Oracle Adaptive Access Manager makes exposing sensitive information, transactions and business processes to consumers, remote employees or partners via the internet, intranet and extranet safer. Cost effective real-time risk analytics, risk-based authentication, anti-phishing and anti-malware capabilities provide exceptional return on investment. A high degree of usability for end users, administrators and deployment engineers makes the solution both strong and operationally sound.

Introduction

Organizations that expose services and applications on the internet, intranet and extranet are concerned about security, and rightly so. Fraud and abuse can incur both direct and indirect costs for an enterprise. Fraud is not only a consumer facing problem anymore. Employee and partner accounts are being compromised and misused at the expense of the enterprise. Fraud and abuse is being conducted across multiple access channels using a large variety of methods. Also, the popular approach of deploying stronger forms of credential based authentication is not preventing fraud as new forms of threats break and circumvent these authentication mechanisms. Also, because of new and evolving regulations governing online data privacy, organizations are being required to quickly introduce reliable, cross channel access security solutions to ensure that fraudulent activities are detected and prevented.

Oracle Adaptive Access Manager provides an innovative, comprehensive feature set to help organizations prevent fraud and abuse. Strengthening standard authentication mechanisms, innovative risk-based challenge methods, multiple types of real-time risk analysis, intuitive policy administration and integration across both the Identity and Access Management Suite and third party products makes Oracle Adaptive Access Manager uniquely flexible and effective. Oracle Adaptive Access Manager provides real-time and batch risk analytics to combat fraud and abuse across multiple channels of access. Real-time evaluation of multiple data types helps stop fraud as it occurs which can save time, money and reputation.

Oracle Adaptive Access Manager provides a rich and adaptable set of deployment options including native application integration, reverse proxy interceptor and batch based as well as basic and advanced integration with Oracle Access Manager and Oracle Identity Manager. Through Oracle’s large partner network other options are available using third party products such as WAM and SSL VPN. The variety of available deployment methods, out of the box integrations and easy to administer security policies make enabling advanced security and ensuring regulatory compliance straightforward and cost effective.
Oracle Adaptive Access Manager provides a number of cost effective and rich features to strengthen existing web application login flows. Regardless of the type of authentication in place, Oracle Adaptive Access Manager can improve the level of both security in a usable manner. Insider fraud, session hijacking, stolen credentials and other threats cannot be eliminated by strong, credential based authentication alone. As in figure 1, adding a risk-based challenge layer behind existing authentication can greatly increase the level of security with minimal impact to the user experience – a critical factor for large deployments where help desk calls can dramatically impact the bottom line. Oracle Adaptive Access Manager’s suite of virtual authentication devices combats phishing personalized images and phrases known only to the server and the end user. Furthermore, through the use of virtual devices such as KeyPad and PinPad, security of the user’s credentials during entry can be assured by not capturing or transmitting the actual credential of the end user. This protects the credential from theft by malware and other similar threats. The virtual authentication devices are 100% server driven; all features are provided without any client-side software or logic that can be compromised by key-loggers and other common malware. Additionally, Oracle Adaptive Access Manager performs device fingerprinting and behavioral profiling on every access to determine the likelihood that the authentication is being attempted by the valid user.

Device Fingerprinting

One extremely valuable capability Oracle Adaptive Access Manager (OAAM) offers customers is the ability to independently identify devices and track their usage. A mixture of proprietary clientless technologies and an extensible custom client integration framework makes OAAM very flexible. Device usage is tracked to determine if there are any anomalies which may elevate the level 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 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, easy to deploy and secure.

Answer Logic

Answer Logic increases the usability of Knowledge Based Authentication (KBA) challenge questions by accepting answers that are fundamentally correct but may contain a small typo,
abbreviation or misspelling. For example, if abbreviation Answer Logic is enabled and a user is challenged with the question “What street did you live on in high school?” they may answer “1st St.” which is fundamentally correct even though when they registered the answer six months ago they entered “First Street”. By allowing a configurable variation in the form of correct answers, Answer Logic dramatically increases the usability of registered challenge questions making the balance between security and usability firmly in the control of the enterprise.

OTP Anywhere

OTP Anywhere allows end users to authenticate themselves by entering a server generated one-time-password (OTP) which they can receive via SMS, email, instant message or voice channels. When the OTP is sent via SMS, the user’s cell phone serves as a physical second factor that the user has in their possession. As well, the authentication is being sent out-of-band to increase the level of assurance that only the valid user has access to the one-time-password. When authentication methods such as Answer Logic and OTP Anywhere are applied based on the level of risk it can dramatically increase web application access security in an exceptionally cost-effective and usable manner.

Figure 2. Answer Logic Configuration

Self-Service Password Management

Giving end users the ability to securely create and reset their password without assistance dramatically reduces help desk costs and limits the impact on users’ productivity. However, if the flows are not user friendly there will still be high volumes of users calling the help desk. Exposing password management and other sensitive flows on intranet, extranet and internet sites requires advanced security measures to protect them from exploitation by criminals. As seen in figure two, security professionals can easily set the level of answer logic in the administration console user interface. The answer logic level controls how close the given answer string must match the answer string given at the time of question registration. Oracle Adaptive Access Manager 11g provides out of the box integrations with Oracle Identity Manager 11g and Oracle Access Manager 11g to provide real-time risk analytics and risk-based challenge mechanisms including KBA challenge questions and OTP Anywhere. These integrations dramatically strengthen the security of these self-service flows which not only increases usability but also reduces risk, making the solution valuable for any enterprise.

Risk Analytics

Oracle Adaptive Access Manager evaluates the level of risk for a specific situation by
analyzing event/transaction and contextual data from a variety of sources, including application data, user profiles, device fingerprints, IP addresses, geo-location, other network data and 3rd party data feeds. OAAM combines highly configurable rules, auto-learning patterns and predictive techniques to analyze risk in real-time. By looking at various risk factors simultaneously Oracle Adaptive Access Manager can determine the relative risk level, alert investigators and take steps to proactively prevent fraud using challenge methods and/or blocking. In addition, a detailed forensic trail of the analytics and actions taken is captured to allow thorough investigations and proper auditing compliance.

**Behavioral Profiling**

Oracle Adaptive Access Manager dynamically identifies high risk situations in part by learning what normal behavior is for users, devices, locations (IP address, city/state/country, etc) and entities (credit card, address, etc). Oracle Adaptive Access Manager evaluates an individual’s behavior against their own history and the history of all other individuals. This “auto-learning” is constantly being updated in real-time so changes in behavior are captured and ready for use in risk evaluations. As a result, Oracle Adaptive Access Manager is constantly adapting to the changing behaviors of users and user populations without the need for manual intervention.

**Predictive Risk Analytics**

Oracle Adaptive Access Manager integrates with Oracle Data Mining to provide statistical risk analysis in real-time. This form of risk analysis “trains” over time so it nicely compliments the highly configurable rules and behavioral profiling which do not require training. The more training each model does, the more accurate the risk analysis becomes. The out of the box predictive models are trained in two ways. The anomaly detection model trains automatically when fed historical access data. The fraud classification model trains on the findings of human fraud investigators. Additional models can be configured as required to meet specific deployment use cases. This open approach to predictive risk analysis allows OAAM customers to clearly see on which decisions outcomes are based and allows augmentation as required.

**Universal Risk Snapshot**

Oracle Adaptive Access Manager provides business user friendly administration interfaces to easily configure detailed and targeted security policies scoped to user groups, events, transactions and applications. The Universal Risk Snapshot is used to back-up, restore and migrate entire security configurations, including policies. This feature is very useful for rollbacks, disaster recovery and test to production migration. Making change control simple ensures smooth operation and eliminates any guesswork or mis-configuration between environments.

**Investigation and Forensics**

Oracle Adaptive Access Manager provides access to a rich set of forensic data to power investigations and auditing. Oracle Business Intelligence Publisher provides the reporting engine allowing reporting to be fully customized to meet requirements. Out of the box report templates are included that can be used as is or altered. The intuitive administration console interface makes it quick and easy to cut through the noise and narrow in on the important data and relationships. This allows a security analyst to better understand the relationships between various security events and as a result, find related situations that otherwise might not be identified. Furthermore, OAAM provides fraud case management tools to collect findings from fraud investigations and automatically feed them back into the risk analysis engine to tune rules and improve results. Oracle Adaptive Access Manager leverages the common audit framework from Oracle Platform Security Services to capture full audit trails for administration console users.
Conclusion

As companies aggressively embrace the extranet for sales, self-service, profile management, remote employee access and many other functions, online security is increasing in urgency. Consumers need to be well protected while using the web to access sensitive information and transactions via a plethora of devices and through a range of different channels. Furthermore, compliance rules are constantly changing and mandates exist to ensure that companies respond to the threats that this new way of interacting dictates. In addition, as organizations are aiming to enable online access for their partners and mobile employees, they are facing a strong need to better protect their extranet and intranet environments and to proactively manage risks associated with remote access to critical business applications. To address the growing security expectations for both consumer-facing and partner/employee-facing environments, Oracle Adaptive Access Manager 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.

Contact Us

For more information about Oracle Adaptive Access Manager visit www.oracle.com/identity or call +1.800.ORACLE1 to speak to an Oracle representative.