ORACLE

IDENTITY MANAGEMENT

An Oracle White Paper
July 2012

The Oracle Identity Management Platform: Identity Services at Internet Scale

ORACLE

Introduction

Identity systems are indispensible to the security, governance, and usability of online resources. Whether for authentication, personalizing user experience, or access certification, identity is at the core of making processes function properly. But for many organizations, the need to support broad user populations across a wide range of devices is driving up the complexity of identity management (IdM) systems. And deploying point products for each new requirement only exacerbates problems of complexity. IT organizations have come to realize that collections of point solutions don't equate to an identity system.

In recognition of the rapidly expanding scope of identity systems, Oracle offers a platform approach to IdM. The platform approach provides organizations with a comprehensive set IdM functions, combined with middleware for data integration and Application Programming Interfaces (APIs) for application integration. Oracle's approach enables organizations to insert critical controls into existing network resources over a series of projects, with each project increasing the maturity of the controls infrastructure. And the platform is extensible to support growth from departmental to enterprise and Internet scale.

Oracle's platform approach to IdM has already proven to deliver both scale and business value. Oracle's IdM products are deployed at thousands of organizations, and are the backbone of cloud, telecommunications, and e-commerce websites. Oracle even uses this same IdM platform for Oracle Cloud, for Fusion Applications, and for its own IT operations.

This paper outlines Oracle's platform approach to IdM, and how IT organizations can make the business case for the platform.

Identity and Access Management: Coming of Age

Over the last decade, the mission of identity and access management (IdM) systems has expanded to include a range of business objectives. Whereas early identity systems served primarily to simplify account management, today organizations are building IdM technologies into their controls infrastructure. Additionally, as applications outgrow traditional network boundaries through cloud and mobile channels, organizations are using IdM technologies to create a secure, integrated user experience. And the constant specter of hacking, insider threats, and consumer fraud also necessitates identification-based access controls throughout the enterprise. In short, the demands on IdM infrastructure are only increasing in diversity, scale, and importance. Figure 1 lists some of the common uses of IdM technologies.

Figure 1: Identity Use Cases

The use cases in Figure 1 are all served by technologies in the IdM market. But as the uses of identity technologies grow, the more difficult it becomes to achieve all of these objectives with a single solution. Large organizations in particular struggle to instill IdM technology across a digital "urban sprawl" of applications, databases, and platforms among lines of business, partner networks, and cloud applications.

The magnitude of identity systems also continues to grow: whereas the IdM market formed in departmental, single-purpose deployments, IdM systems are now at the backbone of e-government services, commercial websites, telecommunications networks, social networking, and healthcare exchanges. Both by their size and significance, IdM technologies are critical to the online world.

From IAM Suite to Controls Infrastructure

In reaction to this heightened demand for IdM infrastructure, the market continues to deliver an impressive array of products. And organizations' urgency in resolving complex security problems has cultivated a market for special-purpose tools. For every new regulation, security exploit, and managerial nightmare it seems some new standard, product, or company emerges to solve the problem. As shown in Figure 2, the IdM market now includes products for accountability, governance, privilege management, access controls, information security, commerce enablement, fraud reduction, federation, and usability.

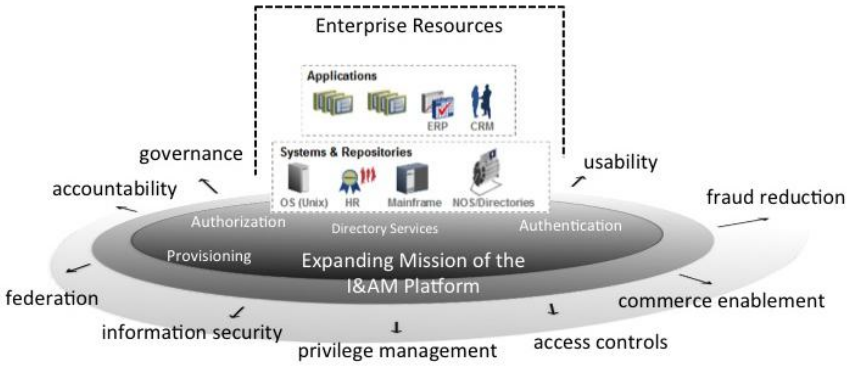

Figure 2: The identity management market is expanding to cover a wide range of use cases, creating tension for IdM products

The segmentation in the IdM market borders on fragmentation. In many cases, it's unclear where one product category starts and another ends. For example, should a role management product help organizations only to create roles or should the product also discover access violations and remediate them? There is a product for every corresponding answer to this question. As a result, organizations needing IdM technology are left with the perplexing task of completing urgent, targeted projects while implementing technology from a vast, highly nuanced, and rapidly expanding market.

The Point Solution Approach Contributes to Complexity and Risk

Pressing problems can require organizations to react quickly, often making it difficult to pursue strategic solutions. For example, a critical audit finding obliges an organization to remediate the deficiency immediately. Similarly, in the wake of a security breach, an organization will quickly tighten specific controls. So as a practical matter, organizations often choose to reduce scope of an identity project to meet near-term objectives. For example, the project team may decide that that a single sign-on (SSO) project is only for Windows applications, or that a roles project should focus only on role mining, or that an account certification project is only for SOX applications running on a particular platform.

In the context of a narrow scope, a point solution may seem simpler, quicker, and cheaper. But over time, the reactive approach proves economically and architecturally unsustainable. In practice, point

solutions contribute to the mounting difficulty of managing networked resources. Adding yet another product with a narrowly scoped purpose—with its independent data stores and requirements for special skill sets—increases IT complexity, leading to greater overall instability of the system. This is particularly true of products in an organization's security and controls framework. A patchwork of security solutions is no solution at all.

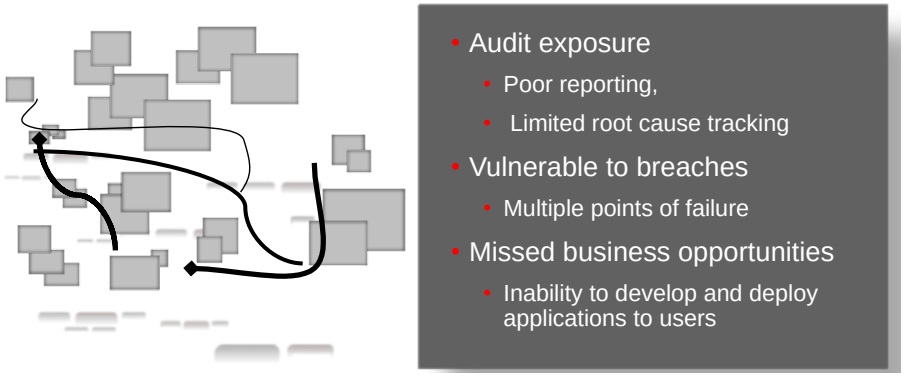

Figure 3: The patchwork approach to security and controls exacerbates the problem

Oracle recognized this market dilemma and began developing and acquiring IdM technologies and packaging them into product suites. Suites were innovative in that they enabled organizations to deal with a single vendor for sales and support, while benefitting from integration across identity products. For example, suite vendors merged meta-directory and provisioning technologies into a single product category. Similarly, Web Access Management (WAM) and identity federation products are now often sold and deployed in tandem. Such innovations are important, but ultimately don't provide organizations with what they need: a way to deploy a controls infrastructure that can be continuously expanded through a series of smaller projects.

The Platform Approach to Controls Management

The objective of a controls infrastructure is to establish order in a chaotic or poorly regulated environment, but point products are ill equipped to deliver that kind of strategic value. So if organizations require broad, strategic, and comprehensive solutions for securing networked resources, then the question becomes how best to introduce such pervasive infrastructure into an existing, heavily utilized network. The proverbial "forklift" model of replacing existing systems with a ready-made solution is rarely—if at all—possible. But with careful planning and proper oversight—and with a platform-centric solution—organizations can introduce a cohesive IdM infrastructure over a series of projects.

From a technology perspective, what's needed is a platform approach to controls management. A platform differs from point solutions and suites by offering essential services for integration, reuse, expansion, and scale. A platform approach also separates platform technology from custom development, so upgrades to either side can be accomplished smoothly and independently. In other

words, a platform is more than just a collection of point solutions—it's a cohesive and comprehensive set of technologies that is economical to extend, even to meet urgent and unforeseen demands. The following table contrasts important characteristics of a controls platform to a security point product.

TABLE 1: DIFFERENCES BETWEEN A POINT-PRODUCT AND PLATFORM APPROACH TO IDM

CHARACTERISTIC	POINT PRODUCT	PLATFORM
Integration	Standards-based interfaces with no explicit integration Proprietary connectivity and extension methods Limited options and tested configurations for OS, database, directories	Coded and tested integration with other platform components and with 3rd party point products Integration with other platforms and products through standards-based-interfaces Data tools for integration (such as virtual directory)
Reuse	Data reuse only through custom integration No reuse of management and monitoring UI – product specific for each component Reuse of components only within a single product or product family	Common definitions, data models, policy models and methods Same monitoring and management tools for entire platform Same technology for workflows, data storage, and integration Externalized security and authorization services Same connectors can be used for provisioning, password management, privileged account management, and monitoring
Expansion	Customizations relevant only within the product; often version-specific Product-specific data model or scripting language Additional use cases tax the system substantially	Clean separation of product code from custom code Portable, reusable customization Customizations not affected by upgrades Expansion to orthogonal use cases won't adversely affect performance
Scale	Often unknown or untested and only discovered once the upper bound is reached	Reliably scales from initial use case with hundreds of users to dozens of use case and millions of users

Table 1: Differences between identity point products and an identity platform

In contrast to Oracle's platform approach, point solutions implement proprietary data models, workflow engines, and scripting languages. On a deeper level, point solutions don't support a comprehensive set of applications, platforms, or topologies. For example, integrating with business applications like SAP and PeopleSoft, as well as with legacy platforms such as mainframes is nearly impossible for independent vendors to develop, test, and support. And enabling scale for controls platform is critical: the product must be able to support anything from 5,000 users to hundreds of millions of users, running as a departmental server or in active-active data center configurations with wide geographic dispersion. Few vendors have the resources and market presence as Oracle does to build products for such a wide range of uses, at scale, across difficult topologies.

A Blue Print of the Identity Platform

The figure below offers a blue print of how the identity platform supports the people and computing systems for an organization with a diverse and complex environment.

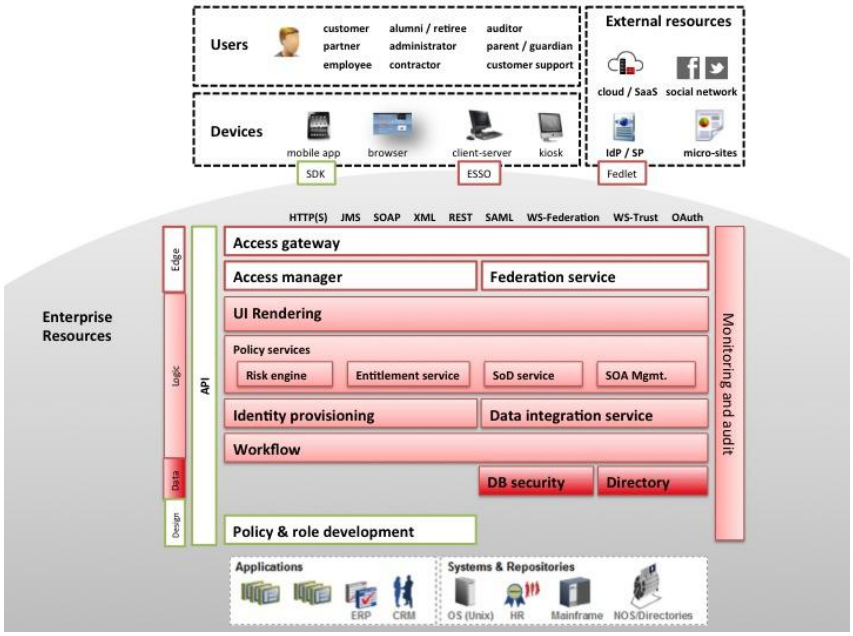

Figure 4: A high-level blueprint of the platform approach, showing connectivity to users, data, applications, etc.

In Figure 4, a gateway provides a multi-protocol "front door" to the enterprise or cloud service. The gateway represents an important identity-aware enforcement point at the edge of the network. Also at or near the edge of the enterprise network or cloud service are access management and federation services. These services help manage sessions for SSO within the environment and in connecting to external, federated services. Just below the presentation tier is a group of logic components that makeup the intelligence of the identity platform. A risk engine works with edge systems and other components to assess the contextual risk of transactions. As risk increases, the risk engine applies policies for step-up authentication, access control, and alerts. The entitlements service is an externalized decision point for assessing whether actions or transactions should proceed. Similarly, the

Separation of Duty (SoD) service evaluates whether any transactions result in a violation of policy, particularly for separation of duty.

The policy development tools provide design interfaces for administrators and policy managers to create roles, set policies for access, and policies for compliance. The identity provisioning system then ensures that policies are put into effect and that all identities are certified for use and that they contain accurate information. Data integration services enable the identity platform to easily connect to databases, directory servers, applications, platforms, and other services for data exchange, monitoring, and policy control. And finally, all actions of the identity platform are logged for monitoring and auditing purposes.

The blue print in Figure 4 illustrates why the platform approach is superior to point solutions. In particular, the platform approach is more adept than point products at handling crosscutting use cases. Consider a simple SoD use case, with the following application policy:

Approver ≠ Requester

A standalone role management product can help create the roles "Approver" and "Requester"; some standalone products can apply roles to the appropriate user accounts. The product may even offer SoD violation checking to ensure the two roles aren't assigned to the same person. But the policy above doesn't actually say one person can't possess both the Approver and Requester roles; rather, it states that for any given transaction, the Requester and the Approver must be two different people. For contextual authorization, the solution must also include Policy Enforcement Points (PEPs) and an entitlements engine—something a platform provides but point solutions can't. A platform also provides a comprehensive audit trail of how the roles were created, assigned, applied, and used.

Another example is mapping identities when no consistent common identifier exits across applications. A point solution requires a data cleansing project before SSO can begin. The platform approach enables users to start with Enterprise Single Sign-on (ESSO), which enables users to map their own accounts and receive immediate benefit of SSO. Because the ESSO product is part of the platform, it can share mapping information with provisioning service so that other IdM services can be extended to these users quickly.

Many such crosscutting use cases are why organizations now prefer IdM platforms to point products.

Economies of Scale for the Platform Approach

Organizations that take on more than three controls projects will find the platform approach cost-effective and much easier to complete. In a study by Aberdeen Group, a leading market research firm, of 160 organizations, those that took a platform approach to controls management saved 48% in costs, achieved 46% more responsiveness, and had 35% fewer audit deficiencies when compared to organizations that adopted point solutions.

48% Cost Savings

46% More Responsive

35% Fewer Audit Deficiencies

The platform approach creates synergies that provide greater value and automation when the solutions are integrated. Here are a few additional economic benefits documented in the Aberdeen report.

- Increased end-user productivity – The organizations that chose a platform approach provided end user self-service 30% faster than organizations that did not have an integrated self-service capability. In addition, platform adopters were more agile by on-boarding and changing user access 73% faster than organizations that took a point solution approach.
- Faster application deployment – By having an integrated platform, organizations were able to deploy new applications with identity management enabled 64% faster.
- Improved administrative ratio – The study showed that companies that adopted a platform approach achieved an average of 5,500 users per administrator compared to 2000 users per administrator with the point solution approach.

By taking an organizational approach with a platform, the organizations that had a long-term roadmap for identity management achieved better economies of scale. Instead of solving the challenges of a single department, they were able to set a foundation to address the requirements across departments. As a result, the platform adopters showed greater indication of standardization and repeatable reporting processes. In particular:

- Platform adopters were twice as likely to have standardized workflows to automate the user lifecycle and provide workflow-based exceptions.
- Platform adopters were twice as likely to have more mature controls like separation of duties and attestation reporting in place.

The platform approach offers a better financial model than do point solutions. Using the findings from the Aberdeen study and Oracle's Return on Investment (ROI) calculation tool, customers can estimate how a platform approach will benefit their organization. Figures 5 and 6 (below) illustrate an ROI calculation for a platform approach compared to a point solution approach over a period of five years.

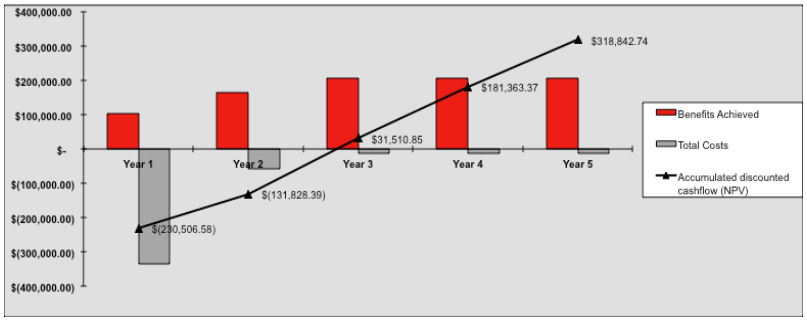

Figure 5: ROI example from a platform approach to identity management

Figure 5 illustrates a platform approach to an identity management project. Given parameters for hard and soft costs, including software licenses, the customer will be able to achieve a breakeven point in Year 3 and has doubled the ROI by Year 5.

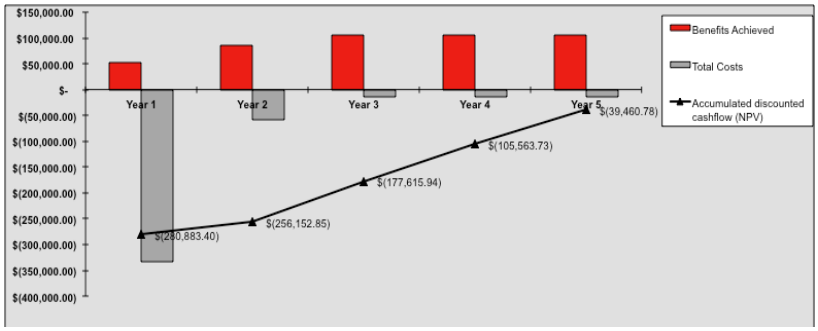

Figure 6: ROI example from a point solution approach to identity management

In contrast, Figure 6 (the point solution approach) uses the same parameters as the project in Figure 5. The calculator shows that because of additional costs, complexity, and delays, the project approaches the break-even point in Year 5 and the benefits aren't fully realized.

Anatomy of a Platform: Inside the Oracle Identity Platform

Oracle's approach to IdM recognizes organizations' need for comprehensive controls. For this reason, Oracle has focused relentlessly on creating a complete, open, and integrated platform for IdM. With a design center of enabling a broad set of control objectives from a single platform, Oracle's IdM technologies include "classic" identity management capabilities, such as directory, provisioning, and Web Access Management (WAM), in addition to platform services (such as virtual directory and entitlements services), data security, and Application Programming Interfaces (APIs). These technologies enable organizations to construct a foundation for instilling "controls in depth," in a pervasive manner across applications and data, across all access channels.

Oracle's identity platform consists of three functional pillars and underlying platform services, as shown in the following figure.

Figure 7: Functional groupings in the Oracle 11g R2 Identity Platform

Identity Governance involves setup of the environment in advance of access, as well as review of the environment to ensure policies are enforced as intended. The *Access Management* pillar includes the

technologies involved in run-time enforcement of access—that is, when users are actively using the system. *Directory Services* operate at the data layer to provide identity context to the other two pillars. Oracle also provides *Platform Security Services* that enable developers to access any component in the pillars, externalize security decisions, and take advantage of platform security features.

In the 11g R2 release, the Oracle identity platform consists of the following technologies:

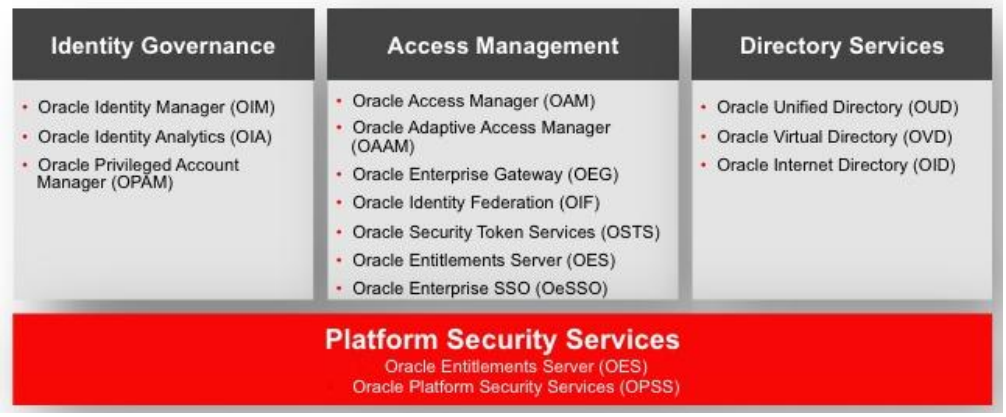

Figure 8: Oracle products and technologies in the 11g R2 IdM Platform

The function of each of these products is explained below.

- **Identity Governance** products:
    - **Oracle Identity Manager (OIM)** is an identity provisioning product. OIM includes features for self-service password management, access request forms, delegated administration, approval routing workflows, and entitlement management across any number of connected systems.
    - **Oracle Identity Analytics (OIA)** collects logs from IdM products and other systems to report on usage, build effective IT roles, and detect account-related audit issues such as orphaned accounts.
    - **Oracle Privileged Account Manager (OPAM)** secures accounts with elevated access, such as root accounts on Unix systems and databases, by implementing a password checkout system.
- **Access Management** products:
    - **Oracle Access Manager (OAM)** is a Web Access Management (WAM) product that enables SSO across an organization's web presence.
    - **Oracle Adaptive Access Manager (OAAM)** enables organizations to apply stronger, risk-based, and multi-factor access control to an organization's web presence.
    - **Oracle Enterprise Gateway (OEG)** is a soft-appliance XML gateway for securing and managing application and web access to an organizations web presence.

  - **Oracle Identity Federation (OIF)** provides standards-based identity federation capabilities for enabling SSO across websites.
  - **Oracle Security Token Service (OSTS)** is a WS-Trust compliant STS implementation. An STS converts security tokens of various types, enabling compatibility and trust across federation boundaries.
  - **Oracle Entitlements Server (OES)** is a fine-grained entitlements service that supports a variety of externalized authorization mechanisms including XACML 3.0.
  - **Oracle Enterprise Single Sign-On (OeSSO)** is a client-based SSO product that enables users to access web, client-server, and legacy applications though a single, strong authentication "wallet" for authentication.

- **Directory Services** products
  - **Oracle Unified Directory (OUD)** includes both a highly scalable LDAP directory service based on Java and the Oracle Virtual Directory (OVD) product. See the section below for more information on OVD.
  - **Oracle Internet Directory (OID)** is a scalable LDAP directory service based on Oracle database technology.

The Secret Sauce: Oracle's Middleware for the Controls Platform

The Oracle IdM platform is unique in its inclusion of middleware for connectivity and security. In Oracle's experience with business applications, these technologies are indispensible to a successful IdM deployment. In the 11g R2 release, these technologies are as follows:

- **Oracle Virtual Directory (OVD)** enables efficient and elegant integration to data sources.
- **Oracle Entitlements Server (OES)** provides a scalable approach to fine-grained entitlement controls, contextual role enforcement, and run-time policy evaluation.
- **Oracle Platform Security Services (OPSS)** provide developer access to essential security functions.
- **Oracle Enterprise Gateway (OEG)** enables SOA applications to establish an identity-based control at the edge of enterprise networks. OEG also provides REST-ful interfaces to the identity platform for mobile applications. And when combined with Oracle Web Services Manager (OWSM) also adds encryption, PKI, and related policy control to web services.
- **OWSM** secures and applies identity to SOA interactions.

Fulfilling Critical Use Cases with the Oracle IdM Platform

With this broad set of integrated technologies, the Oracle Identity Platform enables organizations to deploy all the use cases referenced in this paper. For example, the Oracle Identity Platform enables "closed loop" access certification—that is, the platform not only reports on uncertified access, it also

helps to remediate any findings. The platform also continuously maintains SoD policies while automating access changes through self-service, delegated admin, and access request workflows.

The platform also enables organizations to manage access policies globally. The "access pillar" of the Oracle Identity Platform includes SSO for legacy and Web applications, including out-of-the-box integration with leading platforms, databases, devices, and applications. Because of the common management framework, organizations can view and manage user sessions in real time. The platform also includes risk-based controls over access through the Oracle Adaptive Access Manager (OAAM) product. With OAAM, organizations can perform device fingerprinting and assess security risks in real time. For example, organizations can control access based on the location of a connected device and the sensitivity of the transaction, combined with the behavioral patterns of the authenticated user. If the risk factors appear high, access manager can require the user to perform a step-up authentication, use a one-time-password, or meet some other requirement before permitting access.

The following figure shows how Oracle's IdM platform fulfills some of the critical use cases discussed at the beginning of this white paper in Figure 1.

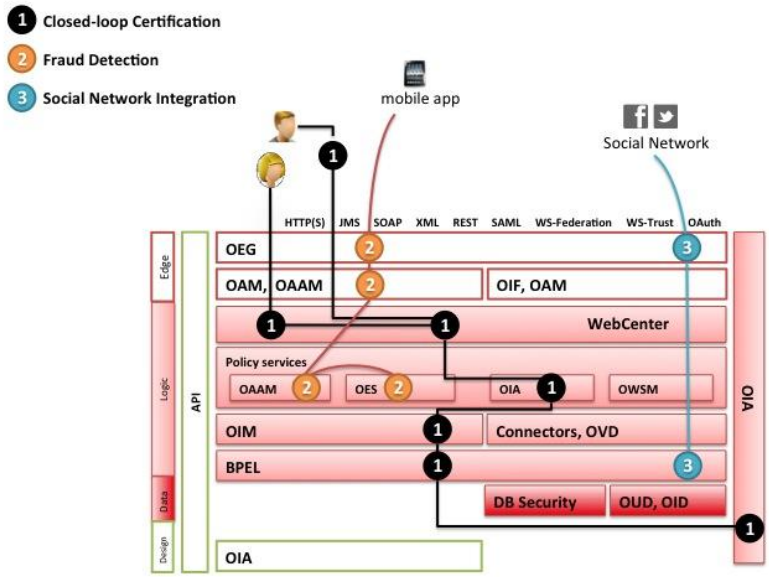

Figure 9: Oracle IdM products fill out the architectural blueprint

The three use cases identified in Figure 9 flow as follows:

1. **Closed Loop Certification.** To provide a Closed-Loop Certification process, identified as flow "1" in Figure 9, an employee first uses a self-service applet to request access privileges. The user's view of applications and entitelments is set by policy in OES. OIA verifies that the request doesn't violate any Separation of Duty (SoD) violations based on the user's existing privileges. OIM then orchestrates various workflows to collect and record any requisite approvals and then sets roles and privileges in the directory service and any connected systems affected by the change. Periodically, OIA can be used to report on the user's overall access, gather and record the appropriate approvals, and extend the user's privileges and revoke any excess privileges.

2. **Fraud Detection.** When a user attempts to access a web resource, OAAM captures information provided by the broswer, including MAC address, IP address, browser type, etc. OAAM uses this device "fingerprint" and the associated user authentication (provided by OAM) to rate the risk of the transaction. If the risk score is high, OAAM can require the user to provide additional information before allowing access. Also, based on the risk score and user information, OES provides policy on whether the user can access the target resource.
3. **Social Network Integration.** A user who has authenticated to a social networking site can use those credentials to access certain low-risk portions of the organization's website. Using social federation services provided by OAM, the user can also use credentials from other sites to create a profile on the organization's site.

Modular and Best-of-Breed

Oracle's platform approach is founded on a long-term architecture of modularity, with best-of-breed components. Accordingly, as Oracle continues to increase integration among its identity products, each product will deliver best-in-class performance for its category. Oracle has already delivered on this promise: with the 11g platform, Oracle's identity products are recognized as market leading by Gartner and other analyst firms. Oracle's platform approach ensures that the benefits of using products in combination will be greater than in isolation, but Oracle builds no interdependencies into its identity products.

Oracle's identity products are likewise built and tested to support a number of non-Oracle operating systems, application servers, and IAM products. Many identity platform customers use Oracle identity products in combination with other vendors' infrastructures and applications.

Oracle's stance on openness and modularity isn't just good for customers, it's critical to Oracle's business model as well. The nature of a controls platform is to be connected to all systems in the enterprise, including other identity solutions. The open approach also takes advantage of common skill sets required to operate the platform. And as Oracle moves toward a shared services architecture, where components of technology are reused among products as appropriate, the modular approach emerges as the superior architectural model.

Support for Open Standards

The Oracle Identity Platform supports all relevant standards, including LDAP, SAML, WS-Trust, WS-Federation, XACML, OpenID, OAuth, and SPML. Oracle also continues to innovate in the standards community. Recently, Oracle sponsored JSR 351 to introduce the notion of "identity" into Java. Oracle also is participating in the IETF around adding "enterprise" profiles for OAuth to enable mobile SSO. Oracle also proposed standards for open authorization (OpenAz) and the Identity Governance Framework (IGF) for attribute sharing.

Connecting to Third-Parties and to the Cloud

The identity platform offers technologies that make it easy to integrate with partners, suppliers, and cloud services. The access technologies support all the major federation standards, including SAML 1.x and 2.x, WS-Federation, and OpenID. The access suite also includes a Secure Token Service (STS), which enables token exchange and trust brokering for propagating access and identity across applications and web services, and the OWSM provides a WS-Trust 1.4 implementation.

Maturity and Scale

All components of the Oracle Identity Platform are tested for extreme scalability and reliability, supporting millions to hundreds millions of users. Oracle's platform is also engineered to support Oracle's Exadata and Exalogic platforms, as well as Real Application Clusters (RAC), for database clustering, and Coherence, Oracle's in-memory data grid technology. These technologies have proven to scale under heavy load, with sub-second response times even at extreme scale.

The 11g R2 release offers all the trimmings of a mature product, including language support for 28 languages, dedicated field and technical support personnel, partner support among major and boutique integrators, and a large and active user community. Oracle has thousands customers of its identity products in virtually every vertical and geographic market. Customers also include ISVs that are re-platforming their custom solutions with Oracle identity products.

Strong market support for Oracle's IdM platform also promotes the security and longevity of the overall product. Because Oracle's access products have been battle-tested through their presence on large Internet portals, government websites, financial services implementations, and telecommunications infrastructure, all customers benefit from the resulting refinements. Oracle also employs hundreds of trained security experts to write and test the code of each release. In addition, Oracle offers security products for a database firewall, SOA gateway, and data encryption that customers can use to secure the identity platform as well as networked resources.

All Oracle products are engineered to support on-premise deployment as well as hybrid cloud, private cloud, and public cloud models. The Oracle IdM platform is already being used for Cloud applications, including applications delivered through Oracle Public Cloud. As announced at OpenWorld, the Oracle IdM platform supports the following configurations through Oracle Public Cloud:

- Platform as a service (Java, app server and DB) with all IdM provided by Oracle IdM platform
- Software as a service (CRM and HCM) with all IdM provided by Oracle IdM platform
- Unique enterprise IdM features: full delegated administration and self service, bulk on boarding, and customizable UIs

Many of Oracle's identity customers are service providers themselves, and as such they require high scalability, multi-tenancy support, and open connectivity. Today customers are using existing versions of Oracle identity platform to support Cloud requirements. For example, Oracle OnDemand hosts OAM, OAAM and OIF for a large banking customer. Oracle partners with Simeio and Accenture hosts OIM/OIA for customers like their large clients. And partners like Sasktel have stood up OIM as a Cloud IdMaaS for SMB and vertical market customers.

Platform for Developers

A key difference between point products and platforms is the developer API. A platform enables developers to reuse and extend a common framework, whereas point products only enable programmatic access to a limited set of functions related to the application. The Oracle Identity Platform boasts the most functional, versatile, and open programmatic interfaces on the market.

OPSS provides extensive access to security features in the Oracle platform. The platform itself is based on Java, but developers can take advantage of these features from a range of APIs. For example, a mobile application can use the REST-ful interface to authenticate and authorize access. OPSS also supports a SOA interface. Developers can similarly rely on the platform to execute policies based on Business Process Execution Language (BPEL) and Extensible Access Control Markup Language (XACML). And as developers externalize application security to a common platform, organizations achieve the added benefits of centralized oversight and administration. Oracle Application Developer Framework (ADF) enables user interface (UI) designers to quickly create powerful user experiences. The identity platform is also integrated with Oracle Web Services Manager (OWSM), part of Oracle's SOA Suite. OWSM enables developers to use standards-based methods to secure and identity-enable SOA services.

Oracle's connector framework includes toolkits and templates to simplify application integration for most leading infrastructure, platforms, and applications. These connectors can then be reused for provisioning, password management, privilege management, and identity analytics.

Oracle's Commitment to IdM

Despite strong overall market growth, a large number of identity vendors have been acquired or have exited the market. Other companies have slowed their release cycles leaving customers to fend for themselves while waiting years for new functionality.

In contrast, Oracle has made an unprecedented commitment to its identity products. For starters, Oracle's Fusion Applications—including middleware and business applications—rely on Oracle's IdM products for authentication, authorization, and security services. Oracle Public Cloud also uses the Oracle Identity Platform for IdM features. Consequently, Oracle's internal requirements have helped to justify significantly greater investment than the competition and have allowed Oracle to prove out the platform's architecture and capabilities internally before releasing the platform to the market.

More importantly, the Oracle Identity Platform is a thriving business unit within Oracle. With thousands of customers worldwide, dedicated sales and support teams, and double-digit revenue growth, the identity platform is a crucial component of Oracle Fusion Middleware.

Platform Approach with a Pay-as-You-Grow Pricing Model

Oracle's Identity Platform is architected to support an organization's growth. Many customers begin with a distinct project and then evolve and extend their implementation toward a broader and more complete identity management solution. This benefit extends from product architecture to licensing. Oracle offers flexible licensing options that enable growth without requiring detailed "user counting"

and provide the ability to mix-and-match products to address a broader variety of requirements and use cases, via suite licensing options.

What's Next for the Oracle Identity Platform?

Oracle has already made significant progress on building out a platform for identity and controls, and the path ahead is even more ambitious. Oracle is extending the platform for greater integration with mobile devices, social networks, and cloud applications, and is continuing to refine the user interfaces for administrator and end users.

Simplification and Usability

Oracle continues to refine the platform by rationalizing the data model across the platform, improving the user experience (both for administrative uses and end users), and simpler deployment and manageability. The platform interface will soon sport a simpler interface, with the experience based on familiar UI metaphors such as catalogs and shopping carts. The UI will also be simple to customize using drag and drop changes direly in the browser—no special design or engineering tools are required. Common use cases like self-service password management, access requests, delegated administration, user certification, and workflow approvals will also have a common data model and UI. Oracle will also soon release a Privileged Account Management (PAM) component that will provide secure check-in/out of root, administrator, and service account passwords.

Securing Applications on Mobile Devices

Mobile computing is rapidly changing the application landscape for enterprises. As organizations wrestle with security and management repercussions from a tsunami of mobile devices on their networks, the Oracle Identity Platform will make these devices a managed part of the enterprise network. In 11g R2 Oracle added REST-ful interfaces to the identity platform, which will extend IdM features to iPhones, iPads, and Android-based devices. In addition, the platform provides a Mobile SDK, which enables organizations to create their own identity-aware applications that can be distributed using the Apple's App Store. The REST-ful interfaces and the Mobile SDK will provide mobile applications with commonly used IdM capabilities including password management, yellow & white page lookups, and workflow approvals. The Oracle Identity Platform will to continue to grow its support for REST-ful interfaces and mobile applications.

Cloud

Oracle also continues to enhance support for cloud computing through the identity platform. Oracle is extending its provisioning connector framework to support multiple cloud and on-premise environments. Through the ESSO product, Oracle will also offer federation to the desktop with prebuilt templates for Cloud providers and multifactor authentication. Enterprises will soon have the option to use the platform as a full enterprise-grade SaaS offering for user, role, and request management as well as authentication services. And the platform will soon boast tighter integration among its Web Access Management (WAM), federation, Security Token Service (STS), entitlements

service, and adaptive authentication components to deliver high performance and scale for complex authentication and authorization schemes.

Conclusion

The rapidly changing business environment is forcing organizations to rethink their IdM strategy. Research has shown that a department level, point-product approach is costly and ineffective due to lack of integration, gaps in security, and restrictions in scope and scale.

What is needed is a platform approach that serves the immediate security and compliance needs while providing an extensible and secure foundation for a long-term enterprise IdM strategy.

Oracle's IdM suite of integrated, secure, and highly scalable products meets these requirements, and positions forward thinking enterprises for success as they enable their users to take advantage of cloud applications and mobile devices.

For more information on Oracle's IdM platform, see www.oracle.com/identity as well as blog posts on blogs.oracle.com/OracleIDM.

Oracle Identity Platform
March 2012
Author: Mike Neuenschwander

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together