# ORACLE ADAPTIVE ACCESS MANAGER

PROACTIVE ENTERPRISE SECURITY

KEY FEATURES

- Fingerprint all types of devices whether access is via browser or native mobile application.
- OTP Anywhere - Risk-based, one-time password (OTP) authentication.
- Universal Risk Snapshot – Configuration backup, migration and recovery.
- Answer Logic – Balancing security and usability.
- Risk Analytics - Real-time and batch data analysis.
- Active Compliance – Incident prevention and rich audit trail.
- Deployment Options – Web Access Management, Native, Reverse Proxy, Listener.
- Secure Self-Service Password Management – through Oracle's IAM suite integration.

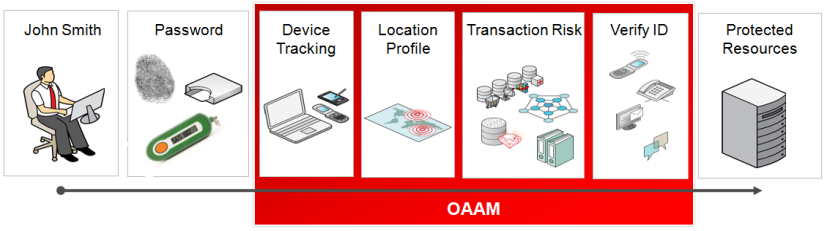
*Oracle Adaptive Access Manager (OAAM) improves the security of sensitive online operations—such as data access, financial transactions, and business processes—by providing real-time risk analytics, risk-based authentication, anti-phishing, and anti-malware capabilities. With its renowned usability and full integration with back-end identity management infrastructures, OAAM provides a security solution that is both strong and operationally sound.*

## Introduction

OAAM provides innovative, comprehensive features to help organizations prevent fraud and misuse of online resources. By strengthening existing authentication mechanisms with risk-based challenge methods and by providing real-time risk analysis, OAAM provides a unique multi-factor authentication solution. In addition, OAAM's risk analytics features help security experts to preemptively detect fraud and abuse across multiple channels of access.

## Layered Access Security

OAAM layers additional security measures on top of existing authentication to strengthen browser and mobile application login flows. These security layers include user device tracking, location profiling, transactional risk analysis, risk-based identity verification, and behavioral profiling.




## Device Tracking

OAAM has the ability to automatically identify devices and profile their actions on the website. Known as "device fingerprinting," this feature detects anomalous behavior by the device and adjusts the user's risk level accordingly. 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.

## 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, variation, or misspelling. For example, if a user is challenged with the question "What street did you live on in high school?" she may answer "1st St.", which is fundamentally correct even though the answer on file is "First Street."

KEY BENEFITS

- Single security platform for browser and mobile applications.
- Risk-based authentication via out-of-band channels including SMS, email or instant message adds layered security in a cost-effective manner.
- Answer logic improves usability for security challenge questions, which reduces help desk calls and brings overall solution cost down.
- Helps preventing fraud and misuse before it occurs, saving money by avoiding costly manual reviews, remediation, and compliance penalties.

## OTP Anywhere

OTP Anywhere sends users a one-time-password (OTP) via SMS, email or instant message channels to increase the level of identity assurance.

## Risk Analytics

OAAM 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 third-party data. OAAM combines rules, auto-learning patterns, and predictive techniques to analyze risk in real-time. A detailed forensic trail of the analytics and actions taken is captured to allow in-depth investigation and proper auditing compliance.

## Behavioral Profiling

OAAM dynamically identifies high-risk situations by learning a baseline of normal behavior for users, devices, locations, and entities (e.g., credit card or addresses). This “auto-learning” is updated in real-time so changes in behavior are ready for use in risk evaluations.

## Predictive Risk Analytics

OAAM integrates with Oracle Data Mining to provide statistical risk analysis in real-time to complement rules and behavior profiling. OAAM’s anomaly detection model trains on historical access data and 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.

## Investigation and Forensics

OAAM provides forensic data to power investigations and auditing leveraging specialized tools and Oracle Business Intelligence Publisher. The administration console interface helps a security analyst to better understand the relationships between various security events. 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.

## Conclusion

OAAM 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 and 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.





ORACLE