Whitepaper

A Comprehensive Guide for Your Customer Identity Maturity Journey

Table of Contents

State of modern Identity

Several recent converging trends have made Identity and Access Management (IAM) both a necessity and a ubiquitous enabler for any modern business. More and more companies are moving towards distributed, dynamic workforce models to reach and retain top talent while increasingly delivering their products and services digitally in search of market growth. To stay competitive and deliver the secure, seamless user experiences demanded by today's online-first world, businesses of all sizes are exploring the value of modern Identity technologies in addressing these workforce and customer-facing challenges.

Each organization's progress in tackling these demands varies based on its holistic approach to Identity. And while the need for a robust solution is evident, the path towards an effective, successful implementation is often not. Some companies may have a mature Workforce Identity strategy in place but are just starting to launch new digital experiences and safeguard customer identities. Others struggle to move away from legacy or disjointed user authentication and other homegrown services — hindering their ability to innovate and creating undue budgetary pressures across the organization.

A cohesive, future-proof path forward

It can be challenging to know where to start when trying to weave a future-proof Identity fabric throughout your business. Many teams lack the expertise, strategy, and tools to effectively address their litany of requirements, including walking the tightrope between user experience and security.

Based on patterns and collective best practices we've observed across thousands of Okta customers, we've developed a comprehensive maturity model that provides an optimal journey and evaluation criteria for all your Identity needs. This series of papers starts with Customer Identity, which centers on external users (such as consumers, suppliers, and other constituents), while traditional IAM manages Identity and access for workforce users (such as employees and partners).

Read on for guidance about specific steps to take at each stage throughout the Customer Identity maturity journey, so you can get on the path towards delivering superior and new digital experiences, protecting against security threats, and improving operational efficiencies by modernizing IT and infrastructure. Our approach is flexible enough to address varying business needs, with the aim of helping any company advance its Identity posture.

The State of Secure Identity Report

- In the first **90 days of 2022**, signup fraud accounted for approximately **23%** of signup attempts on our platform.
- Also in the first **90 days of 2022**, credential stuffing accounted for **34%** of overall traffic/authentication events on our platform.
- **58%** of all Auth0 customer applications have experienced at least one attack using breached/leaked credentials.

What is an Identity maturity model?

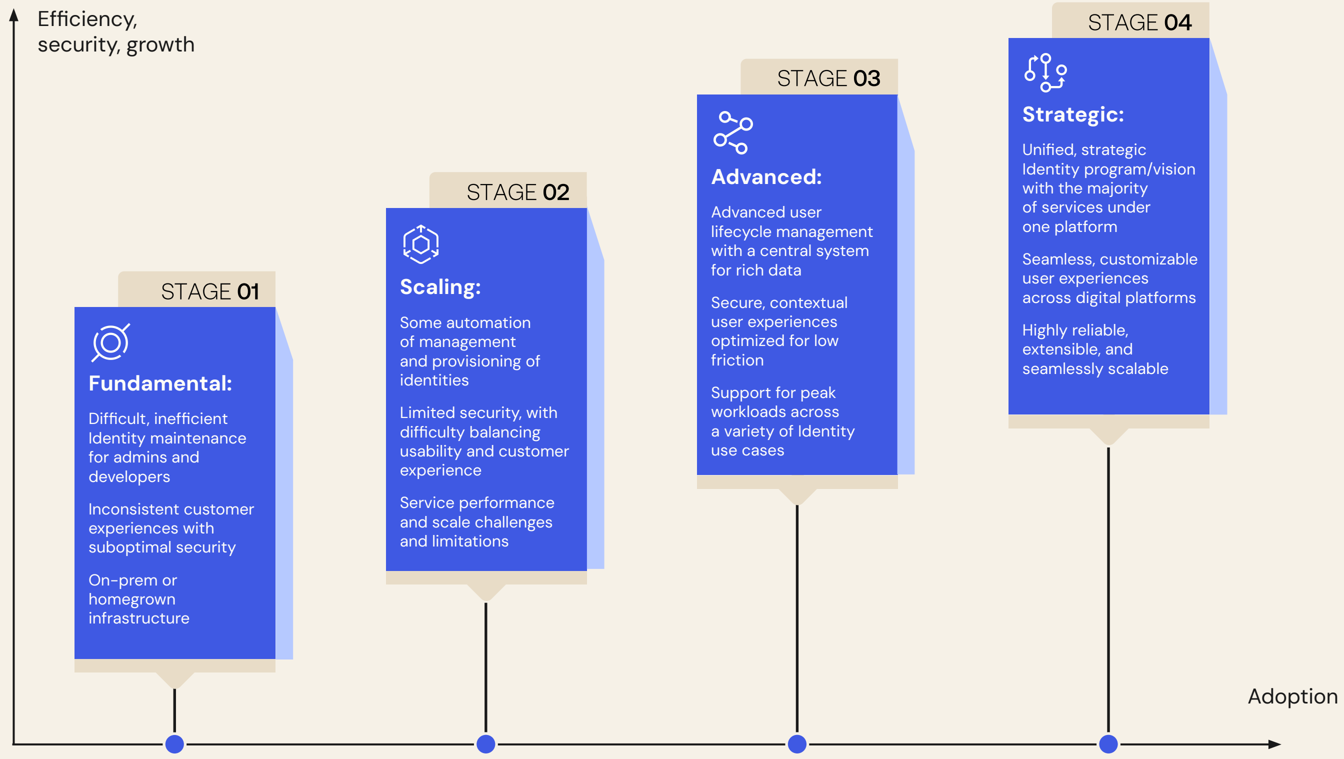
Okta's Identity Maturity Model (IMM) is a framework for assessing the current state of your Identity capabilities and effectiveness, creating a plan to improve them, and measuring ongoing success and value. By understanding the maturity of your IAM landscape and through evaluating the Identity and security capabilities required to achieve your organization's long-term business objectives (i.e. where you're at and where you're going), you'll know how to focus your efforts and investments best. This will ultimately position your business to more easily scale in response to new Identity and security requirements, as well as shifting end-user demands.

Estimate the potential value of a Customer Identity solution

Determine your savings

Assessing key areas of Identity maturity

The first step on this journey is to conduct a thorough and realistic assessment of your company's existing approach to Identity, including key capabilities and challenges. This evaluation should examine five critical categories: agility, experience, security, reliability, and strategy.



STAGE 01

Fundamental:

Difficult, inefficient Identity maintenance for admins and developers

Inconsistent customer experiences with suboptimal security

On-prem or homegrown infrastructure

STAGE 02

Scaling:

Some automation of management and provisioning of identities

Limited security, with difficulty balancing usability and customer experience

Service performance and scale challenges and limitations

STAGE 03

Advanced:

Advanced user lifecycle management with a central system for rich data

Secure, contextual user experiences optimized for low friction

Support for peak workloads across a variety of Identity use cases

STAGE 04

Strategic:

Unified, strategic Identity program/vision with the majority of services under one platform

Seamless, customizable user experiences across digital platforms

Highly reliable, extensible, and seamlessly scalable

Category	Description	Key Metrics for Evaluating Identity Success
Agility	**Ability to develop, deploy, and manage Identity-related services and flows:** FTE time spent on Identity administration, developing Identity-related code, integrating Identity into new digital properties, and customer support related to access issues; time to market	● Are you able to quickly and cost-effectively deploy new Identity features and enhancements? ● Can your developers easily integrate applications to your Identity service? ● Does your Identity service provide extensive SDKs and APIs to ensure fast onboarding and efficiencies for new developers? ● Do administrators have an intuitive and centralized service for managing external identities and their access requirements?
Experience	**Ability to deliver effective, desirable, and convenient experiences to end users:** End-user abandonment rates at both login and registration, conversions (visitor-to-registered account), and customer experience scores (e.g. NPS, CSAT)	● Do external users have simple, low-friction experiences for all required Identity services such as registration, sign in, password reset, etc.? ● Do you provide a consistent and unified access experience for them across digital properties and channels? ● Can customers self-serve to resolve authentication-related issues? ● Are you able to capture and integrate user data incrementally along the customer journey?
Security	**Ability to proactively and effectively mitigate and remediate security risk and incidents:** Time to detect (and respond to) Identity-related security issues, number and cost of account takeover incidents (ATOs), and the cost of a security breach	● Are your external users' identity credentials adequately protected? ● Are you leveraging modern, sophisticated Identity tools to secure customer access experiences? ● Do you securely store your customers' personally identifiable information (PII) and preserve privacy in accordance with regulatory requirements? ● Can your internal teams quickly uncover and resolve Identity-related security incidents?
Reliability	**Ability to provide a resilient, high-performing, and future-ready Identity service at any scale:** Minutes of unplanned downtime per month and the cost of 60 minutes of downtime on your business in lost revenue/customers; service level agreement (SLA) time	● Do you experience outages that impact your revenue-generating business and/or customer experiences? ● Is your Identity service able to handle large spikes in user traffic without interruptions, even when unexpected? ● Are you able to scale your service to address demand fluctuation in a timely and cost-effective manner?
Strategy	**Ability to plan and deliver holistically, intelligently, and with a focus on innovation:** Annual investment in Identity-related technologies, term of fully-funded Identity program, Identity service ROI and TCO To see an example of how you can calculate ROI for your Customer Identity solution, visit https://www.okta.com/roi/	● Is your Identity strategy aligned across all of your key business units? ● Is it fully funded, multi year, and supported by executive buy-in? ● Do you have a dedicated team to manage and administer your Identity service? ● Can you proactively measure and maximize the ROI of your Identity services?

Charting your journey stage-by-stage

In this section, we'll provide a more detailed overview of each maturity stage along with common goals and challenges. At the end of each section, we'll recommend steps to get started with increasing your Identity capabilities en route to the next maturity level.

Stage 1: Fundamental

Goals & challenges

This is the earliest stage of maturity, with organizations typically just beginning the process of extending digital services, online portals, or software to their customers. These companies have the bare essential capabilities and architecture for managing customer identities and securing their data. Teams spend significant time and resources on building and maintaining a nascent on-premises or homegrown service, and lack expertise and insight around how Identity fits into their broader business strategy.

At this stage, most companies are primarily concerned with onboarding customers to the system and digitally managing their identities. They've implemented only basic capabilities around authentication (user sign-in), authorization (access rules, policies), and user management (user sign-up).

Category	Actions to Take	Business Benefits & Security Outcomes
Agility	● Basic Identity administration user interface (UI) for user lifecycle and policy management (although you may still be highly reliant on manual execution from IT/development teams)	● Reduction in IT time spent managing user/group access
Experience	● Basic end-user authentication with a single factor, such as password, PIN, etc. ● Basic single sign-on (SSO) in the form of social authentication so end users can leverage existing credentials from Google or Facebook ● Simple self-service functions, such as credential reset, password recovery, attribute management, or self-registration (although frequent customer support assistance may still be required)	● Improvement in end-user productivity / increased utilization due to faster application adoption and access ● Reduction in user friction with self-service options for basic account management
Security and Governance	● A simple user repository for storing identity data and attributes with basic security encryption and hashing ● Authorization server compliant with modern standards, e.g. OpenID Connect (OIDC) and Open Authorization (OAuth) 2.0, and basic access policies for APIs	● Reduction in account lockout resulting from malicious attacks

Category	Actions to Take	Business Benefits & Security Outcomes
Reliability	- Basic Identity infrastructure with limited high-availability architecture, failover and disaster recovery capabilities, service level agreement (SLA) standards, etc.	- Increased system uptime and availability
Strategy	- Limited BU-specific strategies with disparate solutions - An evaluation of whether Identity is critical enough to build/maintain in-house or offload to third-party vendor	- Increased visibility into application landscape and access rights - Identity investment ROI and expected benefits

Stage 2: Scaling

Goals and challenges

Once companies graduate from Stage 1, they have typically launched more than one application or portal and are committed to building and delivering great digital products and services repeatedly at scale. This requires a focus on creating differentiated and trustworthy customer experiences to effectively compete for market share and grow the user base.

Concurrently, companies must bolster internal operational efficiencies to support business growth. For example, you might be looking to increase automation so you can boost productivity for admins and developers alike. This effort can stand to benefit from Identity features such as intuitive admin portals and centralized, low-touch user lifecycle management.

At this juncture, businesses often begin to understand the myriad benefits of a fully automated and intelligent Customer Identity service — and at the same time, start realizing the deficiencies in their current systems that are preventing them from getting there.

Category	Actions to Take	Business Benefits & Security Outcomes
Agility	- Partially automated user lifecycle management for onboarding and offboarding customers and partners, managing downstream system and application access permissions, etc. - Some/limited support for modern protocols and open standards such as Security Assertion Markup Language (SAML), OIDC, OAuth, Fast ID Online (FIDO), etc. - Some SDKs and APIs with limited support, guides, and documentation	- Reduction in time/cost to maintain Identity infrastructure - Reduction in help desk tickets related to access issues/requests - Faster provisioning/deprovisioning of users - Reduction in developer time needed to scale Identity

Category	Actions to Take	Business Benefits & Security Outcomes
Experience	● Limited SSO federation capabilities and protocols to support third-party Identity provider (IdP) usage for customers and partners with existing identities (e.g., AD, LDAP, SAML) ● Extended integrations with social Identity providers, such as Apple, etc. ● Limited, partially customizable customer sign-in and registration experiences that only prompt for required attributes to minimize friction	● Improvement in end-user productivity with reduced time waiting to get appropriate access to SaaS offerings ● Expanded support for regionally popular social Identity providers ● Reduction in user friction with better sign-in and registration experiences
Security and Governance	● Multi-factor authentication (MFA) with limited assurance factors (e.g., SMS, email) and user context considered during authentication ● Audit and monitoring tools, such as coarse-grained reporting logs, for enhanced security and administration ● Integration with standards-based API gateway(s) for consistent view of end-user authorization	● Strengthened security posture via MFA availability ● Reduction in time/cost to prepare for audits and compliance reviews
Reliability	● Expanded Identity infrastructure to support performance and reliability at scale ● A plan for bursts/spikes that often require ad-hoc investments and manual intervention	● Reduction in frequency and duration of outages impacting the business and workforce
Strategy	● Alignment and communication between diverse stakeholder teams leveraging Customer Identity technologies to define specific areas of ownership and responsibilities ● Realistic evaluation of Customer Identity gaps and requirements to drive development of remediation and investment plans	● Increased solution ROI through collaborative efforts to prioritize the effectiveness of Identity

Stage 3: Advanced

Goals and challenges

An organization at this stage is typically fully focused on optimizing and scaling digital offerings, while safeguarding the security and privacy of end users and their data. Customer expectations are high, with a growing mix of users demanding frictionless and personalized experiences. To deliver, organizations should invest in a plethora of advanced Customer Identity capabilities.

First, they must implement solutions that streamline the customer experience, so that users enjoy convenient, yet secure, access throughout the digital journey. This requires a variety of authentication options and intelligent access policies that minimize friction.

Also paramount is the ability to integrate Identity within your broader technology stack (e.g., marketing engine, content management system, data management platform, etc.). When you're able to do this successfully, you can consolidate data silos and gain a single view into a customer's profile and data. This enables a unified and consistent brand experience, as well as rich data and analytics to learn more about customers and their preferences.

Lastly, organizations need to consider enhancing their backend Identity systems and infrastructure by introducing more advanced automation and process efficiencies. This will minimize any intervention required from IT and developers, freeing up these teams for more important priorities that can help move the business forward.

Category	Actions to Take	Business Benefits and Security Outcomes
Agility	• Advanced automations to codify a majority of user lifecycle management business rules and minimize the need for manual developer and IT intervention • Some out-of-the-box integrations with business and marketing platforms/systems to track and identify customers across devices and channels • A variety of SDKs and APIs with advanced support and documentation	• Reduction in IT and engineering time spent creating custom-built integrations • Improved insights from customer data and interactions across channels • Further reduction in developer time needed to scale Identity with a diverse set of support and documentation

Category	Actions to Take	Business Benefits and Security Outcomes
Experience	● Automated end-user account linking/merging to enable a single access experience for consumers with one login ● Advanced customizations and logic for customer authentication experiences ● Progressive profiling of customers to build tailored registration experiences that capture user attributes over time, lessening friction ● Passwordless technology using email magic links or WebAuthn to bolster user experience and eliminate credential-related Identity attacks ● Sophisticated user onboarding with fully integrated, best-of-breed Identity proofing and account verification	● Enriched customer profiles with data over time, yielding better results from targeting promotions ● Drive revenue with advanced user customization and branding ● Reduce customer support costs with passwordless experiences ● Reduce fraud with advanced account verification methods
Security and Governance	● Intelligent MFA with adaptive features that leverage a variety of high assurance factors and behavioral inputs to assign risk and step up authentication only when needed ● Identity platform event and activity data for proactive risk detection and attack prevention ● Some out-of-the-box integrations with third-party tools/systems to capture and manage security events and signals ● Some out-of-the-box integrations with privacy and compliance tools to track customer preferences and requirements	● Reduce customer friction with non-intrusive MFA prompts ● 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	● Built-in service resiliency with redundant servers, load balancers, and high-availability infrastructure ● Built-in service buffers to handle traffic spikes of users, devices, etc. that need to be stored in a database	● Reduction in frequency and duration of outages impacting the business
Strategy	● Formal and ongoing processes, plans, and organizational ownership for evaluating Identity posture ● Ability to track and quantify a variety of Identity-related KPIs/metrics to demonstrate measurable improvement ● Trained, dedicated Customer Identity experts in-house	● Increased solution ROI through increased security posture while minimizing customer friction ● Effort to reduce total cost of ownership by consolidation of point solutions

Stage 4: Strategic

Goals and challenges

Only a small percentage of companies advance far enough in their Customer Identity journey to reach Stage 4. Those that operate at this level have mature digital and omnichannel initiatives that optimize for both user experience and security, and they view Identity as strategic to success.

Companies typically have a robust and growing customer base that is diverse and often global. These customers interact with your business via multiple channels, while demanding more advanced features, integrations, and Identity capabilities for delightful yet trusted experiences. Different teams across the company work together to devise, develop, sell, and scale these digital offerings, but each has its own set of distinct requirements and priorities.

Addressing the varied and ever-evolving demands of both internal and external stakeholders at this stage is a balancing act like no other. As companies scale and evolve, so do customer expectations, the security threat landscape, regulatory requirements, and the Identity industry. During Stage 4 maturity, businesses must focus on the goal of innovating and enhancing digital offerings with rich, differentiated, and up-to-date Identity features — and they must do this seamlessly. This is a continuous journey that is unique for every organization, rather than an end-point destination.

Category	Actions to Take	Business Benefits and Security Outcomes
Agility	● Full automation of Identity and security policy management, user lifecycle management, and complex Identity-related business workflows ● A centralized, intuitive admin UI with a unified view of all users ● Out-of-the-box integrations with best-of-breed third-party solutions related to fraud, risk, compliance, privacy, marketing, and others	● Improved IT and engineering operational efficiency ● Faster product utilization and increased retention with out-of-the-box integrations
Experience	● Highly customizable and extensible customer access experiences ● Consistent, seamless, and personalized omnichannel experiences ● Deep integrations with the broader technology stack to create a single view of the customer organization-wide	● All around improved user experience with minimal friction, delivering secure yet seamless experiences across all channels

Category	Actions to Take	Business Benefits and Security Outcomes
Security and Governance	● Intelligent MFA engine with the ability to ingest and analyze risk signals from a variety of sources ● Fully automated security workflows that support incident response and Identity orchestration ● Risk-based, fine-grained authorization capabilities	● 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
Reliability	● Resilient infrastructure that seamlessly and dynamically scales with demand spikes, including during unforeseen, highly trafficked events	● Reduction in overhead spent managing, scaling, and supporting Identity infrastructure ● Improved uptime, availability, and business continuity
Strategy	● Fully-funded, multi-year Identity program with executive buy-in ● Diverse internal stakeholder teams collaborating on Identity strategy and program like a well-designed machine	● Optimized Identity investment ROI through faster time to market for integrations ● Lower TCO and payback period through faster adoption of new systems and applications

Stage 1: Fundamental	Stage 2: Scaling	Stage 3: Advanced	Stage 4: Strategic
Goals and challenges			
– Building and maintaining a nascent on-premises or homegrown service – Lack expertise and insight – Primarily concerned with onboarding customers – Basic capabilities	– More than one application or portal – Focus on creating differentiated and trustworthy customer experiences – Bolster internal operational efficiencies to support business growth	– Focus on streamlining the customer experience – Intelligent access policies – Integrated Identity within technology stack – Consolidate data silos – Advanced automations and process efficiencies	– Mature omnichannel initiatives – Advanced features, integrations, and Identity capabilities – Innovating – Enhancing digital offerings differentiated – Identity features seamlessly

Our recommended steps and capabilities for each maturity level

Stage 1: Fundamental	Stage 2: Scaling	Stage 3: Advanced	Stage 4: Strategic
Agility			
– Basic user lifecycle management and policy management	– Partially automated user lifecycle management – Some/limited support: SAML, OIDC, OAuth, FIDO – Some SDKs and APIs	– Advanced lifecycle management and automations – Some out-of-the-box integrations – Variety of SDKs and APIs	– Full automation of policy and user lifecycle management – Centralized admin UI – Out-of-the-box integrations
Experience			
– Single factor authentication with options for basic social authentication – Simple self-service functions (registration, password recovery, etc.)	– Limited SSO federation capabilities support for third-party Identity providers – Extended social authentication options – Limited, partially customizable customer sign-in and registration experiences	– Automated account linking/merging – Advanced authentication customizations and logic – Progressive profiling – Passwordless – Identity proofing and account verification	– Highly customizable extensible authentication – Consistent, seamless, and personalized omnichannel experience – Deep integrations within technology stack
Security			
– Basic security encryption and hashing – OIDC and OAuth 2.0 – Basic access policies for APIs	– Basic MFA – Audit and monitoring tools – Integrations with standards-based API gateways	– Adaptive MFA – Risk detection and attack prevention – Some out-of-the-box security, privacy, and compliance integrations	– Intelligent MFA able to analyze risk signals from a variety of sources – Fully automated security – Fine-grained authorization
Reliability			
– Limited high availability – Limited failover and disaster recovery capabilities	– Plan for bursts/spikes often requiring ad-hoc investments and manual intervention	– Redundant servers, load balancers, and high-availability infrastructure – Service buffers to handle traffic spikes	– Infrastructure dynamically scales
Strategy			
– No holistic Identity strategy, or strategies with disparate solutions	– Alignment and communication between diverse stakeholder teams – Evaluation of gaps and requirements to drive development investment plans	– Formal and ongoing processes for evaluating Identity posture – Identity-related KPIs – Identity experts in-house	– Multi-year Identity program with executive buy-in – Diverse stakeholder collaboration on Identity strategy

Benefits of Identity maturity

Following Okta's Customer Identity Maturity Model allows you to deliver new, superior digital experiences to your customers while unlocking several valuable business outcomes along the way, such as:

- **Increased Identity effectiveness and ROI** with each stage of maturity unlocking more value than the last.
- **Operational and developer efficiencies** thanks to intuitive, comprehensive tools for Identity administrators and app developers.
- **Revenue acceleration via customer acquisitions and conversions.** Superior digital customer experiences turn Identity into a business growth driver.
- **Enhanced brand trustworthiness** with the ability to mitigate security risks and recover promptly when incidents do occur.
- **A cohesive, forward-looking Identity strategy** that accelerates value through more holistic, proactive planning.

Unlocking Customer Identity's business value

Once you know where you're at in Okta's Customer Identity maturity journey, your organization can better assess next steps and monitor success. With clarity around new opportunities to innovate the digital customer experience, protect against security threats, and drive business growth — you'll be a step ahead of your competition.

In the next edition of this maturity guide, we'll share how maturing your Customer Identity posture will map to real business capabilities that generate value for your company.

As a proven Customer Identity partner, Okta frees up your organizations' time and resources so it can focus on core products and services while we monitor the Identity and security landscape and deliver innovations. Our Customer Identity solution grows along with your business and allows your teams to do their most meaningful work. To learn more about how Okta can get you on the path to Customer Identity maturity, visit okta.com/customer-identity.

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at **okta.com**.

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.

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.

Bot Detection: Form of attack protection in which Auth0 blocks suspected bot traffic by enabling a CAPTCHA during the login process.

Suspicious IP throttling: Form of attack protection that protects your tenant against suspicious logins targeting too many accounts from a single IP address.

Brute-force protection: Form of attack protection that safeguards against brute-force attacks that occur from a single IP address and target a single user account.

Breached password detection: Form of attack protection in which Auth0 notifies your users if they use a username/password combination that has been compromised in a data leak on a third-party website or app.