opentext™

White paper

Secure access to enterprise information with identity and access management

Digital transformation is driving decentralized operations and increasing risk of information breach

To optimize efficiency, agility, and drive greater collaboration, it is essential for the enterprise to be able to share information, resources, and applications with external value chain partners in a trusted manner. This white paper explores how identity access management (IAM) provides the policies and processes for ensuring that the right people in an enterprise have the appropriate level access to secure resources, at the right time—improving security, efficiency, and visibility.

opentext™

Contents

opentext™

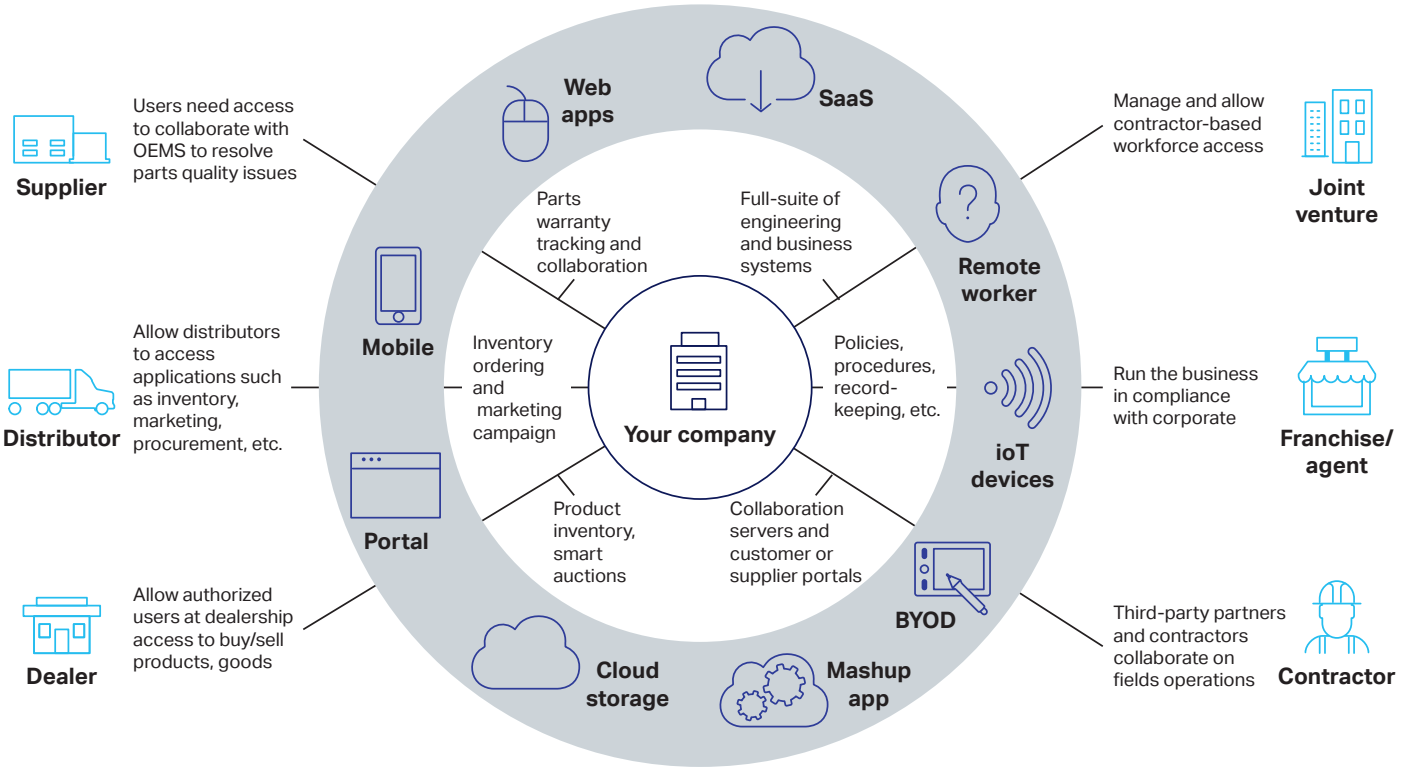
Introduction

Over the past decade, businesses have become more global as they decentralize and externalize non-core business functions, transitioning them to a network of suppliers, factories, warehouses, transporters, and other value chain stakeholders. As a result, the value chain has become even more complex and vulnerable than in years past.

This trend is most evident in global manufacturers, where ongoing decentralization is essential to introduce efficiency, reduce cost, and reduce risk to disruption in the supply chain. At the same time, these companies are pursuing multiple strategies to maximize the value of the distributed functions across multiple external businesses. Most frequently, value is maximized by increasing supply chain efficiency through application integration between the OEM and suppliers, as well as direct access by external users to OEM applications. Regardless of whether the applications are Product Lifecycle Management (PLM), engineering, Enterprise Resource Planning (ERP) or any other function, each integration or access grant bridges multiple security domains. Each new integration and access grant then represents a potential point of access for unauthorized users looking to exploit security flaws with malicious intent—or simply accidental information access by unknowing users.

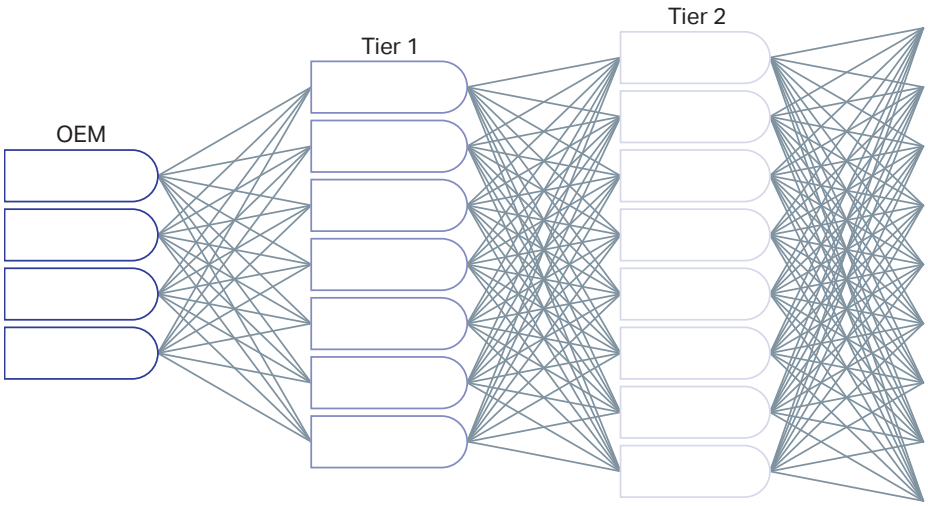
Globalization has opened the door to immeasurable opportunity. The focus has shifted from cost of materials and labor to process innovation and optimization, today's pathway to competitive advantage. Expanding business overseas has exposed the growing complexity of the value chain ecosystem, to an ever more sophisticated set of security risks. Digital assets and resources once secure in walled gardens now need to be available equally to employees in globally distributed facilities, as well as to an ever-changing group of suppliers, partners, distributors, logistics providers, and other value chain partners.

Access to your information is highly distributed



Beyond globalization, enterprises are undertaking significant digital transformation initiatives to integrate more applications and automate processes in a bid to increase productivity and increase the pace of innovation. These initiatives frequently involve the integration of information technology with operational technology, even bridging security domains, through direct integration with value chain partners. Digital transformation initiatives deliver significant value, but potentially put more resources at risk and increase the enterprise security threat surface.

Historically, as the supply chain has decentralized, the enterprise has instituted ad hoc 1:1 connections with suppliers, and directly managed identities and access to secure resources. The individual, point-to-point integrations and access management authorizations are implemented as a mesh network, with each new supplier endpoint representing an exponential increase in the threat surface, exposed to risks such as orphaned or easily compromised accounts, or data integrations with little or no identity or access management controls.



High degree of complexity with multi-tiered partner and user relationships

To optimize efficiency, agility, and drive greater collaboration, it is essential for the enterprise to be able to share information, resources, and applications with external value chain partners in a trusted manner. However, a complex global network of external suppliers, distributors, and other partners also increases the surface area for security vulnerability, and a security breach can have devastating consequences for a brand. To add to the complexity, employees and external stakeholders are also accessing back-end systems and information in a growing myriad of channels—from web portals, to mobile devices, and bring your own device (BYOD). Each may have different security configurations.

opentext™

This creates a path of risk and liability...

1. Companies that will have a major data breach within the next two years[i]: 1 in 4
2. The average cost of a data breach,[i] not including 5% avg. drop in share value[iii]: $3.6M
3. Percent of data breaches that come from human error in data access, not hacking[i]: 53%
4. Internet enabled devices in use by 2020, 40% for business use[iv]: 20B
5. Increase in fines projected under GDPR, starting in 2018[ii]: 4,500%

Managing external identities, determining who should have access to what resources, and validating and auditing access requests to key resources across channels creates significant administrative overhead for the enterprise. The inherent risk in granting access to mission-critical resources to people and organizations outside the enterprise's control is compounded by:

- Lack of visibility into an external organization's hierarchy to validate user requests for access to resources
- Inability to identify orphan accounts, audit whether users are still active at an organization and still need access to resources or know when they leave or change roles and should be de-provisioned or re-provisioned
- Compromised accounts
- External changes in value chain, e.g., mergers and acquisitions or divestiture among suppliers

BYOD and IOT

90%

Percent of organizations not "fully aware" of all network devices, IOT creates significantly more identities to be tracked

Insider threat

34%

Percent of cybercrimes committed by an insider, compared to 31% by people with no valid relationship–exacerbated by growth of third parties and contract labor

Cloud

5-10X

Number of times more cloud services are being used than known by IT, exponential growth of accounts to be managed

Passwords

61%

Percent of users who report using the same password on multiple sites—your corporate credentials are probably being used on Gmail

Enterprise managers require visibility into the organizations on whom they depend, and must be able to delegate administration of people and resources to trusted individuals within the supplier organization if they want to have the agility they need.

i Ponemon Institute: 2017 Cost of Data Breach Study. June 2017

ii David Gurney, Manging Director, Alchemetrics, as quoted by DBM Today. May 2017

iii Ponemon Institute: THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE. June 2017

iv Gartner Inc.: Gartner Press Release located at http://www.gartner.com/newsroom/id/3598917. February 7, 2017

At the same time, they need to be able to govern those external users are authorized to do. This requires regular processes whereby delegated administrators attest to users' validity and the resources to which they have access for a complete audit trail and to ensure compliance.

Identity and access management defined

Identity and access management (IAM) is a technology framework and a set of policies and processes for ensuring that the right people in an enterprise have the appropriate level access to secure resources. IAM systems fall under the overarching umbrella of IT security.

Beyond the most basic function of directory services that maintain the metadata associated with an identity, IAM covers two main functions:

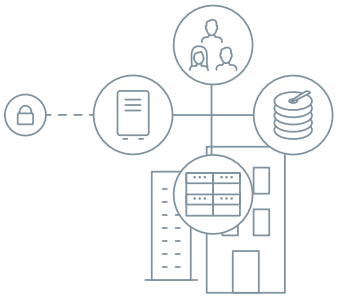
Authentication—the mechanism for establishing the veracity of a user's credentials, effectively determining that a user is who they claim to be, then communicating that authentication across security domains via federated single sign-on or other means.

Authorization—the mechanism for administrating access rights/privileges to protected resources typically related to implementing an information security control point, application access, and role management. Authorizations are typically governed via a defined access policy, incorporating workflow and certification.

IAM is, at its core, the responsibility of the IT department. Paramount is the department's ability to manage the identities their business interacts with—including people, partners, systems, and things. But the business side of the enterprise now has a vested interest in identity management, as well. Many business users rely on their digital identity to do their jobs. If things don't work or they don't have the correct access, they can't get their job done.

The number of digital identities is only going to grow—and enterprises must be able to keep up with this growth for their businesses to continue to grow. Especially with the explosion of connected devices forming the Internet of Things (IoT), the billions of devices need digital identities to manage what information they send and to whom. How do you manage all the external identities that touch your enterprise? Give users access to the resources they need to drive your success? Ensure all interactions are secure, authorized and compliant? De-provision organizations and users when access is no longer appropriate as roles change or business relationships end? Do you even know when an employee of a partner organization no longer works at that organization, or do they take access with them to their new employer?

Is your enterprise cloud ready?



Traditional security

Designed for static devices behind traditional network protection

Cloud-ready security

Designed for elastic cloud environments

opentext™

How does the OpenText™ Covisint™ solution for IAM enable you to manage your most critical identity and access management challenges?

OpenText Covisint offers a robust set of IAM capabilities—entirely hosted in the OpenText Cloud—that provide solutions for customer problems of varying levels of complexity. We have provided cloud-based identity solutions for more than 15 years, and have the track record of successful solutions to prove it.

OpenText Covisint identity cloud services enables enterprises to centrally manage the entire identity lifecycle of their internal and external users, as well as their access to critical resources across the enterprise. The platform provides a comprehensive set of capabilities to connect and manage the people, systems, processes, and things that span the extended enterprise. Our IAM solution addresses identity and access management challenges in three key areas:

1. Onboarding and provisioning

Onboarding and provisioning is a business problem, which deals with the policies, rules, technology, and user experience pertaining to creating and managing user accounts.

Enterprises need robust approval-based access requests, the ability to audit access grants, and the ability to provide answers to the questions of who has what, and why—and for how long?

2. Authentication and access

With network security perimeters disappearing and data flowing freely within and between companies, identity has become the crucial point to help manage, control, and govern access to data, applications, and cloud resources.

This requires the enterprise to master non-core capabilities such as single sign-on, password management, advanced authentication, role-based access control, and directory services integration.

3. Privacy and security

The rise in awareness about compliance management—as well as a growing list of regulations on the matter such as GDPR in Europe—is driving the adoption of IAM solutions for security purposes.

Enterprises must prevent sensitive information from being disclosed to unauthorized recipients. They must reduce or eliminate the risk of financial loss, public embarrassment, or legal liability from unauthorized disclosure of sensitive and/or critical information.

The Covisint solution for IAM mitigates many of the risks inherent in a diverse, globally distributed supply chain. Starting with comprehensive identity and access management capabilities, we can ensure only the right people have access to the most trusted resources when they need them. Adding comprehensive tools for audit and attestation means that the enterprise can easily determine who has access to what resources at any time, as well as how they got access and when they actually accessed the resource.

opentext™

Today, enterprise security is:	What if we could enable…
Opaque High quality, productivity-enhancing, cloud-based tools have gone viral. Enterprises struggle to understand data leakage and other risks.	**Visibility** Provide visibility into behaviors and activities across all applications–both on-premises and in the cloud. View audit logs, analytics, reports, and alerts to identify trends and insights.
Legacy Security architectures are fragile, aging, overdue for costly upgrades, and dependent on the heroics of scarce, expensive staff.	**Cloud readiness** Significantly improve both cost and security with advanced architectures that optimize on-premises with cloud.
Fragmented Separate accounts for new cloud applications cause huge problems with password management, user account updates, and employee termination.	**Unified identity** Ensure that all cloud and on-premises apps leverage a single identity store, authenticating users directly against a single cloud directory.
Non-compliant "Shadow IT" is a concern for many enterprises as users adopt cloud apps without the approval, support, or oversight of official IT policies and procedures.	**Robust compliance** Control and audit who is allowed to access a particular app, and under what conditions and context. Enable policies by applications, or even by functionality within an application.

Increase the security of your supply chain without compromising agility and innovation

A foundational element of secure collaboration across an extended supply chain is a secure, scalable capability to manage the identities of all the external organizations and people that comprise the extended supply chain ecosystem.

The OpenText Covisint solution for IAM provides a robust set of tools to manage all of the identities that touch your enterprise. While most solutions simply provide single sign-on (SSO) for internal users (employees) to access cloud applications from inside the enterprise outward, the OpenText Cloud solution helps manage, automate, and govern the complex network of external identities that need "outside-in" access to internal applications and resources. Managing access for users that are not employed by your organization is a significantly larger challenge than internal SSO.

At OpenText, our advanced identity features such as delegated administration, authorization management, and automated provisioning have been designed and hardened over years of experience with some of the largest global companies to secure information flow amongst complex, multi-level networks of products and people that reside external to organizations—outside-in.

The platform is able to act as the system of record for all the enterprise's external users and organizations, or integrate with existing systems, synchronizing user profile and authorization information. OpenText supports a wide range of user and authorization provisioning scenarios including:

- Synchronization with enterprise directories (LDAP, AD, etc.)
- Provision users and entitlements (applications authorizations) to enterprise Web Access Manager (WAM)
- Synchronization of user profile information and privileges to legacy or cloud applications
- Support for a wide range of implementation patterns and protocols including Just in Time provisioning on first federation, out of band synchronization, SPML, SCIM, and custom implementations using Covisint IDSync and IDBridge components

Self-service tools allow the enterprise to enable external organizations to register, build, and populate their own organizational hierarchies of user identities. The external organization can define its own organizational hierarchy on the platform without effort or involvement from enterprise administrators. Once the enterprise administrator has delegated administrative capability to a user at an external organization, that external organization can add users, and also add additional delegated administrators within that organization.

These self-service administration and delegation capabilities make it possible for the enterprise to:

- Streamline the process for managing access to resources
- Reduce administrative workload for the enterprise administrators
- Increase security related to validating requests and user registration by placing the decision-making capability closest to local knowledge
- Enable delegated administrators to manage multiple applications from multiple different security domains

These identity governance features are most important and useful when managing large groups of external users and are the best in the industry. Covisint delegated administration features allow the business partner's administrators, those that know the users best, to manage their users' access while still giving administrator oversight. Configurable workflows allow the process for users to gain access to applications to be as simple or complex as policies require.

OpenText's attestation capabilities keep administrators on task to verify that users and organizations have the access they should. This protects your business from a policy and regulatory standpoint and also helps ensure information is only in the hands of people that should have it.

opentext™

OpenText provides a set of automated tools and workflows for quarterly and annual user and application audits. These tools require delegated administrators to review and attest to both the validity of user accounts and the applications granted to those users. Even though the enterprise administrator has no visibility into whether a particular user is still employed by a supplier, or whether they should or should not have access to a particular application, that enterprise administrator can delegate the administration of a supplier's users and their access to applications, and then enforce governance through these automated tools.

As organizations grow and evolve, those same delegated administrators can manage merging of divisions and user lifecycles. For the enterprise, the platform also provides the capability to merge organizations and manage authorizations and access throughout the lifecycle of those external organizations.

The combination of data exchange, identity management, and IoT services ensures that bi-directional exchange occurs between the right constituents (across legal entities, your supply chain, or your dealer network, for example). The ability to apply fine-grained authorization access controls to people, systems, and applications outside your organization ensures that trusted information gets to the right people and things at the right time.

What OpenText does, better than anyone else, is provide the tools needed to model and manage the extremely complex organizational hierarchies of your business partners. This ensures they have timely yet secure and authorized access to the information needed to do business with you.

IAM lays the path to savings and value

1. 310% — ROI vs. DIY software, which is 85% more expensive than cloud IAM[i]
2. >28M — Annual savings with Covisint self-service ID administration e.g., avoid help desk calls for password resets[iii]
3. 75% — Reduction in your threat surface area by adopting an identity hub model with SSO[i]
4. >100K — Supply chain companies administered globally via Covisint delegated access administration[ii]
5. >$1B — Compliance penalties avoided across customer base with audit, attestation, and de-provisioning[ii]
6. 60% — Average reduction in users with excessive privileges with identity management solutions[iv]

i Forrester Research, Inc.: Use Commercial IAM Solutions To Achieve More Than 100% ROI Over Manual Processes. October 2012

ii Internal OpenText / Covisint

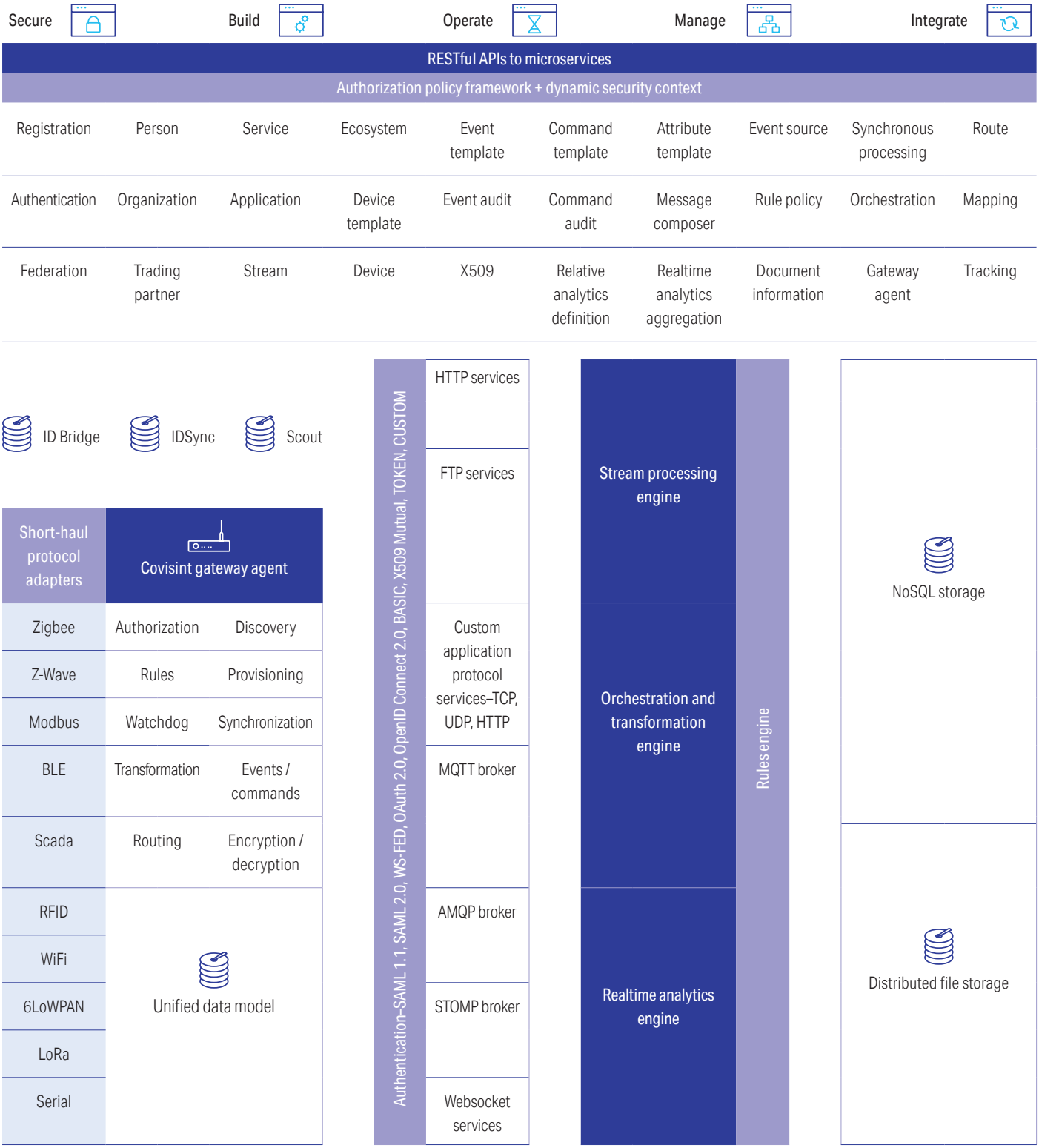
iii Mandylion Research Labs: ROI calculator located at http://www.mandylionlabs.com/PRCCalc/PRCCalc.htm

iv Forrester Research, Inc.: Brief: Reframe The Business Case For Identity And Access Management In Security Terms. March 2015

opentext™

OpenText Covisint solution components

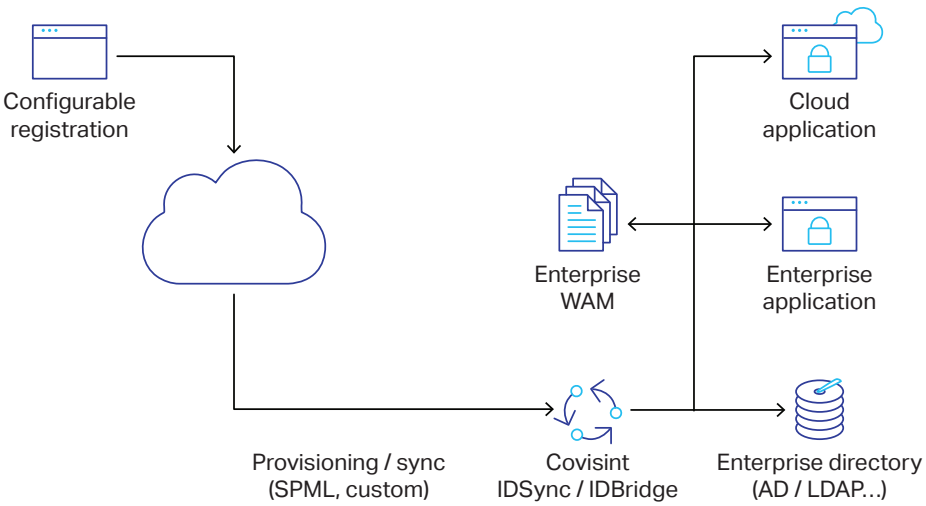
The OpenText platform is comprised of a set of integrated and modular cloud-based technologies purpose-built for simplified collaboration, IoT, and identity-centric solutions across your extended business ecosystem.



OpenText API's and developer tools accelerate new solution and application development while increasing security. OpenText Covisint enables enterprises to create frameworks for managing the complex relationships between identities and critical business resources.

Identity Manager

Designed for comprehensive identity lifecycle and access management across the complex ecosystem of enterprise identities.

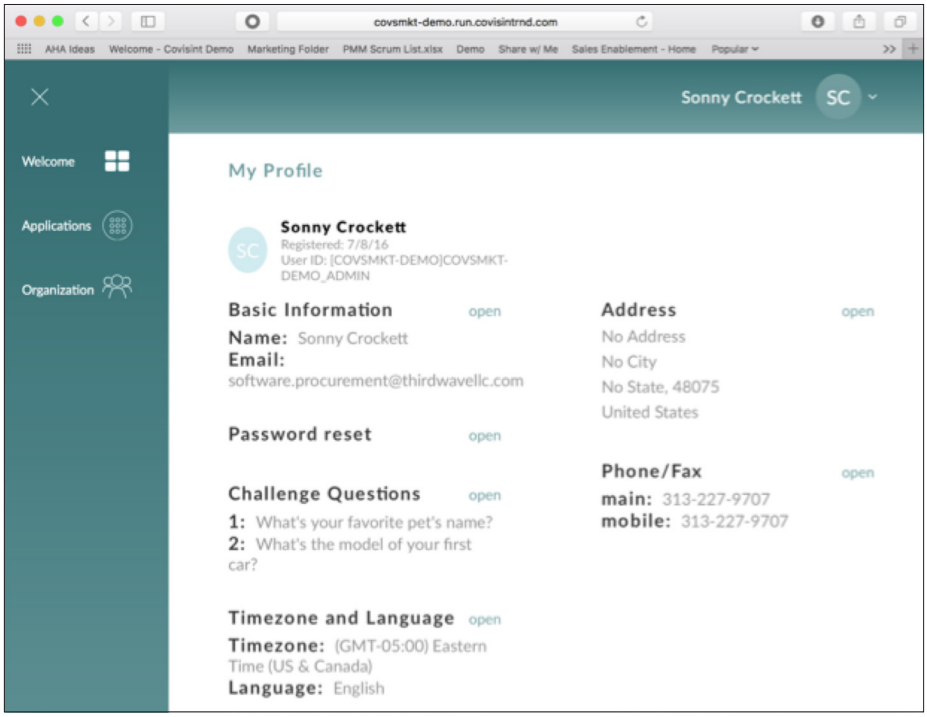


Features

Identity lifecycle management—Capabilities to manage an identity from provisioning through changes in role, access, and administration, and ultimately to de-provisioning.

Password and policy management—Self-service password management with end-user challenge questions/answers, and admin password resets that allow for higher-touch support. Policies include facilities for defining and enforcing customer password policies such as password length, age, and complexity.

Role and profile management—Self-service management of standard and custom user profile attributes with multi-lingual UI support. Definition and management of standard and custom roles, privileges, and assigning roles to users with synchronization to external systems.



Example user profile

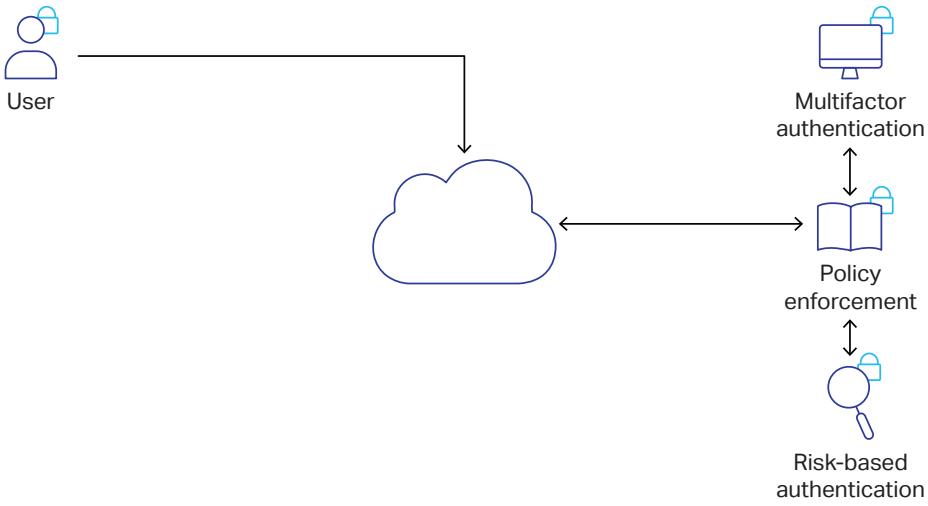
Authentication and policy management—Define and enforce authentication policies and establish policy order precedence mode based on role, division, top-level organization, or realm.

Basic authentication—Support for end-user entry of credentials in the form of a user ID and password when making a request to access an application or resource.

Multifactor authentication—Wide range of multi-factor authentication options, including SMS, email, and phone call, providing the user with a numeric code and requesting entry of the algorithmically-generated time-synchronous numeric code. OpenText Covisint supports:

- Flexible multi-factor support
- Integrated with RBA
- Up authentication with multi-factor
- Second factors
- IDcipher TM
- SMS
- Phone call
- Soft token
- Google authenticator
- Out-of-band push
- Third-party

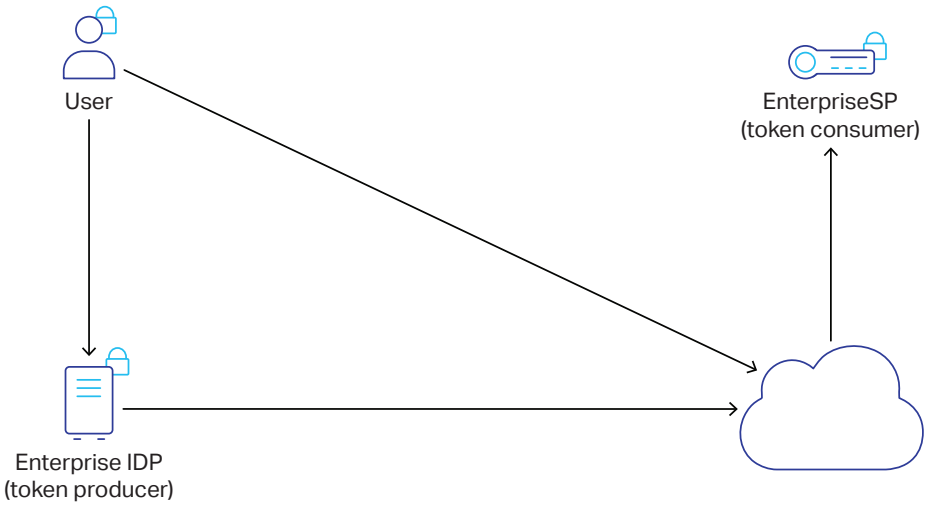
Risk-based authentication—Risk-based authentication to identify scenarios such a user authenticating from an unknown device, location, or unusual time. Scenarios are defined by control triggers, used to configure system actions according to preferences.



OpenText has implemented a risk-based authentication module that utilizes both user provided (e.g., username) and system collected user information (e.g., registered device or network) to authenticate the user's request to the protected target resources. User provided data includes username and password, or SAML assertion for federated users. Collected user data includes attributes provided from the internet communications between the user and the authentication system (e.g., the user PC's IP address) as well as customer behavior and transaction patterns (e.g., log-in time and frequency). The collected information is used to evaluate the risk level of the access request. The risk level is evaluated against a set of pre-defined risk criteria and is used to decide if a higher authentication mechanism (e.g., SecureID or the OpenText provided ID Cipher Card authentication) is needed. Risk-based authentication assessments occur at log-in or federation time.

- Risk-based authentication criteria
- Federated access
- Registered device
- Registered network
- Time of day
- Time since last access
- High frequency access
- Repetitive access
- First-time log-in

Identity federation—Establish trust relationships across security domains for moving authenticated identities among and between entities in a federated model.



Single sign-on provides user access to multiple applications with one authentication process.

- ID/password authentication
- Industry standard SSO support
- MDSO launched in 2001
- SAML, OpenID Connect, OAuth, WS-Fed
- Optional discovery services for federated users

SSO for B2C, B2B, B2E plugin—Single sign-on provides user access to resources within multiple security domains with one authentication process, plugins, and reference implementations for B2E, B2C, B2B, and Industry Exchange identity scenarios.

Authorization Manager

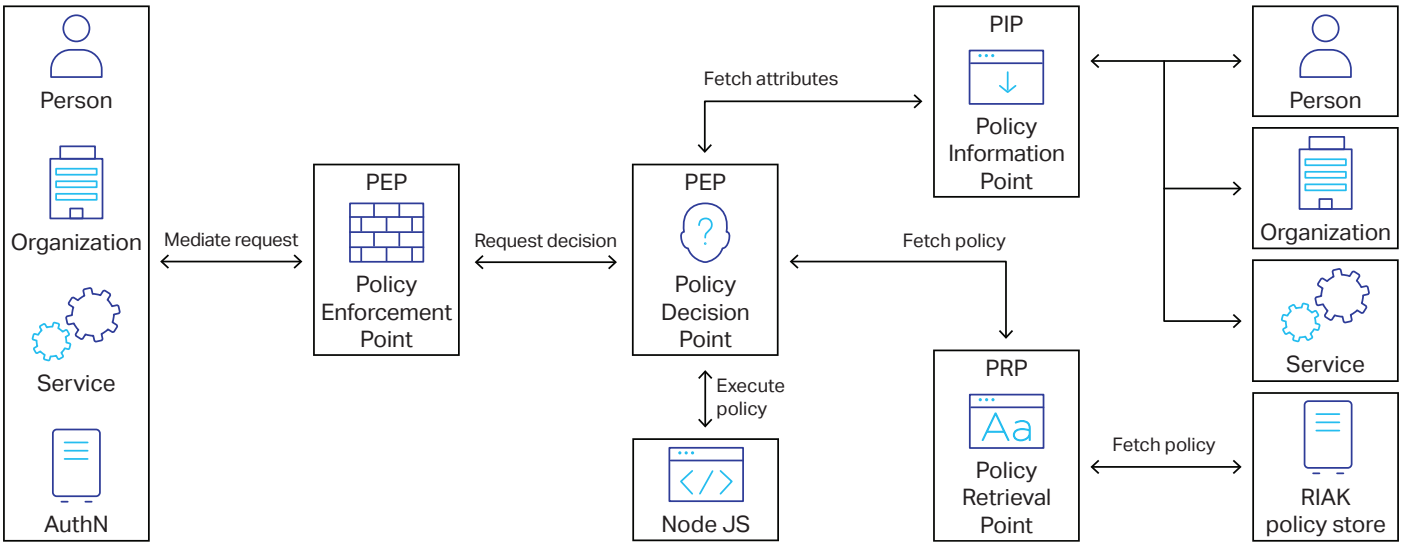
Establish access and authorization administration, delegation, and policy management framework.

Features

Attribute-based authorization—Attribute-based authorization based on authorization policy framework provides API-based and automated access management for delivering personalized user context.

Authorization policy framework—The authorization security layer that acts as the gatekeeper for access to protected resources delivering a highly performing dynamic security context.

The Covisint solution for IAM also includes an authorization policy framework to apply authorization policies at API endpoints, delivering a highly performant, dynamic security context for external applications that call OpenText or third-party APIs. The authorization policy framework is the authorization security layer that acts as the gatekeeper for access to protected resources. When an application calls any API exposed through Covisint on behalf of a user of the application, the authorization policy framework evaluates that API request.



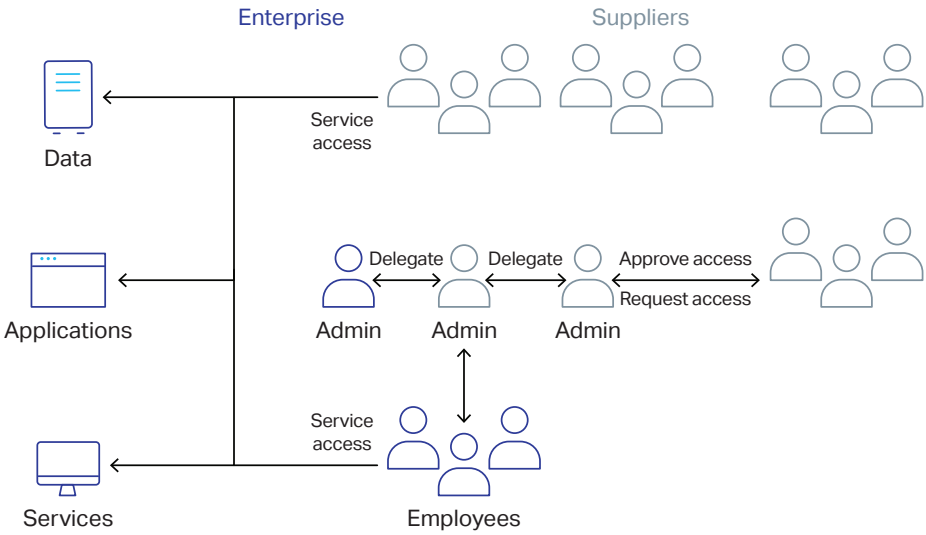
Each API endpoint has an authorization policy. Policies are based on the subject, resource, and action in the API request.
1. Subjects can be a person or device
2. A resource can be person, organization, group, service, device, authentication, etc.
3. The action is the verb of the service, for example: update person, add service package, etc.

Authorization policies determine if a subject is authorized to perform the requested action on a resource.

Multi-protocol support—Efficiently connect IDPs and SPs in a many-to-many relationship model with cross-domain SSO, support for all standard federation protocols including SAML, WS-Federation, OAuth, OIDC, custom legacy federation interfaces, and translation and mapping between different protocols.

Delegated administration—User access management can be performed by designated administrators within or outside the organization, by administrators in higher-tier organizations, or by application/service owners with full audit and audit enforcement.

Delegated administration offers configurable administrative roles and span of control to enable external organizations to manage their own user access to corporate resources. Organization administrators, or application/service owners in higher-tier organizations, delegate user access and authorization management to designated administrators within the external organization. This flexible delegated model provides an effective and scalable approach for administering user permissions at scale.



Audit and attestation—Constant change in employee and external user status requires audit and attestation to ensure proper access at all times. For internal and regulatory compliance, periodic notification of administrators requiring a review of their assigned users ensures that each user's status and access rights are correct.

User attestation

- User verification
- Typically quarterly
- By organizational administrator
- Delegated function
- With oversight reporting
- Automated enforcement

User attestation

- User verification
- Typically quarterly
- By organizational administrator
- Delegated function
- With oversight reporting
- Automated enforcement

Workflows and delegation—User self-service application requests that trigger a standard, configurable workflow. Once an organization has been granted access to a particular application, users within that organization may request access triggering a notification to their administrator to approve/deny the request. Upon completion, the requesting user is notified of the decision.

The default workflow options for the platform constructs are as follows:

Workflow	Organization	Person	Package
Manual approval	×	×	×
Manual approval			×
Manual approval	×	×	×
Manual approval	×	×	×

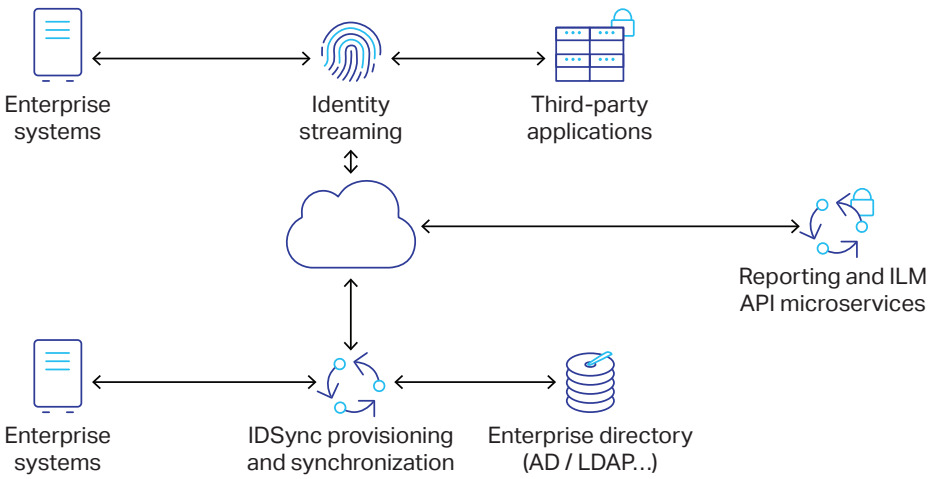
Centralized access management—Deep functionality for managing access to services and applications via hierarchical authorization rules with delegation. Services can be configured with multi-step approval workflows.

Secure token service—Issue security tokens for access requests to secure software applications/relaying parties. Instead of the application authenticating the client directly, the client is redirected to the IAM solution, which authenticates the client and issues a security token.

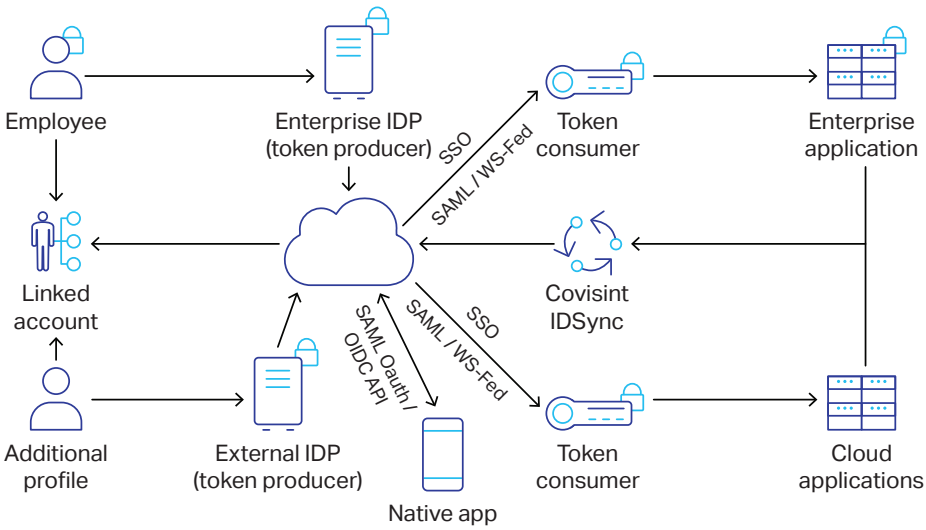
Identity Sync, Analysis & Intelligence

Aggregate, synchronize, inspect, and analyze identity, access, and end-point data—then convert it to actionable information and insight.

Identity synchronization—Synchronize identity and access management information between enterprise systems and the Covisint platform, ensuring that users created, updated, and deleted in the Covisint Cloud directory or the enterprise user directory are propagated to the appropriate resources, enabling effective user provisioning, authorization management, and access revocation.



Account linking—Aggregate and link user profile, authentication, access, role, and entitlement data across multiple user profiles in disparate applications and resources and/or related to multiple identity providers.



Identity reports—Standard role-oriented reports available through a web-based interface displaying usage and audit information across all users and resources under management to various administrators of the system.

Identity intelligence—Analytics and reporting of identities, entitlement assignments, and administrative actions to drive greater visibility for governance across the IT landscape.

API-driven reporting—Reporting capabilities are also readily available through standard API interfaces to feed identity intelligence data into other business systems.

Threat policies—Integration between identity streaming, stream analytics, and the Covisint Rules Engine stream threat indicator-related identity events through unified messaging to SIEM and UEBA applications.

Identity Event Streaming Engine

Cloud-based directory and the tools to integrate and synchronize directories and identity-related data.

Identity event framework—Framework for performance optimization and data syndication/synchronization through which all actions on entities in the identity domain model produce event messages.

Identity adapters—Adapters to ingest and publish identity data from/to third-party data stores and enterprise systems and integration of third party web services.

Identity verification—Identity verification enables corroboration of identity information against a real-world information source, such as DEA prescribing physician number or employee ID.

Identity event streaming—Industry standard pub/sub model for subscription to Identity and Access Management events enables systems to stream identity events for provisioning, synchronization, or security information and event management (SIEM) integration.

Rules engine—Robust engine that enables authoring of JavaScript rules, providing real-time decision making based on identity event triggers, allowing programmatic integration with workflow and APIs to take automatic actions based on rules.

SIEM adapters—Security information and event management (SIEM) adapters support threat detection and security incident response through the real-time collection and analysis of security events from a wide variety of event and contextual data sources across disparate sources.

Pub-sub engine—Real-time messaging service for publishing and subscribing to events and exchange messages. Events generate messages with a payload that can be subscribed by applications or APIs.

The OpenText difference

Differentiation is in the solution—a cloud-based service that unlocks customer and partner led development and faster innovation in the application layer.

- **Purpose-built**—The only platform designed for your extended B2B ecosystem, connecting people, processes, systems, and things
- **Offered as a cloud service**—to drive operational simplification and reduce costs through economies of scale
- **Infrastructure agnostic and highly scalable**—to meet the privacy, security, and performance demands of increasingly global businesses
- **Proven**—Manages access to 500+ General Motors Company (GM) apps by 150K users at 50K companies, with only two security admins. Drove a 40 percent increase in Hyundai BlueLink service retention. Manages >25M identities, including all GM vehicles with OnStar
- **Stable**—Backed by size, leadership, EIM focus, and OpenText investment

opentext™

Case studies

Daimler

Does your enterprise have an extended supply chain or joint venture network? Do you need them to work securely and seamlessly together to deliver key products and services to the right place at the right time?

Daimler AG is a multinational automotive corporation headquartered in Stuttgart, Germany. By unit sales, it is one of the largest vehicle manufacturers in the world.

Daimler's use of the supplier engagement portal began in early 2002. A need for a common platform to share data amongst automotive suppliers was formed to establish a unified approach in supply chain engagement through seamless integration. In a hyper-connected and cloud-based world, intense competition and increased cost of raw materials and labor and cost down initiatives are fueling automotive suppliers to provide flexibility with a wide variety of solutions.

Initiative

In order to inform Daimler partners about business process, relevant changes, and current projects, the development of Daimler's registration application followed suit. Daimler also faced new challenges to improve interaction with its supply base, support, request interaction, and knowledge exchange, and sought to increase competitive advantages and loyalty between partners with Covisint's Supply Portal.

"At the beginning it was only a platform to use applications, and it has changed to a communications tool and also the way a supplier registers. We developed our applications further and we had a lot more users on the portal," said Sabine Braendle, senior manager of corporate procurement communications at Daimler.

As one of the world's leading cloud-based B2B platforms for simplifying supply chain collaboration, Covisint's Supply Chain Portal allows suppliers to work with each other through seamless integration.

In addition, its scalability allows Daimler to handle massive volumes of transactions generated by many different systems. Covisint enables automotive organizations like Daimler to securely exchange information across the largest B2B platform in the world.

Results

Daimlers Supplier Portal includes dynamic mobile device detection, enhanced content and document management, and more robust and user-friendly search functionality to streamline the registration process for suppliers. These enhancements make it easier and faster to respond to the ever-changing demands of effective supply chain management. It improved simplicity, usability, mobile accessibility, and time-to-value for Daimler by:

- Providing only relevant and customized information to each user, letting users 'search' for the relevant data
- Using improved technology to interact with suppliers
- Focusing on a cooperative and sustainable business model with suppliers
- Asking for feedback and interacting closely to improve processes

It also promotes flexibility, allowing trading partners or customers to communicate through their own language or system, while reducing costs to remain agile. A single solution connects with all trading partners around the globe, offering support anytime, anywhere with industry-leading SLAs and uptime.

"We try to align to the new communication standard by providing information in a more active and interactive way. In the future, you cannot force your partners to read over long internet pages, you have to find a way to make it interesting and interactive. Our suppliers already gave us feedback on what they want, and are willing to give us feedback to improve the whole process on both sides," said Ralph Greiner, manager of corporate procurement communications at Daimler.

The portal provided these key features:
- Single entry for users and administrators
- System checks for existing company registration at the first step
- Reduced pages when coming from Daimler portal pages
- Faster supplier onboarding and reduced helpdesk calls

"The major benefit is that it's easier, you have fewer helpdesk calls, and the registration process is easier. Our target was an ease of process and we value OpenText Covisint in the sense that we believe in the model of a common platform to do so," said Breandle.

About 70,000 users engage in Daimlers' Supplier Portal with 5,000-10,000 new users every year.

Shell

Shell is a global group of energy and petrochemical companies with around 90,000 employees in more than 80 countries and territories. Shell's aim is to meet the energy needs of society, in ways that are economically, socially, and environmentally viable, now and in the future. Shell uses an innovative approach to technology that ensures they are ready to help tackle the challenges of the new energy future.

Shell global projects utilize a significant number of non-Shell personnel to complete. Non-Shell employees require a Shell ID to access Shell systems. OpenText Covisint provides Identity Provisioning Services for these some 75,000 people. The IAM solution provides attestation, auditing, password maintenance, and reporting of these activities. In addition, OpenText provides a gateway to authenticate and authorize non-Shell employees on Shell applications.

Challenge

- Diverse, loosely coupled workforce with special identity and security requirements
- Need to provide provisioning services for 75,000 identities of contractors and joint ventures
- Goal to institute highly secure provisioning throughout extended workforce

Results

- Quick provisioning and de-provisioning
- Improved security and auditing
- Better security visibility across contractors and joint ventures

opentext™

About OpenText

OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

opentext.com/contact

(10/207)08223ENrev1