• Create a comprehensive inventory of all on-premises and cloud applications, to guide decisions and help assess coverage • Develop an Identity business case to secure budget and executive support by tying technical use cases to business outcomes	• Increased visibility into application landscape and access rights • Identity investment ROI and expected benefits

STAGE 2

Scaling: Layer Security Controls

Prepare your organization for efficient and graceful growth by automating and consolidating key Identity functions, laying the groundwork for Passwordless and phishing resistant capabilities

With fundamental Identity functions in place, focus turns to refinements and extensions that can help the organization scale.

Typically, these initiatives emphasize productivity increases for end users and a lessening of the administrative burden that falls upon IT administrators and application owners.

Importantly, these progressive steps cannot come at the expense of the organization's security posture; fortunately, many of the same Identity capabilities that enable user productivity and administrative efficiency also reduce risk.

For large organizations that have been around for decades and built critical on-prem IT infrastructure and proprietary technology, some of which will continue to stay on-prem for the long term, extending modern Identity functions to these on-prem resources is a critical step towards enabling an optimal user experience, streamlining administrative processes, and strengthening organization's overall security posture.

Advanced capabilities that streamline success

Operational Efficiency: Extend least-privileged access and Zero Trust principles to legacy, on-prem web apps to meet data residency requirements.

Security: Secure users with adaptive policies that scale with expanding population.

Governance: Automate provisioning of users for onboarding and offboarding ensuring employees are productive day 1, and securely deactivate access upon termination.

Problems to Solve

Organizations in the Scaling stage are frequently impacted by:

- **Fragmented Identity repositories:** Workforce IAM is spread across multiple environments, with shared and duplicated users causing additional costs and user frustration.
- **Reliance on password rules:** Rules are in place for password complexity and change frequency, leading to misplaced confidence in the security posture while adding burdensome overhead to administrators; the lack of multiple additional assurance factors continues to create risk.
- **Global access policies:** A lack of granular access controls creates a permissive access environment that favors convenience over security.
- **Limited use of MFA:** With only a limited use of MFA and little (or no) established compliance baseline, there are few backstops to prevent threat actors from abusing stolen credentials; where MFA is implemented, the organization may have low enrollment and may be burdened by fallbacks to outdated methods.
- **Manual onboarding and offboarding:** Organizations struggle to manage employee application and resource access throughout the user lifecycle — e.g., onboarding (joiner), promoting/transfering (mover), and offboarding (leaver) — in a timely and policy-based manner, resulting both in approval delays that impede productivity and legacy overprovisioning that runs counter to least-privilege and compliance goals.

Actions, Business Benefits, and Security Outcomes

Actions to take at the Scaling stage address legacy systems and insufficient controls that impeded productivity, contributed to an assortment of costs (both known and hidden), and that harm the organization's ability to withstand security incidents.

Table 3: Stage 2 actions, business benefits, and security outcomes

Category	Actions to Take	Business Benefits & Security Outcomes
Agility	• Retire legacy systems, including applications that: are monolithic/siloed applications, with their own user store; are difficult/impossible to integrate (e.g., no or outdated public APIs); have no SSO/Federation capabilities; are difficult to maintain/upgrade, etc. • Partially automate user lifecycle management and provisioning (i.e., through the unified user directory)	• Reduction in IT Admin time/cost spent administering users, groups, policies, applications, and devices in separate environments • Reduction in time/cost to maintain Identity infrastructure • Reduction in Help Desk tickets related to access issues/requests • Faster provisioning / deprovisioning of users
Experience	• Extend SSO capabilities for employees, contractors, and partners with support for third-party Identity providers, and on-prem business critical applications • Launch more fully operational self-service functions such as self-enrollment	• Improvement in new employee productivity with birthright access to key applications/systems • Improvement in workforce productivity with reduced time waiting to get appropriate access to critical applications and systems
Security & Governance	• Extend MFA (with at least two factors) across applications (both on-prem and cloud), contractors, and other business partners • Consolidate security/access controls across cloud and on-prem apps • Implement role-based access control (RBAC) • Implement secure passwordless access to your cloud and on-prem applications • Take initial steps towards Zero Trust (e.g., dynamic access policies) • Introduce security and compliance audit and monitoring tools	• Reduction in time to detect and respond to malicious attacks • Increased compliance with least-privilege access related mandates (e.g., SOX) • Reduction in time/cost to prepare for audits and compliance reviews
Reliability	• Fine-tune a resilient infrastructure that scales seamlessly and dynamically without hindering reliability	• Reduction in time/cost to maintain and scale infrastructure • Reduction in outages impacting the business and workforce
Strategy	• Establish alignment and communication between business units • Perform a gap analysis to inform requirements and drive investment plans	• Increased cross functional alignment and support for Identity investments • Increased visibility into future investments requirements and budgetary needs

STAGE 3

Advanced: Automate and Elevate Experience

Leave legacy approaches behind as you increase the role of automation and extend security controls to safeguard against sophisticated threats

At this Advanced stage, organizations have a broad range of Identity systems in place, and those systems are integrated with the wider IT and security stacks. The focus continues to be on increasing efficiency, largely by automating tasks or entire processes, as well as by consolidating and deprecating legacy technologies.

From a GRC perspective, attitudes are shifting from doing things out of obligation to doing things out of a genuine motivation based upon benefits that extend well beyond compliance — including improving the organization's security posture and reducing administrative burdens.

Advanced capabilities that streamline success

Operational Efficiency: Automate sophisticated downstream provisioning and onboarding events with no-code workflows.

Security: Employ passwordless authentication using native biometrics across all major platforms for best UX; Ingest device security signals into access decisions across all managed and unmanaged devices; Easily choose phishing resistant authentication methods from those automatically suggested by the admin UI.

Governance: Automate access requests for JIT provisioning using collaboration tools like MS Teams or Slack; Improve enterprises' security posture by following principles of least privilege through recertification campaigns to provide visibility and control over who has access to which digital resources within their organization.

Problems to Solve

Although the organization is well on the workforce Identity maturation journey, a handful of problems persist:

- **Risk associated with remote workers:** Remote workforces pose greater security threats without properly enforced Identity policies, but many organizations that introduced remote working capabilities don't fully recognize the added threat vectors associated with VPNs, home networks, and unmanaged devices.
- **Contextless access policies:** Access policies are strictly based on static factors (e.g., roles, attributes, devices, networks, etc.) and ignore dynamic aspects like users' behavior and context (e.g., an impossible travel scenario), creating unnecessary friction and increasing risk.
- **Limited visibility into and tracking of access:** Adhering to the principle of least privilege and meeting governance obligations requires clear visibility into (and control over) who has access to what resources, and when, but getting and maintaining this visibility requires planning and execution, and is key to Zero Trust efforts.
- **Inefficient processes and more manual intervention than is necessary:** Process evolution often lags the introduction of new technologies, resulting in the continuation of burdensome manual activities that extend timelines and introduce the risk of human error.
- **Balancing user experience and system security:** Organizations recognize the value of both user experience and security, but continue to struggle to ensure an optimal balance between these two needs.
- **Difficulty adopting and integrating Passkeys for passwordless authentication:** Passkeys offer a promising solution but there are concerns related to their integration and adoption within multiple ecosystems, such as Apple and Google, if simultaneously used — and particularly regarding unmanaged devices.
- **Maintaining availability of secure authentication:** Advanced authentication measures like MFA and passwordless are dependent upon additional system components (such as additional IDPs or directories, on-premise RADIUS servers, or on-premise certificate services), and a failure of these components may render the larger functions unavailable — organizations need to ensure that there is redundant infrastructure in place.

Actions, Business Benefits, and Security Outcomes

Actions at this stage tend to focus on extending, integrating, automating, and leveraging existing solutions — so that Identity functions and processes work with the wider IT environment to enable the workforce, reduce manual activities, lower administrative costs, and bolster the organization's security posture.

Table 4: Stage 3 actions, business benefits, and security outcomes

Category	Actions to Take	Business Benefits & Security Outcomes
Agility	• Employ advanced lifecycle management, with automation for common tasks (e.g., access requests and approvals, app provisioning, etc.) • Leverage out-of-the-box integrations with HR systems (or any other source of truth) • Automate (event-based) user access recertification • Configure access request automation workflows	• Reduction in IT and engineering time spent creating custom-built provisioning scripts • Reduction in IT and management time spent running manual recertification campaigns and audits • Reduction in time spent by managers and workplace teams managing employee lifecycle (e.g., onboarding and offboarding employees, adjusting access to match role changes, etc.) • Faster adoption of new business systems and applications
Experience	• Implement risk-aware and phishing-resistant authentication • Deploy fully automated processes supporting incident response and orchestration • Enable self-service access requests	• Increased employee productivity due to more self-service automations and faster access • Improved employee satisfaction scores with better access experiences (e.g., fewer delays, fewer clicks, ability to leverage preferred collaboration tools, etc.) • Users can access any applications, whether on-prem or in the cloud securely and with a familiar end user experience
Security & Governance	• Institute attribute-based access control (ABAC) • Enforce least-privilege access to APIs, critical infrastructure, apps, etc. • Leverage out-of-the-box integrations with third-party tools to capture security events • Implement secure passwordless access to critical infrastructure such as servers, Kubernetes clusters, databases, etc. • Adopt recurring (scheduled) user access recertification	• Reduction in security breaches and cost of breach • Reduction in time to detect and respond to security incidents • Reduction in time/cost to document audit and compliance
Reliability	• Ensure you are deploying a solution that provides redundancy to all services across the platform	• Reduction in frequency and duration of outages impacting the business and workforce
Strategy	• Adopt formal, ongoing processes for evaluating Identity posture • Measure and make decisions based upon Identity-related KPIs • Hire in-house Identity experts	• Increased solution ROI through integration with security orchestration/automation

STAGE 4

Strategic: Optimize and Extend Identity

Extend Identity's reach to all corners and fine-tune your implementation to provide your organization with a strategic advantage

Identity is now well established as an enabler of the organization and an important aspect of governance, risk management, and compliance; moreover, automation is widespread, with only a few activities still requiring manual intervention.

Advanced capabilities that streamline success

Operational Efficiency: Fully automate Identity-related IT operations and security operations workflows.

Security: Automate Identity-based actions to detect, mitigate, and remediate the risk of Identity threats - such as blocking high risk IP addresses, remediate over provisioning or execute device logouts.

Governance: Enforce Zero Standing Privileges by democratizing JIT access to all privileges accounts and resources.

Problems to Solve

With the large majority of Identity infrastructure and processes already in place, attention turns to some final challenges:

- **Optimizing use of the cloud:** Many applications and services are already in the cloud, but the organization's needs continue to change; with the digital transformation well underway, the challenge shifts to fully leveraging the cloud while reducing waste and continuing to optimize for a single source of truth to achieve organizational Zero Trust goals.
- **Securing the edge:** Stakeholders recognize the importance of understanding where all organizational data resides and have a firm grasp of organizational Identities, but securing users and applications at the edges often proceeds in increments; the perception of diminishing returns can result in dangerous gaps.
- **Static and discrete security elements:** The organization has many Identity security measures in place, but these safeguards often rely on static rules and discrete risk assessments, rather than employing intelligent, contextual, and continuous authentication and authorization that can keep pace with modern-day intrusions, a key component to Zero Trust.
- **Rigid Identity processes:** At this stage, using Identity to do more with less, to provide a better user experience, and to help manage security risks all benefit from a custom approach to Identity processes, but a lack of requisite tools and expertise can impede such efforts.
- **Legacy standing privileges:** Access to some critical resources may still be provided via "standing" privileges — but true Zero Trust requires dynamically provisioning and deprovisioning access to such systems.

Actions, Business Benefits, and Security Outcomes

In the Strategic stage, the organization looks to implement remaining optimizations and to close gaps, while maintaining a modern access experience that achieves the dual goals of user experience and hardened security.

At the same time, Identity receives — if it hasn't already — executive- or even board-level visibility, alongside other strategic programs. Clear KPIs track the organization's progress on the maturation journey and ensure attention on Identity doesn't fall by the wayside.

Table 5: Stage 4 actions, business benefits, and security outcomes

Category	Actions to Take	Business Benefits & Security Outcomes
Agility	• Fully automate policy, user lifecycle management, and Identity-related IT operations and security operations workflows • Implement a centralized, intuitive admin UI	• Improved IT and engineering operational efficiency • Faster creation of customized integrations • Faster integration and time-to-market after M&A activity
Experience	• Leverage Identity capabilities to deliver highly extensible and frictionless workforce and partner experiences, across all devices • Encourage (or enforce) widespread adoption of passwordless login	• All around improved workforce productivity and satisfaction with secure yet seamless access experiences
Security & Governance	• Extend Passwordless authentication, including Passkeys, hardware solutions (e.g., YubiKey), and software-based authenticators • Deploy fully automated processes supporting incident prevention, detection, and response • Risk-based, fine-grained authorization • Automate (event-based) user access recertification • Ensure zero standing privileges remain; all credentials for shared privileged accounts should be managed in secure vaults	• Significantly reduced risk and impact of intrusion/breach • Increased visibility across the ecosystem into user activities for purposes of reporting, investigations and certifications • Reduced regulatory and compliance risks (e.g., fines for non-compliance or due to a breach) • Security orchestration enabling tools to respond to incidents in harmony due to increased automation • Progress on organizational Zero Trust initiatives
Reliability	• Ensure your SaaS vendor has the necessary resilience in place and can showcase compliance with regulations that support NIST and NIS 2 guidelines.	• Reduction in overhead spent managing, scaling, and supporting Identity infrastructure • Improved uptime, availability, and business continuity
Strategy	• Institute a multi-year Identity program with executive buy-in • Ensure diverse stakeholder collaboration on Identity strategy	• Optimized Identity investment ROI through faster time to market for integrations • Lower TCO and payback period through faster adoption of new systems and applications

Okta Can Help

Okta offers an extensive collection of products and features to support your progress on the Workforce Identity maturation journey — click on a link to learn more.

Table 6: Okta's Workforce Identity capabilities allow organizations to steadily mature their Identity posture

Stage 1: Fundamental	Stage 2: Scaling	Stage 3: Advanced	Stage 4: Strategic
• Single Sign-On (SSO): A single set of secure credentials that grants end users seamless access to cloud and on-prem enterprise applications from any approved locations and devices. • Multi-Factor Authentication (MFA): Use two or more authentication factors — knowledge, possession, or inherence factors — to validate a user is who they say they are to protect critical resources and data. • Universal Directory (UD): Flexible, cloud-based user store that offers a consolidated view to customize, organize, and manage users, groups, and devices, across Identity sources.	• Single Sign-On (SSO) • Universal Directory (UD) • Adaptive MFA: Enhance phishing-resistant capabilities with additional risk signals, allowing for dynamic policy changes and step-up authentication in response to changes in user and device behavior, location, or other contexts. • Okta Integration Network (OIN): The Okta Integration Network (OIN) is the Identity industry's broadest and deepest set of pre-integrated cloud apps that make it easy to manage access management, user provisioning. • Lifecycle Management (LCM): Automate user provisioning and deprovisioning with seamless communication between applications and cloud directories based on triggers from HR systems and IT resources. • Okta Access Gateway: Extend cloud-native Identity access management capabilities to on-prem web applications, enabling IT to manage both on-prem and cloud applications from a single Identity platform.	• Single Sign-On (SSO) • Adaptive MFA (AMFA) • Okta Integration Network (OIN) • Universal Directory (UD) • Lifecycle Management (LCM) • Okta Access Gateway • FastPass: Enable passwordless and phishing resistant access into anything you need to get your work done, on any device • Workflows: Reduce risk from manual, custom scripts for Identity tasks across IT and Security. Workflows' no-code platform enables you to automate key processes with pre-built templates and connectors. Examples include customizing lifecycle management, automating operational tasks like reporting, or protecting against security breaches by automatically responding to suspicious activity. • Okta Identity Governance (OIG): Govern access to maintain principles of least privilege and meet compliance requirements.	• Single Sign-On (SSO) • Adaptive MFA (AMFA) • FastPass • Okta Integration Network (OIN) • Universal Directory (UD) • Workflows • Lifecycle Management (LCM) • Okta Access Gateway • Okta Identity Governance (OIG) • API Access Management: API Access Management combines the Okta Single Sign On experience with the underlying capabilities of Universal Directory to ensure that only authorized users and applications can access your APIs, and their access is limited to the policies you put in place. With API AM IT teams are able to view, manage, and secure API access from one central control point, instead of spreading policies between APIs, gateways, and applications. • Okta Privileged Access: Gain visibility, meet compliance requirements, and enforce zero standing privileges with just-in-time access policies for critical cloud and on-prem infrastructure.

Glossary

Attribute-based access control (ABAC): An approach to access control that assigns access and actions based upon the user, resource attributes, environment, and other factors.

Directory sprawl: The state of having multiple Identity directories.

Federation: A method used to link a user's Identity across multiple separate Identity management systems, allowing for seamless authentication and access control across different platforms and applications.

Fine-grained authorization (FGA) goes beyond RBAC and ABAC to enable greater flexibility for enterprises with complex permission models. FGA allows organizations to centralize access control across every application they build or acquire, and makes it easy for app developers to implement advanced permissions and sharing strategies.

Multi-factor authentication (MFA): An added layer of security that asks users to provide different types of information or "factors" to gain access to an account or application.

Password sprawl: The state of having too many passwords, usually as a result of having multiple independent IAM systems.

Passwordless authentication: General term that applies to a range of techniques that allow a user to authenticate without the use of a password; effective passwordless systems decrease user friction but preserve — or even enhance — security.

Role-based access control (RBAC): An approach to access control that assigns access and actions according to a person's role within the system.

Threat surface: The different points where an unauthorized user can attempt to gain access into, and move within, an environment.