Datasheet October 2023

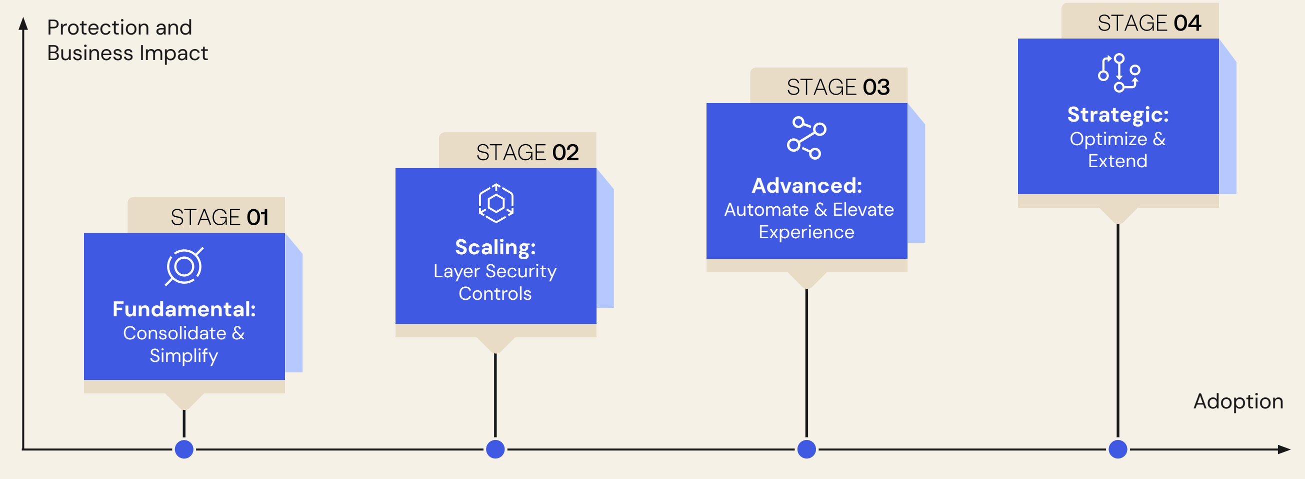
okta

Securing your Workforce in four stages

For Small and Medium-sized Businesses (SMBs)

Creating a secure, agile, and well-coordinated organization can be a time-consuming and challenging task, especially for small and medium-sized businesses. SMB leaders often understand the big picture but don't have enough time or dedicated resources to implement a solid plan. While there's no universal solution to achieve these goals, building an Identity strategy within your organization is a great first step towards better security, workforce productivity, and streamlined operations. Identity also establishes a foundation for continuous workforce improvements as your business grows.

The Okta Workforce Identity Maturity Model provides a framework to kickstart and evaluate your organization's Identity maturity journey, helping you understand how Identity can support your broader business goals and identify the next steps to optimize your Identity practices towards better security, automation, and productivity.



Stage 1 - Fundamental: Consolidate & Simplify

SMBs at this stage of Identity maturity are struggling with disconnected initiatives, causing an increased risk surface and directory sprawl. They are looking to move away from manually managing users and applications, and are focused on increasing their defense against Identity based attacks.

Current Challenges

- Fragmented user Identities across the tech stack with poor visibility
- Hybrid IT infrastructures highlighting Identity issues
- High risk security posture due to password reliance
- Inconsistent policies across technology and limited federation

Actions to Take

- Consolidate and synchronize user repositories across legacy directories and systems of record
- Install an authorization server compliant with modern standards
- Basic SSO & MFA with role-based access policies
- High-availability architecture, SLA standards and develop a comprehensive inventory of on-prem and cloud applications
- Create a comprehensive inventory of all on-premises and cloud applications, to guide decisions and help assess coverage

Business Benefits & Security Outcomes

- Reducing time spent maintaining and synchronizing user stores
- Improving end-user productivity (faster application adoption, easier access, and less account lockouts)
- Faster time to value for acquired businesses and newly invested technologies with seamless integration

Stage 2 - Scaling: Layer Security Controls

SMBs at this stage of Identity maturity are looking to increase productivity within their organization to ease IT administrator burden, as well as improve their security posture and simplify user access to applications, laying the groundwork for Passwordless and phishing-resistant capabilities.

Current Challenges

- Fragmented Identity repositories
- Increased risk from global policies, reliance on password rules, and limited use of MFA with no compliance baseline
- Operational challenges associated with password reliance and manual onboarding/offboarding of users

Actions to Take

- Retire legacy systems and adopt a unified modern user director
- Automate across the user lifecycle and provisioning
- Extend SSO capabilities for the entire workforce (employees, contractors, partners) with self-service options
- Limited MFA with access policies and at least 2-factors
- Initiate early stages of a Zero Trust architecture with dynamic access policies
- Implement secure passwordless access to your cloud and on-prem applications

Business Benefits & Security Outcomes

- Reducing time and costs from managing access
- Faster adoption of new systems and applications with faster time to value
- Improving employee productivity and management of onboarding/offboarding employees
- Improving time to detect and respond to malicious threats

Stage 3 - Advanced: Automate & Elevate Experience

SMBs at this stage are focused on automating any remaining manual processes at scale to increase efficiency for a dynamic workforce, while also consolidating and deprecating legacy technologies, and ensuring all systems are connected.

Current Challenges

- Risk associated with remote workers
- Inefficient processes with manual intervention
- Balancing user experience and system security
- Difficulty adopting and integrating Passkeys for passwordless authentication

Actions to Take

- Out-of-the-box integrations
- Automate across access requests/lifecycle management/user access recertification
- Define Zero Trust initiatives with least privilege access
- Engage in-house Identity experts with Identity-related KPIs and ongoing evaluation of their Identity posture
- Implement secure passwordless access to critical infrastructure such as servers, Kubernetes clusters, databases, etc.

Business Benefits & Security Outcomes

- Significant reduction in IT and development time
- Increased ROI from integrated security orchestration and automation with improved security posture
- Consolidated end user and admin experience across all authentications
- Familiar end user experience and security
- Reduction in costs associated with audits and adhering to compliance standards

Stage 4 - Strategic: Optimize & Extend

SMBs are focused on supporting modern access experience while also reducing reliance on passwords, ensuring a fortified security architecture with an Identity-powered security strategy.

Current Challenges

- Optimizing use of the cloud
- Securing the edge
- Static and discrete security elements
- Rigid Identity processes
- Legacy standing privileges

Actions to Take

- Full automation for policy management, user lifecycle management, streamline operational processes, incident response and orchestration, and access certification
- Implement centralized and intuitive admin UI
- Widespread passwordless login
- Intelligent MFA configured to analyze risk signals from multiple sources
- Risk-based granular access controls and phishing-resistant MFA
- Resilient infrastructure that scales seamlessly and dynamically

Business Benefits & Security Outcomes

- Faster provisioning and deprovisioning of users
- Reduction in employee lockouts
- Fewer breach incidents and reduced costs associated with regulatory fines
- Reduction in overhead spent managing different access across all systems
- Comprehensive visibility across the entire ecosystem
- Event driven solutions in near real time to limit attack vector surface
- Faster time-to-market for integrations that require IAM and faster adoption of new business systems and applications

Even with a roadmap, this journey can be challenging and time consuming. Okta is here to support you as you look to progress your Identity maturity, regardless of your business size and challenges.

To learn more about how Okta helps you grow your business simply and securely, check out the **Okta for Small Business solutions page**.

And to access our in-depth framework with suggestions and benefits, visit the **Workforce Identity Maturity Model**.

Interested in discussing next steps?

Get in touch

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.**