An Oracle White Paper

Feb 2012

Buyer's Guide for Access Management

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Overview

The enterprise identity management landscape is maturing and evolving. In recent years, economic and market forces have forced companies explore ways to reduce costs via data center and license consolidation. This has also forced companies to embrace cloud computing, either in the form of private or public clouds, to access new services at reduced costs. At the same time, changes to healthcare and privacy laws along with a large set of regulatory requirements have forced corporations to rethink their approach to enterprise security. In addition to legal and regulatory considerations, today's businesses are bombarded daily by new threats and emerging technologies that challenge and endanger sensitive enterprise data and applications. The nature of threats to the enterprise has become more sophisticated – witness the rise of Malware, Session Hijacking, Botnets, Social Engineering, Phishing, Pharming, and Keyboard Logging, to name a few. Security in today's dynamic business environment must not only be nimble enough to adapt to these external threats but it must also protect against internal threats as well. Passive security and compliance measures are no longer good enough for today's complex and ever changing security climate. Ultimately, businesses must have solutions that proactively mitigate risk and actively comply with current and future measures and regulations.

In this challenging environment, companies must develop a holistic and proactive strategy based on risk management principals. Companies that use a reactionary approach to security, selecting different identity-based solutions to protect web applications, host or client-server applications, web services, and federated or partner-based applications will ultimately fail. Reactionary approaches result in a brittle security infrastructure that is difficult to maintain and, as a consequence of inconsistent security policy management, prone to data leaks or worse.

Today, many vendors offer access management solutions that go beyond access management basics providing analytics, dashboards, and forensic tools. Many of the products offered today cover multiple aspects of access control, making it difficult to

select the right security solution. So how do you select an access management solution that is right for you? A robust access management solution should not only provide basic access management functionality but also provide -

Security from disk to web: The access management solution you choose should be an all-in-one solution that covers multiple aspects of security management. It should be able to provide solution for securing applications, data, digital assets, web services, and cloud-based services.

Flexible, Scalable, Simplified Deployment: The best access management solution is optimized for scalability, performance, and ease of development. It can plug into an application security framework, so different security mechanisms can be applied throughout the lifecycle of an application. It is also scalable to expose business applications and data securely to a wide variety of users including remote employees, customers and partners – all across a heterogeneous environment.

Third party integrations: A good access management solution provides Out-of-the-box integration across, various components to simplify and streamline deployments.

Monitoring and Diagnostics: The access management solution you choose should ideally provide robust monitoring for large-scale deployments that allow system and network administrators to proactively manage important enterprise assets.

Integrated user experience: An effective access management solution ideally provides a common user experience across the entire range of products thereby increasing user productivity and cost-effectiveness.

This buyer's guide will help you evaluate and develop a clear understanding of key features that fit your unique security needs, business drivers and infrastructure requirements, now and in the future. It provides a detailed list of product features and vendor capabilities that many customers consider when evaluating the components of an access management solution.

Business Drivers

Although there are many practical reasons to consider security solutions, it is helpful to understand how they can positively impact the business. In this section of the whitepaper, we'll take a look at key business drivers for adopting Access Management solutions in today's enterprise:

Security Simplified: Security should be easy to manage, ensuring timely and effective deployments and creating a uniform user experience. By establishing a simplified approach to security, the business can be assured of tighter control, reduced operations costs and a more consistent solution.

End-to-End Security: Enterprises today are looking to adopt solutions that can provide end-to-end protection. A complete solution will protect sensitive data at every tier - from the DB, to end user facing applications and even external documents that leave the firewall.

Performance for Cloud and Extranet: Organizations are increasingly looking for their partner network and the cloud to provide competitive advantage or to serve their customers with new innovative services. Access Management security must be able to perform at Cloud or Extranet scale to serve the modern enterprise.

Active Compliance: Security solutions today must do more than protect data - they must also assist in attesting to various regulatory and compliance needs. A comprehensive Access Management solution will provide detailed audit and reporting data to not only ensure compliance - but also help to exceed compliance standards in many cases. Complete Access Management solutions must provide not only visibility in what systems a user has been granted access but must be able to provide data on who and how often a user has accessed a system.

Risk Mitigation: With so many types of threats facing the enterprise, a complete Access Management solution must do more than simply log risky or anomalous events. It must also proactively reduce risk. By comparing historical data against current activity, and by automatically learning which user behaviors are normal and which are not, organizations get e piece of

mind and assurance that threats to their intellectual property, their business operations, and their user identity data are responded to in real time.

Collaborate and Protect Data at its Source: Organizations want to stimulate collaboration within the organization but they want more control on how that data is shared internally and externally.

Customer Problems

Organizations today are focused on solving a few key problems in their environments that involve access and authentication.

Authentication and Authorization: The traditional challenge of authentication and authorization, whether for a few thousand or for millions of users, still exists and is a core problem for organizations. Authentication for core business applications has extended to applications that require network or services in the cloud. Organizations need to leverage their identity data to create new products and services, federate with partners, meet aggressive timelines, and facilitate mergers and acquisitions. These organizations need proven performance, and cost effective ways to access data without changes to application code or upsetting political owners of that data. Additionally, authentication alone is not enough to prevent fraud and misuse. An advanced capability to actively monitor user behavior and take preventative actions is required for a complete security solution.

Identity in the cloud: With organizations under direct pressure to reduce operational costs and expand revenue, federation has begun take a central role in defining organizations identity architecture. Organizations need solutions that can meet the performance and scalability requirements of Internet authentication, aggregate identity attributes from multiple applications and synchronize data between on premise directory services and cloud-based identity services all in one solution.

Identity Security: Organizations are faced with a continually challenging security environment where threats need to be managed internally and

externally. They need an authentication solution that can store the appropriate authentication attributes and policies needed to make the relevant access decisions. Organizations struggle with creating password policies for applications based on their risk profile and business needs. They need open solutions that allow them to respond to dynamic security threats quickly and in a cost effective manner.

Data Center Consolidation: Operational budget's can consume up to 60% of an IT budget. Organizations are looking for tools and projects to reduce the cost of their data center. This includes consolidation of technology and licenses as well as doing more with less. Performance and serviceability are also key business drivers in their purchase of new solutions.

Collaboration: Employees and partners require collaboration to stay in-synch and continue to innovate. The employee and partner networks are distributed globally and work from remote locations. The portals, email, calendaring, IM, and other collaboration tools need to rely upon one authentication source to ensure they can login and have access to the right tools.

Oracle Access Management Suite Plus Overview

Oracle Access Management Suite Plus is the industry's most complete end-to-end security solution, providing best-in-class components that protect applications, data, documents, and cloud-based services through an innovative combination of flexible authentication and single sign-on, identity federation, risk-based authentication, proactive enterprise fraud prevention, and fine- grained authorization. It also provides the industry's most comprehensive solution for securing applications, data, web services or SOA, and cloud-based services. It helps companies strengthen application, and data security, prevent fraud, satisfy audits, and improve user experience. Oracle Access Management Suite Plus provides a uniquely integrated, modular architecture that gives customers the flexibility to deploy a complete solution, to focus on deploying

individual, best of breed capabilities, or to easily and quickly integrate 3rd party security services into a single solution, offered at a single price point.

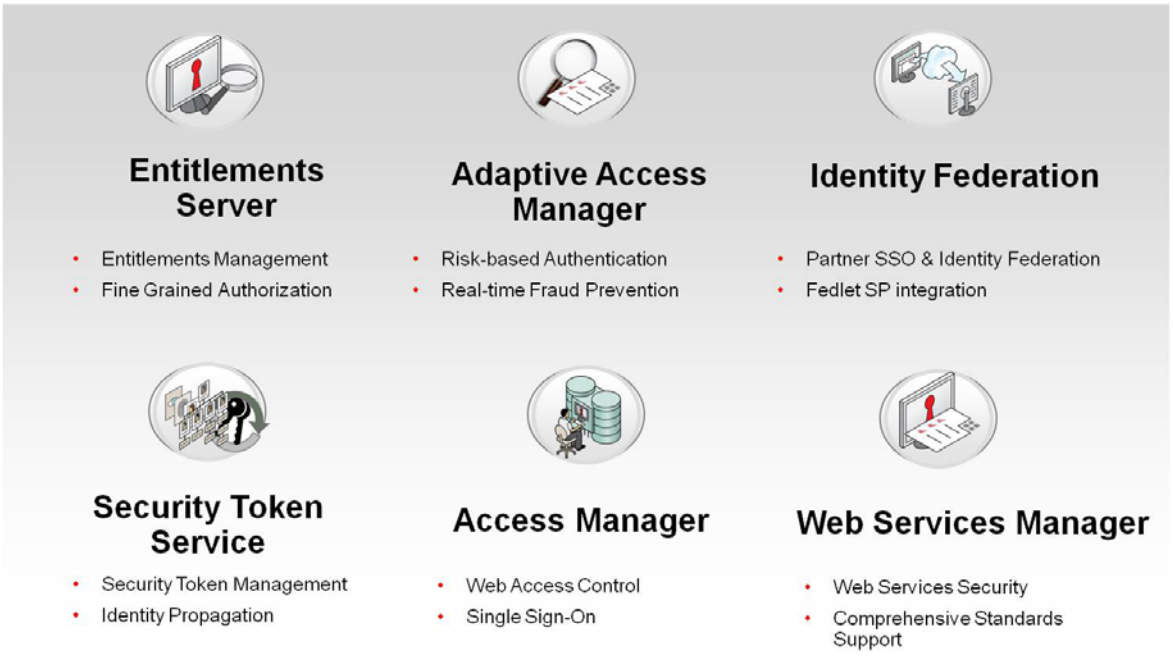
Key Components

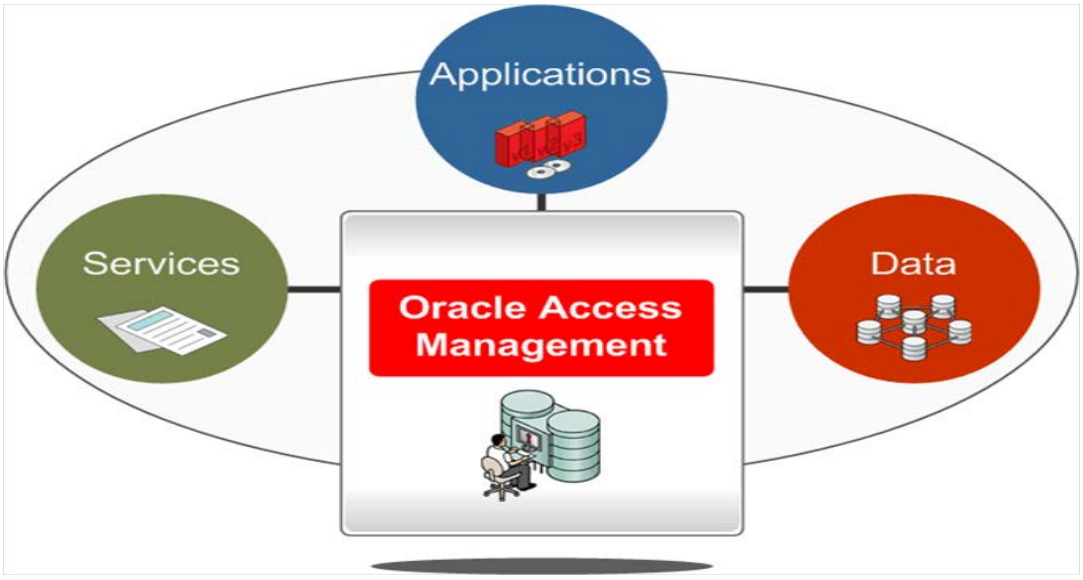
Oracle Access Management Suite Plus includes:

- **Oracle Access Manager,** which delivers critical functionality for access control, single sign-on, and user profile management centralized session management, and agent management in anther heterogeneous application environment.
- **Oracle Adaptive Access Manager,** which provides real-time and batch risk analytics, behavioral analysis, risk-based authentication mechanisms and authentication strengthening capabilities.
- **Oracle Entitlements Server,** which provides risk-aware fine-grained application and data authorization.
- **Oracle Identity Federation**, which provides cost effective, standards-based federated single sign-on, federated identity management capabilities, and the industry's simplest integration and deployment options. It also enables secure identity information exchange between partners. It significantly reduces need to manage unnecessary third-party identities and lowers the cost of integrations through support of industry federation standards.
- **Oracle OpenSSO Fedlet,** which allows organizations to quickly and easily set up standards-based federations with service provider partners, create a standard integration pattern for additional partners, and achieve secure sign-on across partners in a matter of hours.
- **Oracle Enterprise Single Sign-On,** which enables users login to enterprise applications using a single password or with stronger credentials including PKI, Smartcards, and Biometrics to access any protected application on the desktop, network or Internet.

- **Oracle Web Services Manager**, which extends identity driven security to your web services and service oriented architecture.
- **Oracle Security Token Service**, which enhances access management and Identity security with standards-based identity propagation and security token issuance and management.

Oracle Access Management Suite Plus





Key Features

End-to-end Security: Access Management Suite Plus provides real-time risk analysis end-to-end authentication, single sign-on, and fine-grained application protection and helps align and integrate point solutions to provide context across various infrastructure tiers. It also provides stronger security and less complexity through a single suite of products. It simplifies how customers secure consumer applications, internal web apps, Java apps, web services, and SOA and also lets the customer extend that security seamlessly to federated business partners.

Suite level integration: Access Management Suite Plus delivers well-integrated functional components to provide better security and value to customers. Access Management Suite Plus simplifies installation, deployment, and integration through a unique, modular architecture that builds upon the strengths and capabilities of Oracle Fusion Middleware. In addition, enhanced manageability, superior diagnostics, and

innovative features ensure a lower total cost of ownership and a simple, easier to manage operational environment.

Innovative anomaly detection, transaction security, and multi-factor authentication: Access Management Suite Plus provides a unique layer of fraud detection and authentication security on top of the existing security features of web SSO, federation, and application entitlements management. It provides strong yet flexible protection for businesses and their end users by strengthening login processes, self-service password management flows, providing risk-based challenge methods and harnessing real-time and batch based fraud prevention/detection strategies. Access Management Suite Plus can also help evaluate the level of risk for each individual access request or transaction based on the location, device, user behavior and other factors. Features such as Knowledge Based Authentication Answer Logic and OTP (One Time Password) Anywhere furnishes extra layers of identity assurance for web application access in an exceptionally cost-effective and user friendly manner.

Centralized Application Security and Authorization: The authorization features of the Access Management Suite Plus centralize security for enterprise applications and SOA by providing comprehensive, reusable, and fully auditable risk-aware authorization policies. With a user-friendly administration UI, customers can easily build structured authorization policies to fulfill the most complex application security use cases. Additionally, the distributed runtime policy enforcement for applications simplifies how enterprises secure diverse and heterogeneous environments such as SOA, JEE applications, packaged enterprise applications; sensitive data stored in databases, or enterprise portals.

Lower operational costs and better IT agility: The Security Token Service simplifies the orchestration of standards-based and proprietary tokens between web services clients and providers, enabling businesses to abstract security from web services. Access Management Suite Plus helps improve IT agility with the Fedlet, which quickly and securely on-boards partners to form a federated trust relationship.

Extranet Security at Cloud Scale: The Access Management Suite Plus provides unique capabilities that allow organizations to leverage the innovation and services from their partners and cloud service providers to maintain competitive advantage. Using proven best of breed technology and standards, organizations can adapt to quickly changing global environment and assemble the services and applications for its customers.

Enterprise Access Management Checklist

Suite Level Integration

Key Feature	Benefit
End to End Security	•Better integration between functional components of the suite
Aligned Admin consoles	•Consistent Authentication Administration, Agent Administration, Fraud Prevention Administration, and Authorization Administration
Risk-based Authentication	•Highly usable challenge questions •One Time Password via SMS, IM, email, voice •Pluggable authentication framework
Malware & Phishing Protection	•Identity protection for customer and enterprise users
Secure Password Management	•Out of the box interoperability using risk-based authentication •Single source of truth for password resets •Consistent user experience
Secure Self Service Password Management	•IAM Suite interoperability that largely replace the need for help desk calls can save a lot of money
Enterprise ready	•Enterprise features like policy simulation, system snapshots, diagnostics & troubleshooting available
Out of the Box Suite-wide security	•Pre-integrated platform •Secure access by default

Fraud Prevention and Risk Mitigation

Key Feature	Benefit
Simplified Security Administration	•Simplified, streamlined flows for creation and management of complex fraud policies via rich web interface
OTP (One Time Password) Anywhere	•Add risk-based authentication to SSO and self-service flows •Utilize any cell phone as a second factor •Authenticate users out-of-band
Universal Risk Snapshot	•Easily backup and restore security configuration •Migrate security configuration between environments
Answer Logic	•Add highly usable security to vulnerable self-service password reset flows •Avoid unneeded help desk calls by allowing variable forms of valid challenge question answers
Real-time risk analytics & interdiction	•Risk evaluation logic that "figures out" the level of risk at a given moment based on a multitude of data points •Risk based proactive actions can block fraud attempts in their tracks
Behavioral Profiling	•Behaviors automatically profiled in real-time so anomalies are detected immediately. Zero lag time so that the solution can adjust quickly and spot fraud with lower false positive and negative rates
Device tracking	•Devices used to access applications can be tagged and tracked throughout a session to offer enhanced protection from threats such as session hijacking
Location intelligence	•Network and geographic location awareness enables advanced risk analytics
Multiple Deployment Options	•WAM, Native, Reverse Proxy, Listener, Batch

Authentication

Key Feature	Benefit
Session Management	•High performance access to distributed session data •Enforce session constraints •Persists session data for authenticated users in an embedded Coherence Grid
AppSecure Control Center	•Centralize application protection •Simplify ongoing administration by manage Agent creation, management, and diagnostics from a central Admin console
Simplified Application Integration	•Next Generation Architecture Java EE based server •Consolidated SSO architecture Backward compatibility across OAM, OSSO
SSO Security Zones	•Prevents unauthorized access from spreading to multiple applications •Scopes encryption keys for data passed to an application enforcement point, creating security zones that prevent unauthorized access from spreading to multiple applications
Self-Service Password Management	•Gives end users the ability to create and reset their password without assistance to dramatically reduce help desk costs and helps to keep users productive
Centralized Policy Administration	•Simplify policy creation, management, and propagating security policies through a central Admin console

Extranet Security at Cloud Scale

Key Feature	Benefit
Fedlet	•Ability to create relationships with service providers and test those relationships in matter of hours
Improved SaaS integration experience	•Federate quickly and easily with Google and SalesForce. Use industry best of breed security standards like SAML, OAUTH and OpenID

Key Feature	Benefit
Secure Session Control	•Scale with confidence to the cloud using the best of breed session management solution
Federated Directories	•Works seamlessly with Oracle Virtual Directory to virtualize your data in legacy applications without changing code. This will allow you to quickly and easily assemble new services with cloud or a partner
Support for industry standards	•Support for industry standards, SAML, WS-Federation
Support for OpenID 2.0	•Relying party and OpenID provider •OOTB RP / OP configurations (Yahoo, Google, & Facebook)
Secure Attribute Exchange	•API for the applications to "push" attributes to and from OIF

Scalability and High Availability

Key Feature	Benefit
Proven Deployments for Multi-million User Populations	•Supports environments with multi-million user populations
Clustering	•Solution is deployable in a clustered environment
Load Balancing	•Each server side component of the solution can be load balanced. Load balancing options include hardware-based and native
Dynamic Failover	•Each server side component of the solution can be setup for failover

Auditing and Logging

Key Feature	Benefit
Reporting, audit and compliance	•Provides both the framework and tools necessary to track, report and verify all of the significant events
Reports generated from local audit data	•Locally stores audit data so that reports do not require frequent target resource accesses
Data archiving tools	•Provides automated tools for managing high volumes of audit data and archiving data into an archiving database
Suite integrated reporting	•Single console integrates audit reporting across the entire identity and access management suite

Secure Web Services

Key Feature	Benefit
Standards based Security solution	•OOTB support for security solution that issues, validates, or exchanges security tokens and acts as a trusted authority that an enterprise web services infrastructure may use to enforce appropriate security token policies across web services providers and consumers
WS-Trust Token service	•Facilitate secure identity propagation and token exchange between Web Services
Standard Security Token support	•Username, X.509, Kerberos SAML 1.1/2.0 supported
Enterprise scalability	•Deployable as a war on Weblogic or Glassfish J2EE containers •Provides WS-Trust protocol based clients to access STS •Leverages OWSM as the provider for WS-Security and WS-Policy

Centralized Application Security and Authorization

Key Feature	Benefit
Enhanced Security and Compliance	•Manage security from a single place •Provides finer control over the protection of all resources •Separates security decisions from application logic •Offers robust auditing of events
Support industry protocols and standards	•Supports XACML, ABAC, RBAC, ERBAC, ACL's, LBAC, Advanced Data Security
Centralized Policy Management	•Centralized administration through the OES Admin Server console •Common policy model/store for all target systems
High Scalability & Flexibility	•Allows for highly distributed environments where policy decisions and enforcement happen far away from the actual policy management •Provide customer with a range of deployment options
Custom and packaged application support	•OES can support custom J2EE applications, but can also support-packaged applications like SharePoint
Dynamic policy changes	•OES can dynamically change policies at runtime without disrupting applications. The ability to immediately effect running applications without any scheduled down time or maintenance helps lower IT costs

Conclusion

Oracle's Access Management Suite Plus is the most comprehensive suite of Access Management solutions in the market today. It is the only solution that protects access from the end-point to the cloud and provides with a complete set of products that include:

- **Oracle Access Manager**
- **Oracle Adaptive Access Manager**
- **Oracle Entitlements Server**
- **Oracle Identity Federation**,
- **Oracle OpenSSO Fedlet,**
- **Oracle Enterprise Single Sign-On,**
- **Oracle Web Services Manager**,
- **Oracle Security Token Service**

This comprehensive set of solutions engineered to work together on the cutting edge hardware platforms from Oracle and Sun provide value for customers. Value is critical in your software and hardware platform to free up critical resources to solve the tough business problems such as end-to-end security, performance for cloud and extranet, active compliance, risk mitigation, and collaborate and protect data at it's source.

Buyer's Guide for Access Management

Feb 2012

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

0109