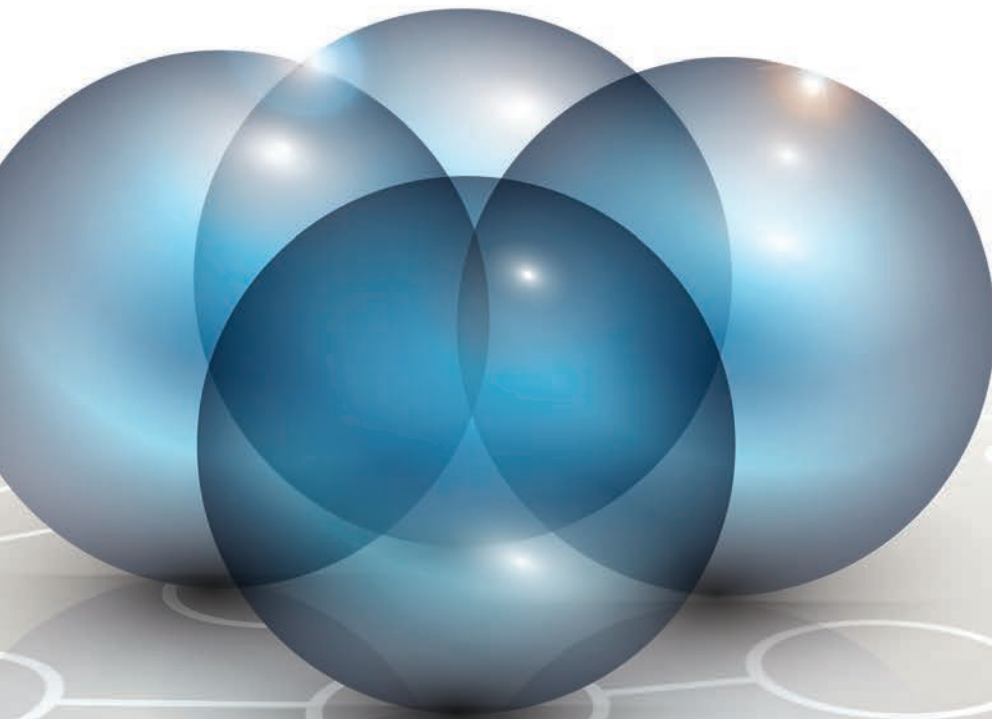


Cloud Identity Services

Extended Workforce Security



| a Compuware Company



Cloud Identity Services

Your company is like many organizations today: enterprise-wide security is a necessity, but not a core competency. The need to manage individual identities across a broad network of internal and external employees, customers, partners, and other stakeholders takes time and resources away from your normal business support activities. Barriers to providing simpler, more cost-effective solutions that allow your users to access the information they need, continuously grow in numbers. These challenges include:

- Allowing your users to securely connect with external organizations and partners given a multitude of standards and protocols
- Providing a positive end user experience as your users search across an unmanageable number of systems that require different ID and password combinations
- Having enough IT resources or budget to support the complexity of your global business without additional IT capital expense
- Decreasing time-to-market for new applications and systems to maintain your competitive edge
- Maintaining visibility and enforcing policies with business constituents located outside your organization's firewall
- Decreasing your risk and cost associated with non-compliance and adherence to an ever-growing set of regulations

Industry analysts estimate the annual cost associated with identity and password administration can average \$100 per user per identity. Given an enterprise with 5000 business users, each with three to seven system identities, ID and password management can amount to between \$1.5 and \$3.0 million in costs per year.

These issues and many more, are the reason many organizations like yours are turning to cloud solutions to manage system

and application security for their users. Industry studies have proven that the “cloud” offers a more cost effective method to manage identities than the traditional approach of developing and deploying in-house solutions.

Simplifying Connectivity and Collaboration

Cloud Identity Services, at the core of the Covisint Platform, drastically reduce the burden of integrating complex systems, managing multiple IDs and passwords across a wide network of constituents, performing time-consuming administration and reporting, and ensuring compliance. Cloud Identity Services enable organizations to simply and securely manage digital identities across virtually any combination of internal/external systems and end user groups.

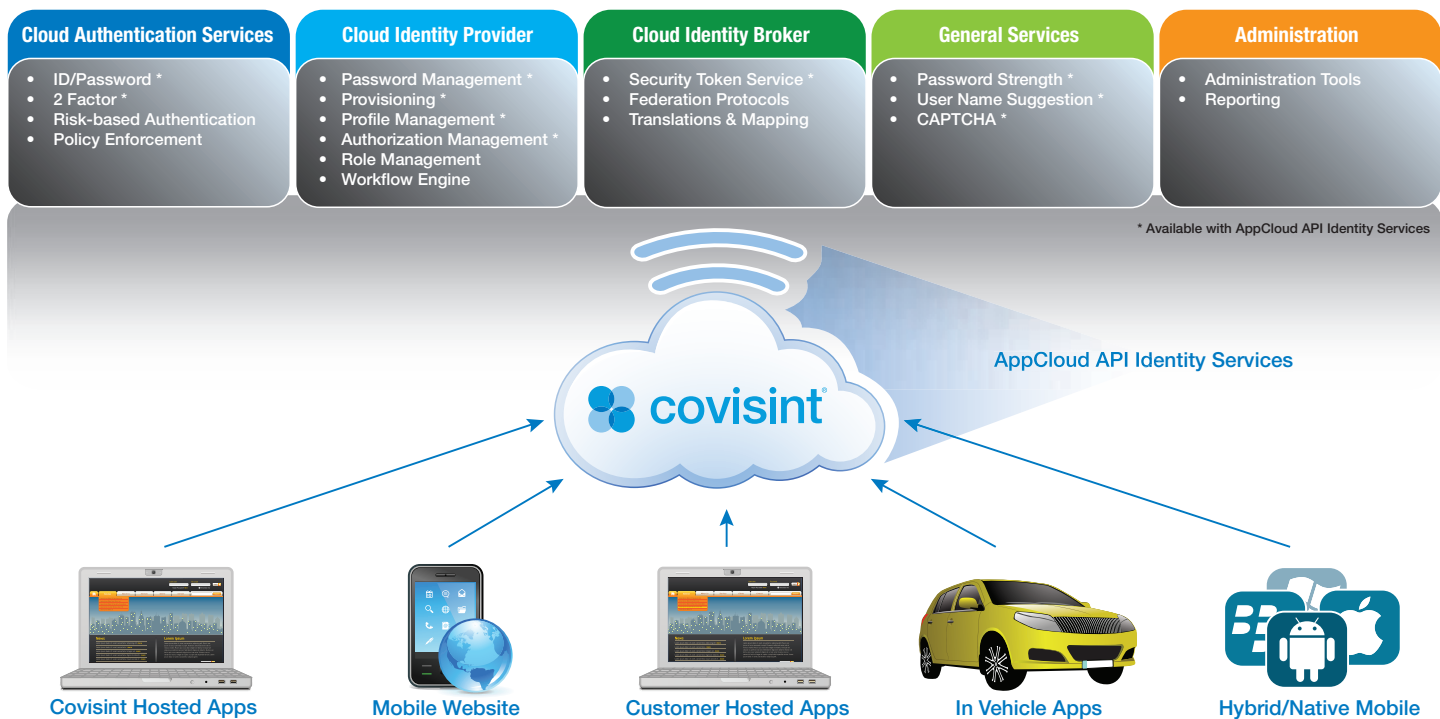
Delivered as an on demand set of services, Cloud Identity Services centralize and automate processes surrounding the exposure, acceptance, and monitoring of digital identities across security domains. These services enable organizations to leverage industry-leading services while remaining insulated from the cost and complexity of “do-it-yourself” approaches. Cloud Identity Services include a set of comprehensive services described below.

Cloud Authentication Services

Authentication services are provided to confirm a user or computer's identity before they access your systems. This service prevents unauthorized users from hacking into your systems.

Cloud Authentication Services provide primary authentication to your users regardless of whether they are employees, contractors, suppliers, partners, clients or customers. This is done by directly binding the user to their credentials, and then providing him/her with a domain specific security token to be used for session security.

Cloud Authentication Services provides two-factor authentication and also provides support for identity risk scenarios at the time of authentication. Upon receipt of the unique code, a user simply enters it, along with their password, to gain access. If



desired, two-factor authentication can also be a mandatory requirement for your users, each time they log into your system. Our risk-based authentication can identify such scenarios as when your user is authenticating from an unknown device, location, outside of normal time parameters, and more. The following multi-factor authentication techniques are supported: SMS Text, Phone Call, Email, Mobile Push Notification, Smartphone Passcode and IDCipher™. When mandatory two-factor and risk-based authentication are combined, it is a very powerful tool to secure your systems.

Cloud Identity Provider

Cloud Identity Provider allows your organization's appointed Administrators to manage group and user information, and the applications that are available to them.

Cloud Identity Provider allows for the creation and management of an identities lifecycle. With this service you are able to invite, register, and approve identities, as well as suspend and remove identities once the user is no longer engaged with your organization.

Other key features of this service include:

- Delegated administration
- Management of user access to applications with flexible workflow capabilities
- Attestation (auditing of user access)
- Reporting
- Inbound and outbound provisioning to customers and third-parties based on SPML and RestFul JSON techniques

Cloud Identity Provider features provide support for delegated administration that allows the administrative workload to be distributed within an organization and among partners and affiliates. Configurable workflow processes are supported which can also include real-time messaging to remote locations that will be able to receive and respond to events that are part of a workflow.

There are administrative features available to manage:

- The information associated with a group or user
- System administration roles associated with a user
- Application specific roles associated with the user

Cloud Identity Broker

Cloud Identity Broker is a service that includes an enterprise federation “hub” that allows your users to federate with other providers applications. As a hosted security service, this offering centralizes and automates the process of exposing, accepting and monitoring digital identities across multiple security domains.

Cloud Identity Broker helps organizations leverage state-of-the-art digital identity management services while insulating them from the cost and complexity using “do-it-yourself” approaches. A single connection to Covisint drastically reduces the burden of complex systems integration, management of multiple IDs and passwords, time-consuming reporting, security rules enforcement and help desk administration.

With one single connection to Covisint, your organization is insulated from the concern over any 3rd party integrations, future standards and/or upgrades. Covisint is able to implement any integration with 3rd party technology or systems on your behalf – they just “plug right in” and your organization is ready to go.

The Cloud Identity Broker supports protocol translation, which allows you to select the technology and standards (ex. SAML 1.1, SAML 2.0, Open ID 2.0, OAuth 1.0, 2.0, GFIPM, WS-Fed 1.1, etc.) best suited to your organizations backend environment, without fear of dependencies or interoperability issues with other partners.

The Cloud Identity Broker also supports attribute mapping that allows an identity provider and service provider to utilize a standard set of broker attribute names that can then be mapped to specific names that are required by the identity provider or service provider.

AppCloud® API Identity Services

Covisint provides ready-to-use API’s for its leading authentication and provisioning services so that your developers, and other third parties working with your organization, may secure your applications and systems with our industry leading identity services.

AppCloud API Identity Services can be used to build your own administrative tools for registering and managing identity lifecycles, as well as managing an identities access to applications. Covisint’s AppCloud API Identity Services can be used for enabling and supporting mobile and other devices.

AppCloud® API Identity Services include a Developer Portal. This feature-rich portal provides a console that allows developers to execute test API transactions, obtain help documentation, as-well-as utilize social tools such as forums and blogs. As part of the service, you will receive a full analytics view of how all of your transactions are performing, with overall usage rates.

There is no software to install. Covisint’s AppCloud API Identity Services are provided in the cloud and include industry leading enterprise SLA’s.

Covisint: Leveraging the Benefits of On Demand

Covisint's on-demand approach to identity management results in reduced complexity, automation of organizational processes, and improved policy compliance. As a hosted cloud identity service, Covisint provides a service-based approach to federated identity management that centralizes and automates the process of exposing, accepting and monitoring digital identities across security domains.

Covisint Identity Services are fully hosted and managed solutions that allow organizations to take advantage of the latest generation of identity management technologies without the financial burden of owning dedicated hardware and software. Like traditional identity management solutions, Covisint's hosted service provides organizations with the ability to manage the entire end user lifecycle and automate the management of identities, access rights and resources across multiple IT applications and business processes.

Using Covisint Identity Services, end users experience a unique ability to access relevant information and applications through a single digital identity and sign-on. Organizations like yours leverage a trusted partner to support end-to-end identity management and realize the following benefits:

- Reduced cost and complexity associated with managing identities and access privileges across constituents

- Seamless integrations with systems and applications; simplified endpoint connectivity and collaboration
- Anytime, anywhere access to applications for users across the extended enterprise
- Improved end-user experience via single sign-on to multiple systems and applications
- Faster deployment versus in-house or on-premise
- Simple compliance with regulations and enterprise policies—for users inside and outside a firewall
- Unparalleled security, service; and access to a global help desk

At the Core: Covisint Platform

As a recognized pioneer in cloud computing, Covisint has driven the on-demand evolution in the way enterprises connect, communicate, and collaborate with all the stakeholders required to achieve optimum performance. The industry proven Covisint Platform includes services for identity management, community collaboration, and electronic messaging. Underlying these core service offerings are Covisint Support Services including unparalleled security, availability, response times, and global customer support.



“Covisint ... a cloud computing pioneer” - Forrester Research



“Covisint ... a hosted identity access management market share leader” - Forrester Research



“Covisint ... ‘in a league of its own, with no direct competitors,’ and ‘one of the pioneers in identity and access management’” - IDC

To learn more about Cloud Identity Services, visit identity.covisint.com today.



Covisint is a recognized pioneer in cloud computing , driving the digital shift in how industries and enterprises connect, engage, and collaborate with external business partners to achieve optimum performance.

NORTH AMERICA

Covisint
World Headquarters
One Campus Martius
Detroit, Michigan 48226
United States of America
888.222.1700 phone
313.227.7300 phone
313.227.6410 fax

Covisint
280 Mangum Street
Suite 540
Durham, North Carolina 27701
United States of America
919.425.0555 phone
919.425.0577 fax

EUROPE

Covisint
An der Trift 65
63303 Dreieich
Germany
49.6103.9488.0 phone
49.6103.9488.88 fax

ASIA-PACIFIC

Covisint
Suite 804, United Plaza
1468 Nanjing Road West
Shanghai, China 200040
86.21.6247.9222 phone
86.21.6247.0683 fax

www.covisint.com

All Compuware products and services listed within are trademarks or registered trademarks of Compuware Corporation. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All other company or product names are trademarks of their respective owners.