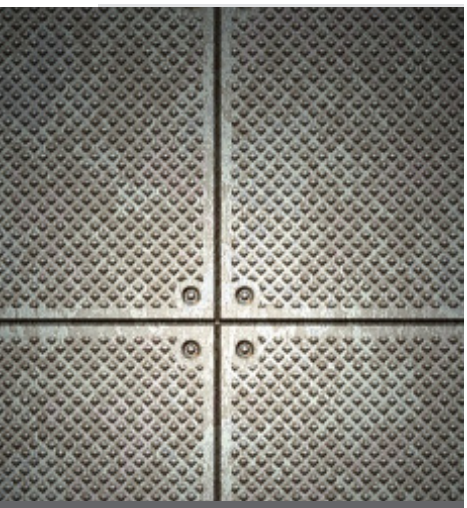


Large Midwest Financial Company

Overview

Oracle Adaptive Access Manager helps companies prevent fraud and misuse by strengthening existing authentication flows, evaluating the risk of events as they happen and providing risk-based interdiction mechanisms. Intuitive policy administration and standardized integrations with the Identity and Access Management Suite components makes Oracle Adaptive Access Manager uniquely flexible and effective at reducing an enterprise's security exposure. Oracle Adaptive Access Manager provides real-time and batch risk analytics to combat fraud and misuse across multiple channels of access while resulting in saved time and money.

The financial arena today is on the upswing after the hardships of the recession. Many of these companies are able to hire full time employees again, and in turn, take on more clients and customers. This Midwestern Financial Company is successful by helping its customers meet their financial goals through insurance and asset management, but they also need to meet the compliance and reporting requirements that are set forth by the government. The Company needed to have access to accurate and timely reporting of risk analytics and misuse reports while still working within a regulated budget.

This Midwest Financial company serves millions of clients worldwide. This high volume of login requests requires an effective technology in place for its end-user access security. Confirming that the correct customer is accessing the correct accounts and information is a tough task for such a large company. The Company required Zirous to help them utilize their existing Oracle Adaptive Access Manager to its full potential. The Company also needed to meet government regulations for reporting standards and required OAAM to help them accurately produce these reports.

Company Challenges:

The Company wanted OAAM to improve various business and end-user functions.

- Better performance tuning for their existing security policies
- A reduction in the number of devices generated by OAAM in order to improve the user's experience with faster login times
- Extension of their existing rules and policies for better coverage of common fraud scenarios
- Overhaul existing policies to include patterns and anomalies in user login behavior for improved security

Solution Details:

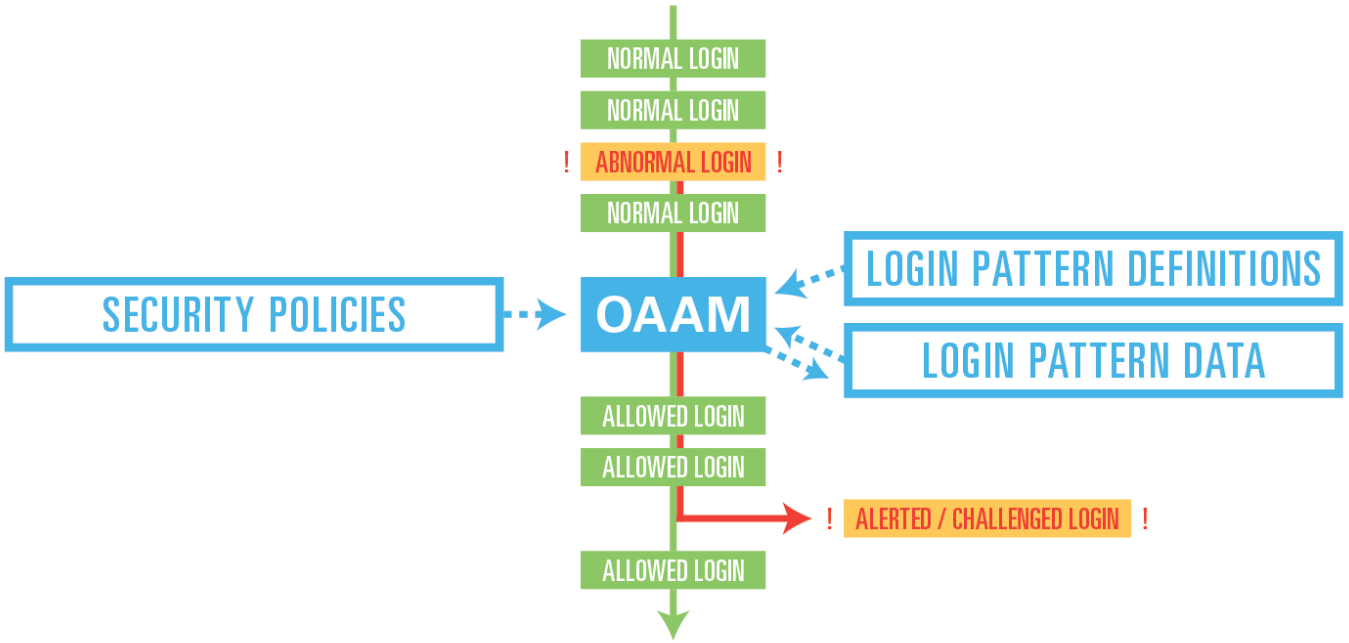
Zirous began by conducting change-impact analysis and inspecting the Company's

Technology Stack:
Oracle Adaptive Access Manager
ARM Automator
OAAM Offline
Oracle Database

existing infrastructure in order to make recommendations for improvements.

- Simplified the design of existing policies according to OAAM best practices to improve performance and increase maintenance capabilities
- Integrated login patterns and transactions to better detect irregular user behavior during and after login and to reduce alert false positives
- Utilized the ARM automator, a fraud testing tool, for functional and regression testing of policies and to improve test quality while still reducing testing costs
- Leveraged OAAM Offline, which references historical, or non-real time data to conduct change impact analysis for both policy functionality and performance without impacting any online users

Overall, Zirous was able to reduce the average execution time of the pre-authentication run-time by over thirty-five percent. The improvements also resulted in about a twenty five percent improvement in average execution time for a successful, unchallenged end-user login. On top of these successes, Zirous was able to identify some solutions that could be put in place in the future to reduce the new device creation rate by up to ninety percent.



This diagram represents the process flow used in the Financial company's solution.