IBM

IBM Cloud Identity

Secure user productivity with born-in-the-cloud identity-as-a-service (IDaaS)

Highlights

- Leverages a born-in-the-cloud platform for B2E, B2B and B2C use cases
- Accelerates business adoption of new cloud applications
- Secures external-facing applications and services
- Balances security and convenience with seamless MFA
- Speeds routine identity management processes
- Secures user productivity from any device with SSO

Identity has become the cornerstone of the enterprise security agenda. In a world of ever-changing threats and attack vectors, effective identity and access management (IAM) programs remain the best defense against most threats. It is imperative for the organization to know who users are and to watch what they do.

The fundamental tenants of sound IAM haven't changed much in the past 20 years. But rapid enhancements in cloud computing, mobile applications and social media have introduced new pressures on IT and security teams, forcing a widespread re-evaluation of legacy architectures and processes. Users are moving faster than ever before, and the complexities of maintaining strong security hygiene in light of those changes have never been greater.

IBM Cloud Identity is a comprehensive platform of IAM capabilities. Its clean, business-friendly interface, delivered from the cloud, can help you reduce your total cost of ownership and reduce your dependence on specialized and hard-to-find security skills. IBM Cloud Identity allows IT, security and business leaders to not only adapt to the current cloud-computing era, but also to future-proof their IAM programs against the next generation of innovations in user productivity.

IBM Cloud Identity supports users' requirements for frictionless access to applications, business leaders' needs to increase productivity, developers' needs to roll out new services quickly, and IT requirements to more rapidly respond to business change.

Connect users to applications with SSO

A major benefit of the cloud is easy access to business tools, whenever and wherever users need them. But when tools—and the passwords they require—multiply, that benefit can turn into a hassle. Many cloud-based applications that users want do not have built-in security and authentication features. IBM Cloud Identity enables you to design and enforce access control policies for thousands of cloud-based applications such as Microsoft Office 365, Concur, Workday, IBM Box and IBM Verse. It also includes prebuilt templates to help you integrate in-house applications.

- Employee-facing launchpads to access any application

- A cloud directory for organizations that don't already have a user directory

- The ability to sync on-premises directories like Microsoft AD for use with cloud applications

- Support for multiple federation standards, including SAML, OAuth and OpenID Connect

Verify user identities with frictionless MFA

Achieving the right balance of convenience and security when it comes to authentication policies is a major challenge for today's security leaders. For consumer-facing services, creating delightful authentication experiences is a business imperative. For employee-facing programs, implementing the latest and most secure methods is imperative to ensure only the right people access enterprise resources. Whether your authentication program needs to serve internal or external users, the MFA capabilities that IBM Cloud Identity provides can help you ensure a frictionless experience.

- A simple user interface (UI) for defining and modifying access controls

- One-time passcodes delivered via email, SMS or mobile push notification

- Biometric authentication, including fingerprint, face, voice and user presence

- Second-factor authentication for virtual private networks (VPNs)

- The ability to use context from enterprise mobility management and malware detection solutions for risk-based authentication

- Software development kits (SDKs) to easily integrate mobile applications with the broader access security platform

- Risk-based user authorization and authentication policies that use:

  ○ Context about the endpoint (device fingerprint, jailbreak status, EMM enrollment status)

  ○ Identity (groups, roles and fraud indicators)

  ○ Environment (geographic location, network and IP reputation)

  ○ Resource/action (what is being requested)

  ○ User behavior (location velocity)

IBM

Govern access rights to ensure appropriate access

For many organizations, provisioning and recertifying user access to applications to meet compliance mandates can be onerous, laborious and operationally expensive. IBM Cloud Identity governance capabilities help organizations speed up adoption of new technologies by delivering crucial identity governance and administration functions from the cloud. This gives organizations the tools required to manage the employee access lifecycle and compliance at a lower operational cost.

Better understand access risks with identity analytics

A typical IAM environment stores information about who users are and what they have access to, but this doesn't always provide an accurate picture of access-related risks. To get a holistic view of access risks, you need a full understanding of what users are actually doing with their access privileges. Identity analytics capabilities from IBM Cloud Identity makes IAM smarter by enhancing existing processes with a holistic view of risk, including decision support which is accompanied by recommended mitigation actions powered by machine learning.

Balance security and convenience with adaptive access

What level of authentication do you need to require of users when they log in to access your application? It's not simple to balance

the business demand for seamless experience with your organization's security requirements. And most approaches to authentication involve setting a static policy based on a fixed number of attributes — location, device, etc. Cloud Identity helps your organization deliver a frustration-free access experience without sacrificing risk considerations with adaptive access. Adaptive access combines advanced risk detection with a robust access policy engine to assess the full context of a user's identity as they attempt to access a digital service. The solution is easily integrated into applications with low to no coding required, through an API for custom applications and pre-built templates for commonly used cloud apps.

- Artificial Intelligence-powered risk detection that synthesizes context on mobile devices, web sessions and VPN access to dial up or down the level of user authentication required

- A simple policy editor that allows administrators to quickly design and apply adaptive authentication policies

- The ability to detect anomalies in user attributes based on behaviour, biometrics, known fraudulent patterns, device, location, and IP address

- Resources for developers to add adaptive authentication into native, web, mobile and cloud applications with little to no coding required

- Support for multiple federation standards, including SAML, OAuth and OpenID Connect

Your organization is building exciting new digital services to grow your business.

Securing those services with strong consumer identity and access management (CIAM) controls is key to brand trust. But customers may abandon your brand if they can't get fast and simple access. Cloud Identity helps your organization balance these concerns, giving you the tools you need to protect both new and old customer-facing services with seamless security.

- APIs, software development kits, and developer resources to customize your identity experience to look and feel like your brand.

- Adaptive authentication to prompt customers for MFA only when risk is detected

- Social login capabilities that allow users to register and log in using their LinkedIn, Google, Facebook and Twitter accounts, as well as other regional and geography-specific social networks

- Pre-built templates for enrollment, registration, username/password reset, and other identity operations

- The ability to track customer consent and privacy preferences to support compliance with the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA)

IBM®

Why IBM

To make a successful transformation to the cloud, you need ways to integrate and extend your existing enterprise IAM policies that can help ensure security without disrupting the business. IBM provides true integration across mobile, cloud, and on-premises applications, enabling lower costs and greater operational efficiency across your enterprise. IBM Cloud Identity delivers all of this from the cloud with no installation or infrastructure required.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors more than one trillion events per month in more than 130 countries, and holds more than 3,000 security patents.

For more information

To learn more about the IBM Cloud Identity offering, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/us-en/marketplace/cloud-identity-connect

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing