ORACLE

FUSION MIDDLEWARE

ACCESS MANAGEMENT

An Oracle White Paper

January 2014

Oracle Adaptive Access Manager 11g

ORACLE

Overview

Fraud and misuse of resources can have far reaching consequences to organizations and individuals, including financial loss, damaged reputations and even severe penalties for executives.

Traditional access management technologies are struggling to identify and react to the ever increasing sophistication of external attacks, let alone insider misuse of corporate resources – deliberate or accidental.

A different approach to access management is required, one that assesses risk in real-time and adapts its capabilities based on various factors, including method of access, behavioral patterns and level of confidentiality. Furthermore, this new level of fraud prevention, risk analysis and adaptability must be standard across all access management touch points.

Oracle Adaptive Access Manager (OAAM) is this new approach to access management. It provides powerful, unique fraud prevention capabilities and is a key component of Oracle Access Management Suite Plus, delivering risk-aware, context-driven access management across the industry's most complete set of access management services.

This white paper describes the features and benefits of Oracle Adaptive Access Manager.

Business Challenges

Given the current threat environment, securing applications and services is a daunting task for any enterprise. Fraud is on the increase, stolen credentials continue to be a major vulnerability and the use of mobile technology is further complicating the situation.

Fraud is increasing

Many constantly changing factors contribute to the proliferation of electronic fraud and misuse. The depressed global economy, easy access to hacking technology, growing richness of targets and more recently online activism are all contributing factors. The 2012 Verizon Data Breach Investigation Report found 855 incidents involving 174 million compromised records in 2011 which was up from 4 million compromised records in 2010[(1)]. It is likely that this dramatic 4,350% increase represents only a portion of the total number of attacks attempted in 2011, when accounting for undetected and unsuccessful attacks.

Stolen Credentials are a major vulnerability

According to the 2012 Verizon Data Breach Investigation Report, among large organizations 30% of the breaches that accounted for 84% of stolen records was a result of stolen login credentials[(2).]

Historically the reaction of many security professionals to this broad threat has been to adopt stronger credentials such as hardware tokens or enforce stricter password policies that require complex password formatting and frequent changes. Unfortunately, these practices make it more difficult for users to keep track of passwords, often resulting in some form of easily compromised written record of the password that negates the stricter password policies.

Risks of Mobile Access

According to a market study conducted by Canalys in 2011, smart phone sales grew 63% overtaking personal computer sales for the first time in history [(3)]. Unfortunately, security is often a lower priority than quick time-to-market when it comes to mobile application development and existing security infrastructures are not geared to handle these new devices, which is a major concern as more confidential data is exposed via mobile devices.

Security and Compliance

Global compliance mandates are evolving alongside security requirements. Healthcare is a good example of an industry being pushed to adopt truly modern access controls and access monitoring. In the United States, HIPAA/HITECH requires more than the ability to run audit reports when there is an incident. Healthcare providers must have the ability to actively monitor access to electronic medical records and report on any misuse. In addition, these new compliance mandates have real penalties for breach incidents, including public disclosure, fines and possible incarceration.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) addresses these business challenges in a cost-effective and scalable manner.

OAAM provides an extensive set of capabilities including device fingerprinting, real-time behavioral profiling and risk analytics that can be harnessed across both Web and mobile channels. It also provides risk-based authentication methods including Knowledge Based Authentication (KBA) challenge infrastructure with Answer Logic and OTP Anywhere server-generated one-time passwords, delivered out of band via SMS, email or IM channels. OAAM also provides out-of-the-box integration with Oracle Identity Management, the industry leading identity management and Web SSO products, which are integrated with leading enterprise applications. Independent analyst firm IDC found that on average OAAM customers interviewed realized 100% ROI in the first year of deployment [(4)].

With OAAM, corporations can protect themselves and their online users against potent fraudulent attacks, such as Phishing, Malware, Transaction and Insider Fraud, in a cost-effective manner. The following table summarizes the threat and OAAM defense mechanisms, which are further detailed in later sections.

THREAT	OAAM DEFENSE
Phishing	• A phishing site cannot easily replicate the user experience of the OAAM 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 a 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 OAAM virtual devices shows an end user that it was created for this session. 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 send a random string of numbers over the wire that only OAAM can decode. 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 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

The OAAM risk engine provides multiple forms of risk evaluation logic. Working together the different capabilities of the risk engine combine to form a powerful tool to combat fraud.

Auto-Learning

OAAM employs a unique mixture of real-time and predictive auto-learning technology to profile behavior and detect anomalies. Because of this, OAAM can spot high risk activity and proactively take actions to prevent fraud and misuse. Also, as OAAM is evaluating and learning behaviors in real-time it constantly learns what is "normal" for each individual user and for users as a whole. In addition to the auto-learning, the continuous feedback from experienced fraud and compliance investigators "teaches" the OAAM engine what constitutes fraud and misuse. In this way, OAAM fully harnesses both the human talent in your organization and multiple forms of machine learning to prevent fraud and misuse.

A simple example would be the behavioral profiling and evaluation of access times for a nurse. Nurses often work in a couple hospitals; they may work different shifts on a rotating schedule, but they will most likely work one shift more than the others in any given month. In such a scenario, OAAM keeps track of when a nurse is at work accessing the medical records system. If during the same month a nurse has been working mostly PM shifts and some graveyards to fill in, then, seeing an access request from her between 10:00 am and 12:00 pm would be an anomaly. This of course does not mean fraud or misuse is occurring, but the risk is elevated, so OAAM could challenge the nurse for additional identity verification. As the nurse accesses various applications and information during the day shift, OAAM learns in real-time that this is normal and is therefore low risk.

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 access evaluations. Oracle Adaptive Access Manager automates not only risk evaluations but also keeps track of changing behaviors so humans don't have to. Based on this dynamic risk evaluation, proactive action can be 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

The OAAM 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 combination of configurable rules, real-time 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 business user friendly

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 any number of configurable rule conditions. Both access and transaction based rules are created from the library of conditions included out-of-the-box.

OAAM also 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 don’t 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 what data was evaluated and the specific evaluations that occurred.

Mobile Access Security

OAAM provides mobile security features both directly and via the Mobile and Social Access Services component of Oracle Access Management using the ASDK and RESTful web services. Users accessing OAAM protected web applications through a mobile browser will navigate UI and flows optimized for the mobile form factor without doing any development. OAAM also provides out-of-the-box security policies that dynamically adjust when user access originates from a mobile device.

This improves the range of analysis and accuracy of the risk evaluation, which reduces false positives. For example, IP geolocation velocity rules behave differently if the access request is via a cell connection than it does when using a WIFI connection.

When customers utilize the Mobile and Social (MS) Access Services component of the Oracle Access Suite, OAAM provides enhanced device fingerprinting, device registration, mobile specific risk analysis, risk-based challenge mechanisms as well as lost and stolen device management. Mobile Access Services allow enterprises to extend their existing access security solution to cover both the web and mobile access channels. This saves money and doesn’t introduce brittle and siloed point solutions.

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 a full copy of all OAAM 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

OAAM provides both proprietary, clientless technologies and an extensible client integration framework for device fingerprinting. Device usage is tracked and profiled to detect elevated levels of risk. OAAM customers can secure both standard browser-based access and mobile browser-based access without additional client software or choose to integrate a custom developed client such as a JAVA applet. For securing access to mobile applications, customers and partners can easily integrate OAAM device fingerprinting capabilities via the Mobile and Social SDK and REST interface. OAAM generates a unique single-use cookie value mapped to a unique device ID for each user session. The device cookie value is refreshed on each subsequent fingerprinting process with another unique value. The fingerprinting process can be run multiple times during a user's session to allow detection of mid-session changes that could indicate session hijacking. OAAM monitors a comprehensive list of device attributes. The single-use cookie and multiple attribute evaluations performed by server-side logic and client extensions make OAAM device fingerprinting flexible, easy to deploy and secure.

Virtual Authentication Devices

OAAM 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 and all logic is on the OAAM server, not on the client where it is vulnerable to exploitation.

Figure 1: TextPad Virtual Authentication Device

Figure 1 shows TextPad, 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.

Figure 2: PinPad & KeyPad Virtual Authentication Devices

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.” On the wire, 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 required 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.

Figure 3: QuestionPad Virtual Authentication Devices

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

OAAM includes a 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

Answer Logic 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: signature

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 and instant messaging. 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 SMS 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.

Fraud Investigation Tools

Oracle Adaptive Access Manager provides a streamlined and powerful forensic interface for security analysts and compliance officers. Users can easily evaluate alerts and identify related access requests and transactions to uncover fraud and misuse.

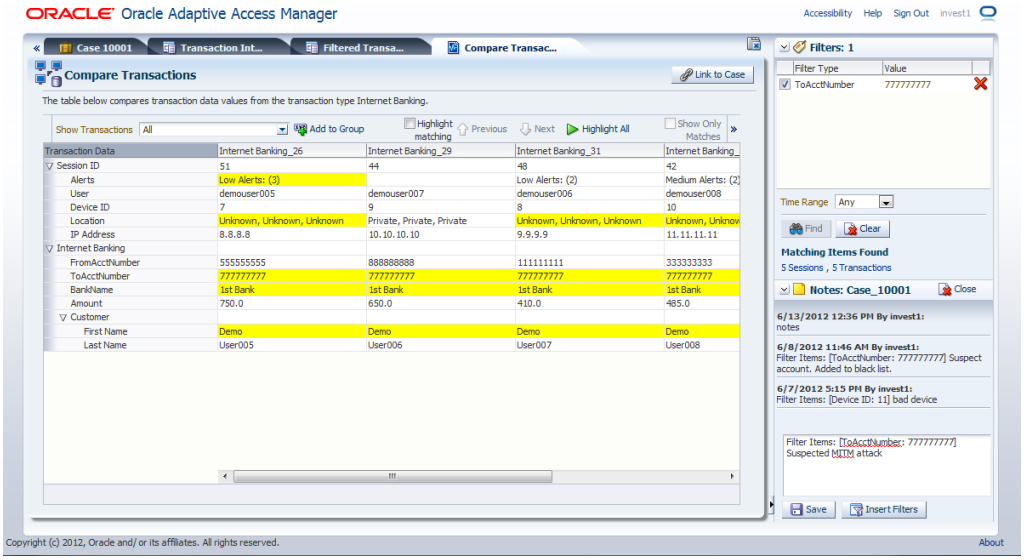

Figure 4: Investigation Interface

Agent Cases

OAAM provides case management functionality tailored to forensic investigation. Agents are provided a repository for findings and investigation workflow management. Security analysts and compliance officers' record notes and link suspect sessions to a case as they perform an investigation so all findings are captured for use in legal proceedings and to influence future real-time risk analysis.

Search and Compare Transactions

OAAM provides an intuitive interface for security analysts and compliance officers to search and compare transactions that have been subjected to risk analysis. The full data and context of each transaction is available even for encrypted data fields. This allows security and compliance professionals deep visibility into user activity while still protecting the data from administrators or other types of enterprise users. The ability to compare multiple transactions side by side is extremely useful for expanding investigations from known high risk transactions to transactions that may not have initially appeared high risk on their own.

Utility Panel

The investigation utility panel provides a persistent interface for common operations security analysts and compliance officers perform multiple times in the process of an investigation. Both quick search and case notes are always available regardless of what other functionality is being used. This ensures that findings from any process can be combined to search for suspect sessions and transactions. Also, the utility panel ensures that any thoughts or findings can be captured in case notes.

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.

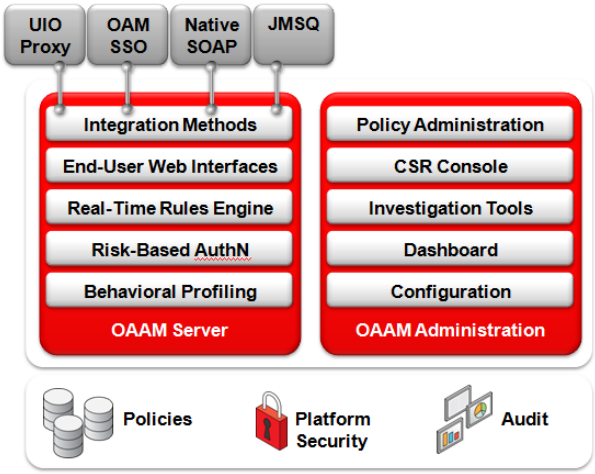

Figure 5: Oracle Adaptive Access Manager 11g Architecture

High Availability

Oracle Adaptive Access Manager 11g is architected to ensure dependable uptime and 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 investigation 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 but instead look to a shared database as the common source of truth. 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 and high availability requirements. Also, Oracle Adaptive Access Manager leverages the high availability features of Oracle's database technology.

Deployment Options

OAAM supports a number of deployment options to meet the specific needs of practically any enterprise. The decision of which deployment type to employ is usually determined by required use cases and the applications being protected. Some deployments may require a hybrid deployment approach, for example SSO integration for login flows and SOAP web service calls for transactional risk analysis.

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. Oracle Adaptive Access Manager can also be quickly integrated with third party single sign-on products by Systems Integrator partners.

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 isn't available. The flows are consistent with the 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 or deploy an SSO product.

Native Application Integration

Oracle Adaptive Access Manager can be integrated with an application via native JAVA APIs to provide extreme high performance and highly customizable security. Through native integration OAAM can be embedded 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 .Net and 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.

Java Message Service Queue Integration

Customers with access monitoring requirements involving multiple applications and data sources now have the ability to take a proactive security and compliance posture. Using the provided Java Message Service Queue (JMSQ) customers can implement near real-time risk analysis to actively identify suspected fraud or misuse.

CONCLUSION

Oracle Adaptive Access Manager is the perfect solution to help combat modern fraud and misuse. OAAM is a key component of Oracle Identity Management Complimenting the other suite capabilities. The unique combination of device fingerprinting, real-time behavioral profiling, risk analysis and risk-based identity verification capabilities allows enterprises to confidently expose applications and services on the Internet. The ability to apply these same capabilities across both web and mobile channels allows businesses to meet the needs of their users in a secure and sustainable fashion. With these extensive access controls and deep forensic visibility businesses can also exceed current compliance requirements and be prepared for future mandates.

Oracle Access Management as a whole enables 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 of solution longevity and stability.

Footnotes

1. Verizon RISK Team. 2012 Data Breach Investigations Report. Verizon, 2012, p. 1
2. Verizon RISK Team. 2012 Data Breach Investigations Report. Verizon, 2012, p. 26
3. Canalys. Press release 2012/021, Smart phones overtake client PCs in 2011. Canalys, February 3rd 2012, p. 1
4. Sally Hudson, Randy Perry. Adaptive Access Management: An ROI Study. IDC, September 2010, p.8

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

Oracle Apaptive Access Manager 11g
Architecture and Technical Specifications
January 2014
Author: Derick Leo
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

SOFTWARE. HARDWARE. COMPLETE.