

# OpenText Covisint Cloud Identity and Access Management

Securely connect the people, systems and things within, across and into the enterprise



**Provide secure access** for networks of external business users to internal and external resources



**Manage the identity lifecycle** from identity creation to access revocation



**Provide users with secure and convenient access** with multi-factor authentication and single sign-on

**A fully connected enterprise is a benefit of digital transformation, but also provides an enormous challenge—giving users secure access to information. IT teams must figure out how to solve this issue, which is complicated by large user populations, integrating old and new technologies and cloud and Internet of Things initiatives. Enterprise application managers might have to manage internal employee access and give external users, such as suppliers and logistics carriers, access to collaborate on specific systems (in a very controlled way), as well as provide consumers with an enhanced experience.**

To make this possible, digital identities need to be managed in a way that is simple for IT teams, that can align with business processes and, perhaps most importantly, bolster enterprise security—not compromise it. With OpenText™ Covisint Cloud Identity and Access Management, organizations can provide access to their systems across their entire external ecosystem. They can govern user access to information through role-based control, regulating access to systems or networks based on each user. This also makes it possible to securely store identity and profile data to ensure that only data that is necessary and relevant is shared.

## Secure access for external users

We hear a lot about data breaches—when someone finds a way into an enterprise system without secure access. Technology analysts at Forrester say that companies can reduce their threat surface by more than 75 percent by adopting an identity model for systems access. In addition to security, this makes collaboration quicker and easier. For example, one of the largest supply chains in the world—an automotive OEM with multiple supplier tiers across the world—is enabled through Covisint Identity and Access Management.

## Enhanced consumer experience

The right identity and access management (IAM) strategy and technology can also help brands engage more directly with consumers and provide a more complete customer journey. This begins with a single, secure identity. The challenge is to create a consistent experience across the entire customer base—and one that allows customers to control how, when and where they engage. Organizations want to ensure they are presenting the right information to the right consumers and when dealing with sensitive data, they must resolve the tension between being open and convenient and being secure and reliable. An IAM platform provides the flexibility to present and receive trusted information in whatever form, format or device consumers choose.

## Identities managed across the lifecycle

Covisint Identity and Access Management helps organizations manage the sheer number of identities and enables them to manage changing identities and access rights. This is accomplished by approaching identities holistically and understanding that they go through a lifecycle. From identity provisioning, authentication, authorization and then deprovisioning, IT teams need to consider specific actions and protocols.

The most common challenges include a lack of visibility into who has access to what systems and resources, inability to provide certification, audit and attestation for external users or when someone leaves their job and takes their access with them. This is especially challenging when it happens at an external trading partner. With Covisint Identity and Access Management, organizations have visibility into, and control over, who has access to what resources across the distributed ecosystem, ensuring that information resources are changed only in a specified and authorized manner and that access can be easily revoked when teams change.

Covisint Identity and Access Management focuses on an outside-in approach, which is when an organization has external users and things requesting to gain access to information resources inside the organization's network. This may include consumers, business-to-business and Internet of Things ecosystems.

OpenText was the first company to solve this problem and build technology to handle it at scale—in the cloud—focusing on business-to-business (B2B) and business-to-consumer (B2C) use cases, leaving employee identity management to other vendors. OpenText focuses on securing access into and across large and complex ecosystems, including a connected vehicle offering, which connects people, systems and things. OpenText does all of this in the cloud, which leading technology analysts say is more cost-effective and secure. With thousands of globally distributed external partner users, a global Oil & Gas leader needed a way to manage access to critical applications and information.

**Connected joint ventures**

**With thousands of globally distributed external partner users, a global Oil & Gas company needed a way to manage access to critical applications and resources**

 Identity and access management

 APIs and developer resources

 Cloud innovation and experience

**The business challenge**

- Quickly create, manage and decommission joint ventures
- Exploration is based on point-of-access to trusted information at the right time—for the right person
- Speed up time to reserves

**The results**

- Accelerated joint venture initiatives
- Platform for future business initiatives
- Improved visibility and auditability for data access and compliance

**Leading global Oil & Gas company improves security and efficiency**

Leveraging the OpenText™ Covisint Identity solution, the company was able to synchronize joint venture partners' user identities with their internal Microsoft® Active Directory® enterprise identity store, enabling realtime identity creation, user provisioning, access revocation and full-audit and reporting capabilities. This allowed the company to securely onboard thousands of joint venture partners, manage access, decommission identities as necessary and safely dissolve the ecosystem when their energy project was complete.



The identity components required for connecting an ecosystem of people, systems and things

## Learn more

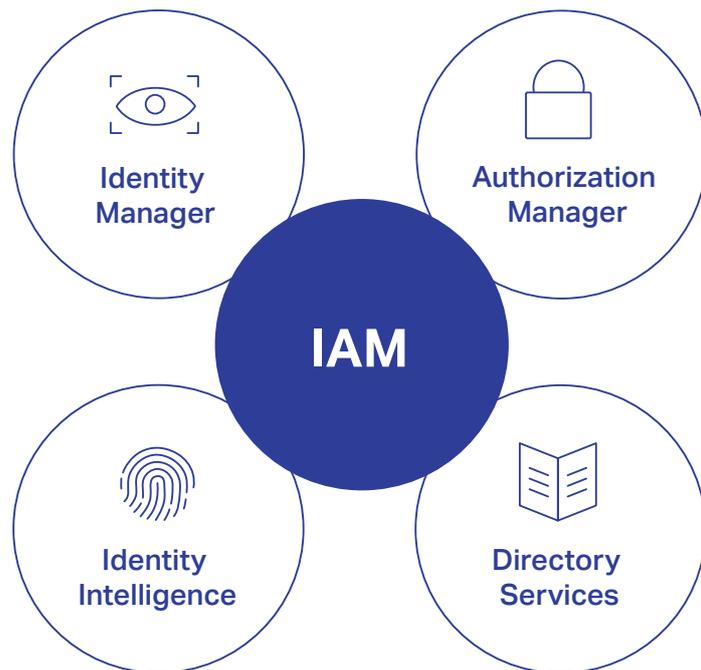
Meeting the GDPR requirements

The Identity of Things is here

From identity provisioning to managing IoT ecosystems

Identity and access management would prevent most of today's data breaches

## Keep up to date



B2B and B2C IAM secures access to critical resources, offers new experiences

- **Identity Manager:** designed for comprehensive identity and access management across the complex ecosystem of enterprise identities
- **Authentication Manager:** validate that a user is who they claim to be and establish trust across domains for single sign-on.
- **Identity Intelligence:** inspect identity, access and endpoint data and convert it to actionable information and insights – great for responding to GDPR
- **Directory Services:** cloud-based directory and the tools to integrate and synchronize directories

In addition to managing the identity lifecycle, Covisint IAM also addresses many common challenges with identity governance and administration (IGA). Whether it is a lack of visibility into who has access to what resources across the organization or an inability to provide certification, audit and attestation for user identities, this solution can easily handle these complexities.

Digital business transformation begins with securely managing digital identities because it sets the foundation for how users, systems and devices interact with the information and resources within an enterprise. Covisint Identity and Access Management helps enterprises create identities, authenticate them and establish and govern complex access rules across large and complex ecosystems.

Contact us to learn more about how identity and access management could work for your business.