# Oracle Adaptive Access Manager

*An Oracle White Paper*
*Updated January 2008*

ORACLE

## EXECUTIVE OVERVIEW

Businesses, government agencies, and consumers all face the growing threat of internet fraud. Oracle Adaptive Access Manager provides superior protection for businesses and their customers through it core components.

Adaptive strong authenticator and adaptive risk manager are two primary components of Oracle Adaptive Access Manager. Together they create one of the most powerful weapons in the war against online fraud. This white paper describes these components and their functionality.

## INTRODUCTION

**With the increasing sophistication of fraudsters and regulations governing online data privacy, organizations need a robust security solution. Effective security solutions evaluate risk and confirm identities by validating multiple aspects of a user.**

Consumers and the enterprise lose when internet fraud occurs. With the increasing sophistication of fraudsters and regulations governing online data privacy, organizations need a robust security solution. Such a solution must ensure that online activities are legitimate.

Effective security solutions evaluate risk and confirm identities by validating multiple aspects of a user. They also take action against fraud in real time. Adaptive access systems can provide the highest levels of security with context-sensitive online authentication and authorization. Thus, situations are evaluated and proactively acted upon based on various types of data.

Oracle Adaptive Access Manager delivers the next generation of risk-based evaluation, enabling real-time blocking of fraudulent access requests. It also delivers advanced alerting mechanisms. The product protects your business and your customers from a full range of attacks. Such types of attacks can include phishing, Trojans, viruses, fraudulent transactions, and Man-in-the-Middle attacks.

Oracle Adaptive Access Manager includes two core components. Adaptive strong authenticator includes a suite of highly secure virtual authentication devices. Adaptive risk manager works in real time or offline to detect and prevent fraud.

## STRONG AUTHENTICATION SECURITY

Oracle Adaptive Access Manager uses industry standards for all security features. A range of independent security analysts and experts have scrutinized the product including the Computer Security Institute and Integral Business Solutions. This is an independent contractor for the U.S. Air Force that oversees security controls

and compliance with regulations and standards such as HIPAA; Gramm-Leach-Bliley Act; Sarbanes-Oxley Act; Peripheral Component Interconnect; ISO 1779; and the National Institute of Standards and Technology, or NIST.

Oracle Adaptive Access Manager relies on standards-based technologies that include supporting components certified by the U.S. Department of Defense in a Department of Defense Information Technology Security Certification and Accreditation Process, with the following key characteristics:

- Relative cryptographic strength (for example, NIST and Common Criteria levels)
- Cryptographically strong pseudorandom number generator, which complies with Federal Information Processing Standard (FIPS) 140-2, section 4.9.1: *Security Requirements for Cryptographic Modules* (http://csrc.nist.gov/cryptval/140-2.htm)
- Cryptographically strong sequences as described in RFC 1750: *Randomness Recommendations for Security* (www.ietf.org/rfc/rfc1750.txt)
- J2EE, Microsoft .NET, JSR 94-based rules engine

## ADAPTIVE STRONG AUTHENTICATOR

**Leveraging a soft, two-factor authentication solution, adaptive strong authenticator provides fraud protection against online identity theft by encrypting password data inputs at the point of entry.**

Common authentication methods today have many weaknesses:

- Data remains raw between the point of creation and where the encryption process is invoked. Moving raw data over open lines increases the opportunity for, and likelihood of, theft.
- Every protection implemented on a data source depends on a human being to maintain its state of security, which can be compromised.
- Any new computing environment can be well studied and misused due to its predictable behavior.

Oracle Adaptive Access Manager's adaptive strong authenticator was designed specifically to overcome these limitations.

Leveraging a soft, two-factor authentication solution, adaptive strong authenticator provides fraud protection against online identity theft. It does so by encrypting credential data inputs at the point of entry. This ensures maximum user protection because information never resides on a user's computer. Nor does information reside anywhere on the internet where it can be vulnerable to theft.

### Protecting Corporations and Their Customers

As corporations embrace the internet, they must ensure that customer transactions and data are safe. Adaptive strong authenticator enables corporations to deploy a highly effective security solution that offers their customers the required protection as well as the ease of use needed to engage in and grow online relationships.

Adaptive strong authenticator is hardware and software independent and does not rely upon cached data. End users can invoke the authentication process from any browser, over any network (public, private, Wi-Fi, kiosk). They can also use any user touch point to protect their information during session initiation or during in-session transactions.

#### Low Cost of Ownership

**Adaptive strong authenticator does not require any special databases, proprietary software, extra hardware, or third-party servers resulting in a lower cost of ownership than other authentication options.**

An added benefit of adaptive strong authenticator is that it offers a low cost of ownership. This is in comparison to other authentication alternatives. The solution does not require any special databases, proprietary software, extra hardware, or third-party servers. Furthermore, there are no customer support needs to consider associated with lost or damaged cards/tokens.

Using adaptive strong authenticator, corporations can defend their customers and their data against the most potent fraudulent attacks.

| Attack | Defense |
|---|---|
| Phishing Environment | The PIN data required to authenticate only exists in a form understood by the user and the server. Therefore it can't be interpreted and used for fraud. An impostor internet site cannot simulate the operational aspects of the authentication. |
| Phishing (Social Engineering) | Equipping end users with their own personalized device is the first step. Ensuring adaptive strong authenticator is used for entry of all sensitive credentials (password, PIN, challenge questions, etc.) is the second. Finally, adaptive risk manager prevents the fraudulent use of credentials if end users have fallen prey to phishing. |
| Trojan Viruses | Adaptive strong authenticator foils keyboard, mouse click, and screen capture loggers; cookie hijackers; "over the shoulder" spies; and all other forms of known attacks. This is because no sensitive data is entered using the keyboard, mouse, or cookies nor is any sensitive data handled by the browser. |
| Fraudulent Transactions | Adaptive risk manager collects and evaluates end-user data points. These data points can be used to authorize, challenge, deny, or put online transactions on hold. |
| Password Theft | Adaptive strong authenticator generates a unique set of random data for every user session. It is virtually difficult for a password to be guessed and reused. |

## Comprehensive Features and Functionality

Adaptive strong authenticator is an enterprise-licensed platform that includes a number of user interfaces. These interfaces are for managing fraud and identity

theft protection. Whether making payments, accessing sensitive documents, entering passwords, or answering challenge questions, users and data are protected.

### QuestionPad and QuizPad

**QuestionPad and QuizPad protect the sensitive information in challenge questions by changing the way the information is entered.**

QuestionPad and QuizPad take data entry to another security level. With challenge questions becoming more-commonly used in financial institutions and other enterprises, it opens up another target for fraudsters. QuestionPad and QuizPad address this issue by changing the way users enter these new credentials.

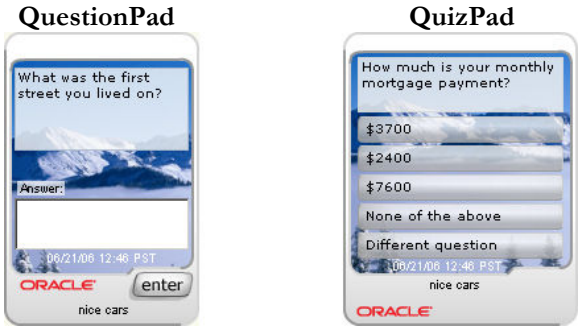



**Figure 3: QuestionPad and QuizPad**

Both QuestionPad and QuizPad offer several deployment options. Oracle can host the challenge questions and provide the question bank. Alternatively, the question bank can be integrated with internal customer information databases. They can also be integrated with external third-party question providers.

### KeyPad

KeyPad is a configurable virtual keyboard. It can be used to enter alphanumeric and special characters found on a traditional keyboard. That makes it ideal for


entering passwords and other sensitive alphanumeric information.

**Figure 4: KeyPad**

### PinPad and TextPad

PinPad is an authentication entry device used to enter a numeric PIN. It can be invoked at the time of login or transaction. TextPad is a personalized device for

entering a password or PIN using a regular keyboard. This method of data entry helps to defend against phishing.

PinPad and TextPad help protect against phishing.


**Figure 5: PinPad and TextPad**

### Slider

Slider is one of the most secure data entry mechanisms currently available. In traditional encryption processes, all entities involved in the encryption/decryption process are parts of the computing environment. However, Slider uses the end user as a functional part of the encryption/decryption process. This makes it a unique, authentication security solution.


**Figure 6: Slider**

**"[Oracle's] technology offers an approach that should appeal to companies looking for flexible and scalable authentication solutions…[It] offers a strong alternative for institutions looking to resolve trade-offs between security and deployment, which can represent some of the main challenges of selecting an online security solutions."**

***Source:*** **IDC,**
***FFIEC Guidelines Require Financial Institutions to Ramp Up Online Security***
**(December 2005)**

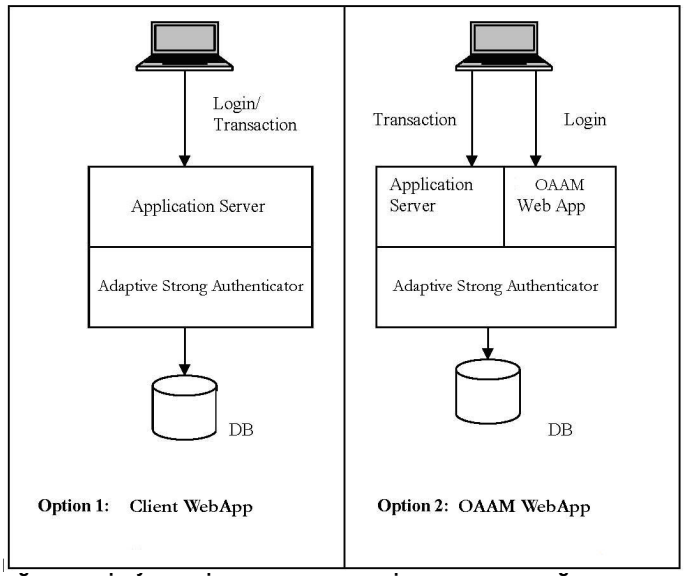
## Deployment Options

### Without Oracle Adaptive Access Manager Web Application

With this deployment approach, the client stores all credentials. The client also uses the adaptive strong authenticator library only for encoding and decoding inputs.

### With Oracle Adaptive Access Manager Web Application

With this deployment approach, customers can configure their own Web interface. They do this by leveraging packaged Web pages and flows from Oracle. These pages and flows can then be altered to meet corporate branding requirements.




## ADAPTIVE RISK MANAGER

**Adaptive risk manager allows enterprises to evaluate and score risk for each online login and transaction so enterprises can monitor high-risk situations in real time.**

Adaptive risk manager, a core component of Oracle Adaptive Access Manager, enables an enterprise to evaluate and score risk. They can do so for each online login and transaction. As a result, the solution increases authentication security in real time for high-risk situations.

Adaptive risk manager provides a strong second and third factor of security for the enterprise. It can serve as a standalone solution that offers increased security, with no change to the user experience. But it can also be used in combination with adaptive strong authenticator. Together the components provide further anti-identity theft and fraud protection.

The solution is currently licensed to some of the world's leading institutions. It has more than 27 million users in 67 countries. Adaptive risk manager satisfies federal guidance such as the Federal Financial Institutions Examination Council. It is recommended by leading security analysts as an approach to satisfy mandates for higher authentication security.

### Multiple Factor Risk Protection

Adaptive risk manager verifies each user's computer and location ("something you have"). It also verifies a user's behavior patterns to confirm identity ("something you are"). These verifications are added to existing enterprise requirements for login/password credentials and additional knowledge-based authentication ("something you know"). This offers the enterprise multiple strong factors of antifraud protection.

Adaptive risk manager uses dozens of "tentacles," including proprietary one-time use secure cookies, Flash objects, and other patent-pending technologies. These serve to recognize and fingerprint the device you typically use to log in such as

your computer, laptop, or a kiosk. In this way, adaptive risk manager makes your personal computer your second factor—without requiring any change in your behavior.

**Adaptive risk manager's proprietary, real-time device and location fingerprinting can determine whether a login attempt is fraudulent.**

Also patent pending is the unique process used for device fingerprinting. It is a process that creates a fingerprint good for use one-time only. Therefore it is immediately invalidated if a fraudster attempts to reuse it.

Adaptive risk manager evaluates the pre-, post-, and in-session characteristics of each transaction. This ensures fraud detection and transactional integrity.

The solution's proprietary, real-time device and location fingerprinting can determine whether a login attempt is high risk. These determinations are made with a high probability, prior to authentication. Subsequently, each individual transaction attempted in session is further scored for risk, resulting in an even higher level of confidence.

Adaptive risk manager then governs the institution's response to risk, whether it is an alert, user challenge, or secondary authentication. This is done in real time using adaptive strong authenticator.

## Comprehensive Features and Functionality

Adaptive risk manager is an open, standards-based system. It is available as a single-server installation or a cluster of servers that can be integrated with existing enterprise Web applications using prepackaged APIs.

Adaptive risk manager includes the following standard features:

- **Engine.** State-of-the-art, real-time rules and risk scoring is provided.
- **Integration support.** Third-party integration is supported via open APIs and shared authentication and fraud services infrastructure.
- **Proprietary fingerprinting.** Patent-pending fingerprinting methods for device, location, and workflow use second and third factors for identification.
- **Models and rules.** Customizable scenarios invoke any set of rules. They are driven entirely by the needs of the organization and the level of security defenses required.
- **Intelligent algorithms.** Embedded intelligence and powerful algorithms allow customers to reduce "noise" and hone in on actual fraud.
- **Administration tools.** Comprehensive user interfaces are provided to maximize leverage and usage of the application. This includes dashboards, reports, and modeling tools.

### Adaptive Risk Manager Engine

The adaptive risk manager engine offers state-of-the-art, real-time rules and risk scoring. The robust engine combines analytics, including states, rules, and pattern recognition. This ensures intelligent real-time operations and maximum enterprise protection against online fraud.

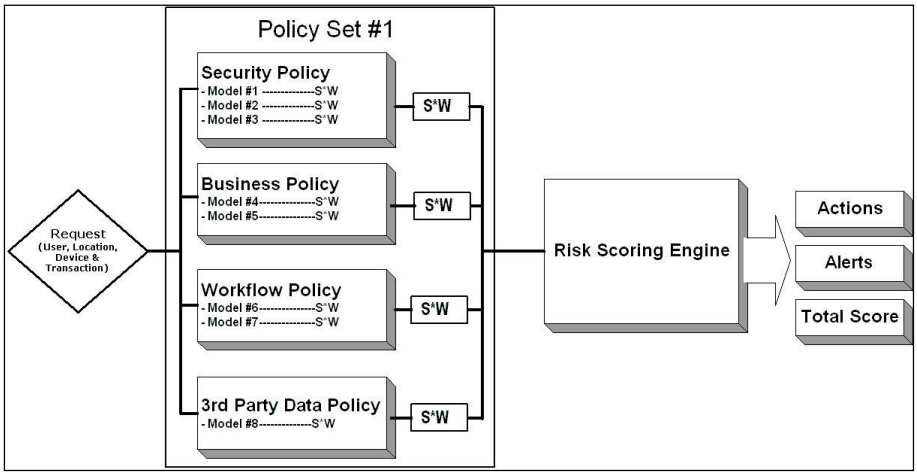



**Figure 8: Adaptive risk manager engine.**

Adaptive risk manager analytics are designed for high performance and scalability. The adaptive risk manager engine works by automatically preanalyzing policies (sets of modules) and models (sets of rules). Then it actively monitors each user's transactional data flows to identify those elements that might impact the models.

**Adaptive risk manager analytics are designed for high-performance and scalability.**

The adaptive risk manager engine uses a proprietary structure to simultaneously maintain the necessary parameters. It then updates and tests them against the relevant models.

#### *Rules Engine*

The adaptive risk manager engine triggers actions and alerts based upon rules. These rules are housed in models configurable by the institution and are established according to the institution's policies:

- **Security policies (pre- and post-authentication).** Uses standards for detecting fraudster behavior developed from cross-industry best practices:
  - Anomaly detections
  - Misuse detections
  - Intrusion detections
  - Predefined fraudster models (the figure shows a subset of the fraudster rules that are standard in adaptive risk manager)
  - Customizable models

Adaptive risk manager's extensive fraudster models are enriched by Oracle's cross-industry customer base. Its customer base covers financial services, e-commerce, healthcare, and the military, among others.

- **Fraudster rules (subset).** A collection of some basic anti-fraud rules.

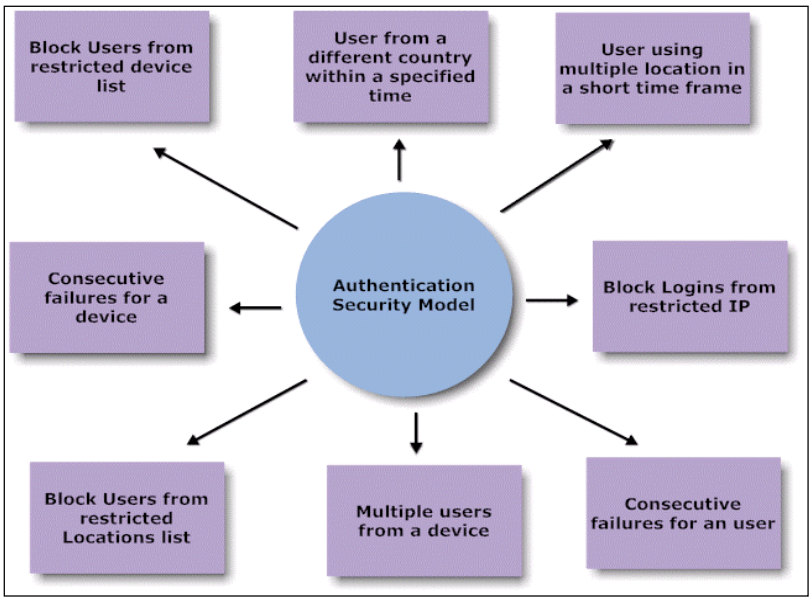



**Figure 9: Adaptive risk manager security policies**

- **Transaction policies (in session).** Invokes rules based upon parameters established by the business for mitigation of transaction risk, including
  - In-session transaction monitoring
  - Business-defined transaction rules
  - Key value-driven logic
  - Customizable models

**The adaptive risk manager engine triggers actions and alerts based upon rules housed in configurable models that are established according to the institution's policies**

- **Workflow policies.** Uses common online activity patterns as a benchmark for detecting transactions that are out of pattern:
  - Historical transactions
  - Behavioral analysis
  - Event, time, and value pattern recognition
  - Temporal analysis
  - User profiles
  - Predefined customizable risk models
- **Third-party data.** Offers prepackaged integration with third-party data providers, developed through Oracle's strategic partnerships. Thus, third-

party data can be called and evaluated in adaptive risk manager as part of the risk score:

- IP intelligence
- Risk data
- Historical data (data warehouse)
- Customer data
- Fraud network data

Oracle also has the Fraud Intelligence Network for data sharing as part of its proactive fraud detection model. Rather than conduct reactive services to dismantle fraud, Oracle proactively enhances fraud detection across its network.

Oracle works with customer and partner institutions across a variety of industries to share data on new threats. It also shares data on updated models to combat those threats.

#### *Risk Scoring/Forensics*

**Risk is scored within adaptive risk manager using dozens of tentacles, which are fingerprinted within the system. If any one is a mismatch, the system will yield an elevated risk score.**

Adaptive risk manager risk scoring is a product of numerous fraud detection inputs such as a valid user, device, location, or workflow (see "Proprietary Fingerprinting"). Also included are third-party data and historical customer data. These inputs are weighted and analyzed in real time within adaptive risk manager's fraud analytics engine.

Risk is scored within adaptive risk manager using dozens of tentacles, which are fingerprinted within the system. If any one is a mismatch, the system will yield an elevated risk score. The degree of elevation can be adjusted with the weight assigned to the particular risk. If the risk is scored above a certain threshold, adaptive risk manager initiates a response.

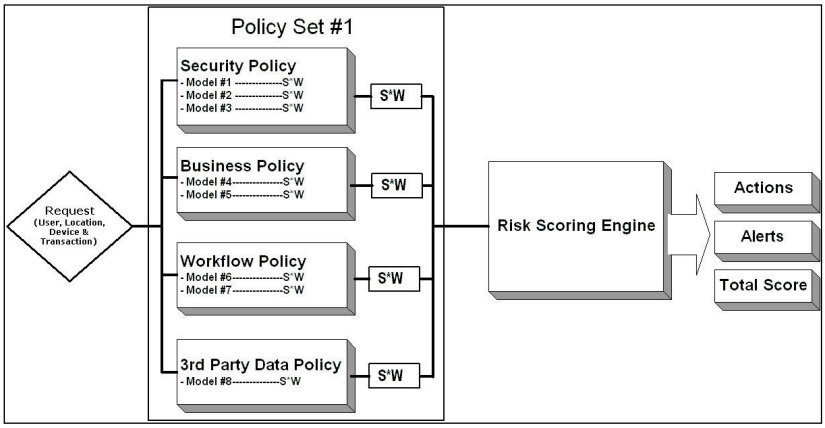



**Figure 10: Scoring risk with adaptive risk manager**

- **Confidence levels.** Risk scoring in adaptive risk manager is weighted and cumulative. The type of the first factor (for example, a token), device and location fingerprint, and other information available at login influence the risk scoring for transactions conducted during a session. This lends a high degree of accuracy to the system to minimize false positives.
- **Design.** Adaptive risk manager's risk scoring engine is designed to maximize accuracy. It is also designed to reduce the configuration and support burden for the institution. This is accomplished through the following features:
  - **Customer models/rules.** Any custom rule can be set, according to business need, to become activated if a transaction is scored above a certain risk threshold.
  - **Nested models.** Nested models can be assigned to ensure a higher degree of accuracy for the risk score. A nested model is a secondary model. It is used to further quantify the risk score in instances where the original result output by the system is inconclusive. A nested model is run only when a specific sequence of answers is returned from the primary model. Nested models therefore reduce false positives and negatives.
  - **Preset (automatic) risk scores.** Automatic risk scores are available when the institution does not want to assign a risk score or nested model. Thus, extensive risk scoring capabilities are available out of the box. The institution does minimal custom configuration.

#### *Real-Time Response*

**Adaptive risk manager is configured, based upon rules, to initiate a real-time response to an elevated risk score.**

Adaptive risk manager is configured, based upon rules, to initiate a response to an elevated risk score (see "Models and Rules"). Responses can include the following:

- **Internal flag/watch list.** For follow-up investigation within the institution.
- **Secondary authentication.** Out of Band:

- **Voiceprint.** Through its partnership with industry-leading voice authentication providers, Oracle has created prepackaged integrations with voiceprint authentication capability. The capability is so advanced it is even certified to issue voice digital signatures. This is a two-factor solution that requires users to give both a challenge response and a biometric voiceprint that is one of a kind. Adaptive risk manager also integrates with voice providers to enable "second single-factor" authentication.
- **Short Message Service/e-mail.** Users might be asked to contact the institution or to enter a secure code or token.

- **Secondary authentication.** Online:
  - **Challenge questions.** Adaptive strong authenticator can be used to provide further defenses against in-session attacks. It can also enable "weakest link" security by protecting the challenge/response process.
  - **Tokens, smart cards, and so forth.** Any existing authentication solution can be used and integrated with adaptive risk manager.

#### Integration Advantages

**Adaptive risk manager is an open, standards-based platform designed for minimal integration work and maximum compatibility with existing enterprise and third-party systems.**

Adaptive risk manager is an open, standards-based platform. It is designed for minimal integration work and maximum compatibility with existing enterprise and third-party systems. Adaptive risk manager features best-of-breed integration capabilities that enable the institution to speed up and simplify its deployment. These capabilities also enable the institution to leverage data from external systems for adaptive risk manager.

A list of prepackaged APIs is available in the current version of adaptive risk manager. APIs are available in the areas of Active Directory, Lightweight Directory Access Protocol, fraud, Annotation Markup Language, customer relationship management, Single Sign-On, compliance, and mainframe systems.

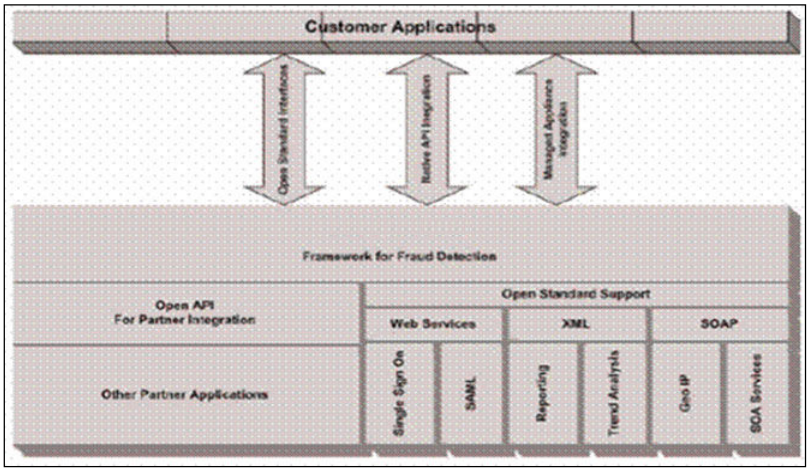


**Figure 11: Integrating Oracle Adaptive Access Manager into the enterprise**

### Proprietary Fingerprinting

Much of adaptive risk manager's power lies is in its patent-pending fingerprinting methods for device and location. Adaptive risk manager stores and uses multiple second and third factors to establish these fingerprints. The figure below shows a partial list. Additions are ongoing via industry partnerships and Oracle's own research and development.

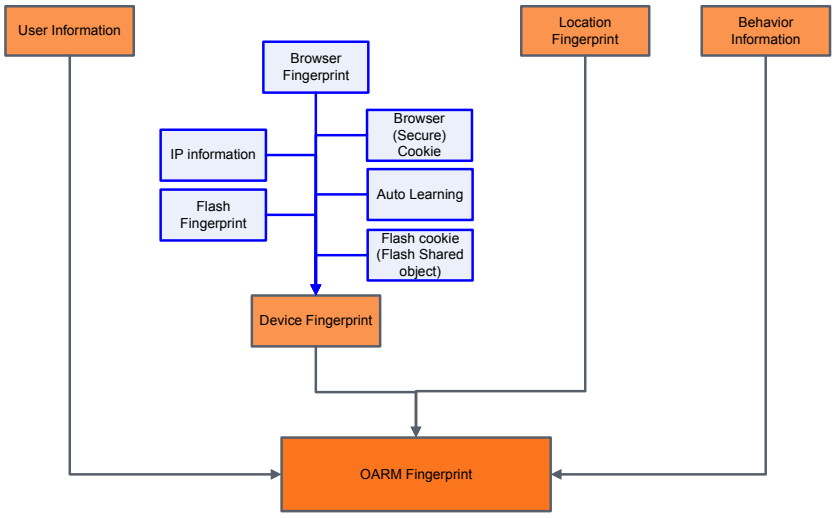



**Figure 12: Factors used to establish fingerprints**

**Adaptive risk manager has patent-pending fingerprinting methods for device and location. Multiple second and third factors are used to establish these fingerprints.**

#### *Device*

Adaptive risk manager monitors a comprehensive list of device attributes. If any attributes are not available the device can still be fingerprinted.

Adaptive risk manager's patent-pending method for device fingerprinting generates a one-time fingerprint for each user session. That fingerprint is unique to the individual's device. It is replaced upon each subsequent visit with another unique fingerprint. This ensures that a fingerprint cannot be stolen and reused for fraud.

#### *Location*

Adaptive Risk Manager contains sophisticated location fingerprinting capabilities. A blend of IP intelligence data is used to identify locations by geography and many other data points crucial to accurate fraud detection.

### *Multilevel Security*

**Adaptive risk manager workflow models and rules use historical behavior pattern data to limit fraud. If a user does something out of pattern, adaptive risk manager can trigger actions and send alerts to another system to counteract fraud.**

The benefits of adaptive risk manager fingerprinting and risk scoring are cumulative. The figure below illustrates this. Device and location fingerprints are already verified by the time a user attempts a transaction in session. Thus, Oracle Adaptive Access Manager achieves an additional level of confidence.

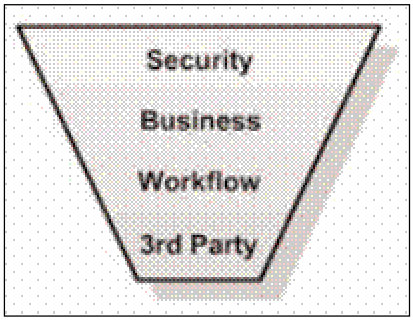



**Figure 13: Adaptive risk manager reduces risk by fingerprinting and scoring.**

Adaptive risk manager workflow models and rules use historical behavior pattern data to limit fraud. If a user does something out of pattern, adaptive risk manager can trigger actions and send alerts to another system to counteract fraud.

Workflow rules are administered by specifying acceptable ranges of variation in pattern. To further enhance Oracle's proprietary methods, adaptive risk manager also features prepackaged integration with partners. These partner solutions also monitor the customer experience at the individual user level.

Third-party data can be fed into the adaptive risk manager analytics engine as part of the fingerprint. This enhances the overall picture of customer activity.

### Models and Rules

**Institutions can deploy adaptive risk manager in a variety of customizable scenarios to invoke a set of rules based on the needs of the institution and the level of security required.**

Institutions can deploy adaptive risk manager in a variety of customizable scenarios to invoke any set of rules. These rules are driven entirely by the needs of the institution and the level of security required. Rules can also be applied in any combination to different segments of users. This can be done in any way the institution wants to segment its user population.

As previously discussed, adaptive risk manager monitors and evaluates activity by four main criteria: user, device, location, and workflow. Each criterion contains various pieces of adaptive risk manager data. That data is used to detect fraud risk (and, optionally, data seamlessly integrated from third parties as well).

Within adaptive risk manager, data is organized into groups corresponding to these criteria. These groups are then linked to compatible models containing rules used to evaluate activity.

#### *Expanding and Improving Models over Time*

Over time, there are several ways the institution can continue to expand and develop the models.

- **Learning.** Adaptive risk manager features intelligence gathering, which enables the administrator to learn from experience over time. Anomalies are recorded that enable new models to be built and existing models refined. Thus, adaptive risk manager becomes more valuable and accurate over time as the rules engine becomes more robust and tailored to specific aspects of the institution's business and user population.
- **Periodic downloads.** Oracle customers can receive periodic downloads and bulletins as new models are created. This ensures each institution is proactively keeping pace with the latest threats.

### Intelligent Algorithms

- Embedded intelligence and powerful algorithms in adaptive risk manager allow the institution to reduce "noise" and hone in on actual fraud. Time is spent resolving real issues rather than trying to identify them. The algorithm takes into account patterns of different entities like user, device, location, transactions, etc and co-relates them to reduce false positives.

### Comprehensive Administration Tools

Comprehensive user interfaces are a standard part of adaptive risk manager to help the institution leverage the system. A fraud monitoring dashboard, reporting, customer care, risk modeler, and case/risk management tools are all included in the administration area of the adaptive risk manager fraud analyzer.

#### *Dashboard*

The dashboard provides real-time visibility into potential fraudulent activities. It provides performance and summary statistics as well as reports on locations, scoring, devices, and rules and alerts. These help analyze online traffic; identify suspicious behavior; and design rules for proactive fraud prevention, risk monitoring, and case management.

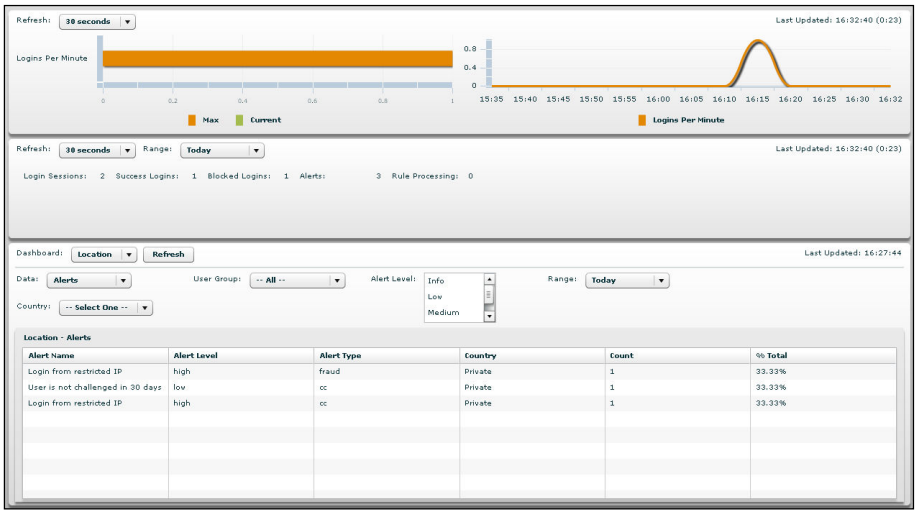



**Figure 14: The dashboard offers a real-time view of the site so you can see potentially fraudulent activities in progress.**

**Dashboards provide real-time visibility into potential fraudulent activities. It provides performance and summary statistics as well as reports on locations, scoring, devices, and rules and alerts.**

- **Performance and summary.** The performance and summary panels provide views of statistics on the current rate of logins and an overview of activity. This includes login sessions, successful logins, blocked logins, alerts, rules triggered, and rules run.
- **Dashboards.** The dashboard panel provides access to four dashboard types: Location, Scoring, Device, and Security. The dashboard offers a real-time view of the secured site. It delivers a high-level personalized business view of the current status of user behavior and key transactions.

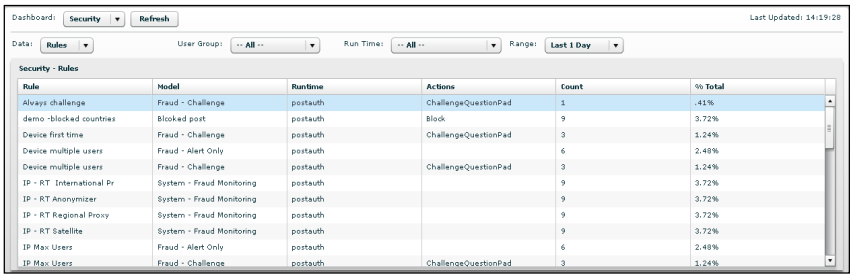



**Figure 15: The dashboard panel provides aggregated statistics in an easy-to-view format.**

- **Location.** Provides aggregated location statistics including location, device, and users detected.
- **Scoring.** Displays statistics on risk score, runtime, and the number of sessions.
- **Devices.** Provides statistics on the browser, OS, number of sessions, and percent of total.
- **Security.** Displays statistics on alerts that were run during the time frame, including runtime; alert level and type; and information on rules that were run during the time frame, such as model, runtime, action, and count.

### *Reports*

**Oracle Adaptive Access Manager's comprehensive reporting area enables detailed risk management and analysis through drill-down capabilities for viewing information.**

Oracle Adaptive Access Manager's comprehensive reporting area contains reports to assist with enterprise-level and individual customer–level fraud management. The reports enable detailed risk management and analysis through drill-down capabilities for viewing information. Such views are by location, device, user, and transactions over specific time ranges and schedules.

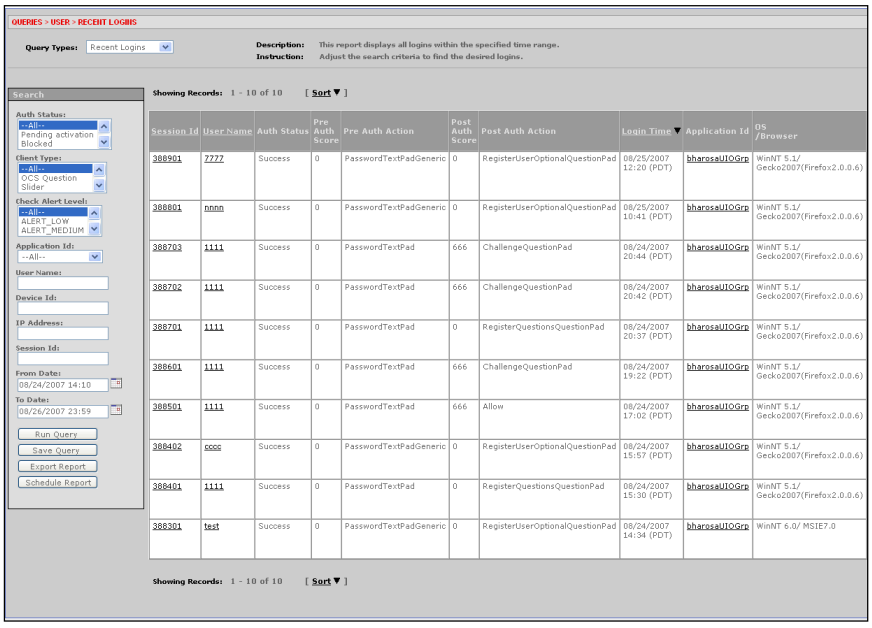



**Figure 16: Comprehensive reporting area**

### *Risk Modeler*

There are powerful tools available that enable fraud, risk, and security departments to model risk. Offline capabilities can be used to import data and test scenarios to develop and refine models and rules. The models can be run in mass runs as well as used to investigate and troubleshoot individual cases. Based on the offline results and live performance, models can be modified for optimal results.

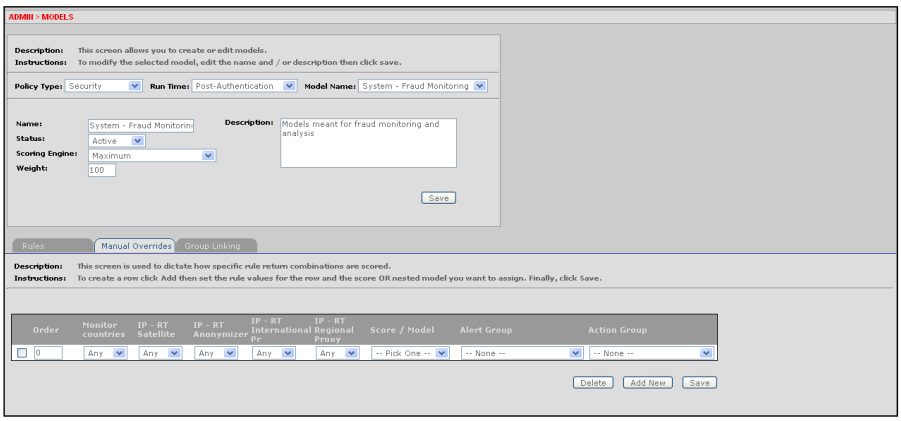



**Figure 17: Risk modeler**

### Customer Care

**Oracle Adaptive Access Manager offers case management and customer care tools to support customer service inquiries associated with adaptive risk manager.**

Case management and customer care tools support customer service inquiries associated with adaptive risk manager. Through these tools, customer service representatives can review service logs for each user. This would enable them to investigate the reasons certain actions were taken or understand why alerts were triggered. For example,

- View the reason a login or transaction was blocked
- View a severity flag with alert status to assist in escalation
- Issue a temporary allow or unlock a customer

The customer care capabilities can be customized and managed according to roles and company procedures.

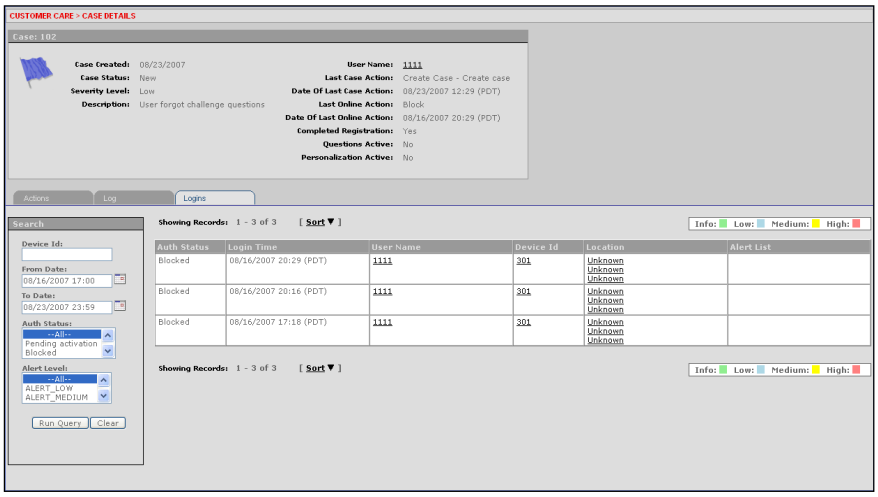



**Figure 18: Case management and customer care tools**

## CONCLUSION

Oracle Adaptive Access Manager offers the unique and powerful advantages that you expect of the next generation of adaptive, risk-based access management systems. The table below summarizes the value of adaptive risk manager and adaptive strong authenticator.

| Adaptive Risk Manager | Adaptive Strong Authenticator |
|---|---|
| **Forensics.** Patent-pending device and location fingerprinting methods. | **Devices.** Patent-pending technology offers the security strength of a hardware token and the flexibility, affordability, and ease of use of the Web. |
| **Engine.** Robust engine offers state-of-the-art, real-time rules and risk scoring. | **Versatility.** A solution that is easy and intuitive enough for online banking customers and secure enough for the U.S. Air Force. |

| Adaptive Risk Manager | Adaptive Strong Authenticator |
|---|---|
| **Ease of deployment/low cost of ownership.** Requires no proprietary hardware or software of any kind and employs standard Web technologies. | **Security.** Secures the end-user's computer, where most threats originate. Credentials are secure even if the computing environment has been compromised.<br><br>Proprietary process for entering a password or PIN where the data does not reside anywhere on the user's machine or on the internet, where it could be vulnerable to theft. |
| **Extensive tools.** Dashboard, reporting, customer care, and case/risk management tools are all a standard part of adaptive risk manager. | **Longevity.** Solution evolves to offer stronger authentication security over time to combat new threats, without changing the user experience. Other solutions offer no upgrade when an image or watermark no longer meets the institution's needs. |
| **Ease of integration.** Open, standards-based platform offers prepackaged APIs and integration with third-party data and solutions. This ensures maximum interoperability with existing architectures. | **Experience.** Solution has been developed from extensive customer-led enhancement and innovation. |
| **Best-of-breed partner integration.** AD, LDAP, fraud, AML, SSO, compliance, mainframes. | **Fraud Intelligence Network.** Proactive (rather than CRM, reactive) fraud response services. |

## APPENDIX: ORACLE ADAPTIVE ACCESS MANAGER HARDWARE AND SOFTWARE REQUIREMENTS

| | |
|---|---|
| **Client computer** | Industry-standard computer with internet connectivity and graphical internet browser. |
| **Server requirements conform to latest industry standards** | Supports industry-standard server hardware and software. Minimum: Dual 3GHz Xeon/1GHz Ultra SPARC/POWER5/POWER5+ processors with 4GB RAM and minimum 160GB SCSCI RAID 1/5 hard disk, with any industry-standard operating system, including Linux, Solaris, Windows 2003 Server, HPUX, and AIX. |
| **External, Web based** | Adaptive strong authenticator and adaptive risk manager purely Web-enabled products. |
| **Database size requirements (adaptive risk manager only)** | Approx. up to 1KB/user/transaction number of transactions per days of retention. |
| **J2EE compliant** | Yes |
| **.NET compliant** | Yes |
| **Security model** | Network- and accounts-based security model |
| **Data center hostable** | Yes |
| **NOC supportable** | Yes |
| **Supports Netscape, Internet Explorer, Firefox, Mozilla, and Safari** | Adaptive strong authenticator is supported on the following browsers: Internet Explorer (5.5 and above); Netscape (4.7 and above); Firefox (1.0 and above); Mozilla (1.0 and above); Safari (1.0 and above). Adaptive strong authenticator is supported on the following platforms: Windows (98 and above including ME and 2003); Mac OS (9.x and above); Redhat Enterprise Linux (WS v.3 and 9); Solaris (8 and above). |
| **Source language** | The server is based on industry-standard Java/.NET technologies. Adaptive strong authenticator clients are developed in industry-standard formats including DHTML, Flash, Java applets, SVG. |
| **Other vendor product dependencies (depends on deployment option)** | Relational databases: DB2, Oracle, MySQL, Sybase. Optional integration with third-party geolocation services: GeoBytes, Quova. |

**Oracle Adaptive Access Manager**
**Updated January 2008**

**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**