ORACLE FUSION MIDDLEWARE 11g
ACCESS MANAGEMENT SUITE

An Oracle White Paper
May 2011

Oracle Adaptive Access Manager 11g Architecture & Technical Specifications

ORACLE

Executive Overview

Businesses, institutions and end users face the constantly growing threat of fraud and abuse. Failure to comply with industry security regulations can severely hurt the bottom line and even land people in jail. As well, deploying an incomplete security solution can be very costly in the long term. Security professionals need a strong, adaptable and cost effective solution to meet their current needs and be able to scale to meet their future needs without breaking the bank. Oracle Adaptive Access Manager provides powerful, unique, transparent and flexible protection for organizations and their users through its core capabilities and deep integrations with the Oracle Identity and Access Management suite. This white paper describes in detail the features and benefits Oracle Adaptive Access Manager provides customers.

Introduction

Users and organizations lose when fraud occurs. Increasing sophistication, speed of fraud attacks and expanding regulations require a new type of security solution with capabilities beyond narrow and outdated single layer, static and reactive methods. Such a solution must take a holistic view of each individual application, event, transaction, user and access request in real-time. It is no longer enough to simply authenticate users with a “strong” credential or passively detect fraud and abuse; fraud and abuse must be prevented before they can occur. An effective access management solution must quickly evaluate risk and confirm identities by validating multiple types of data, all with no need for human intervention. Oracle Adaptive Access Manager captures profiles and processes the full context of an access request to determine the level of risk, which, in turn, automatically determines what if any actions the system must take to prevent an incident or reduce the associated risk. The ever changing variety of fraud attacks and corporate misuse requires a solution to have varied areas of functionality and flexibility to adapt to evolving threats quickly. Threats such as social engineering, phishing, malware, trojans, viruses, session hijacking, man-in-the-middle, man-in-the-browser and many others must be prevented and mitigated if a solution is to have real value. As well, insider fraud such as role abuse and fraudulent impersonation must be preventable. Oracle Adaptive Access Manager includes functionality to protect the entry and transmission of static authentication credentials, fingerprint all types of devices used, profile user behavior, assess situational risk in real-time, challenge or block users based on the current level of risk as well as full audit, reporting and investigation capabilities.

With the increasing sophistication of fraudsters and regulatory oversight, organizations need a next generation access management solution. To be effective an access management solution must look beyond authentication credentials and user roles to indicators that can be evaluated to determine the level of risk and take proactive actions to prevent fraud and abuse.

Mark Karlstrand, Senior Manager, Product Management, Oracle Identity And Access Management

Moving Beyond Traditional Authentication

Traditional authentication processes have many weaknesses:

- In the traditional single layer model, "strong" credential-based authentication is a single point of failure. If and when the authentication method being used is broken there are no second lines of defense.
- Insider fraud and abuse are not prevented by "strong" authentication alone since the individual committing fraud is either the valid user the enterprise provisioned the credential to or someone close to them.
- Even multi-factor authentication alone cannot prevent fraud from occurring. For example, session hijacking happens after primary authentication is successful.
- It is not uncommon to transmit users' credentials in clear text. Moving raw data over open channels increases the likelihood of credential theft.
- Even with SSL in place, the credential data remains unencrypted from the moment a user enters it until the encryption process gets invoked. When the user's device/browser is compromised, SSL becomes useless.
- No matter how much security is in place, organizations can't fully control the end user's computer. Every day, consumer and business applications are being accessed from thousands of devices compromised by key-loggers and other types of malware.
- Requiring users to re-authenticate in-session when there is little risk impacts employee productivity and infuriates customers. As well, sophisticated attacks can pass on the challenge to the valid user and dupe them into entering the credential.

Oracle Adaptive Access Manager was designed with the goal of overcoming these limitations and to enable strong protection for the enterprise and its employees/partners/contractors/customers, even if users are accessing from a compromised environment, the primary authentication credentials have been compromised or there is mal intent by insiders.

Flexibility

Oracle Adaptive Access Manager was architected from the beginning as a platform rather than a point solution. The Oracle Adaptive Access Manager (OAAM) design philosophy offers a unique set of flexible capabilities to customers and partners. Customers have the choice to use the complete out of the box solution provided or develop a fully custom solution harnessing OAAM or a hybrid of the two. A highly configurable risk engine, customizable reporting, both synchronous and asynchronous deployment options, powerful configurable actions to enable rich extensibility without any core product change, as well as a shared libraries infrastructure and challenge processor framework allows almost unlimited deployment possibilities. Furthermore, the highly configurable transaction monitoring, behavioral profiling, risk evaluation and other policy management tasks are all exposed in an intuitive GUI for easy access by business users. Underpinning all the comprehensive capabilities of OAAM is the strength and stability of the Oracle infrastructure and services. Oracle Adaptive Access Manager utilizes Fusion Middleware infrastructure components, so installation, configuration, patching, upgrades, diagnostics, management, audit, logging, reporting, user security and UI frameworks are all shared in common with the rest of Oracle Identity and Access Management products. In other words, OAAM is a truly enterprise grade product complete and open enough to meet the needs of any organization.

Oracle's strategy with OAAM is to provide base policies and rules to meet the access security requirements of any application in any vertical for any type of user base. From this solid base the auto-learning capabilities automatically adjust the risk analysis based on training data before deploying into production, as well as ongoing automated learning once in production. Additionally, each customer deployment has the ability to develop specific models, patterns, policies and rules based on the unique security needs of the specific applications and user groups. This configuration is either performed by customers using standard Oracle product documentation, by expert professional services, or a combination of the two. In this way Oracle provides a flexible and effective fraud prevention solution that can meet the needs of any business regardless of industry or market. Based on our competitive intelligence, this is a very complete and preferable option for many customers. Additionally, Oracle has a number of industry focused business units who can provide vertical specific packages on top of the base OAAM package to meet very specialized customer requirements.

Cost-Effective Online Threat Protection

Oracle Adaptive Access Manager offers many diverse benefits with an exceptionally low cost of ownership. OAAM provides a rich set of capabilities including device fingerprinting, real-time behavioral profiling and risk analytics. It also provides risk-based authentication methods including Knowledge Based Authentication challenge infrastructure with Answer Logic and OTP Anywhere server-generated one time passwords, delivered out of band via SMS, email, IM or voice channels. All of these capabilities are provided in a single license. Also, all of this includes out of the box integrations with the industries top identity management and web single sign on products which are in turn, integrated with the world's top enterprise applications. The value is especially striking when considering the collection of point products and integration effort that would be required to furnish

similar functionality with competitive products. Add to all this the fact that independent analysts IDC found that on average OAAM customers they interviewed realized 100% ROI in a single year of deployment.

With Oracle Adaptive Access Manager, corporations can defend themselves and their end users against the most potent fraudulent attacks in a cost-effective manner.

THREAT	OAAM DEFENSE
Phishing	• A phishing site cannot easily replicate the user experience of the virtual devices (TextPad, QuestionPad, KeyPad, PinPad). As such, users will be tipped off and most likely not enter their password or PIN code. • The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server. If the shared secret is not presented or presented incorrectly, users can be tipped off. • The “freshness” time-stamp displayed in the virtual devices shows an end user that it was created right then for their use. This makes re-presenting old virtual devices on a phishing site suspect to an end user. • If a phishing exercise is successful in stealing a user's login credentials, real-time risk analytics, behavioral profiling and risk-based challenge make using stolen credentials very difficult since the fraudster will almost certainly not have exactly the same behavior as the valid user and therefore would be challenged or blocked by OAAM.
Malware	• The Virtual Authentication Devices combat key-loggers and many other forms of malware that attempt to steal a user’s authentication credentials. • The KeyPad and PinPad allow a user to send a random string of numbers instead of their actual credential. As a result no sensitive data is captured or sent to the server, so it is not easily compromised by automated means. • The same technology can be used to protect any sensitive data point. For example, a user’s Social Security Number could be safely communicated to a server by entering it using the Virtual Devices.
Transaction Fraud	• Oracle Adaptive Access Manager performs both real-time and batch-based risk analysis on session, transaction, event and contextual data. • Possible outcomes of these evaluations include alerts, blocking, risk-based challenge or custom integration actions to affect other systems. • Virtual Devices can be implemented to prevent automated navigation of transaction interfaces and data altering by malware programmed to hijack user sessions post login. For example, if a PinPad is used to enter the destination account number of a transaction, malware cannot easily navigate this process and the random data entered and sent is not the actual account number so it cannot be altered for fraud.
Insider Fraud	• Oracle Adaptive Access Manager profiles user behavior and assesses the risk associated with an access request in real-time. If an employee/partner/contractor exhibits anomalous behavior, alerts can be

generated for security and compliance analysts to review.

- Risk-based KBA or OTP challenge can thwart fraudulent impersonation.

OAAM Risk Engine

Auto-Learning

Oracle Adaptive Access Manager employs a unique mixture of real-time and predictive auto-learning technology to profile behavior and detect anomalies in real-time. Because of this OAAM can truly spot high risk and proactively take actions to prevent fraud and abuse. As well, since OAAM is evaluating and learning behaviors in real-time it is constantly learning what is "normal" for each individual user and for users as a whole. In addition to the fully automated learning, the continuous feedback from experienced fraud and compliance investigators "teaches" the OAAM engine what fraud/abuse does and does not look like. In this way, OAAM fully harnesses both the human talent in your organization and multiple forms of machine learning to prevent fraud and abuse.

A simple example would be the behavioral profiling and evaluation of access times for a nurse. If the nurse works in a hospital they may work different shifts on occasion to fill in but they will most likely work one shift more than the others in any given month. As such OAAM will keep track of when they are at work accessing the medical records system. If this month they have been working mostly PM shifts and some graveyards to fill in, then, seeing an access request from them between 10:00 am and 12:00 pm would be an anomaly. This of course does not mean fraud or abuse is occurring but the risk is elevated, so asking a challenge question would help confirm it's really the nurse. As they make more access requests during the day shift OAAM quickly learns in real-time that this is normal for them. This, however, is a simplistic example of one data point in isolation, when, in reality OAAM is learning and cross referencing large numbers of data points for each request and evaluating them for anomalies.

One of the main goals of automated anti-fraud solutions is to do away with unnecessary manual processes and remove much of the inconsistency and costs that can occur when humans are directly involved in evaluations. Oracle Adaptive Access Manager automates not only risk evaluations but as well keeps track of changing behaviors so humans don't have to. Based on this dynamic risk evaluation, proactive action is taken to prevent fraud with various forms of interdiction including blocking and challenge mechanisms. In this way, OAAM prevents fraud with little or no need for human interaction. However, in instances when human investigators are needed to follow up directly with end users or make final decisions based on additional contextual information, OAAM seamlessly captures their insights to improve the accuracy of future risk evaluations.

Configurable Risk Engine

Configurable Rules	Does a device appear to be traveling faster than a jet speed between logins?
Behavioral Profiling	Has Joe used this device less than 3% of the time in the last month?
Predictive Risk Analysis	Is the probability an access request would look like this less than 20%?

The Oracle Adaptive Access Manager risk engine utilizes a flexible architecture based on highly configurable components. OAAM employs three methods of risk evaluation that work in harmony to evaluate risk in real-time. The powerful combination of highly configurable rules, behavioral profiling and predictive analysis make OAAM unique in the industry. Administrators can easily create, edit and delete security policies and related objects directly in the intuitive administration console. Non-technical business users can understand and administer OAAM policies and view dashboards and reports in the graphical user interface with little or no dependence on IT resources. Security rules are easily created by combining configurable rule conditions. Both access and transaction based rules are created from the library of conditions included out of the box. As well, OAAM profiles behavior and evaluates risk using a fully transparent and auditable rules based process. This allows high performance, flexibility and complete visibility into how and why specific actions were or were not taken during a session. This is in stark contrast to opaque "black box" solutions that do not provide clear visibility into the exact cause of outcomes. If OAAM blocks access for an end user there is a complete audit trail that clearly shows exactly why. In addition to transparent, self-sufficient and flexible functionality within the product, OAAM customers also benefit from enthusiastic, innovative product development teams, 24/7 global support and an active user community.

Universal Risk Snapshot

Change control is very important in an enterprise deployment, especially concerning mission critical security components. The Universal Risk Snapshot feature allows an administrator in a single operation to save off a full copy of all Oracle Adaptive Access policies, dependent components and configurations for backup, disaster recovery and migration. Snapshots can be saved to the database for fast recovery or to a file for migration between environments and external backup. Restoring a snapshot is an automated process that includes visibility into exactly what the delta is and what actions will be taken to resolve conflicts.

Device Fingerprinting

Oracle Adaptive Access Manager contains both proprietary clientless technologies and an extensible client integration framework for fingerprinting devices used during access requests and transactions. Device usage is tracked and profiled to detect elevated levels of risk. OAAM customers can secure both standard and mobile browser based access without additional client software or choose to integrate a custom developed client such as a JAVA applet for additional functionality if desired. For access requests to a web application via a native mobile application customers and partners can easily integrate OAAM device fingerprinting capabilities via the client integration framework. OAAM generates a unique single-use fingerprint mapped to a unique device ID for each user session. It is replaced upon each subsequent fingerprinting process with another unique fingerprint. The fingerprinting process can be run any number of times during a user's session to allow detection of changes mid-session that can indicate session hijacking. OAAM monitors a comprehensive list of device attributes. If any attributes are not available the device can still be fingerprinted. The single-use capabilities combined with multiple attributes evaluated by server-side logic and custom client extensibility make the OAAM device fingerprinting flexible, easy to deploy and secure.

Virtual Authentication Devices

Oracle Adaptive Access Manager includes unique functionality to protect end users while interacting with a protected web application via a browser. The Virtual Authentication Devices strengthen the process of entering and transmitting authentication credentials and provides end users with verification they are authenticating to the valid application. This is accomplished without any proprietary client-side software or hardware required. Only standard web technologies including HTML and simple JavaScript are used. This is because all logic is on the server, not on the client where it is vulnerable to exploitation.

TextPad fig.1

Figure one shows TextPad which is a personalized virtual authentication device for entering a password using keyboard entry. This method of data entry helps to defend against phishing primarily. TextPad is often chosen as the default Virtual Authentication Device for all users in a large deployment then each user individually can upgrade to another device if they wish. The personal image and phrase a user registers and sees every time they login to the valid site serves as a shared secret between user and server. If the shared secret is not presented or is presented incorrectly users will be warned of a possible phishing attack.

PinPad & KeyPad fig. 2

PinPad and KeyPad are indirect authentication credential entry virtual devices. They can be invoked at the time of login or in-session if required. A user navigates using their mouse to click on the visual "keys". In reality the data entered is a string of random numbers that only the OAAM server can decode into the valid password/PIN/data. A configurable number of randomization mechanisms control the balance of usability with the level of strength. The PinPad and KeyPad are generally given as an optional upgrade users can choose to use or not. This flow ensures only users who really want the extra protection utilize it since there is a slight learning curve related to navigation.

QuestionPad fig. 3

QuestionPad is a specialized device used to present KBA challenge questions to an end user. The question text is protected from screen scrapers since it is actually contained in the image file rather than HTML text.

KBA Answer Logic

Oracle Adaptive Access Manager includes a highly user friendly challenge method called Knowledge Based Authentication (KBA). What makes KBA superior to other registered challenge question solutions is the usability provided by KBA Answer Logic. Administrators can easily configure the exact end user experience they require including individual question creation/editing, how many questions users register for, the variety of questions they can choose from and specific validations to be applied to the answers they give. Also, with KBA Answer Logic administrators adjust how exact the challenge answers given by end users must match the answers they gave at the time of registration. If the answer given by a user is fundamentally correct but there are minor variations such as typos, misspellings and abbreviations they should pass. Answer Logic dramatically increases the usability of KBA which reduces or eliminates the need for unnecessary call center involvement in moderate risk situations and self service flows. KBA Answer Logic is a collection of multiple techniques detailed here.

Common Abbreviations & Nicknames

This algorithm matches the words in the following pairs as equivalent. OAAM ships with a predefined list of word-pairs that cover common abbreviations, common nicknames and common acronyms. The list can be updated by customers as required.

- Street - St.

- Drive - Dr.
- California - CA
- Timothy - Tim
- Matthew - Matt

Date Format

When users answer a date related challenge question sometimes they use a different date format than they did when they registered the question. Answer Logic can translate from one format to another to allow variation in fundamentally correct answers. For example, the following would be seen as the same answer:

- 0713
- 713
- July 13th
- July 13

Common Misspellings

Phonetic Answer Logic can account for minor misspellings and regional spellings.

- elephant – elefant
- color – colour

Keyboard Fat Fingering

Fat Fingering Answer Logic accounts for typos due to the proximity of keys on a standard keyboard and transposed letters. The following are some common typos.

- Switching "w" and "e"
- Switching "u" and "i"
- Switching "t" and "r"
- Correct word: signature > Fat finger: signatire

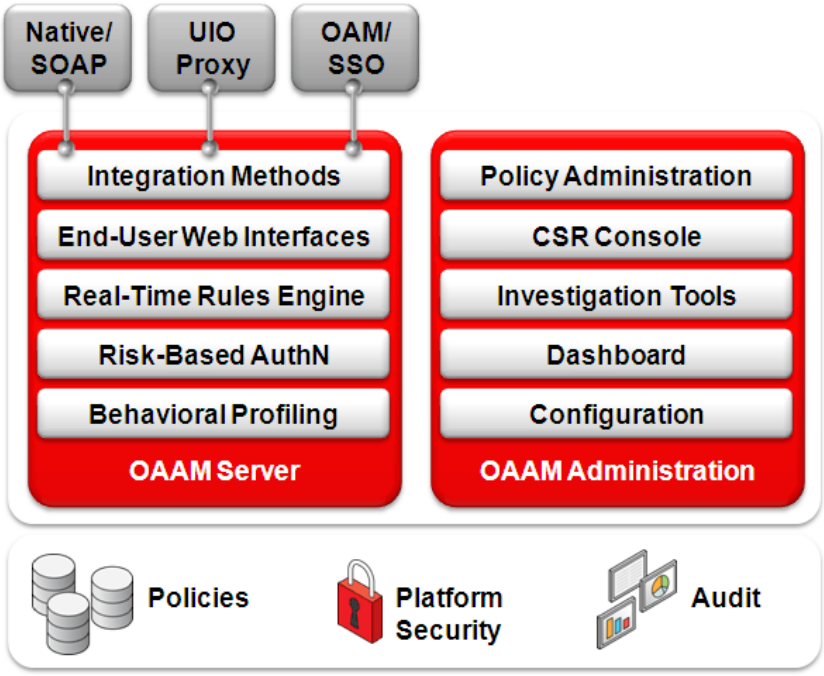
OTP Anywhere

OTP Anywhere is a cost effective, risk-based challenge mechanism consisting of a server generated one time use password delivered to an end user via a configured out of band channel. Supported OTP delivery channels include short message service (SMS), eMail, instant messaging and voice. OTP Anywhere can be used to compliment Knowledge Based Authentication (KBA) challenge or instead of KBA. As well, both OTP Anywhere and KBA can be used based on risk alongside practically any other authentication mechanism required in a deployment. Oracle Adaptive Access Manager provides

an innovative challenge processor framework. This framework can be used to implement custom risk-based challenge solutions combining third party authentication products or services with OAAM real-time risk evaluations. Both KBA and OTP Anywhere actually utilize this same challenge processor framework internally. OTP Anywhere via the SMS channel particularly provides a lot of security value at a relatively low cost. By using a person's cell phone as a form of second factor, the identity assurance level is elevated without the need for provisioning hardware or software to end users. A user only needs a cell phone capable of receiving an SMS. This makes deployment and ongoing costs very low for OTP Anywhere.

Oracle Adaptive Access Manager Architecture

Oracle Adaptive Access Manager is architected to provide a rich selection of capabilities with heterogeneous support for a variety of environments. Functionality is implemented to optimize resources and provide enterprise class scalability and redundancy.



Oracle Adaptive Access Manager 11g Architecture fig. 4

High Availability

Oracle Adaptive Access Manager 11g is architected to ensure dependable uptime performance in demanding deployments. The runtime components including the rules engine and end user interface flows are contained in one logical server while the administration console functionality is separated out into its own managed server. In addition to rule and policy administration, the administration console contains the customer service and security analyst case management functionality which must always be available to employees in potentially large call centers with high call volumes. The two logical

servers do not communicate with one another. Depending on the deployment method used the topology changes slightly. Native application integration deployments embed the runtime components so the administration console is the only additional logical server added to the deployment. Oracle Adaptive Access Manager 11g is also completely stateless and fully supports clustered deployments to meet high performance requirements. As well, all high availability features of the Oracle database are supported for use with Oracle Adaptive Access Manager.

Deployment Options

Oracle Adaptive Access Manager supports a number of deployment options to meet the specific needs of practically any deployment. The decision of which deployment type to employ is usually determined based on the use cases required and the applications being protected. In some deployments a hybrid of deployment options is employed as required.

Single Sign-On Integration

Oracle Adaptive Access Manager has an out of the box integration with Oracle Access Manager 10g and 11g to provide advanced login security including the virtual devices, device fingerprinting, real-time risk analysis and risk-based challenge. New to 11g there are two versions of the OAAM + OAM integration, basic and advanced. The "basic" integration embeds the OAAM engine into the OAM 11g runtime server. It includes many of the login security use cases available from OAAM and reduces the deployment footprint. To gain advanced features and extensibility customers can deploy using the "advanced" integration. Features such as OTP Anywhere, challenge processor framework, shared library framework and secure self-service password management flows require the advanced integration option. Oracle Adaptive Access Manager can also be quickly integrated with third party single sign-on products via systems integrators.

Universal Installation Option Reverse Proxy

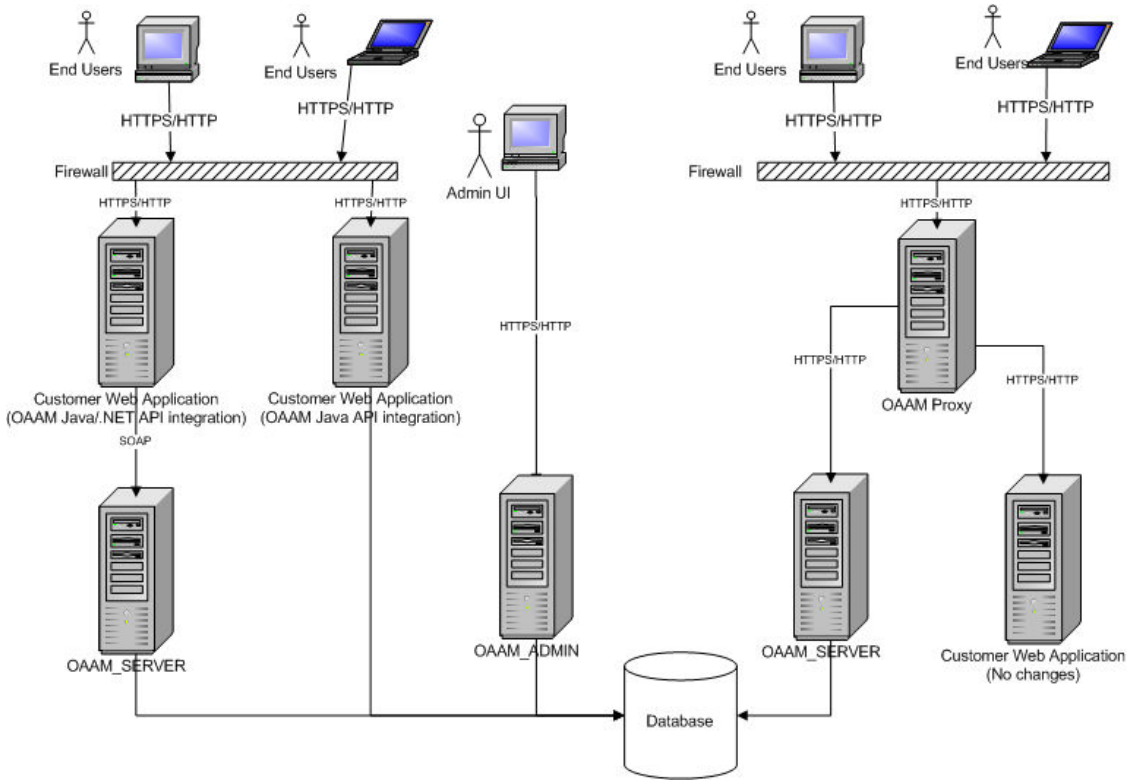
Oracle Adaptive Access Manager can be deployed using an Apache module to intercept login requests and provide advanced login security when an SSO solution is not in place. The flows available are the same as the advanced single sign-on integration option described above. The main benefit of the UIO proxy deployment is that it's "zero-touch", which means there is no need to modify the protected applications.

Native Application Integration

Oracle Adaptive Access Manager can be integrated with an application via .Net or native JAVA APIs to provide extreme high performance and highly customizable security. A native integration embeds OAAM in-process within the protected applications. Advanced transactional risk analysis requires this form of deployment. Additionally this method can be combined with an SSO or UIO Proxy integration to accomplish a hybrid style deployment.

Web Services Application Integration

Customers who have advanced requirements similar to native integration but who prefer to use SOAP web services instead of Java API integration directly can choose this option. A SOAP wrapper over the JAVA APIs allows easy integration and a lot of flexibility.



Oracle Adaptive Access Manager 11g Deployment Options fig. 5

CONCLUSION

Oracle Adaptive Access Manager offers the unique and powerful advantages that you expect of the next generation of risk-based access management. The unique combination of truly real-time anti-fraud capabilities found in Oracle Adaptive Access Manager and the completeness of the Oracle Identity and Access Management suite enable customers to present a proactive security posture with a cost effective and standards based end to end solution. The ease of implementation, flexibility, transparency and breadth of capabilities helps provide excellent return on investment. Finally, the vision and support provided by Oracle ensures that customers can be assured ofthe longevity and stability of the security solution they choose

Oracle Apaptive Access Manager 11g
Architecture and Technical Specifications
May 2011
Author: Mark Karlstrand

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

SOFTWARE. HARDWARE. COMPLETE.