Identity and Access Management Solutions

Buyer’s Guide

Includes a Category Overview
The Top 10 Questions to Ask
An Identity Management Glossary
Plus a Capabilities Reference of the Leading Identity and Access Management Solution Providers
INTRODUCTION:

Username and password, please. You’re asked for it every day and you’ve probably got several combinations—work email, personal email, Facebook, Twitter, Amazon, Online Banking, your CRM system—the list goes on. As of 2016, the average professional is likely to be keeping track of dozens of username/password combinations. Those combinations are the basis of good old-fashioned Identity and Access Management, and, while the process seems to work well enough, it is in fact remarkably old, cumbersome, unreliable, and worst of all, insecure.

The clean line we’ve drawn between the world we live in and the one we work in is blurring. The glut of mobile devices in the workplace and new corporate policies allowing employees to access secure corporate networks with their own phone or tablet further muddy the water. Add to that the advancement of cloud computing and the evolutions of distributed systems, data, and networks, and you’ve got a flood of security challenges for IT professionals. As Bob Dylan once wrote, ‘you’d better start swimmin’ or you’ll sink like a stone, for the times they are a-changin’.

In the modern IT environment, organizations need to know exactly who is accessing what, when, where, why, and how. The stakes have never been higher. From Target to Edward Snowden to the Office of Personnel Management breach, the lack of controls on information systems and sensitive data has caused a remarkable series of scandals over the past decade that have resulted in a loss in consumer trust as well as increased government regulation. So how can modern organizations keep up?

The best practice for the enterprise is to implement an Identity and Access Management (IAM) solution that handles the creation and management of user or connected device information as well as user’s access and authentication into external and internal applications, databases, or networks.

Whether you are a publicly traded corporation, a government institution, a small to medium-sized business, or even a start-up, the need for IAM has never been greater. In fact, given the regulatory, security, and PR implications, the IAM solution may be the single most important information security best practice you will ever implement.

Solutions Review is not in the business of picking winners and losers in a technology solutions sector, we’ll leave that to others. Our job is to help you get started solving the problem. To that end, we’ve listed the top 28 Identity and Access Management solutions providers as a way to as a way to narrow things down a bit.

In our analysis of each vendor, we’ve highlighted the products and services offered, key features, strengths, and markets best served. We’ve also placed each vendor’s core strengths and offerings into four categories: Identity Governance and Administration (IGA), Identity Management as a Service (IDaaS), Customer Identity and Access Management (CIAM), and Privileged Account Management (PAM).

If you need more information on the above terms and what they mean, please reference this document’s glossary. Categories are listed underneath vendor contact information.

In order to help you begin sorting all of this out, below are 10 questions—five for organization, and five for prospective solutions providers—that will walk you through what you want in a solution, what it’s supposed to do for you, how it will work in your IT environment, as well as the solutions offerings, services, and staying power.

As always, If you’d like any more help from us, please feel free to send along an email.

Jeffrey Edwards
Editor
Solutions Review
5 Questions You Should Ask Yourself Before Selecting an Identity Management Solution

QUESTION #1 Should we go with an on-premise solution or a cloud-based IAM provider?

For many organizations, this is as much a political decision as it is a business decision. Many still believe that on-premise solutions provide greater security and control, and, realistically, it’s often the path of least resistance for a large enterprise with the resources to manage the operation and integration. On the other hand, cloud solutions offer immediate cost savings, faster implementation, easy scalability, and much greater flexibility. There’s no right answer here and you’ll find many solutions offer both cloud and on-premise, as well as hybrids of the two, which may be the best answer for getting something in place sooner rather than later.

QUESTION #2 What applications do we need our Identity Management solution to integrate with or support?

Cloud-based Software-as-a-Service (SaaS) applications have transformed the business world and complicated the identity management world. Many IAM solutions are now building libraries of thousands of applications that they can support or integrate. Take stock of every app that you want employees to have access to (and track), then ask the vendors you are considering to provide a list of the business and consumer applications that they support – either in the cloud or behind a firewall – and what advantages that support provides for your implementation.

“Take stock of every app that you want employees to have access to (and track).”

QUESTION #3 Do we need a point solution or a full platform?

Our 2016 Buyer’s Guide includes 28 solutions, a wider range than any of our previous iterations. Some of the solutions included are simple point solutions that will provide smaller organizations or groups with the basic benefits of Identity and Access Management and can be integrated internally with existing systems in a more ad hoc manner. The guide also includes a wide range of larger, more ambitious platform-based solutions that come fully integrated with broad functionality, but bring greater expense and higher switching costs.

QUESTION #4 What business trends impact our needs today? How about in 5 years?

Looking back, it’s remarkable how much the Identity Management market has changed in the past 24 months. From the trend towards BYOD in the office to the rise of IDaaS. When researching new enterprise technology solutions, it’s always a good idea to gaze into the crystal ball and try to gauge what you might require in a solution down the road a few years. Is the solution simple to implement across disparate systems? Is it scalable? Is it well supported with fixes, updates, and new releases? Will your solution be developer-friendly and cost-effective for the duration of its deployment? Even the simplest things are important. For example, you wouldn’t buy a solution that is only offered in English when you’re planning to open an office in China in two years.

QUESTION #5 What size company do I want to work with?

Our list of IAM solution providers contains some of the largest technology companies in the world. It also contains young, small, and aggressive companies that may bring a very different sales and service mindset to the table. Before going into the buying cycle, you should have an idea which type of vendor you’d like to work with. Remember, for better or worse, the vendors you pick today could be the partners you can’t live without in a few short years.
And 5 Questions to Ask Your Potential IAM Solution Provider

**QUESTION #6** Can you describe your solution’s ability to support the following authentication methods Password, soft-token, hard-token, biometric, phone-as-token? Are any additional methods supported?

We’ve included 28 solutions in this Buyer’s Guide, and each one brings a different, strongly-held view of the best way to deliver IAM. Make your prospective vendor take a stand and expand on their model while defending that position against other options. Ask your prospective vendor about their ability to support password, soft-token, hard-token, biometric, and out-of-band mobile device authentication.

**QUESTION #7** How does your Identity Management Solution enable or improve web-based Single Sign-On?

The benefits of single sign-on (SSO) are compelling; reduced password fatigue from different user-name and password combinations, reduced time spent re-entering passwords for the same identity, and reduced IT costs due to less IT help desk calls about passwords. Ask prospective vendors about their relationship to SSO, the applications they support, and their plans for the future.

**QUESTION #8** Explain how Identity Federation does or does not fit into your proposed solution?

As stated above, the need for partners or contractors to securely access internal business applications is becoming a daily reality for many enterprises. Plus, the need to provide employees with access to external providers systems, such as outsourced human resources applications, has created a genuine demand for Federated Identity Management. If not an immediate requirement, FIM is certainly something to consider as your grow.

**QUESTION #9** How do you manage access from mobile devices? What operating systems do you support?

If you’re committed to providing employees, vendors, and consumer’s access to systems from anywhere, at any time, then you need to understand what a prospective solution provider can support with regard to mobile devices. And, if your organization has made a commitment to a BYOD policy, then you’ll need to understand whether an IAM solution can support not only iOS, but Android, Windows, and Blackberry as well.

**QUESTION #10** How is your solution priced?

At some point, you’ve got to get to the bottom line. This can be tough as IAM solutions often have very complex pricing structures, so be persistent. There’s a wide range of sophistication in the solutions we’ve selected, and as such, there’s also a wide variety of pricing models. Some will include line items for various options and others will charge a simple per-user fee. In order to get an apples-to-apples comparison and build a cost model that you can plan around, you’ll need to have put each solution into a sort of “per-user-per-month” cost model. So get all the line-by-line costs and divide by the number of users, then add that to the per-user fees.

“Get all the line-by-line costs and divide by the number of users, then add that to the per-user fees.”
### Solution Provider Profiles

<table>
<thead>
<tr>
<th>Company</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlertEnterprise</td>
<td>6</td>
</tr>
<tr>
<td>Avatier</td>
<td>6</td>
</tr>
<tr>
<td>Beta Systems</td>
<td>6</td>
</tr>
<tr>
<td>Bitium</td>
<td>6</td>
</tr>
<tr>
<td>CA Technologies</td>
<td>7</td>
</tr>
<tr>
<td>Centrify</td>
<td>7</td>
</tr>
<tr>
<td>Courion</td>
<td>7</td>
</tr>
<tr>
<td>Covisint</td>
<td>7</td>
</tr>
<tr>
<td>CrossMatch</td>
<td>8</td>
</tr>
<tr>
<td>Dell</td>
<td>8</td>
</tr>
<tr>
<td>ForgeRock</td>
<td>8</td>
</tr>
<tr>
<td>Hitachi ID</td>
<td>8</td>
</tr>
<tr>
<td>IBM</td>
<td>9</td>
</tr>
<tr>
<td>Ilantus</td>
<td>9</td>
</tr>
<tr>
<td>iWelcome</td>
<td>9</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>9</td>
</tr>
<tr>
<td>NetIQ</td>
<td>10</td>
</tr>
<tr>
<td>Okta</td>
<td>10</td>
</tr>
<tr>
<td>Omada</td>
<td>10</td>
</tr>
<tr>
<td>OneLogin</td>
<td>10</td>
</tr>
<tr>
<td>Oracle</td>
<td>11</td>
</tr>
<tr>
<td>Ping Identity</td>
<td>11</td>
</tr>
<tr>
<td>RSA</td>
<td>11</td>
</tr>
<tr>
<td>Sailpoint</td>
<td>11</td>
</tr>
<tr>
<td>Salesforce Identity</td>
<td>12</td>
</tr>
<tr>
<td>SAP</td>
<td>12</td>
</tr>
<tr>
<td>Simeio</td>
<td>12</td>
</tr>
<tr>
<td>UnboundID</td>
<td>12</td>
</tr>
<tr>
<td>Glossary</td>
<td>13</td>
</tr>
<tr>
<td>About us</td>
<td>17</td>
</tr>
</tbody>
</table>
## Vendor

### AlertEnterprise

Alert Enterprise Corp.
4350 Starboard Drive
Fremont, CA 94538
United States
+1 510-440-0840
www.alertenterprise.com

**Core Offering:**
Identity Governance & Administration

*The AlertEnterprise Market Advantage is a core understanding of application security, IT security and integration with Physical Access Control Systems (PACS). AlertEnterprise delivers a holistic view of risk that can extend into security control systems for critical infrastructure without compromising the production process.*

AlertEnterprise provides a variety of products known as the Enterprise Guardian suite that bridge the gap between traditional Identity and Access Management (IAM) products and physical security, or Physical Access Control Systems (PACS) capabilities such as badging and visitor management.

Organizations in highly regulated industries such as oil and gas, chemicals, pharmaceuticals, and government make up a large percentage of AlertEnterprise's customer base.

### Avatier Corporation

Avatier Corporation
2603 Camino Ramon
San Ramon, CA 94583
United States
+1 (800) 609-8610
www.avatier.com

**Core Offering:**
Identity Governance & Administration

*Our solution represents an integrated business focused platform that simplifies complex environments. Our unique self-service approach unifies enterprise IT through automation and business process standardization. Our patented business friendly IT store with workflow automation serves as a single system of record for all access needs and compliance reporting.*

With its flagship Avatier Identity Management Suite (AIMS), California-based Avatier offers a suite of independently-licensed IAM products focused on usability and quick time-to-value.

Avatier’s strength is its unique self-service approach, which extends IAM automation and self-service capabilities beyond traditional use cases, making AIMS a strong choice for small to mid-sized businesses looking for a simple, manageable product with relatively easy maintenance and a focus on self-service. As an added bonus, Avatier’s interfaces support dozens of languages, including nearly every European language.

### Beta Systems Software

Beta Systems Software
AH Moabit 90d
10559 Berlin
Germany
+49 (0)30-726118-0
www.betasystems.com

**Core Offering:**
Identity Governance & Administration

*Processes like account information, passwords, configuration or access authorizations for employees, business partners and customers can be centrally administered thanks to automatic access management; the solution also guarantees that all processes are implemented securely and transparently across the various systems and platforms.*

Beta Systems boasts a wide range of security solutions including its Security Access Manager Enterprise Identity Manager (SAM EIM) for identity governance and provisioning functions, and its Garancy Access Intelligence Manager (AIM) for access analytics.

Beta Systems’ products are known for their capabilities in mainframe security and for highly customizable environments, often geared towards the technical user. The Germany-based company scores points for strong support and maintenance and makes an especially good fit for European-based companies though they have been making inroads with North American customers as well.

### Bitium

Bitium
2448 Main Street
Santa Monica, CA 90405
United States
+1 (855) 424-8486
bitium.com

**Core Offering:**
Identity-as-a-Services (IDaaS)

*Bitium is a next-generation identity and access management company working with cloud-forward companies on the solutions to unleash the full potential of cloud computing. We provided cloud-based identity and access management solutions, including SSO, password management, and analytics for small, medium, and enterprise businesses.*

With its cloud-based Identity-as-a-Service (IDaaS) solution, California-based Bitium aims to give customers strong security capabilities including single sign-on (SSO), app management, and analytics tools, all without sacrificing ease-of-use. Bitium's SSO app allows users to access over 1,000 cloud-based apps and lets administrators to provision (and de-provision) application access without sharing passwords.

Though Bitium shows strong capabilities in SSO and analytics, the platform doesn't currently feature its own two-factor authentication (2FA) or mobile device management (MDM), capabilities, and lacks customizable reports. Nonetheless, Bitium makes a powerful point solution for organizations looking for SSO and analytics capabilities.
# Identity and Access Management Solutions

## 2016 Buyer’s Guide

<table>
<thead>
<tr>
<th>Vendor</th>
<th>From the Company</th>
<th>Solution Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA technologies</td>
<td><em>Automating the process of granting and verifying application access based on each user’s relationship and role with your organization—whether they are employees, contractors, customers or business partners—improves IT flexibility. It also helps to improve operational efficiencies and reduce security risks by on-boarding new users faster and ensuring people only have access that is appropriate.</em></td>
<td>With its Identity Suite and Secure Cloud IDaaS solution, CA Technologies provides several solutions that can be unified for provisioning that manages user identities throughout their entire lifecycle. Secure Cloud, CA’s IDaaS solutions, includes web SSO, authentication, self-service, and provisioning for both cloud and on-premises applications—a selling point for organizations running hybrid IT environments. The CA Identity Suite is made up of CA Identity Portal, CA Identity Manager, and CA Identity Governance and Administration.</td>
</tr>
<tr>
<td>Centrify</td>
<td><em>Centrify provides Unified Identity Services across data center, cloud and mobile—resulting in one single login for users and one unified identity infrastructure for IT. Centrify's software and cloud services let organizations securely leverage their existing identity infrastructure to centrally manage authentication, access control, privilege management, policy enforcement and compliance across on-premises and cloud resources.</em></td>
<td>Centrify’s IDaaS solution offers secure access to cloud and mobile apps via SSO, user-provisioning, mobile device management (MDM), and multi-factor authentication (MFA) capabilities, and is also compatible with Active Directory (AD). Centrify is particularly notable for its integrated MDM capabilities, which are some of the strongest in the market and match the capabilities of many MDM vendors. Centrify also boasts easy-to-use dashboards and strong reporting capabilities, with nearly 50 out of the box reports, as well as a SaaS Privileged Identity Management (PIM) solution, making Centrify a strong choice for organizations with BYOD policies looking to simplify MDM, IAM and PIM simultaneously.</td>
</tr>
<tr>
<td>Courion</td>
<td><em>Courion’s comprehensive approach to Access Risk Management increases your operational efficiency and transparency, strengthens security and improves compliance. By streamlining the user access process and ensuring only the right people have the right access to the right resources, Courion helps companies reduce the risk of intellectual property theft, loss of reputation and regulatory penalties by identifying, quantifying and managing access risk.</em></td>
<td>The Courion Access Assurance Suite (AAS) allows customers to manage access to applications in the cloud or on-premise through provisioning user access changes, certifying user access, remediating access violations, and generating audit and compliance reports. AAS is built from several modules that may be licensed separately and used as point solutions if desired. Together those modules form a comprehensive approach to access risk management with strong analytics capabilities. Courion is widely utilized in highly-regulated industries and should be considered for enterprises operating in industries operating in fields such as healthcare, banking, and natural resources.</td>
</tr>
<tr>
<td>Covisint</td>
<td><em>The Covisint Platform provides a trusted and secure single entry point for all your business partners, customers, and employees that enables enterprises to centrally manage the entire identity lifecycle of their internal and external users, as well as their access to resources across the enterprise.</em></td>
<td>Detroit-based Covisint was an early innovator in the IDaaS market. Covisint made a name for itself working with the automotive industry, which has given the company a leg up on the competition in developing services for Internet of Things (IoT) use cases. Covisint provides support for a variety of authentication methods and deep federation capabilities. Covisint also operates a Germany-based European data center, making the company a good fit for EU-based businesses looking for vendors with “Identity of Things” capabilities that meet local data-residency requirements.</td>
</tr>
<tr>
<td>Vendor</td>
<td>From the Company</td>
<td>Solution Overview</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Crossmatch</td>
<td>“The Crossmatch DigitalPersona Altus solution delivers a single, cost-effective solution for securing all digital assets in your ecosystem, enhancing your existing security architecture with strong multi-factor authentication and biometrics-based proof-of-presence to drive end-user compliance and mitigate the increasing threat of cybercrime and data breaches.”</td>
<td>Crossmatch’s DigitalPersona Altus platform offers deep MFA capabilities including contextual (risk-based) and application-based authentication, and allows admins to manage accounts, roles, user access privileges with familiar Active Directory tools. Crossmatch also offers a complete portfolio of hardware solutions, ranging from fingerprint readers to OEM modules and embedded sensors, as well as a full menu of professional managed services. Specialized solutions for government, defense, and law enforcement make Crossmatch an attractive solution for public sector orgs. who need both digital and physical identity solutions.</td>
</tr>
<tr>
<td>Dell</td>
<td>“Dell One Identity enables you to securely and efficiently manage the entire identity lifecycle to: Automate account creation with delegated rights; Group memberships and attributes to authorize users; Reduce complexity of common administrative tasks, such as password management; Achieve optimal single sign-on (SSO) for all platforms, systems and applications; and Simplify the management of complex Unix, Linux and Mac environments.”</td>
<td>Dell One Identity Manager’s modular and integrated approach to account management provides rapid time-to-value by offering comprehensive functionality that allows customers to build on existing investments. One Identity Manager is modular, with different ‘editions’ offered to different verticals, including but not limited to communications, banking, insurance, and media services. Strengths include governance, policy management, workflow capabilities, and strong out-of-box capabilities. As of press time, One Identity Manager is offered in 13 languages, and enjoys a strong popularity in overseas markets.</td>
</tr>
<tr>
<td>ForgeRock</td>
<td>“Competitive advantage will now be determined by an organization’s ability to rapidly verify and manage the identities of consumers, partners, employees, and devices, anytime and anywhere, based on context. ForgeRock’ Identity Relationship Management (IRM) platform is designed to help CIOs address these new business challenges at Internet Scale.” California-based ForgeRock is a unique to this list in that they offer the only open source IAM platform on the market. The ForgeRock Identity Platform is built on Sun Microsystems’s open source IAM projects and includes a set of APIs, allowing for the efficient and rapid development of new services ready for deployment in the cloud or on mobile devices. Mobile enhancements to the platform support OAuth 2.0 and OpenID Connect. ForgeRock also offers the ForgeRock Identity Relationship Management platform, aimed at helping CIOs address IAM challenges at internet scale via REST API’s for IAM, an identity gateway, and directory services.</td>
<td></td>
</tr>
<tr>
<td>Hitachi ID</td>
<td>“Hitachi ID Systems, Inc. delivers access governance and identity administration solutions to organizations globally. Products are available either individually or as components of the Hitachi ID Management Suite. The Hitachi ID Management Suite is an identity management and access governance solution designed to simplify and secure the management of user life-cycles, from on-boarding until termination, across most common types of systems and applications.”</td>
<td>Canada-based Hitachi ID’s Hitachi ID Identity and Access Management Suite was designed as identity management and access governance middleware, in the sense that it presents a uniform user interface and a consolidated set of business processes to manage user identity attributes, security rights, and credentials across multiple systems. The Suite consists of several modules including Access Certifier (entitlements), Group Manager (self-service groups), and Org Manager (reporting) that can be licensed separately and used as point solutions. Hitachi’s strengths lie in account and password management, and strong support for policy-based administration.</td>
</tr>
</tbody>
</table>
Identity and Access Management Solutions

2016 Buyer’s Guide

Vendor

IBM

IBM Corporation
1 New Orchard Road
Armonk, NY 10504
United States
+1 (877) 257-5227
www.ibm.com

Core Offering:
Identity Governance & Administration
Identity-as-a-Services (IDaaS)
Customer Identity & Access Mgmt.

From the Company

“We provide Threat-aware Identity and Access Management solutions to help clients manage and secure identities across multiple perimeters, providing secure online access in today’s mobile, cloud, and social environments. IAM solutions are used to improve identity assurance, meet compliance needs, and reduce operational costs by providing insight and enforcement of user access to data, applications and infrastructure.”

Solution Overview

IBM entered the IDaaS market in 2014 with the purchase of Lighthouse Security Group and has since established itself in the market with its Cloud Identity Service offering, a rebranding of Lighthouse’s IDaaS product. Cloud Identity Service is offered as a multitenant model though some components can be delivered in a dedicated model.

IBM’s Security Identity Governance and Administration suite combines IBM Security Identity Manager (ISIM) with IBM Security Identity Governance (ISIG) for strong automation and some of the strongest governance abilities on the market.

IBM’s products typically offer deep functionality and strong connectivity with a broad range of complementary products.

Ilantus

Ilantus
144&144/1, M G Road
Bengaluru, Karnataka
India
+91 80667 39600
www.ilantus.com

Core Offering:
Identity-as-a-Services (IDaaS)

From the Company

“Ilantus IDaaS addresses the newly emerging identity and access management and governance challenges and enables organizations to provide their users with fast, easy, and secure access to enterprise applications/data anytime/anywhere, but with effective measures of control over access and protection.”

Solution Overview

India-based Ilantus provides a variety of IAM point solutions delivered via the SaaS model such as Identity Express (identity administration), Compliance Express (access governance), Sign On Express (SSO), and Password Express (Password management). Ilantus’s services are delivered via a dedicated hosted tenant model. As the only Indian company in this guide, Ilantus is strongly recommended for organizations operating in regulated industries on the Indian subcontinent.

iWelcome

iWelcome B.V.
Soeterweg 300
812 BH Amersfoort
Netherlands
+31-33-445-0500
www.iwelcome.com

Core Offering:
Identity-as-a-Services (IDaaS)

From the Company

“We provide Identity and Access Management as a service. A full set of functionality, offered from the cloud to cater for all sorts of different use cases. Whether dealing with the access rights of internal employees, or the identity platform for your customer facing applications that store millions of users and their profile information.”

Solution Overview

Netherlands-based iWelcome offers an open-source based IDaaS solution that includes authentication, SSO, federation, self-service registration and user provisioning capabilities for both on-premise and cloud applications, all delivered via a dedicated single-tenant delivery model that allows for heavy customization and white-labeling.

iWelcome is an ideal candidate for large, EU-based, enterprise organizations looking for an IDaaS solution that will meet complex business requirements and use-cases, as well as regulatory data-residency requirements.

Microsoft

Microsoft
One Microsoft Way
Redmond, WA 98052
United States
+1 (888) 722-7871
azure.microsoft.com

Core Offering:
Identity-as-a-Services (IDaaS)

From the Company

“Identity and access management in the cloud. Azure Active Directory is a comprehensive identity and access management cloud solution that provides a robust set of capabilities to manage users and groups. It helps secure access to on-premises and cloud applications, including Microsoft online services like Office 365 and many non-Microsoft SaaS applications. Azure Active Directory comes in 3 editions: Free, Basic, and Premium.”

Solution Overview

Perhaps the biggest name brand in this guide, Microsoft only recently made its first foray into the IDaaS market with the May 2014 release of its new Azure Active Directory (AAD) Premium service and the technology giant has already made a large impact on the market.

AAD offers comparable capabilities to other IDaaS offerings and includes access to Microsoft Identity Manager products for use with on-premise systems.

AAD makes a strong choice for enterprise customers deeply familiar with Microsoft’s ecosystem, or who already use Microsoft’s Azure cloud PaaS service. However, customers looking for deep CIAM (B2C) and user-provisioning capabilities should beware, as Microsoft has yet to catch up to the competition in these regards.
### Identity and Access Management Solutions

#### 2016 Buyer’s Guide

<table>
<thead>
<tr>
<th>Vendor</th>
<th>From the Company</th>
<th>Solution Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetIQ Corporation</td>
<td>&quot;NetIQ Identity &amp; Access Management solutions use integrated identity information to create, modify, and retire identities and control their access to enterprise, cloud and mobile resources. We provide Identity Management, Access Management, single sign-on (SSO), access governance, identity tracking and Active Directory (AD) administration.&quot;</td>
<td>Texas-based NetIQ provides a highly scalable IAM suite offered with several optional add-ons, such as Access Review, a governance add-on, and the NetIQ Access Governance Suite (AGS). NetIQ’s Identity Manager centralizes access administration and ensures that every user has one identity—from your physical and virtual networks to the cloud—with a highly flexible solution and strong provisioning capabilities ideal for a variety of business use-cases.</td>
</tr>
<tr>
<td>Okta, Inc.</td>
<td>&quot;Okta is an enterprise grade identity management service, built in the cloud. With Okta IT can manage access across any application, person or device. Whether the people are employees, partners or customers or the applications are in the cloud, on premises or on a mobile device, Okta helps IT become more secure and maintain compliance.&quot;</td>
<td>Okta’s IDaaS offering boasts one of the fastest growing customer bases in the market and the funding to match—the company has reached &quot;unicorn&quot; levels of funding in the last 12 months. The Okta identity management service provides directory services, SSO, strong authentication, provisioning, workflow, and reporting, all delivered as a multitenant IDaaS though some components reside on-premise. Aside from standard IDaaS capabilities, Okta also provides MDM and phone-as-a-token authentication capabilities. Okta features a broad partner ecosystem, but lacks slightly in reporting capabilities. Okta opened an EU-based data center in 2015, making the company an ideal IDaaS solution for small to midsized businesses on either side of the Atlantic.</td>
</tr>
<tr>
<td>Omada A/S</td>
<td>&quot;Omada’s identity solutions work either as stand-alone or as a unified comprehensive solution that covers both identity and access governance and identity and access management. The suite is built on Microsoft technology and covers every aspect of identity management challenges in heterogeneous IT-environments.&quot;</td>
<td>Denmark-based Omada’s Identity Suite (OIS) provides an enterprise platform for identity management and identity governance that is available either by component or as a comprehensive system. OIS features a flexible data model, excellent dashboards and powerful reporting capabilities, including closed loop reporting. Due to its strength in reporting, Omada’s OIS is highly recommended for organizations with a high level of need for auditing and compliance. Omada offers industry-tailor solutions for several verticals including Banking and Finance, Life-Sciences, Manufacturing, Public, Utilities, and Retail.</td>
</tr>
<tr>
<td>OneLogin, Inc.</td>
<td>&quot;OneLogin’s mission is to democratize identity management; making it available to any organization, regardless of size. Historically, identity management has been available only to large enterprises who had the means to purchase expensive software and undertake a complex project. OneLogin gets enterprises up and running in minutes—literally.&quot;</td>
<td>California-based OneLogin provides an on-demand IDaaS solution consisting of single sign-on, multi-factor authentication, directory integration, user provisioning, and a catalog of pre-integrated applications. OneLogin is provided via a multitenant architecture and provides strong capabilities and support for access management policy administration, user directory integration, and end-user self-service. As major proponents of the OpenID Native Applications Working Group (NAPPS), OneLogin has taken a standards-based approach to application integration and established itself as a thought leader in the field of authentication. OneLogin makes an excellent IDaaS solution for organizations of any size looking for powerful SSO, directory, and MFA capabilities.</td>
</tr>
</tbody>
</table>
## Identity and Access Management Solutions

### 2016 Buyer’s Guide

<table>
<thead>
<tr>
<th>Vendor</th>
<th>From the Company</th>
<th>Solution Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ORACLE</strong></td>
<td>&quot;Oracle Identity Management enables organizations to effectively manage the end-to-end lifecycle of user identities across all enterprise resources, both within and beyond the firewall and into the cloud. The Oracle Identity Management platform delivers scalable solutions for identity governance, access management and directory services.&quot;</td>
<td>The Oracle Identity Governance (OIG) Suite is an integrated suite that centralizes security for applications and web services, and provides a single point of contact for support under a single license contract. OIG suite is marketed for, and well-suited to, large enterprise customers. As such, OIG is a highly complex, scalable, and flexible product, but it may be overkill for small or midsized businesses. Oracle is a major player in enterprise IT, and Oracle’s IGA solution is highly recommended for businesses already running a portfolio of Oracle products.</td>
</tr>
<tr>
<td><strong>Ping Identity</strong></td>
<td>&quot;Ping Identity leads a new era of identity management by ensuring secure access to the digital enterprise: for the first time, all users seamlessly connect to all applications, whether mobile, cloud, or legacy. Ping accelerates digital transformation with an extensible open platform and advanced integration capabilities that position enterprises to be ready for anything.&quot;</td>
<td>The Ping Identity Platform is a multi-tenant, web-centric IDaaS offering that provides secure single sign-on from any device and provides administrators with a single dashboard from which they can manage user access for all applications. Ping Identity Platform comes bundled with PingFederate, a federation service supporting all of the current identity standards including SAML, WS-Federation, WS-Trust, OAuth and OpenID Connect, and PingAccess for managing policies on both applications and APIs. Platform customers can use a lightweight self-services bridge component to integrate with AD, Google, or with one of many SaaS providers. Ping delivers this technology as a solution to manage partner employee identities and customer identities through a partnership with UnboundID.</td>
</tr>
<tr>
<td><strong>RSA</strong></td>
<td>&quot;Using a business-driven approach, RSA’s solution integrates access governance, provisioning, authentication, and single sign-on (SSO) in one platform. Whether on-premise or in the cloud, the platform reduces risk and complexity while improving security, visibility, and compliance. RSA’s platform supports the entire identity lifecycle, and provides a unified business view for all types of users.&quot;</td>
<td>RSA, the security division of EMC, which was acquired by Dell in late 2015, offers both IDaaS and traditional identity management and IGA solutions. RSA Identity Management and Governance (RSA IMG) is a highly scalable identity management suite built from separately licensed components. RSA’s Archer Governance, Risk, and Compliance products are highly capable and a good fit for companies with heavy governance needs and stringent compliance requirements. RSA Via is a highly capable IDaaS suite composed of separately licensed SaaS point solutions including access control (SSO, MFA), governance, lifecycle management, MDM, and adaptive authentication.</td>
</tr>
<tr>
<td><strong>SailPoint</strong></td>
<td>&quot;SailPoint provides integrated IAM solutions for compliance, provisioning and access management – delivered either on-premises or as a cloud service with no hardware or software to deploy. And we deliver a unique Cloud On-Ramp that allows you to implement IdentityIQ on-premises today with a smooth migration path to our IDaaS solution, IdentityNow, when you are ready.&quot;</td>
<td>Sailpoint, offers both traditional Identity Management with its IdentityIQ solution, and IdentityNow, a multitenant IDaaS solution. IdentityIQ, offered as a stand-alone on-premises product, with several optional add-ons, is well-regarded for its strong identity governance capabilities and provisioning capabilities. IdentityIQ is also available as a hosted managed service. IdentityNow provides typical IDaaS capabilities such as federated SSO, password management, provisioning, and access certification, but the solutions true strength lies in its access governance capabilities, which build off of Sailpoint’s background as an innovator in identity access and governance.</td>
</tr>
<tr>
<td>Vendor</td>
<td>From the Company</td>
<td>Solution Overview</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>salesforce</strong>&lt;br&gt;Salesforce Identity&lt;br&gt;The Landmark at One Market&lt;br&gt;San Francisco, CA 94105&lt;br&gt;United States&lt;br&gt;+1 (415) 901-7040&lt;br&gt;www.salesforce.com&lt;br&gt;Core Offering:&lt;br&gt;Identity-as-a-Services (IDaaS)&lt;br&gt;Customer Identity &amp; Access Mgmt.</td>
<td>“Identity services for the connected world. Salesforce App Cloud provides an out-of-the-box identity solutions using open standards, including SAML, OpenID Connect, OAuth, and SCIM. Now IT can manage apps, users, and data sharing with simplicity and transparency.”</td>
<td>Salesforce entered the IAM market in 2013 with the release of Salesforce Identity, an IDaaS solution that both offered as an independent service, and included as part of Salesforce’s cloud Platform-as-a-Service (PaaS) offering. Salesforce Identity features baseline IDaaS capabilities for access policy and provisioning, as well as an excellent graphical workflow for policy management, but its SSO lacks password vaulting capabilities. Despite some shortcomings, Salesforce Identity’s pricing (free with Salesforce PaaS, and discounted for Salesforce CRM customer) makes it an attractive offer for customers already utilizing Salesforce products.</td>
</tr>
<tr>
<td><strong>SAP</strong>&lt;br&gt;SAP SE&lt;br&gt;Dietmar-Hopp-Allee 16&lt;br&gt;69190 Walldorf&lt;br&gt;Germany&lt;br&gt;+49 (0) 6227/7 47474&lt;br&gt;www.sap.com&lt;br&gt;Core Offering:&lt;br&gt;Identity Governance &amp; Administration</td>
<td>“Automatically detect, remediate, and prevent access risk violations in your SAP and non-SAP systems with SAP Access Control. No matter the size of your business, this access governance system gives you real-time visibility into your risk position—so you can reduce unauthorized access, fraud, and the cost of compliance across your organization.”</td>
<td>Germany-based enterprise technology giant SAP offers several IAM solutions including SAP Identity Management and SAP Access Control. SAP’s solutions offer strong governance capabilities and an unparalleled level of integration with SAP’s business application ecosystem, making them the go-to choice for organizations already utilizing a portfolio of SAP solutions and applications. However, as SAP’s identity and access management solutions are primarily designed to work with SAP apps, users looking to manage non-SAP-centric environments should look elsewhere.</td>
</tr>
<tr>
<td><strong>Simeio</strong>&lt;br&gt;Simeio Solutions&lt;br&gt;50 Harrison St.&lt;br&gt;Hoboken, NJ 07030&lt;br&gt;United States&lt;br&gt;+1 (201) 239-1700&lt;br&gt;simeiosolutions.com&lt;br&gt;Core Offering:&lt;br&gt;Identity-as-a-Services (IDaaS)</td>
<td>“Simeio’s Identity Orchestrator (IO) platform is designed to simplify the operation of complex, multi-vendor IAM and security infrastructures, and the Simeio Identity Intelligence Center (IIC) is designed to protect corporate resources and information by monitoring the use of digital identities and access privileges, and leveraging that information to deliver actionable business intelligence.”</td>
<td>New Jersey-based Simeio Solutions offers a variety of IAM point solutions as dedicated hosting or on-premise manages services, including Simeio IDaaS, the only fully managed IDaaS offering featured in this guide. Simeio utilizes OEM software from major IAM vendors to bolster its services and is, therefore, capable of providing a wide variety of support for all manner of web and on-premise applications. Simeio’s managed service offerings are recommended for small to mid-sized businesses without the resources or manpower to deploy and managed an IAM solution on their own.</td>
</tr>
<tr>
<td><strong>UnboundID</strong>&lt;br&gt;UnboundID&lt;br&gt;13809 Research Blvd&lt;br&gt;Suite 500&lt;br&gt;Austin, TX 78750&lt;br&gt;United States&lt;br&gt;+1 (512) 600-7700&lt;br&gt;www.unboundID.com&lt;br&gt;Core Offering:&lt;br&gt;Identity-as-a-Services (IDaaS)&lt;br&gt;Customer Identity &amp; Access Mgmt.</td>
<td>“Enterprise customers select the UnboundID Platform to modernize enterprise IAM systems, and enable new customer-facing digital business initiatives that provide real-time personalization and delivery of a consistent customer experience across channels and devices. The UnboundID Platform has an unmatched track record of web scale performance and reliability, and deploys on traditional or virtualized infrastructure and a range of private/public/hybrid clouds.”</td>
<td>Texas-based UnboundID is a developer of highly scalable identity management software, ideal for supporting consumer-facing use-cases such as online retail sites or social networking platforms. The company’s flagship UnboundID platform provides traditional IAM capabilities such as on/off-boarding of users and policy-based data governance, as well as CIAM-specific tools designed to store, protect, and leverage consumer identity and preference data. UnboundID’s scalability and unparalleled focus on CIAM use-cases make the company a strong choice for businesses of any size that require large-scale management of consumer identities. The UnboundID platform can be deployed on-premise or in a range of public, private, or hybrid cloud environments.</td>
</tr>
</tbody>
</table>
Glossary of Terms

**Access Management** – Access management is the process of managing a user’s login and access across a wide range of applications, systems and resources belonging to an organization. Most IAM solutions manage user access to resources but leave access authorization decisions to the application owners.

**Affiliation** – Affiliation is the combination of one’s relationship with an organization and some form of trusted identity (which may not be from within the organization).

**Attribute** – Small pieces of information that make up a digital identity. Attributes may include name, phone number, group affiliation, etc.

**Authentication (AuthN)** – Authentication is the process of validating an identity, whether it be the identity of a user or, as in the Identity of Things, a device. The classic method of validation is the username/password combination.

**Authorization (AuthZ)** – Authorization is the process of determining if a user has the right to access a service or resource, or perform an action.

**Authorization Audit** – An authorization audit is a process that gives a detailed overview of the access capabilities of an entire organization.

**Authorizer** – An individual responsible for approving changes in user authorizations and privileges.

**Central Authentication Service (CAS)** – A single sign-on web protocol which allows a user to access multiple services while providing login credentials only once.

**Compliance** – In IT and data storage terminology, compliance refers to organizational compliance with government regulations regarding data storage and management and other IT processes.

**Credential** – A credential is an item, such as an ID card, or a username/password combination, used by persons or entities to prove themselves.

**Customer Identity and Access Management (CIAM)** – Customer, or Consumer Identity and Access Management (CIAM) is an IAM solution that is specifically tailored to meet the needs of organizations handling large volumes of consumer identity information. Though superficially similar to traditional IAM, CIAM solutions must provide smooth, yet secure customer experience, with the ability to scale quickly to handle large volumes of customer data.

**Data** – Any information stored by a computer.

**Digital Identity** – A digital identity is a set of information (attributes and credentials) that is maintained about an individual in order to associate them with an organization.

**De-provisioning** – The removal of an individual’s organizational digital identity, access, and privileges.

**Event** – An action or the result of an action. Events are often logged and monitored for security purposes.

**Federated Identity** – A federated identity is the product of linking all of an individual’s disparate electronic identities and attributes, which may be stored across multiple identity management solutions.
Federated Identity Management – A Federated Identity Management (FIM) Solution is a technical implementation that allows identity information to be developed and shared among multiple identity management entities, and across trust domains.

FIDO Alliance – The FIDO (Fast IDentity Online) Alliance is a non-profit group formed to address a lack of interoperability between authentication devices, and the challenges that users face in maintaining multiple usernames, passwords, and authentication methods.

Group – In identity management, a group allows the management of multiple entities (I.e. employees or customers) within a single category. Groups are used to define roles and simplify access control.

Identification – Identification is the process by which an entity’s information is gathered and verified for accuracy.

Identity Access Governance – Identity and Access Governance (IGA) solutions establish an identity lifecycle process that gives managers the ability to have comprehensive governance of identities and access requests.

Identity and Access Management – Identity and Access Management (IAM) is a system, solution, or service that addresses an organizational need for a system-wide solution that manages user’s access and authentication into external and internal applications, databases, or networks.

Identity Attribute – See attribute.

Identity Governance and Administration (IGA) – Similar to IAM, IGA is a set of processes used to manage identity and access controls across systems. IGA differs from IAM in that it allows organizations to not only define and enforce IAM policy but also connect IAM functions to meet audit and compliance requirements.

Identity Management (IdM) – Identity Management (IdM) is the act of using processes and solutions for the creation and management of user or connected device information.

Identity Management as a Service – Identity and access management as service, or IDaaS, is an IAM solution delivered as a service. IDaaS solutions are predominately cloud-based and are hosted and sometimes managed by the service provider.

Level of Assurance (LoA) – The Level of Assurance (LoA) is the degree of confidence achieved by the vetting and proofing process used to establish the identity of a user. There are four levels of assurance, ranking from zero (no confidence existing in the asserted identity) to four (very high confidence in the asserted identity’s accuracy).

Log Files – Log files are files that record either events that occur in an operating system or software, or messages occurring on communication software. For example, when a failed login to an E-mail system occurs, a log file is created to record that event.

Logging – the act of keeping a log for an extended period of time.

Management Chain – In an organization, users usually have managers, who in turn may have their own managers. This sequence of managers, which starts with the user and ends with the highest manager in that organization, is known as the management chain. In the context of identity management, management chains are often used to authorize security changes.
Multifactor Authentication – Multifactor authentication adds an additional step (or factor) to the authentication process, typically by pairing something the user knows, such as username and password, with an action, or something the user has, such as an SMS message to their phone, an email, or a token.

NetID – An electronic identifier created specifically for use with online applications.

OAuth – OAuth is an open authorization standard that allows applications to autonomously access resources on behalf of a user. iOS and Android, for example, use this kind of authorization to let users choose whether or not an app can have access to certain functions and parts of the phone.

Offboarding – The process by which a user is removed (with access revoked) from an organization’s IAM system.

OpenID – A standardized, open method of decentralized authentication.

Onboarding – The process of adding new users to an organization’s IAM system.

One Time Password (OTP) – A password that is valid for use one use or session.

Password – A word or string of characters used to prove one’s identity, or authorize access to a resource. Usually, but not always, paired with a username.

Password Reset – The process by which a user changes their own password.

Privilege – A privilege is a construct that allows certain users within an organization to have a number of powers based on their credentials and identity attributes.

Privileged Account/Identity Management (PAM/PIM) – Privileged identity management is a process or technology focused on managing, monitoring, and protecting powerful privileged user accounts within the IT infrastructure of an enterprise.

Privilege Management – Privilege Management is the process by which the owner of a network can modify or assign privileges for applications and resources.

Privileged User – A user possessing specific security privileges and entitlements.

Provisioning – A process that enables users to use their privileges to access applications and services.

Requester – A person who requests a change in user profiles, privileges, or entitlements, either by automated or manual process.

Role – An identity attribute that gives users automatic privileges when assigned. Roles make take the form of groups wherein all members of a group have the same set of privileges.

Role-Based Access Control (RBAC) – A model in which users are assigned “roles” that give them a certain level of access to resources and systems. Assigning a role to a user grants that users a certain set of privileges and entitlements.

System for Cross-Domain Identity Management (SCIM) – A system for cross-domain identity management (SCIM) is an open standard for automating the exchange of user identity information between identity domains, or IT systems, designed to make user identity management in cloud-based applications easier.
Security Administrator – A person responsible for maintaining a list of users, their identity attributes, their passwords, security privileges, or other authentication factors.

Security Entitlement Audit – An official organizational review of security entitlements and user privileges. A periodical entitlement audit is a reliable method for finding and removing old, unneeded entitlements.

Self-Service Password Resets – A self-service password reset is a process that allows users that have forgotten their password to use an alternate process to authenticate themselves and thus reset their password without the assistance of help desk personnel.

Session – A session is an interaction between two or more entities on a network, generally consisting of an exchange of information. In the context of identity management the most important information exchanged is the credentials of each entity and the time-out information for the session.

Single-Factor Authentication – A method of authentication that relies on a single factor, such as username and password, to verify a user’s identity.

Single Sign-On (SSO) – In a single sign-on (SSO) service model users log onto a single platform which gives them automatic log-in access to multiple applications for a particular period of time. When utilizing SSO systems users only need to present one set of credentials, rather than learning or remembering separate credentials for each application.

Support Analyst – A support analyst, in an identity management context, is a user with special privileges that allow him or her to help other users, often by resetting their forgotten passwords or provisioning new privileges.

System of Record (SoR) – A system of record (SoR) is a storage system designated as an authoritative source for a certain identity attribute. As the SoR is the direct line of access to the identity attribute that it controls, all modifications to those identity attributes should be brokered via the SoR.

Termination – The process by which user or customer credentials or privileges are de-provisioned and removed.

User – Users are people whose access to systems and identity information must be managed.

User Provisioning – Technologies or processes that create, modify, and deactivate user accounts, privileges, and profiles across IT infrastructure and business apps.

Vetting – The process of thoroughly investigating and validating information collected from or about an individual for the purpose of issuing credentials or privileges.
About Solutions Review:

Solutions Review is a collection of technology news sites that aggregates, curates and creates the best content within leading technology categories. Solutions Review mission is connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched ten tech Buyer’s Guide sites in categories ranging from Cybersecurity to Wireless 802.11ac as well as Mobility Management and Business Intelligence, Data Analytics, Data Integration and Cloud Platforms.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research. Solutions Review disclaims all warranties, expressed or implied, regarding this research, including any warranties of merchantability or fitness for a particular purpose.