



ORACLE®

Борьба с мошенничеством в Интернет-банкинге
Oracle Adaptive Access Manager (OAAM)

Игорь Минеев ,
ведущий консультант в области
информационной безопасности

И для бизнеса, и для потребителей, важно доверять среде, где они взаимодействуют



"On the Internet, nobody knows you're a dog."

"в Интернете никто не знает то, что ты собака"

Cartoon by Peter Steiner, July 5, 1993
«The New Yorker» (Vol. 69, No. 20)

ORACLE

AuthN и AuthZ на основе оценки риска

- необходимость

Способов мошенничества становится больше

- Bots (robots)
- Keystroke Logging (keylogging)
- Man-In-The-Middle-Attacks(MITM)
- Pharming (farming)
- Phishing
- Phone Phishing
- Social Engineering
- Trojan/Trojan Horse

AuthN и AuthZ на основе оценки риска

- необходимость

Для восстановления доверия и уменьшения риска, заказчики интересуются решениями, расширяющими традиционное управление web-доступом (WAM)

- Контекстным анализом действий пользователей для определения степени риска (угрозы)
- Управлением аутентификацией и авторизацией в зависимости от угроз – балансировка между политиками безопасности и степенью риска
- Многофакторной аутентификацией без применения специальных средств
- Технологиями, повышающими доверие пользователей web-каналам
- Быстрым выявлением мошеннических действий, экономя тем самым на расследованиях и судебных издержках

ОААМ

Oracle Adaptive Access Manager (ОААМ) состоит из двух интегрированных частей, которые служат мощным оружием в борьбе с мошенничеством в Сети:

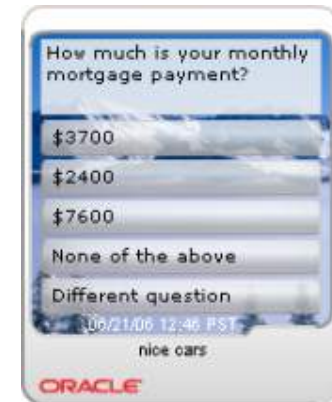
- **Oracle Adaptive Strong Authenticator (ОАСА)**
- **Oracle Adaptive Risk Manager (ОАРМ)**

Oracle Adaptive Strong Authenticator

Ключевые характеристики



- Взаимная аутентификация с помощью персонализируемых изображений
- Виртуальное устройство защищает пароли, PINы и ответы на ключевые вопросы от перехвата с помощью журналирования, фишинга и программ оптического распознавания
- Случайное расположение виртуального устройства на экране пользователя

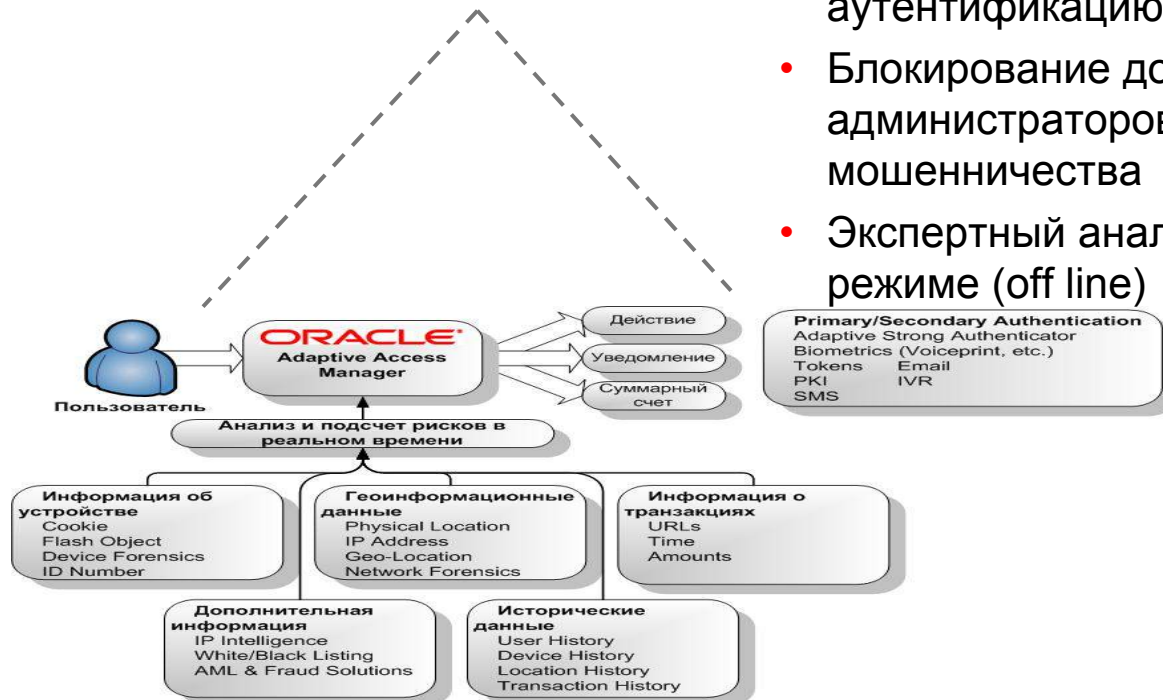


Oracle Adaptive Risk Manager

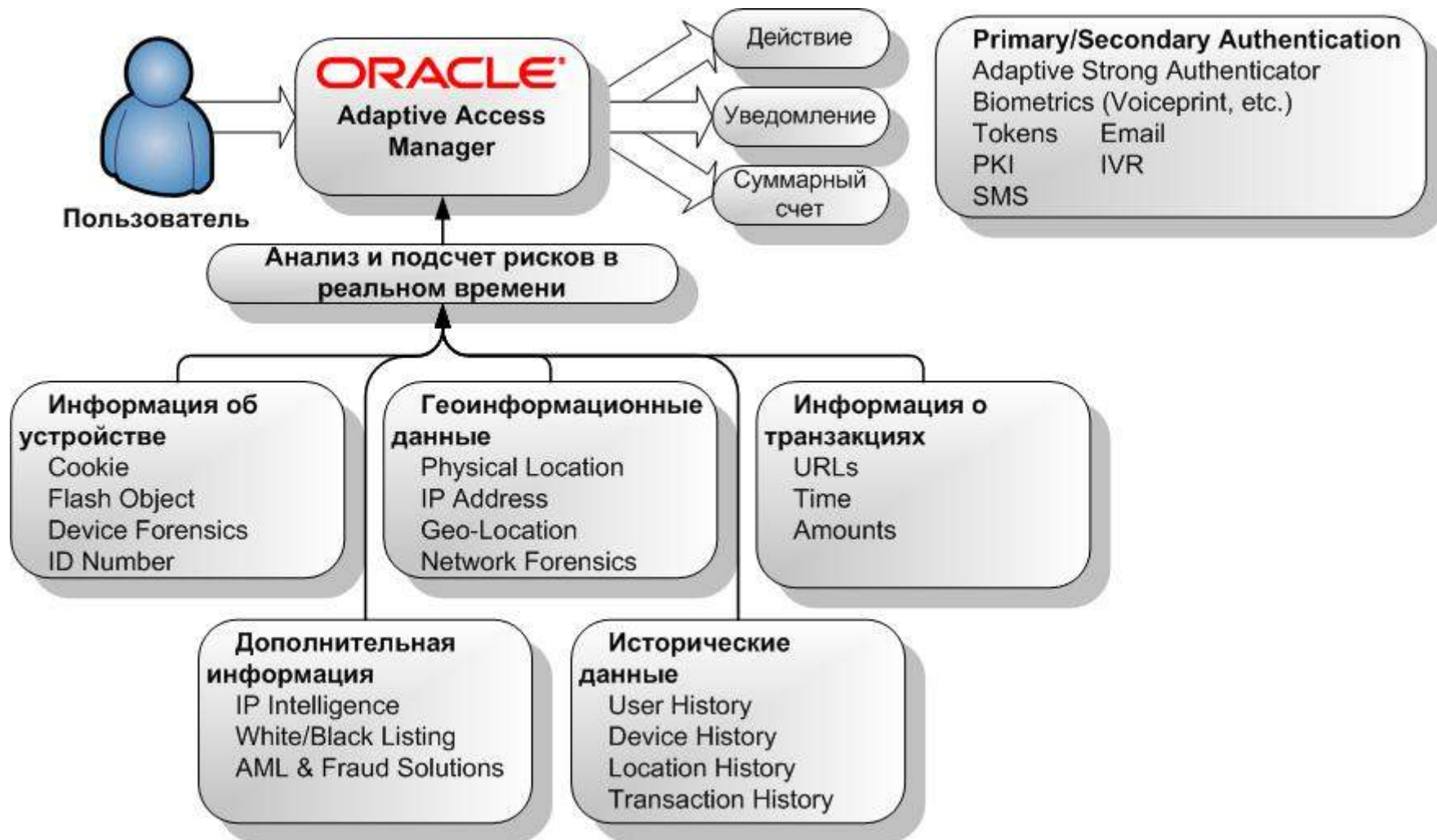
Ключевые характеристики



- Отслеживание web-трафика в реальном масштабе времени, построение профиля «нормального поведения пользователей»
- Контекстная проверка активности пользователей относительно правил
- Генерация запросов на дополнительную аутентификацию или контрольные вопросы
- Блокирование доступа или извещение администраторов в случае вероятного мошенничества
- Экспертный анализ данных аудита в отключенном режиме (off line)



Архитектура OARM



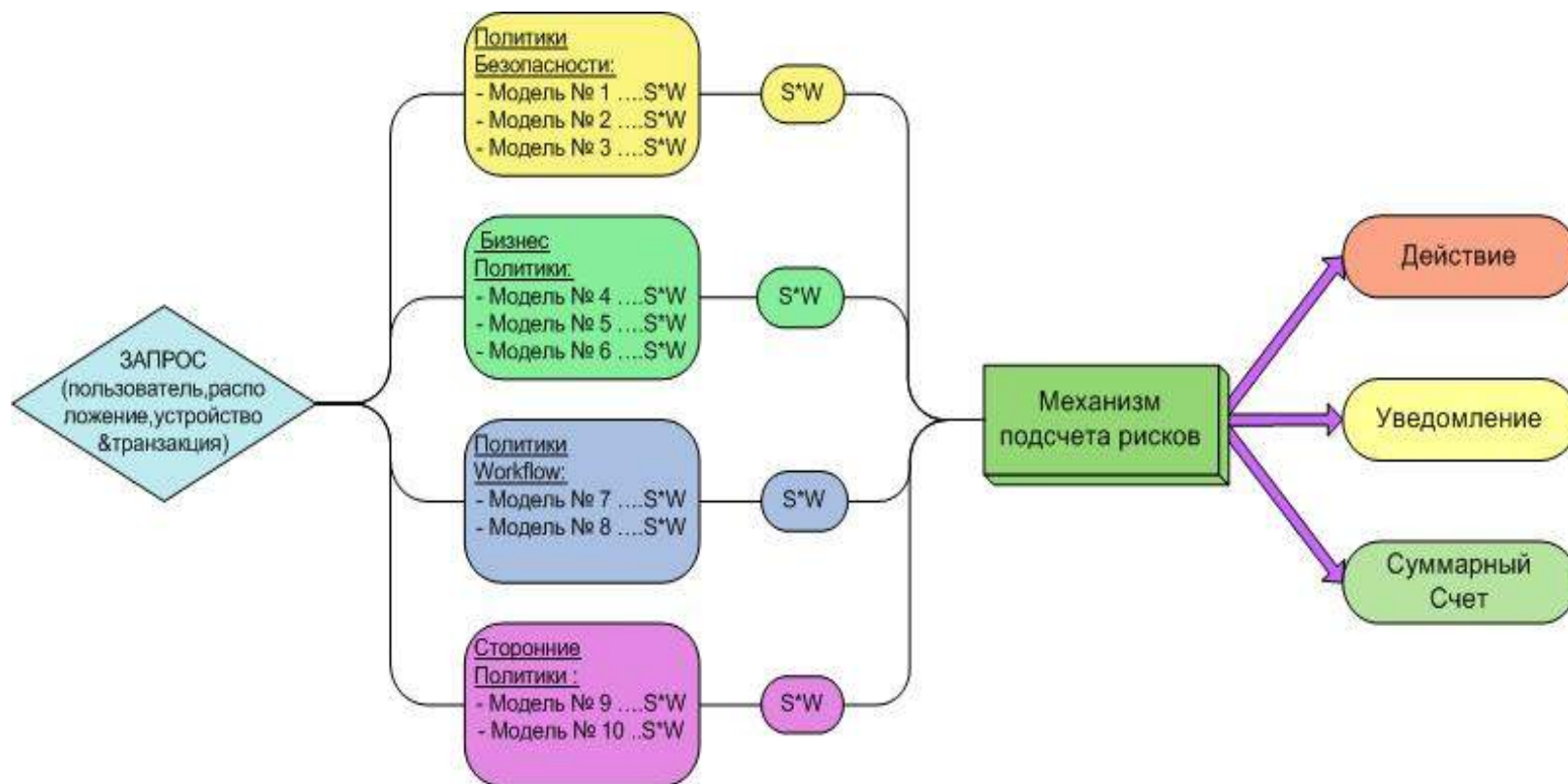
Пример работы пользователя



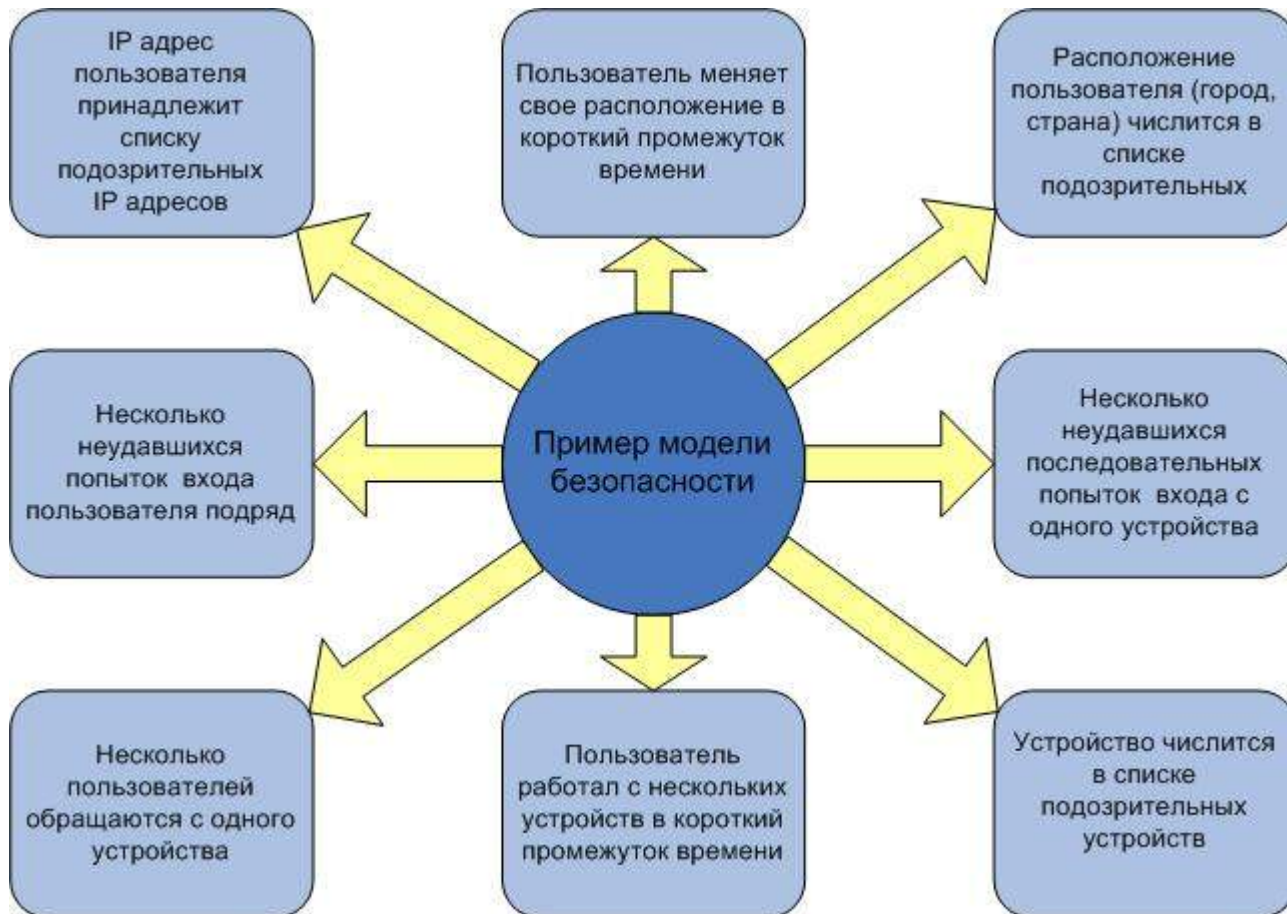
- Просмотр баланса
- Обновить пароль
- Обновить имя
- Изменение предпочтений
- Запросить выписку
- Оплата услуг
- И т.д.

OARM механизм применения политик

- Политика - это набор моделей одного типа
- Модели состоят из правил, которые оценивают возможные риски и вызывают действия, уведомления и накапливают общий счет



Пример модели Аутентификации



Факторы усиленной аутентификации

- 1^{ый} Фактор – что-то знаю
 - Пароль
 - ПИН код
 - КВА вопросы
- 2^{ой} Фактор – что-то имею
 - USB Token
 - Смарт карта
 - Компьютер или мобильное устройство пользователя
- 3^{ий} Фактор – может и сам на что-то сгожусь
 - Голос
 - Биометрические данные
 - Поведение пользователя

Сценарий 1: Key-logger ---- KeyPad

• Атака

- Троянское программное обеспечение попало на компьютер.
- Key-logger фиксирует последовательности нажатия пользователем на клавиши и пересылает их злоумышленникам.
- Мошенник получает информацию по электронной почте, FTP или при помощи другого транспорта.
- Злоумышленники продают идентификационные данные на черном рынке.

• Оборона

- Для ввода пароля применяется KeyPad (виртуальная клавиатура).
- Пароль вводится при помощи мыши. Пользователь выбирает символы на изображении клавиатуры, нажимая на кнопку.
- Координаты пикселей X и Y, которые выбрал пользователь передаются на сервер для преобразования в пароль. Координаты пикселей в разных сессия отличаются.
- Перехватывать не чего

ASA: Виртуальное клавиатура - KeyPad

Сдвиг:

Сессия А

Сессия В



Сценарий 2 : Phishing --- Персонализация

• Атака

- Мошенники создают дубликат веб-сайта банка X.
- Они посылают множество почтовых сообщений клиентам банка X, например, с предупреждением о блокировке счета. В сообщениях присутствует ссылка на псевдо сайт.
- Клиент банка X получает сообщение и переходит по ссылке на сайт мошенников.
- Клиент вводит свой ID для входа в банковское приложение. Мошенники получают доступ к счетам клиента.

• Оборона

- Для ввода пароля применяется KeyPad (виртуальная клавиатура).
- Получив письмо клиент переходит на сайт мошенников, вводит свое имя и видит....
- Виртуальная клавиатура, если она и появляется содержит отпечаток времени не совпадающим с текущим, фоновое изображение и фраза не знакомо клиенту.
- Так, как виртуальная клавиатура не знакома клиенту, он не вводит своего пароля.
- Учетные данные пользователя не похищены

ASA: Виртуальное устройство - KeyPad

Персональное изображение



Отметка текущего времени

Известная фраза

Сценарий 3: Украденные ID --- ARM

• Атака

- Идентификационные данные украдены до внедрения ОААМ.
- Мошенники продали информацию о клиентах банка X на черном рынке.
- Другие злоумышленники пытаются воспользоваться учетными данными клиентов и перевести средства клиентов банка на оффшорные счета.

• Оборона

- Для достижения своей цели мошенники должны пройти множество точек проверки на безопасность. В каждой точке применяются политики безопасности и оценивается риск.
- *Вар. 1:* Злоумышленники пытаются замести следы и используют анонимный прокси сервер. На что система реагирует предложением ответить на дополнительные вопросы. Мошенники остановлены.
- *Вар. 2:* Злоумышленники используют не зарегистрированное за клиентом устройство. Система требует подтверждение личности. Мошенники остановлены.

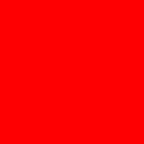
Сценарий 4: Session Hijack --- QuestionPad

• Атака

- Мошенники устанавливают внешний контроль над сайтом банка X.
- Они посылают множество почтовых сообщений клиентам банка X, с просьбой о проверки счетов.
- Клиенты банка X получают корреспонденцию, читают и заходят на сайт.
- Вводят идентификационные данные, проверяют баланс и покидают сайт.
- Злоумышленники перехватывают контекст сессии, переводят деньги на оффшорные счета.

• Оборона

- Клиенты вводят идентификационные данные, проверяют баланс и покидают сайт
- Злоумышленники перехватывают контекст сессии, пытаются перевести деньги на другой счет.
- В ОААМ срабатывают политики оценивающие последовательность действий клиента или его поведение.
- Система реагирует предложением ответить на дополнительные вопросы для уточнения личности клиента.
- Мошенники остановлены



OARM – средства администрирования и поддержки клиентов

Инструментальная панель OARM

- Мониторинг и анализ угроз в масштабе реального времени , сортировка сессий по степени вероятности мошенничества
- Настраиваемое представление по пользователям, устройствам, точкам входа в Сеть
- Мониторинг производительности системы



OARM – моделирование угроз

- Интерфейс для создания и конфигурирования правил и моделей
- Возможность редактирования моделей при проведении тестов и расследовании инцидентов

ORACLE Adaptive Risk Manager Online

DASHBOARD | QUERIES | ADMIN | AUDIT | CUSTOMER CARE | HELP |

ADMIN > MODELS

Description: This screen allows you to create or edit models.
Instructions: To modify the selected model, edit the name and / or description then click save.

Policy Type: Security Run Time: Post-Authentication Model Name: Fraud - Alert Only

Name: Fraud - Alert Only Description: Applied to groups with no challenge option. Only alerts are generated.
Status: Active
Scoring Engine: Maximum
Weight: 100

Save

Rules Manual Overrides Group Linking

Description: This screen is used for adding, configuring, and editing rule instances.
Instructions: Select a rule from the pull down to add and configure it OR select a configured rule from the list below to edit.

Rule: -- Pick One --

<input type="checkbox"/>	Rule Name	Status	Score	Weight	Date	Action Group	Description
<input type="checkbox"/>	Device multiple users	Active	1000	100	09/27/2007 14:25		Multiple users from this device
<input type="checkbox"/>	IP Max Users	Active	1000	100	09/27/2007 14:25		Multiple users trying to login from the same IP ad

OARM – работа с клиентами

Представитель службы поддержки может:

- Выяснить причину по которой был заблокирован пользователь или его действия
- Посмотреть важность предупреждения, и эскалировать его
- Выполнить действия, например, по временному разрешению доступа клиента к приложению

The screenshot displays the Oracle Adaptive Risk Manager (OARM) web interface. The header shows the Oracle logo and the text "Adaptive Risk Manager Online". Below the header is a navigation bar with links for "DASHBOARD", "QUERIES", "ADMIN", "AUDIT", "CUSTOMER CARE", and "HELP". The main content area is titled "CUSTOMER CARE > CASE DETAILS". It shows a case summary with a yellow flag icon and the following details:

Case Created: 09/27/2007	User Name: <u>nikki.burns</u>
Case Status: New	User Id: 78_dfe7a13aebf50666f0067c55b181c52c
Severity Level: Medium	Last Case Action: Access Case
Description: Generated Case	Date Of Last Case Action: 10/31/2007 06:56 (EST)
	Last Global Case Action: Access Case
	Date Of Last Global Case Action: 10/31/2007 06:56 (EST)
	Last Online Action: RegisterQuestionsQuestionPad
	Date Of Last Online Action: 09/27/2007 15:39 (EDT)
	Completed Registration: Yes
	Questions Active: No
	Personalization Active: Yes

Below the case details, there are three tabs: "Actions", "Log", and "Login". The "Actions" tab is active, showing a form with the following fields:

- Action:** Temporary Allow (dropdown menu)
- Allow:** Single Login (dropdown menu)
- Notes:** Authenticated (dropdown menu)

A text box contains the message: "This will allow the customer to bypass any blocks for a single login session." Below the text box is a "Submit" button.

ОААМ предлагает

- Мониторинг подозрительных операций, оцениваемых в правилах безопасности по
 - географическому расположению пользователей
 - типу устройств
 - типам транзакций и другим факторам, например, анализу поведения пользователей
- Механизм предупреждений и действий для сообщения администраторам об инцидентах и блокировки доступа к ресурсам приложений
- Защиту ID данных пользователей, даже в *скомпрометированном окружении*
- Простая интеграция с существующими способами аутентификации: tokens, certificates, smart cards

Кто использует ОААМ?

- Банки
- Кредитные организации
- Биржи
- ВВС США
- Здравоохранительные уч-я
- Университеты
- Страховые компании
- Пр-я электронной коммерции



Решения Oracle Identity & Access Management

Контроль доступа

Access Manager
Adaptive Access Manager
Enterprise Single Sign-On
Identity Federation
Web Services Manager

Администрирование ID-данных

Identity Manager

Службы каталогов

Virtual Directory
Internet Directory
(и Directory Integration Platform)

Аудит и контроль соответствия требованиям ИБ

Oracle Identity & Access Management Suite

Управление

Oracle Enterprise Manager for Identity Management

Решения Oracle Identity & Access Management

Контроль доступа	Администрирование ID-данных	Службы каталогов
<p>Усиленная</p> <p>Аутентификация & Авторизация</p> <p>Оценка рисков</p> <p>Однократная регистрация (SSO)</p> <p>Федеративный SSO</p> <p>Безопасность Web-сервисов</p>	<p>Защита ID-данных</p> <p>Жизненный цикл учетных записей</p> <p>Роли и группы</p> <p>Согласование и доставка идентификационных данных</p> <p>Автоматизация внедрения политик безопасности</p>	<p>Виртуализация</p> <p>Хранение</p> <p>Синхронизация</p>

Аудит и контроль соответствия требованиям ИБ

Аудит данных	Выявление мошенничества	Аттестация	Разделение обязанностей	Контроль
--------------	--------------------------------	------------	-------------------------	----------

Управление

Уровни сервиса	Конфигурирование	Анализ рисков	Производительность	Автоматизация
----------------	------------------	----------------------	--------------------	---------------



O & A



ORACLE IS THE INFORMATION COMPANY