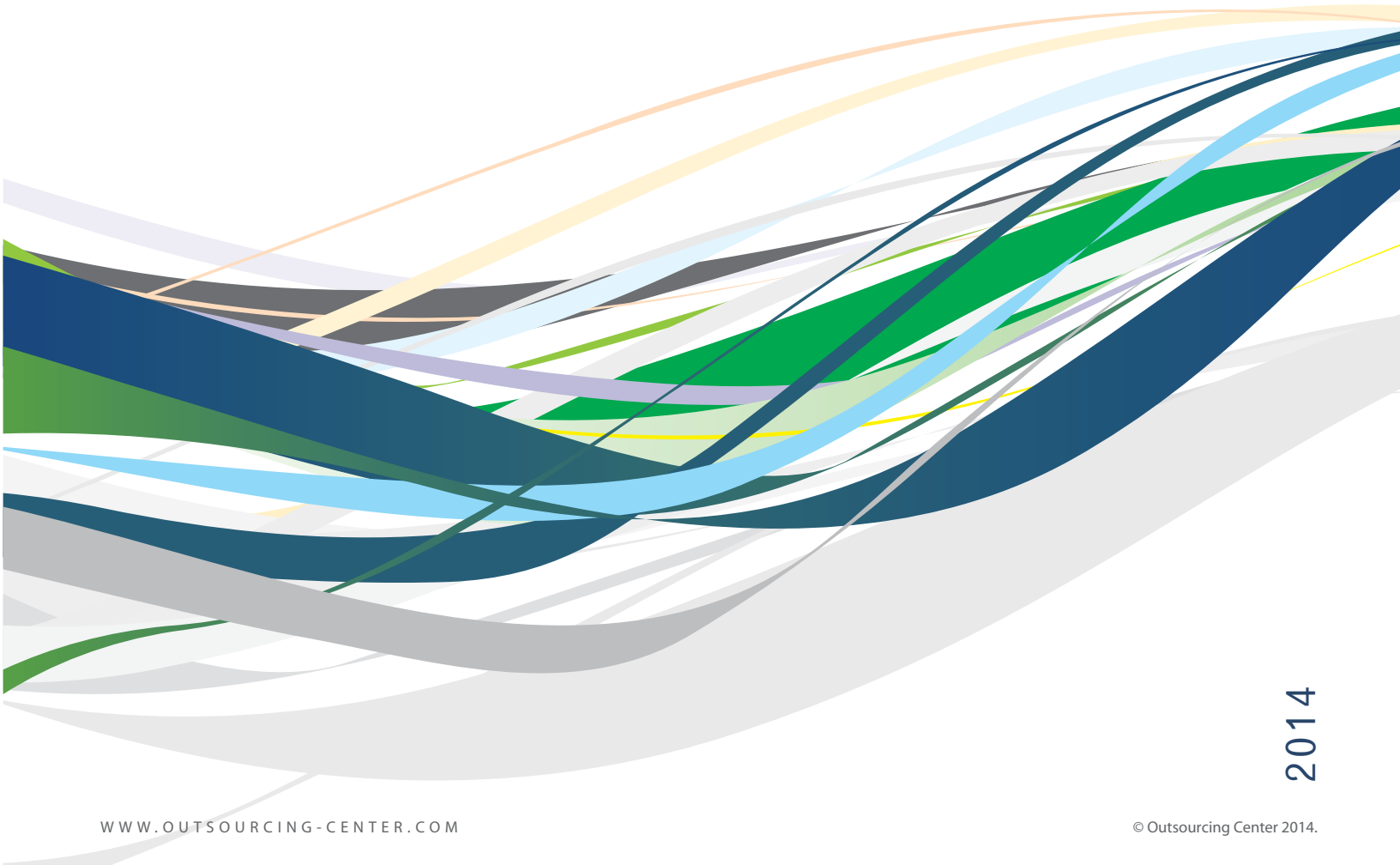
ORACLE
MANAGED CLOUD SERVICES

OUTSOURCINGCENTER

A HIGH-LEVEL GUIDE TO EFFECTIVE IDENTITY MANAGEMENT IN THE CLOUD

By Gail Coury, Vice President, Risk Management, Oracle Managed Cloud Services



2014

Table of contents

Executive Summary

IT security and access management have never been greater challenges.

Fueled by the proliferation of valuable electronic data, hacking has become an industry unto itself. Data breach attempts now occur daily, orchestrated by more sophisticated stealth attackers armed with botnets, malware and constantly changing techniques.

While the criminals get smarter, the IT environments become more complex to manage. Most are a hybrid of on-premise systems and a multitude of cloud providers—transforming the act of role-based access management into a manual nightmare. To compound the challenge, IT may not even be aware of all of the cloud-based applications and services procured by individual business units, which is a reality that could put the company at a security and compliance risk.

Whereas access was previously veiled under the safe confines of the VPN, the world is now collaborative and mobile. As a result, more outside access by employees, partners and clients add new layers of complexity to the already difficult task of credential oversight.

These new challenges can't be solved with yesterday's user access models. To mitigate risk and control costs, comprehensive Identity Management solutions, designed for today's diverse computing environments and mobile workforce, are taking center stage.

With so much at risk, it's no wonder that this new, hot topic is occupying a top position on every CIO's security agenda.

Identity Management is a means of establishing and managing the roles and credentials of individual users to ensure they are valid and authorized to access company applications.

The Basics of Identity Management

By definition, Identity Management is a means of establishing and managing the roles and credentials of individual users to ensure they are valid and authorized to access company applications—and terminating that access when the relationship with your company ends. It's a balance between providing individuals with the tools they need without long wait times and ensuring you have enough safeguards in place to deter attackers, mitigate risk and protect your assets.

The best solutions provide an enhanced user experience, improved operational efficiency and significantly reduced help desk calls. Most importantly, they provide your company with compliance control and protect valuable data from hackers.

It's important to note that Identity Management in the Cloud is not a single, generic service but a comprehensive solution comprised of numerous components. What the ultimate solution "looks" like depends on the organization's individual security needs.

The goal of this paper is to help you explore the options so you can better formulate the right Identity Management strategy for your company today and in the future.

A Quick Rundown of the Options

Single Sign-on

One of the greatest productivity zappers and one of the top reasons people call the help desk is the hunt for the forgotten password or user ID. Between hosted and internal applications, individuals can have 10, 15 or more different passwords to juggle, which not only frustrates the user but also increases the likelihood of theft. The more passwords, the more likely a person is to write these passwords down, tape them to the bottom of his or her keyboard or choose something so simple to remember that a hacker can easily figure it out too.

One of the top reasons people call the help desk is the hunt for the forgotten password or user ID.

Even if you have a well-defined password policy, the more disconnected accounts you have, the more difficult these are to enforce. At the same time, most people are going to do whatever is necessary to access the applications to do their jobs, policy or no.

A single sign-on eliminates all of these issues, from reducing help desk calls to increasing productivity to securing your company data.

A single sign-on service is a solution designed for single network domains, like YourCompany.com. Instead of logging in to individual applications with different passwords, your users go through one centralized, company-branded login screen, using one set of credentials, to access the systems and applications they need.

Not only does this approach reduce "forgotten password" calls to the help desk, but it also makes life easier for your users—enabling them to focus more on their work and less on minding multiple passwords. In addition, self-service password reset capabilities can further reduce cost and productivity loss by making it easier for users to reset forgotten passwords.

More significantly, single sign-on improves security. Your IT department now has one location from which to onboard new employees or contractors or quickly terminate access when those users leave the company. A single login reduces the potential for phishing and malware attacks. And, through the centralized portal, your organization gains a comprehensive view of users, their activities and adherence to password policies, such as password complexities and frequencies of change.

It is the "baseline" of Identity Management and one that every company should consider.

Identity Federation

While single sign-on is an excellent solution for single network domains, enterprises using multiple SaaS products need to take this centralized access one step further, adding identity federation services to their existing single sign-on platforms.

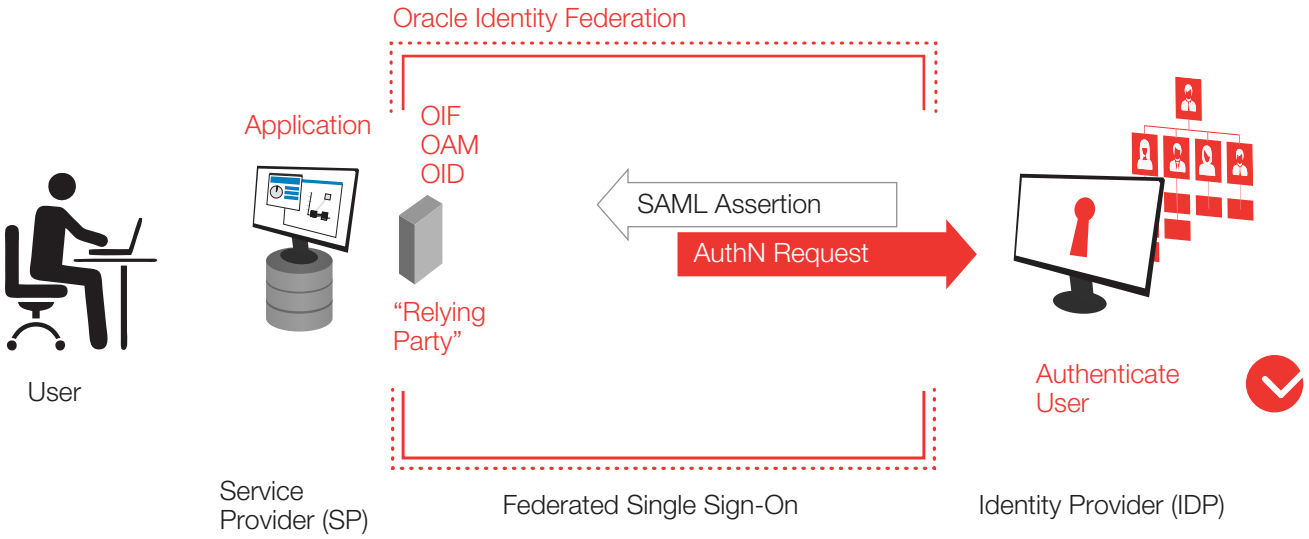
Whereas a single sign-on platform enables you to centrally control authentication for one network domain, identity federation (also called federated single sign-on) enables cross-domain authentication across multiple networks. This solution enables you to maintain centralized control of user authentication, without sharing your corporate directory credentials with your SaaS providers.

Identity Federation enables you to maintain centralized control of user authentication, without sharing your corporate directory credentials with your SaaS providers.

To see the real value, let's contrast how a user would access a SaaS application outside of your company network's domain with and without identity federation.

Without identity federation, a user logs in directly to the third-party application site, then provides a unique user ID and password. Your IT administrator manually tracks which users have access to that application and has to submit a request to the provider to remove access privileges when that employee or contractor leaves. Instead of maintaining control, your administrator has to trust that the service provider actually removed those credentials.

With identity federation, when that user attempts to access the application site, he or she is instantly redirected back to your company's single sign-on screen for authentication. Once authenticated, the system sends a digitally signed assertion, indicating the user was successfully authenticated, back to the application site. The application provider validates the assertion and allows the user to access the desired application. Your users gain access without exposing their credentials to the SaaS provider; you gain an audit trail and maintain control of your identity management.



It's important to note that the assertions are created using Security Assertion Markup Language (SAML), an industry standard, open source protocol supported by most cloud providers. That means if your providers support SAML, you can facilitate this solution without costly interfaces. Application access is centralized for all network domains for better control. And, because everything happens automatically and quickly, the validation process is transparent to the end user.

Multi-factor Authentication

While step one may be managing user identities to ensure the appropriate people have access to the right applications and services, it's also critical to ensure that your users are who they say they are. For that, the best authentication solutions take their cue from online banking.

If you have an online banking account, you probably remember the registration process. When you set the online account up, you probably selected a very specific image, like a set of golf clubs, a penguin or some other icon as your account image. From that point on, you'd see that same image every time you logged in to ensure you were at the actual banking site and not a victim of phishing.

You also chose one or two (or more) "out-of-wallet" challenge questions—meaning questions that someone couldn't answer by simply looking at a stolen drivers' license. For example, "What was your first car?" or "What was your father's middle name?" In case of an unusual pattern or multiple wrong password entries, these questions pop up to validate your identity.

The best corporate authentication solutions include a similar, multi-part authentication that includes a specific account image (which prevents mindless login entry on any screen that appears—a common malady of today's workplace), as well as validation around:

- What a user knows (his or her password and answers to out-of-wallet questions).
- What a user has (specific device(s) associated with that specific user's profile).
- What a user does (individual behavior patterns, including time of day and other characteristics around how he or she uses the application).
- Where a user is (geographic location).

Additional safeguards, like virtualized keyboards and single-use passcodes sent to mobile devices, can also be added as malware deterrents.

With all of these elements in place, a company can determine its own rules for "allow, block and challenge." For example, does an unrecognized device trigger a challenge question, or will a login attempt after 10 p.m. or from any location outside of North America block entry? Each organization has its own criteria, based on its applications, compliance issues, and types of users involved.

Information detailing login anomalies and data on other suspicious behavior are fed directly to a centralized dashboard for monitoring and follow up, mitigating data breaches and creating a cohesive audit trail.

Identity Provisioning

For companies that use a lot of contractors or have fluctuating employee numbers due to the cyclical nature of their businesses, identity provisioning presents a significant challenge. Although no one would argue that automation reduces costs, when it comes to application and system access, companies have to balance that efficiency with a solution that also mitigates risk.

A well-executed identity provisioning solution enables new employees and contractors to gain access to the integrated company applications they need through a simple, self-service process. After the employee is in the HR system, access to company resources can be automatically provisioned. In addition, employees can submit self-service access requests that then travel through a pre-determined approval workflow. Not only does this process save time and expense, but it also provides a comprehensive, omniscient view that maps the individual employee or contractor to application access. Just as important, this single world view enables administrators to quickly recognize and disable orphan accounts and similar vulnerabilities.

When an employee terminates the relationship with the company, de-provisioning is automated as well. As soon as the individual is removed from the corporate HR system or directory, this triggers a workflow to disable access from company systems and software immediately.

Identity Analytics/Role-based Access

In many organizations, software access is either a “yes” or “no,” with all of a particular user type awarded the same level of access. Not only is this inefficient, but it could present a compliance risk. Identity analytics simplifies identity control compliance by managing access based on the users’ roles in the company, instead of by individual user. This access management includes what a defined role can access and what those roles can “do” within each application. When new employees join the company, they are assigned to existing roles, which automatically gives them access to the necessary set of system applications mapped to that role.

All role-based access information, including individual user, position and application scope, is imported into and stored in a centralized identity data warehouse. This information can be used for ad hoc reporting, segregation of duty compliance audits, and other types of analysis.

Managing the Complexity of Identity Management

Although companies now have a variety of options available, it's important to note that Identity Management is not a "one and done" solution. Roles change, people change—that's a given. But what some companies don't realize is the fact that any time an application is changed, updated or modified, that change impacts the security standards tied to that specific application. If it's a custom application, the complexity escalates.

Think ERP implementation over and over and over again. Saying that "it's complicated" is a massive understatement.

Because of this reason, the level of specialized expertise required and the costs associated with implementing and running an effective Identity Management program in house, many companies are turning to managed services solution providers for help—from program set up to ongoing management throughout the Identity Management lifecycle.

Although there are some quick, out-of-the-box solutions available, most enterprises and mid-size companies need a more comprehensive, coherent approach that can evolve with them as their use of cloud-based applications increases.

For a comprehensive Identity Management solution, start at the beginning. Step back and access your current identification architecture to gain a clear view of your on-premise and cloud-based applications, your security requirements and how you're handling access management today.

- **Identify your current state and your desired future state**
  What do you want to accomplish? Reduce manual processes? Decrease costs? Ensure compliance? Gain greater visibility into user access? What is the biggest need/concern you have right now?

- **Assess your vulnerabilities**
  What are your compliance obligations? Do you really know which individuals have access to which applications and systems? Have you had recent data breaches caused by malware, phishing or social engineering? Do your individual business units procure SaaS products without IT's knowledge?

- **Profile your users**
  What does your workforce look like—heavy contractor, remote worker or primarily on-site employees? How deep is your collaboration? Are your software and systems used by employees only, or do you involve suppliers, partners and clients?

- **Identify operational inefficiencies**
  Are you managing third-party credentialing manually? What percentage of your help desk calls is related to passwords and application access? Is there one centralized point for identity management, reporting and audits?

If the process is overwhelming, you don't have to go it alone. The right partner can help you navigate the options and create a custom solution that meets your specific security requirements.

At Oracle, we have created the most extensive suite of Identity Management solution portfolios in the industry, deployed by thousands of leading businesses and government organizations worldwide. As a global company with a workforce that spans multiple continents, we know what it takes to successfully run enterprise Identity Management programs. We are available to help you create a solution that reduces costs, mitigates risk and provides the level of security you need.

Today, Identity Management is more important than ever. Know your options, create a strategy and work with a provider who can give you the security, auditability and visibility you need.

The right solution and the right partner can make all the difference.

About Oracle

Oracle provides the industry's broadest and most complete portfolio of public, private and hybrid cloud offerings. Oracle Cloud delivers a broad suite of subscription-based, enterprise-grade Application Services, Platform Services, Infrastructure Services and Social Services. Oracle also provides a comprehensive portfolio of cloud products and managed cloud services for IT providers to build and manage clouds. For more information about Oracle (NYSE:ORCL), visit www.oracle.com. For more information about Oracle Managed Cloud Services call 719.757.2065.

Trademarks

An Outsourcing Center Report