GlobalLogic
A Hitachi Group Company

UNIFIED DIGITAL IDENTITY

By :
Nimmanapalli Nikhil
Vivek Pandey

Contents

What is Digital Identity?

A digital identity is a set of validated digital attributes and credentials for the digital world, similar to a person's identity for the real world.

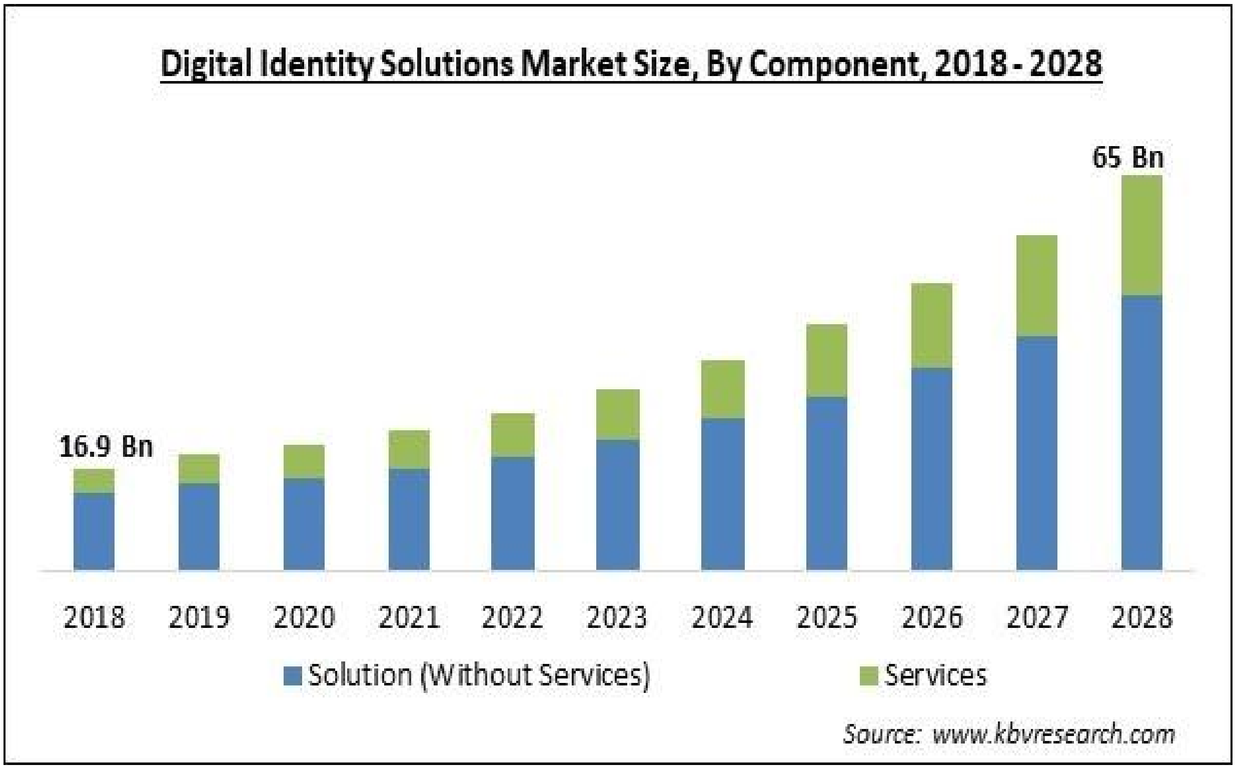
Why is Digital Identity so Important ?
It is essential to have digital identity due to the fact that trust is the basis of any relationship. Without trust, organizations and governments cannot properly develop digital transformations and customers will not be comfortable using online tools, which can lead to missing out on essential services.

- Currently, with the pandemic, more people are relying on remote network connections, the Cloud, and home working, and thus the lack of trust can be an immense problem. Additionally, relying on traditional forms of identity such as passwords is no longer enough to ensure security online.
- According to Gartner, At least 80% of government services that require citizen authentication will support access through multiple digital identity providers by 2023.
- A digital identity solution in healthcare facilities can help professionals enjoy a single view of identity, reduce human error, reduce costs, and improve data security and compliance.
- During the past decade, the number of digital identities has exploded, driven by cloud technologies and machine identifications. A survey conducted by IDSA in 2022 revealed that 98% of security professionals have reported significant increases in the number of identities they manage, mostly as a result of cloud adoption, third-party relationships, and new machine identities.
- Digital identities are necessary to access software-as-a-service (SaaS) and cloud-hosted applications. These resources are often used across the organization, meaning every individual user requiring access will also need a digital account to represent them.

Digital Identity Market trends:

- The global digital identity solutions market size is expected to grow from an estimated value of USD 27.9 billion in 2022 to USD 70.7 billion by 2027, at a compound annual growth rate of 20.4% from 2022 - 27. Rise in ID wallet solutions and explosion of online services offered by commercial businesses in recent years are driving the market growth but threat of privacy and data breach can slow down the Digital Identity market solution.

- Digital identity is enabling decentralization and new forms of verification. Per a recent McKinsey report on technology trends, “self-sovereign identity(SSI)” was called out as one of the most noteworthy technologies in digital identity and trust architecture. Self-sovereign identity (SSI) gives users control over their verified credentials and the ability to elect what they share and with whom.
- According to a study of Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States, digital ID programs could unlock economic value equivalent to 3 to 13 percent of GDP by 2030.
- Authentication into services like PayPal and Amazon is performed using attributes stored in the unfederated account. Identity information is passed from a directory service to a system without any knowledge of the identity being authenticated, or storage requirements for it.
- Governments and digital IDs - The number of users joining digital ID is growing. According to a Juniper Research report, this number will increase by more than 50% over the next few years, from 4.2 billion in 2022 to 6.5 billion in 2026.



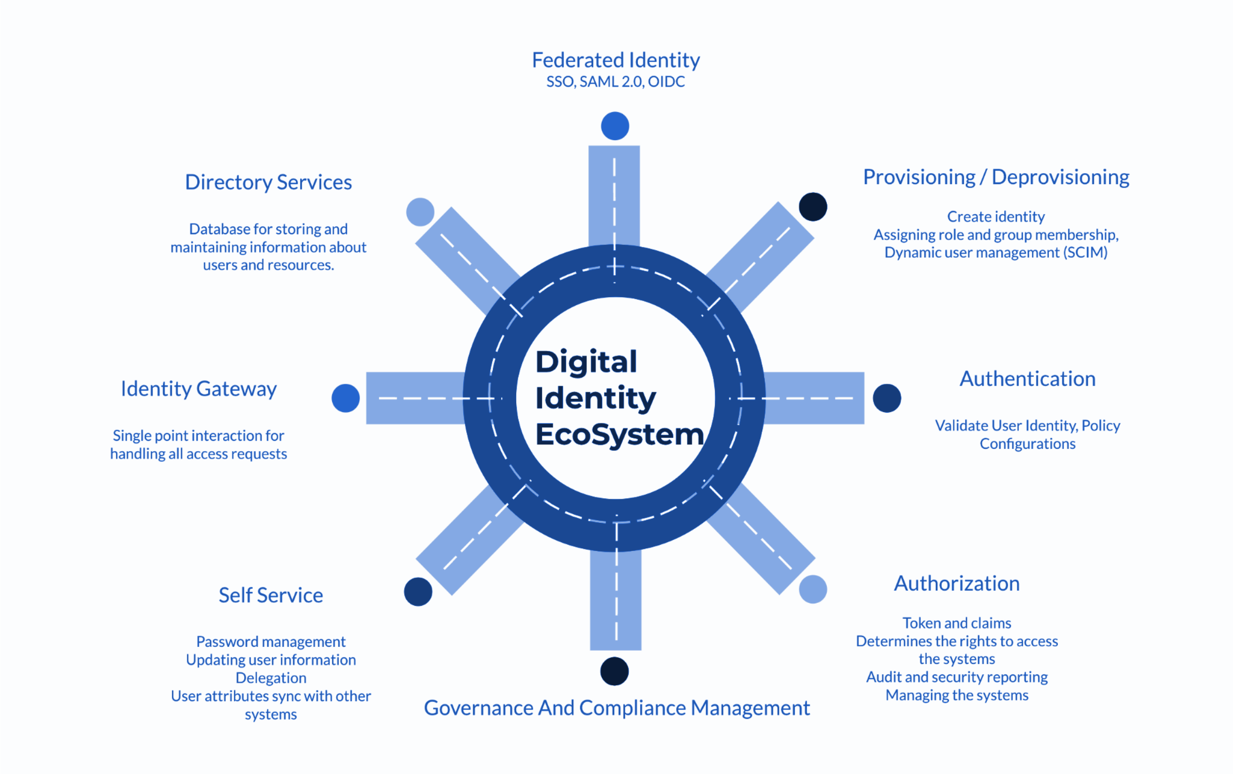
Digital Identity Solutions Market Size, By Component, 2018 - 2028

Source: www.kbvresearch.com

Recent Developments:

- Samsung Introduces Smart All-in-One Fingerprint Security IC for Biometric Payment Cards.
- Star Alliance launched biometrics identity verification system
- Many companies have moved their identity stacks to the cloud, while others are using identity-as-a-service. Deloitte's study, Accelerating agility through everything-as-a-service, found evidence of this trend.
- New “ID wallet” solutions are set to give a serious push to digital identification schemes worldwide. This recent technology defines a secure mobile app to store digitized and encrypted versions of ID documents.
- French govtech application TousAntiCovid (i.e. All Against Covid). It contributes to the fight against the pandemic by detecting contacts at risk of transmission via Bluetooth or QR code scanning. But more importantly, it stores vaccination certificates and Covid-19 tests, as a digital wallet would do.
- India’s biometrics-backed coronavirus vaccine application, CoWIN (COVID Vaccine Intelligence Network), will comply with the government’s forthcoming Data Protection and Privacy Law.
- Smart borders and airports emerged at a faster pace. Combined with the 1,2 billion ePassports now in circulation and a strong push behind biometrics (particularly face recognition), they offered travellers a taste of cross-border movement that is as secure as it is swift and seamless.
- The security industry has been working hard to enhance IAM (Identity and Access Management) and ID verification solutions with, in particular, new secure onboarding apps, including facial recognition with liveness recognition features. Progress is visibly impressive. For example, with the help of artificial intelligence, the accuracy of the best facial recognition algorithms has increased by a factor of 50 in less than 6 years.
- The United Nations (UN) and World Bank ID4D initiative aims to provide everyone on the planet with a legal identity by 2030.

Digital identity Ecosystem:

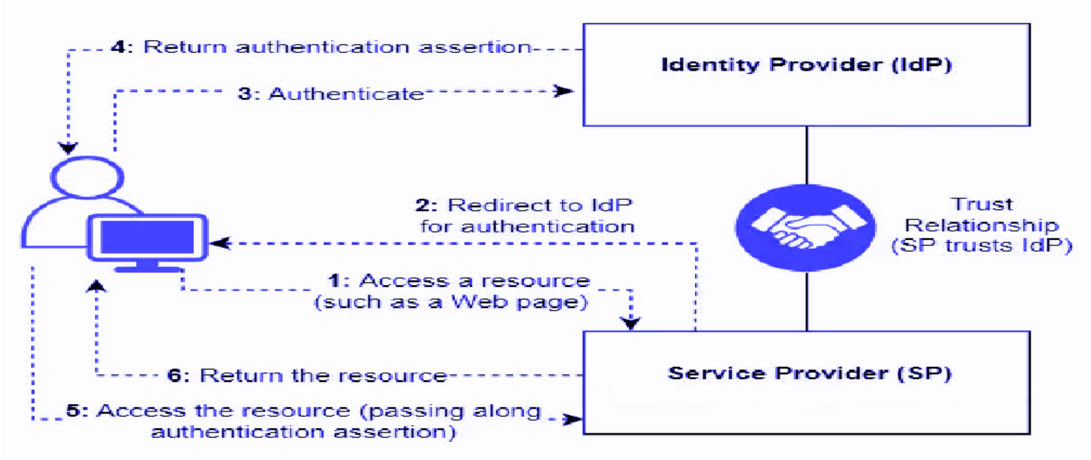

Federated Identity
SSO, SAML 2.0, OIDC
Directory Services
Database for storing and maintaining information about users and resources.
Provisioning / Deprovisioning
Create identity
Assigning role and group membership,
Dynamic user management (SCIM)
Identity Gateway
Single point interaction for handling all access requests
Digital Identity EcoSystem
Authentication
Validate User Identity, Policy Configurations
Self Service
Password management
Updating user information
Delegation
User attributes sync with other systems
Governance And Compliance Management
Authorization
Token and claims
Determines the rights to access the systems
Audit and security reporting
Managing the systems

Federated Identity

Your digital identity is made up of attributes that define you as a unique person moving through the landscape. Federated identity is an agreement between entities about the definition and use of those attributes. Agreements allow you to sign on in one place and then jump to another asset without signing in again.

- **Federated SSO:**
  Federated Single Sign-on or Federated SSO (also known as Federated Identity Management). As it implies, Federated SSO is a service that allows users to login into different Applications/Websites situated across different domains using a single set of login credentials.

  Federated SSO uses standard identity protocols like OAuth, WS-Federation, WS-Trust, OpenID and SAML to pass tokens. Federation provides authentication and security features on both cloud and on premise applications.


4: Return authentication assertion
3: Authenticate
Identity Provider (IdP)
2: Redirect to IdP for authentication
Trust Relationship (SP trusts IdP)
1: Access a resource (such as a Web page)
6: Return the resource
Service Provider (SP)
5: Access the resource (passing along authentication assertion)

- **Why should you implement federated SSO?**

  Your users only require to learn a single password for all organizations in alliance. Now, no more frequent resetting of passwords. Moreover, for employers who use federated SSO for their employees, you can save a lot of money. According to **META group**, a single help desk call for **password reset** costs $25.
  Here are some stats to show how federation can improve password management:-
  - 61% of people reuse their passwords on numerous websites.
  - 60% of people agree that they cannot remember all their passwords.

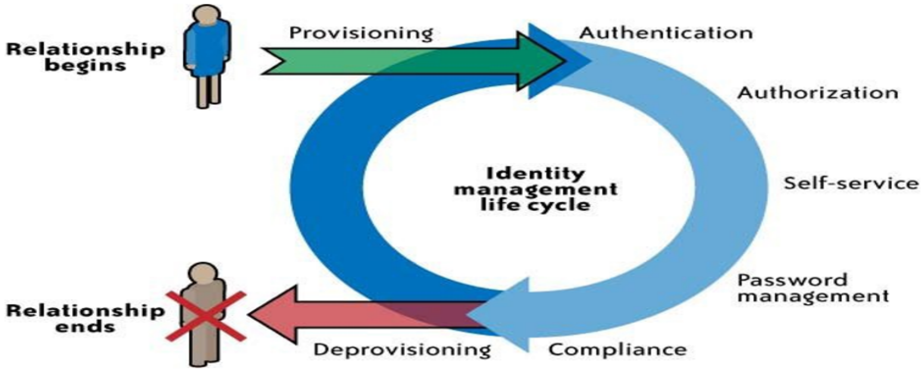
  Well, using federated SSO will solve such problems. Moreover, it will ultimately enhance your security. Federated SSO scores eleven in a scale from one to ten when it comes to user experience. You will definitely skyrocket your user experience.

Provisioning and Deprovisioning

Provisioning and de-provisioning is an identity and access management procedure that involves creating, managing, updating, and deleting accounts (identities) and granting them access to the resources with appropriate rights and permissions.

There are three types of provisioning available:

- **Inbound Provisioning** means provisioning users into the Identity Server by an external application (service provider).
- **Outbound Provisioning** provisions users to a trusted identity provider from the Identity Server.
- **Just-In-Time provisioning** provisions users to the Identity Server at the time of federated authentication.



- **Benefits of provisioning and deprovisioning**
  - ➔ **Easily onboard and offboard employees**: Create and maintain employees' user attributes, and automatically assign access permissions and user accounts based on predefined roles.
  - ➔ **Streamline user management across applications**: Automatically import users from Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and other apps. Provisioning enables you to continuously propagate user profiles to ensure that your systems have the latest updates.
  - ➔ **Increase security and reduce cost**: Use HR-Driven Identity Management (IM) to prevent former employees from having continued online access, to totally eliminate the possibility of zombie accounts sitting idle and at risk of being compromised.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Types of authentication

- **Single-Factor/Primary Authentication** only requires one factor to gain full system access. It could be a username and password, pin-number or another simple code.
- **Two-Factor Authentication (2FA)** reinforces security efforts. It is an added layer that essentially double-checks that a user is, in reality, the user they're attempting to log in as making it much harder to break. Some of the 2FA types used are Email-based, SMS-based, Voice-based, Token/TOTP based, Biometrics based, As a Push Notification etc.

- **Single Sign-On (SSO)** With SSO users only have to log in to one application and, in doing so, gain access to many other applications.
- **Multi-Factor Authentication (MFA),** is a high-assurance method, as it uses more system-irrelevant factors to legitimize users. Like 2FA, MFA uses factors like biometrics, device-based confirmation, additional passwords, and even location or behavior-based information (e.g., keystroke pattern or typing speed) to confirm user identity.

Authorization

Authorization in system security is the process of giving the user permission to access a specific resource or function. This term is often used interchangeably with access control or client privilege. Giving someone permission to download a particular file on a server or providing individual users with administrative access to an application are good examples of authorization. In secure environments, authorization must always follow authentication.

Users should first prove that their identities are genuine before an organization's administrators grant them access to the requested resources.

Authorization Methods

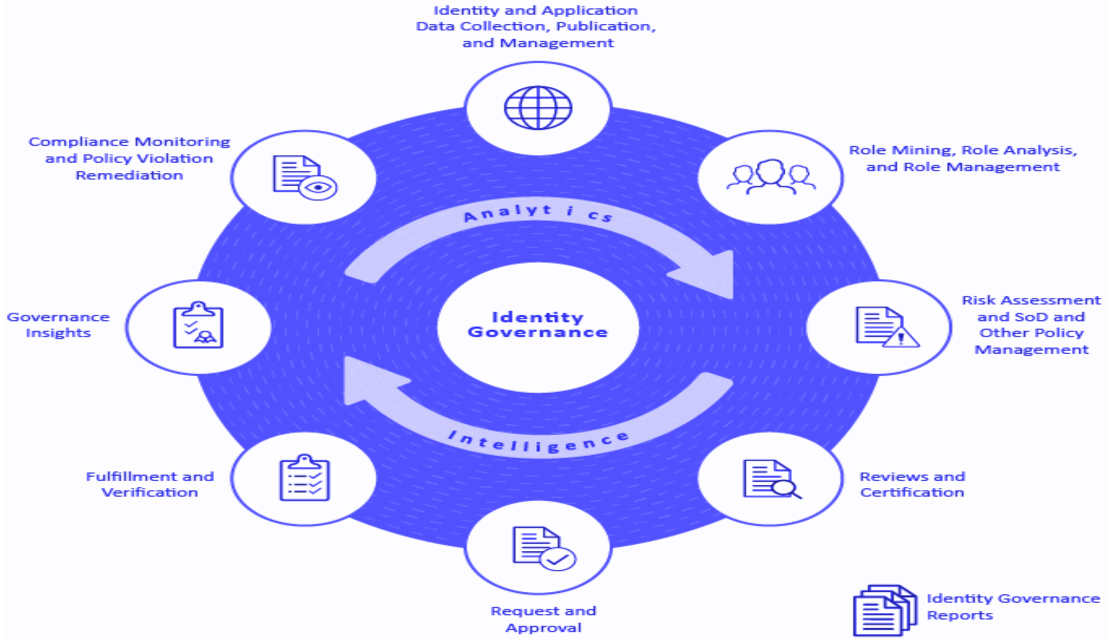
- **Role-based access control(RBAC),** gives users access to information based on their role within the organization.
- **Attribute-based access control(ABAC),** grants users permissions on a more granular level than RBAC using a series of specific attributes.
- **Policy-based access control(PBAC),** uses a combination of attributes to determine whether or not to authorize an access request.

Governance and Compliances

Identity Governance(IG) is an important aspect of managing and protecting an organization's digital assets and resources. Essentially, IG involves establishing and enforcing policies and procedures for controlling access to systems and data, as well as monitoring and reporting on user activity. IG also enables organizations to increase organizational efficiency and agility through automation and intuitive workflows.

Compliances

Organizations must ensure that data privacy is in place as well as having appropriate and secure data access management. IAM plans must incorporate User Identity Definitions, User Authentication Methods, User Access to Resource Locations and User Access Reviews.


Identity and Application Data Collection, Publication, and Management
Role Mining, Role Analysis, and Role Management
Risk Assessment and SoD and Other Policy Management
Reviews and Certification
Request and Approval
Fulfillment and Verification
Governance Insights
Compliance Monitoring and Policy Violation Remediation
Analytics
Identity Governance
Intelligence
Identity Governance Reports

Self Services

User self-service feature that lets customers self-register to a website, securely reset forgotten passwords, and retrieve their usernames. User self-service capabilities greatly reduce help desk costs and offer a rich online experience that strengthens customer loyalty.

Improve the user experience and reduce costs by giving end users their own tools to manage identity and access. From self-service password reset and single sign-on to access request and approval, you'll find everything you need in one IAM platform.

Why is Self-Service Identity management required?

Self-Service Identity management improves the user experience and reduces costs by giving end users their own tools to manage identity and access. From self-service password reset and single sign-on to access request and approval, you'll find everything you need in one IAM platform.

Identity Gateway

Identity Gateway streamlines Identity and Access Management efforts and simplifies the management of user, application, device, and service identities. The Identity Gateway integrates millions of households and individuals email, phone, mobile, and device ID data with your applications, processes, or programs. Identity Gateway provides users with instant access to the industry-leading data assets of Digital Segment, whether it is for enhancing data as it is acquired or appending additional elements to existing data.

There are many uses for Identity Gateway, such as:

- Real Time Data Optimization:
    - When companies acquire data about their prospects and clients, they can rapidly improve the records with different contact details in real time.
- Constructing CDPs and Identitygraphs:
    - By connecting Identity Gateway with the CDP/marketing technology stack, data can be validated, improved, and upgraded automatically.
- Building an Identitygraph from a single point of data:
    - Generate an Identitygraph record from one piece of contact information: email, phone, IP address, mobile device ID, or mailing address.
- Reverse Look-Ups:
    - Utilize any piece of contact data to distinguish the name and mailing address; ideal for developing a total view of that customer from only one data point.

Directory Services

A directory service is a database that stores data you need to do your job, which is sometimes called a data store, LDAP, or directory. These containers hold your login credentials, verification settings, user inclinations, application data, and recently, details related to devices like cellular phones and Internet of Things (IoT).

Over the years, there have been many shifts in how corporations manage and utilize Directory Services, including guidelines from Microsoft, distinct modes of enterprise AD (Active Directory) management, and the introduction of rules and regulations that impact it.
Due to these changes, businesses are now revisiting their AD deployments. By modernizing their AD deployment, they can gain advantages in terms of manageability, security, recoverability, performance, auditability, and governance.

In order to have a contemporary directory server, there are five essential requirements:

1. Optimal efficacy, scope and dependability
2. Consolidated end-to-end protection
3. Matching and combining of identity information
4. Making identity details available to modern and old-fashioned applications
5. Migration resources tailored for previous data stores

Identity as a Service (IDaaS)

IDaaS is a cloud-based service that provides access to various types of data storage and analysis solutions. It enables organizations to store and manage their data in the cloud, analyze it in real time and make use of powerful analytics tools. Additionally, IDaaS offers a range of data integration and security features to help organizations protect their sensitive data. By using IDaaS, organizations can benefit from enhanced scalability, cost savings and access to a wide range of data sources.

Widely used tools in market and their comparison

Parameters	Auth0	Okta	Azure Active Directory	ForgeRock	OneLogin
Overview	A secure access solution for enterprises (B2B, B2C, and employee identity access management)	IAM for your workforce and customers, Platform Services to address specific identity use cases via modular components.	Microsoft's cloud-based IAM solution for enterprises	AI-powered IAM platform for consumers, workforce, and partner network built on the cloud.	A unified platform for customer identity, workforce identity, and developer experience management.
Credential Management	Breached password detection and access blocking until the password is reset; passwordless login to eliminate one of the most common attack vectors.	Features single sign-on (SSO) and strong password management policies for safe credentials.	Authentication and conditional access policies to protect user credentials; machine learning to detect leaked or stolen credentials and suspicious login attempts.	A user dashboard to manage credentials and privacy preferences across various applications/websites; consistent password policies across applications, devices, users, and IoT objects.	Single sign-on (SSO) to securely access multiple apps with one set of credentials; synchronization with directories like Workday, LDAP, etc., for credential porting.
Data security	Secure credential storing in the Auth0 database or in-house enterprise repositories; single sign-on and MFA for secure data access.	Data security measures to prevent cross-site scripting, SQL injections, and forgery requests.	It packs the ability to integrate Azure IAM with user applications (Workday, DocuSign, Jive, etc.) for secure data access	Secure data access via the cloud on endpoints and across the IoT ecosystem.	Context-aware access management to filter access to sensitive data; enterprise sandbox feature for production data cloning.

Pricing	Free for up to 7000 active users, developer solutions for $23 or $1070 (customer-facing) or $1020 (for employees) per month, and enterprise solutions with custom pricing.	Feature-based pricing starts at $ 2 per user per month for only SSO, and goes up to $29,000 annually for B2B integrations.	Starts at $6 per user per month (PUPM).	Custom pricing; free trial and ROI calculator available.	Features-based access starts at $2 per user per month (PUPM).

Conclusion

A digital ID system improves the connection between private and governmental entities and individual citizens. It is an essential component in designing and developing more creative, agile, and responsive services. In particular, it aids in lowering operating expenses, enhancing customer satisfaction, reducing turnaround times, speeding up deliveries, and improving security. As the digital environment is continually changing and assuring a secure digital identity, the young generation will have more secure data and convenience in conducting digital transactions.

References:

https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html
https://www.globenewswire.com/en/news-release/2022/10/24/2540315/0/en/Digital-Identity-Solutions-Market-Size-is-projected-to-reach-USD-116-07-billion-by-2030-growing-at-a-CAGR-of-18-6-Straits-Research.html
https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth