Identity Management Vendor Map

A Solutions Review Buyer's Guide

Choosing the Right Identity Management Solution for Your Needs

Introduction

If any year has driven home the importance of cybersecurity, it was 2016. While other years have featured large-scale cyberattacks, never before have the consequences of those attacks come so visibly and immediately to roost. We have seen a state actor hacking a political candidate to sway an election to her rival. It's seen the hacking tools of the NSA plundered and immediately used against communications infrastructure. If nothing else, 2016 should be a reminder that enterprises need to get their security in order.

As traditional security measures more and more appear to offer only a token countermeasure against identity-based intrusion, it is incumbent upon enterprises to consider strong forms of Identity and Access Management (IAM) to deter bad actors. While there are all kinds of IAM solutions, there are three primary categories of IAM for the workforce: Identity-as-a-Service (IDaaS), Identity Governance and Administration (IGA), and Privileged Access Management (PAM).

> "This document runs down the capabilities of IDaaS, IGA and PAM and a few vendors for each."

Choosing between IDaaS, IGA, and PAM can be difficult. Each solution offers overlapping capabilities and are best suited to different kinds of organizations. Furthermore, you may need pieces of one and not another. In this document, we run down the capabilities of these access control methods, their differences, and similarities, as well as a few potential vendors for each.

IDaaS: Easier Deployment and Foundational IAM Capabilities

Not every business has a large workforce, a deep reserve of IT staff, or the institutional determination necessary for a lengthy implementation process. For these organizations, IDaaS can be used to deliver IAM of basically any variety: IGA, PIM, CIAM, and more. IDaaS doesn't rival IGA and PIM—it delivers them. There are both pros and cons to this approach that are independent of the kind of solution provided.

In most cases, businesses choose IDaaS due to its ease of use. You don't have to set-up or maintain any physical infrastructure for an IDaaS implementation. Management can be handled by a third party, or by lower-skilled IT staff. A comprehensive IDaaS solution should be able to deliver basic IAM requirements such as single sign-on (SSO), multi-factor authentication (MFA), access security, directories, and provisioning. And finally, it's relatively easy to integrate IDaaS with other security solutions.

"In most cases, businesses choose IDaaS due to its ease of use."

On the other hand, convenience comes with some tradeoffs. As a cloud service, IDaaS is easy to integrate—but only with other cloud services. While most IDaaS tools can integrate with legacy on-premise connectors, it may be a messy process. Many IDaaS products also come with a limited feature set. If administrators want to be able to make detailed changes to their access controls, they may want to look towards on-premise applications.

To summarize, IDaaS provides simple IAM quickly, often delivering a training-wheels version of more full-featured IGA or PIM products. For small businesses, this may be enough—but it might not stay that way. For companies looking to pursue IDaaS as a long-term strategy, it's imperative to find a service that offers granular controls.

IDaaS Providers:

- Bitium
- Centrify
- Okta
- Microsoft
- SecureAuth
- OneLogin
- UXP Systems

IGA: Strong Internal Controls

One of the key provisions of regulatory compliance is that businesses should keep detailed records about who sees what data. IGA products exist to make the answer to that question swift and concise. It does this by focusing on entitlements as the preferred method of access control.

To explain the utility of IGA, it's important to understand one of the fundamental components of access management: repositories. Most applications have a repository—an attached database that contains information on who's allowed to access it. As each application has a

repository, and each enterprise may run thousands of apps, administrators face the dismaying task of keeping each repository current—in an environment with thousands of employees.

IGA solves this problem using a system known as "entitlements." Rather than editing access permissions in files appended to applications, entitlements are connected to a specific user. Instead of going to an application and editing its repository to change permissions, an administrator can just navigate to a user, or group of users, and modify their permissions from that central location.

Here are a few advantages of IGA. Like IDaaS, IGA products can handle single sign-on. They rely much more heavily on connectors—most IGA products use connectors to other applications to data models.

These, in turn, provide insights for administrators, allowing them to see when their users might be affected by problems such as access creep. Lastly, IGA provides excellent workflows for access requests.

"IGA provides insights for administrators, allowing them to see when users might be affected by access creep."

On the downside, IGA was always going to be more labor intensive than IDaaS, but there are definitely some unresolved inefficiencies. Writing connectors for enterprises with tens of thousands of users is still a chore, so some organizations are assigning their users to generic roles instead. These roles are then given entitlements. Not every IGA product has good support for roles, however.

Finally, IGA is most focused on managing the accounts of business users. This is ordinarily fine, as business accounts comprise the vast majority of all users. This ignores, however, the fact that privileged accounts have powers that make them much more useful to bad actors when compromised.

IGA Providers:

- SailPoint
- Oracle
- IBM
- Identity Automation
- Saviynt
- RSA

PAM: Guarding the Keys to the Kingdom

Privileged access management is a special case within information security. It can be offered independently of regimes like IGA or as a bundle with IGA products. Its goal is simple: protect the identities of individuals and applications that have the power to create accounts, delete accounts, or edit their privileges in turn.

Protecting these accounts is crucial to the wider information security of an organization. These accounts are choice targets for cyberattacks. In one stunning example, hackers used stolen privileged accounts to bypass strong information security protections and shut down parts of the Ukrainian power grid.

What are the big vulnerabilities in privileged accounts? In most organizations, privileged accounts aren't owned by a single individual. They're shared among administrators and sometimes created on a whim. This can lead to too many people knowing the password to a high-privilege account. Privileged accounts can be created and then eventually forgotten about. Worse, individuals are often given privileged accounts indefinitely when they only need them for short amounts of time.

> "Privileged accounts are much more useful to bad actors when compromised."

Privileged access management solves these problems by putting limits on privileged accounts. Administrators can use PAM to create privileged accounts that automatically delete themselves when they're no longer needed, that automatically change their passwords, and which can automatically revoke access to individuals after a set time. PAM also adds audit functionality—a feature that automatically records who has access to a privileged account, as well as the actions that an individual takes while using it.

PAM Providers:

- CA Technologies
- Centrify
- Core Security
- CyberArk
- Quest
- Crossmatch
- Ping Identity

Conclusion

The major systems of Identity and Access Management often overlap but never exclude one another. IGA and PAM may either be offered as on-premise solutions, or via IDaaS. IGA and PAM can be used both together and separately. For enterprises, the primary concerns should be the following: compliance, granularity, and workforce size.

Does a chosen IAM solution provide enough of an audit trail for your company to satisfy necessary compliance regimes? Does it offer enough granularity to provide adequate security controls? Can you balance the features of the toolset with the number of personnel required to make them work?

No enterprise is going to come to the exact same answer regarding the same product. The goal—and the difficulty—will be to minimize the downsides while maximizing security coverage. It's difficult, but the rewards of success will be reassurance and protection in an age of information uncertainty.

Vendor Comparison Map

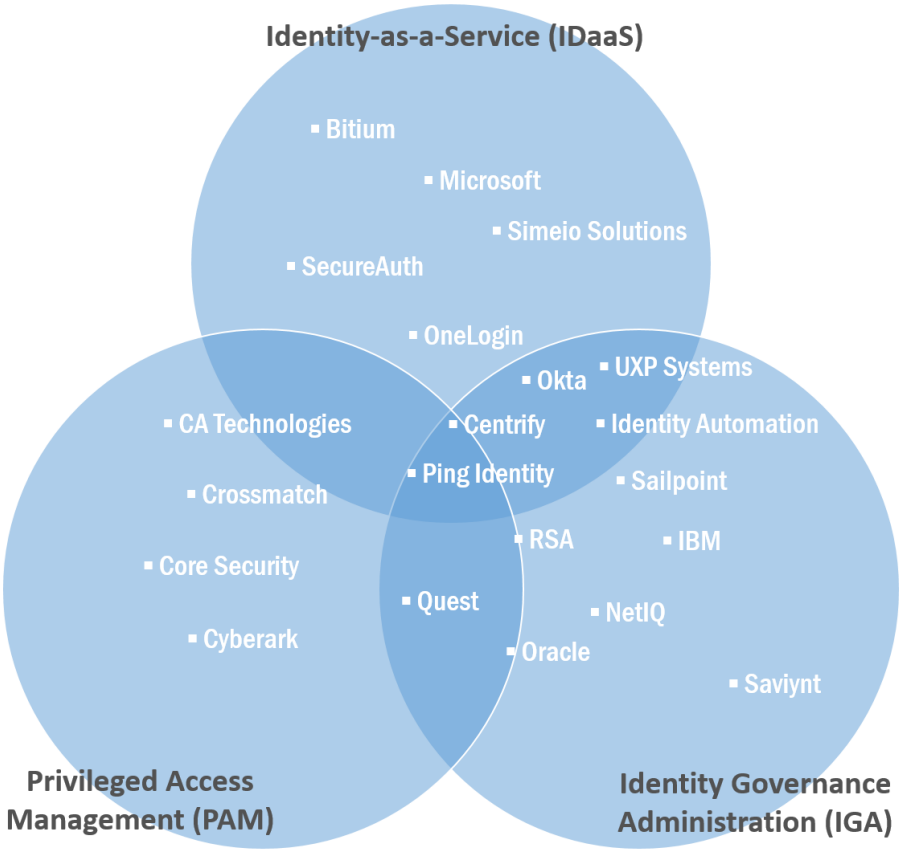
Aimed at simplifying the time-consuming vendor selection and evaluation process, the Venn diagram below offers an at-a-glance reference guide for 20 Identity Management players, the solutions they provide, and the markets they address.

Vendors on the outside of the circles tend to offer highly-specialized point solutions in those markets, while vendors towards the center offer more comprehensive platforms, which address multiple needs but may not do so with the same depth and granularity as point solution providers.

> "Vendors towards the center of the diagram offer more comprehensive platforms."

Many vendors included in this map offer various solutions addressing each of the markets concerned, and we have tried to reflect this in their positioning.

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.



Vendor List

Bitium

With its cloud-based Identity-as-a-Service (IDaaS) solution, Bitium offerings include single sign-on (SSO), app management, and analytics tools. Bitium's SSO app allows users to access over 1,000 cloud-based apps and lets administrators 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 mobility management (MDM) capabilities, and lacks customizable reports.

CA Technologies

Enterprise tech giant CA Technologies became a major player in the PAM market after their August 2015 acquisition of Xceedium and the subsequent rebranding of Xceedium's Xsuite to CA Privileged Access Manager. CA Privileged Access Manager offers broad support for PIV-based authentication, kernel-based authentication for Windows and Linux endpoints, and broad integration with security analytics and identity governance tools. Privileged Access Manager also offers options for CA Threat Analytics, which lets managers assess risk and detect malicious activity among privileged users.

Centrify

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.

Core Security

The Core Security 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. Core Security is widely utilized in highly-regulated industries and should be considered for enterprises operating in industries such as healthcare, banking, and natural resources.

Crossmatch

Crossmatch's DigitalPersonal Altus platform offers deep MFA capabilities including contextual (risk-based) and application-based authentication and allows administrators 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.

"Crossmatch is an attractive solution for public sector organizations."

Specialized solutions for government, defense, and law enforcement make Crossmatch an attractive solution for public sector organizations who need both digital and physical identity solutions.

CyberArk

CyberArk's Privileged Account Security Solutions offers an enterprise-grade, policy-based solution that secures, manages and logs privileged accounts and activities, and uses behavioral analytics on privileged account usage to detect and flag anomalies.

Components of PASS include an SSH Key Manager, Privileged Session Manager, Privileged Threat Analytics, Application Identity Manager, On-Demand Privileges Manager, and Endpoint Privilege Manager.

IBM

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.

Identity Automation

Texas-based Identity Automation's flagship solution RapidIdentity offers tools for self-service, delegation, workflow, access requests, access certification, password management, auditing, reporting, group management, and folder/file access management. Identity Automation is especially popular with higher education buyers looking for an IGA system offering automated provisioning for multiple target systems.

"Identity Automation is especially popular with higher education buyers."

RapidIdentity gives organizations the ability to provide employees and external users fine-grained time-based access to on-premises and cloud-based data and systems and they are also noted for strong customer service and technical support.

Microsoft

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 already has 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.

NetIQ

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.

Okta

Okta's IDaaS offering boasts one of the fastest growing customer bases in the market and the funding to match—the company has reached "unicorn" 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. In addition to standard IDaaS capabilities, Okta also provides MDM and phone-as-a-token authentication. 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.

"In addition to IDaaS, Okta also provides MDM and phone-as-a-token authentication capabilities."

OneLogin

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.

Oracle

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.

Ping Identity

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 to all applications. The 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 provisioners

> “Ping Identity comes bundled with a federation service supporting current identity standards.”

In August 2016, Ping Identity acquired identity management rival UnboundID, adding a scalable user directory for social login, customer preference and profile management capabilities.

Quest

Formerly the largest acquisition and crown jewel of Dell Software, Quest was sold following the 2015 Dell/EMC merger to make room at Dell for RSA (below). Quest's One Identity Solution provides a comprehensive user administration, provisioning, and privileged access management tools. 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.

RSA

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 also offers RSA Via, a capable IDaaS suite composed of separately licensed SaaS point solutions including access control (SSO, MFA), governance, lifecycle management, MDM, and adaptive authentication.

SailPoint

Sailpoint offers 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 Sailpoint's background as an innovator in identity access and governance.

Saviynt

California-based Saviynt's Security Manager combines data access governance (DAG), IGA, and segregation of duties (SoD) functionality in a single platform, as well as modular offerings for access governance across a variety of environments and applications including SAP, Office 365, AWS, and Epic. Security manager is available as-a-service or as on-premise software, and specialized configurations are available for multiple verticals.

Simeio Solutions

New Jersey-based Simeio Solutions offers a variety of IAM point solutions as dedicated hosting or on-premise manages services, including Simeio IDaaS, a fully-managed IDaaS. 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 workforce to deploy and manage an IAM solution on their own.

SecureAuth

California-based SecureAuth's core offering, SecureAuth IdP, is a web-based SSO, identity management, and multifactor authentication solution that can also be installed on-premises. SecureAuth supports over 20 multi-factor authentication methods, including Yubikeys, SMS text messaging, telephony OTPs, question and answer sessions, and e-mail dialogs. It allows the blocking of specific IP address ranges and sets up different workflows for trusted computers and public networks. It also integrates with various enterprise directories/data stores (Microsoft Active Directory and LDAP, Microsoft SQL, Lotus Notes, OpenLDAP, Novell eDirectory and others).

UXP Systems

UXP Systems' User Lifecycle Management™ (ULM) Platform powers digital identity as a strategic service as companies transform to the digital world. ULM uses digital identity as the focal point for managing the digital user, with processes that manage user entitlements, groups, delegation, revocation, roles and sharing, user insight, privacy and more, all as part of an end to end business process framework. The ULM Platform innovates above existing legacy systems to transform the user experience, getting enterprises to digital services faster and more economically.

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's mission is to connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched 14 tech Buyer's Guide sites in categories ranging from Cybersecurity to Mobility Management, Business Intelligence, Data Integration, Cloud Platforms and Content Management.

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.