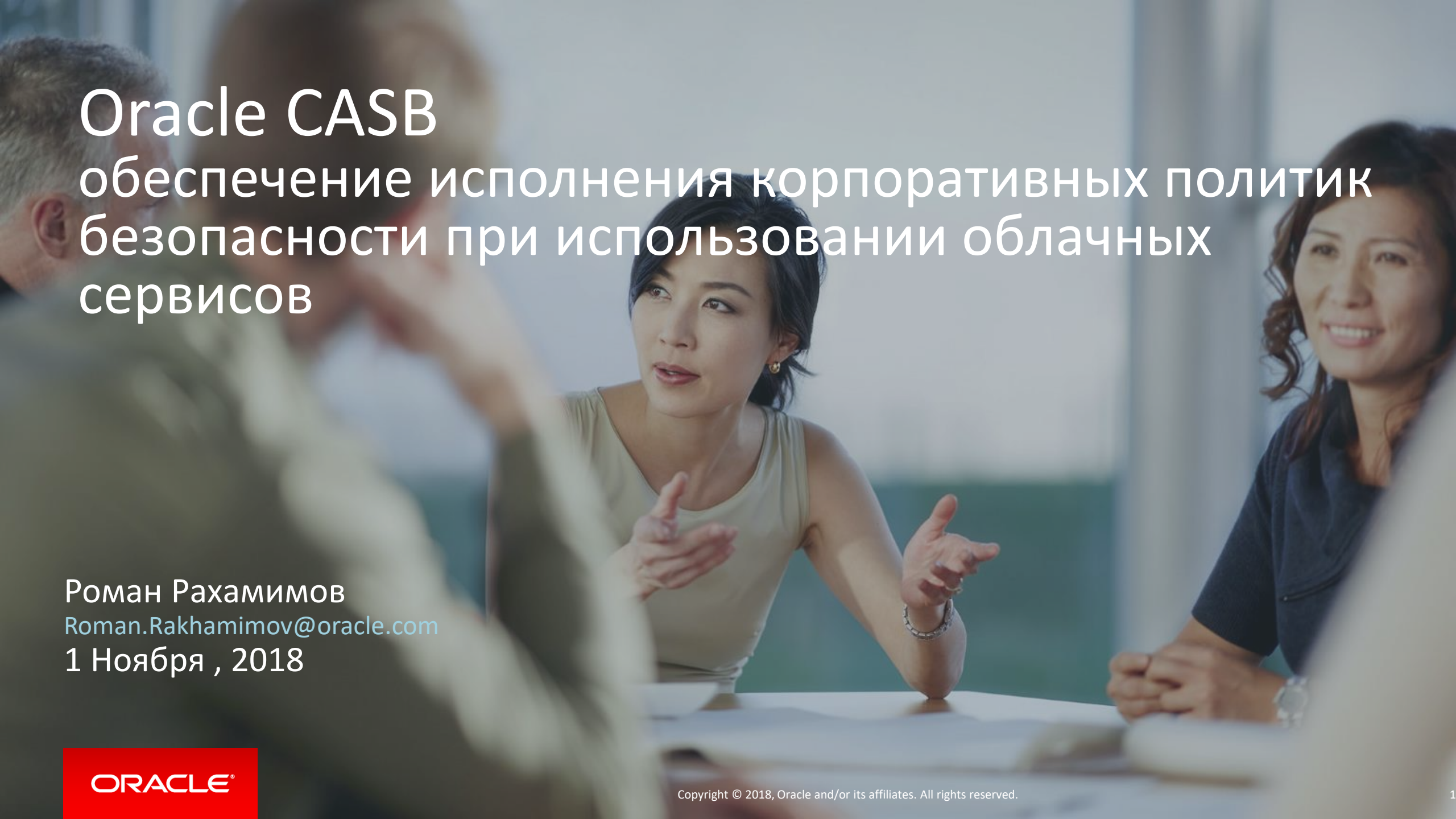
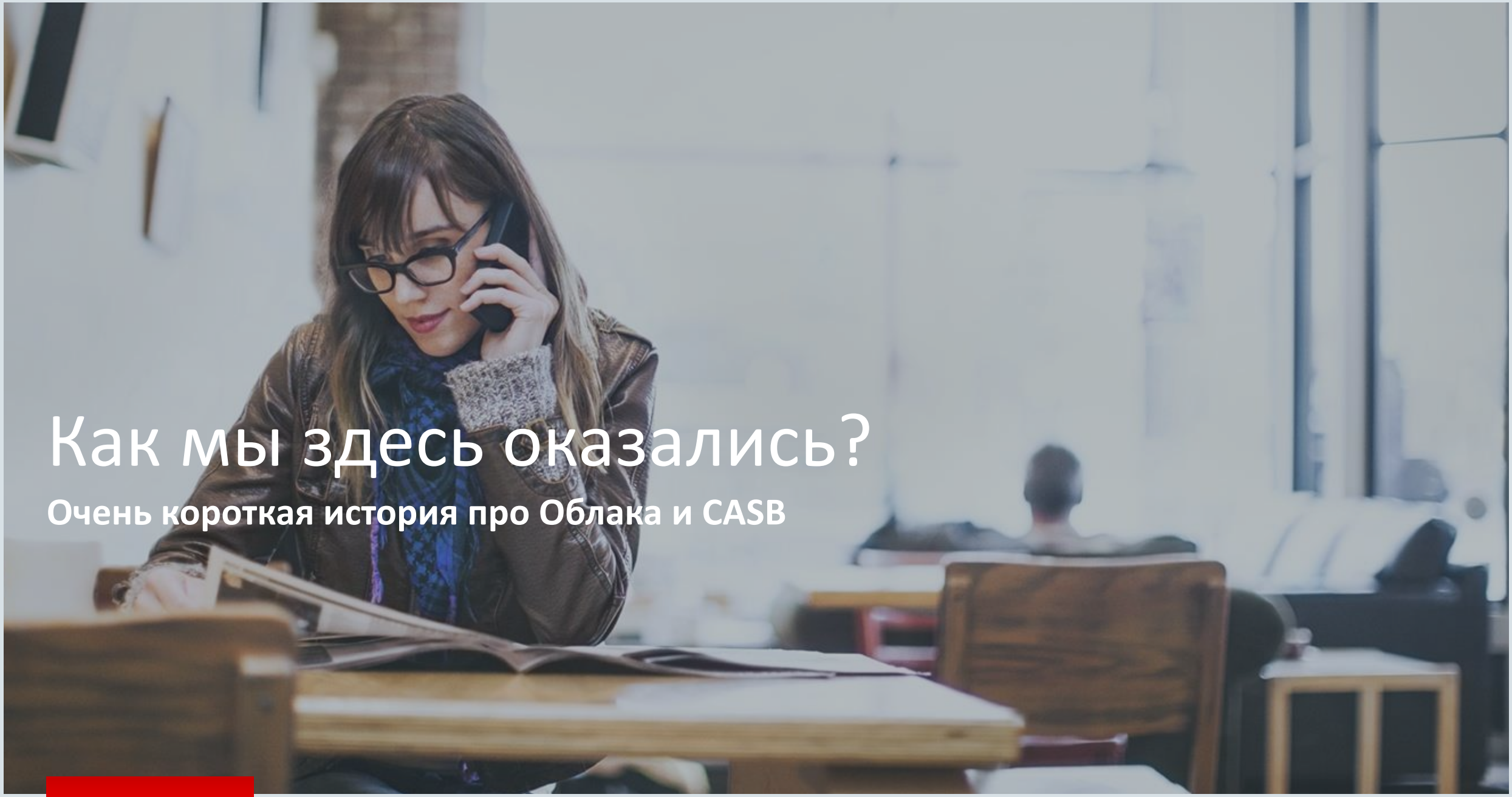


Oracle CASB
обеспечение исполнения корпоративных политик безопасности при использовании облачных сервисов

Роман Рахамимов
Roman.Rakhamimov@oracle.com
1 Ноября , 2018

ORACLE



Как мы здесь оказались?

Очень короткая история про Облака и CASB

Основные тенденции развития

Облачные сервисы - это новая норма

- **83%** глобального трафика к 2019 году будет исходить от облачных сервисов и приложений
- **42%** организаций в финансовом секторе используют SaaS
- **$22.4B** объем рынка IaaS в 2016 году

Эрозия периметра сети

- **50%** работодателей потребует BYOD к 2018 году
- **73%** рост мобильных устройств с 2014 по 2018 год
- **86%** всех рабочих нагрузок в облаке к 2019 году не через локальных пользователей и через неуправляемые устройства

Степень угроз возрастает, профессионалов не хватает

- **1.5M** всемирный дефицит специалистов по безопасности к 2019 году
- **95%** всех уязвимостей облаке к 2020 году будет человеческая ошибка

Рост числа обнаруженных утечек в AWS за последние несколько лет…

Configuration Error Leads to Another Amazon Web Services Data Breach

The records of nearly 200 million U.S. voters were compromised.

NEWS

Hacker puts 'full redundancy' code-hosting firm out of business

Error Exposes 1.5 Million People's Private Medical Records on Amazon Web Services [UPDATED]

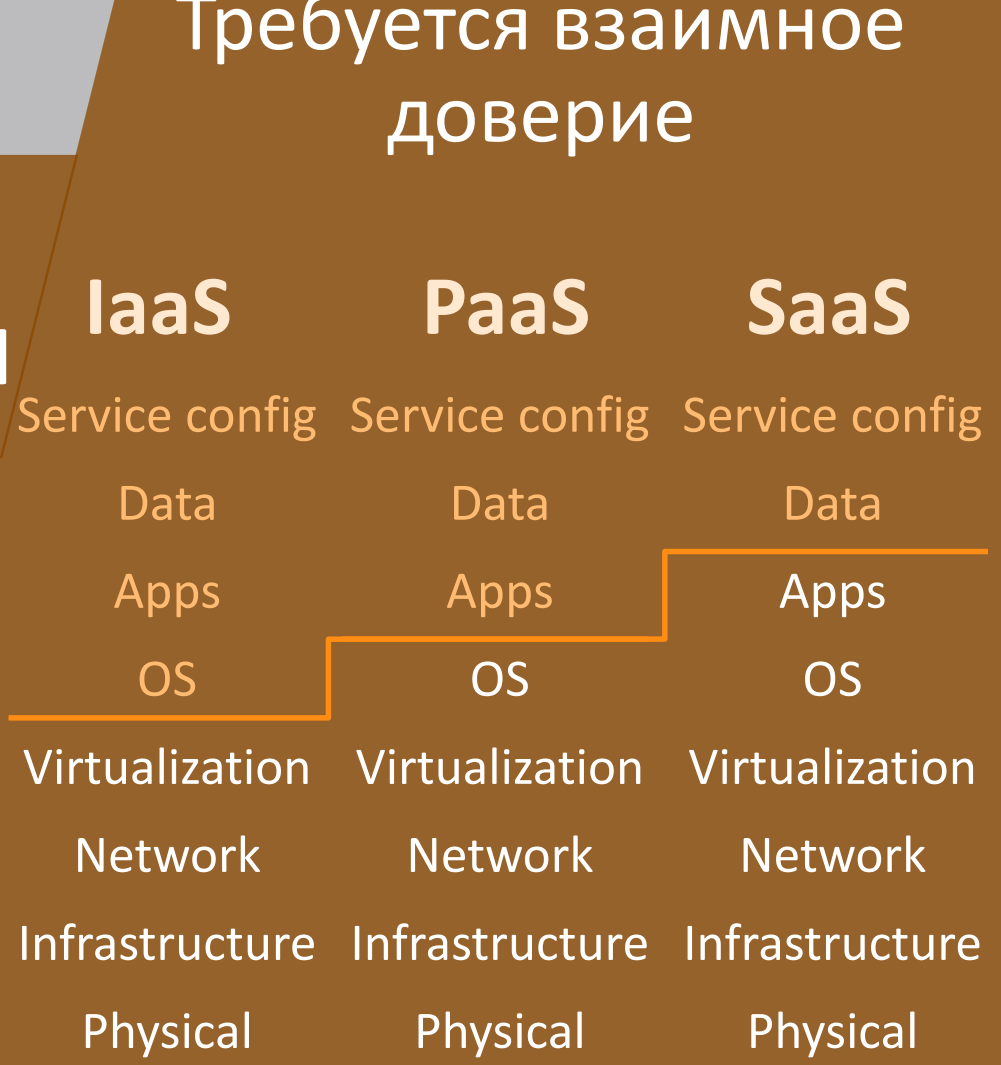
Cloud Leak: WSJ Parent Company Dow Jones Exposed Customer Data

OneLogin suffers breach—customer data said to be exposed, decrypted

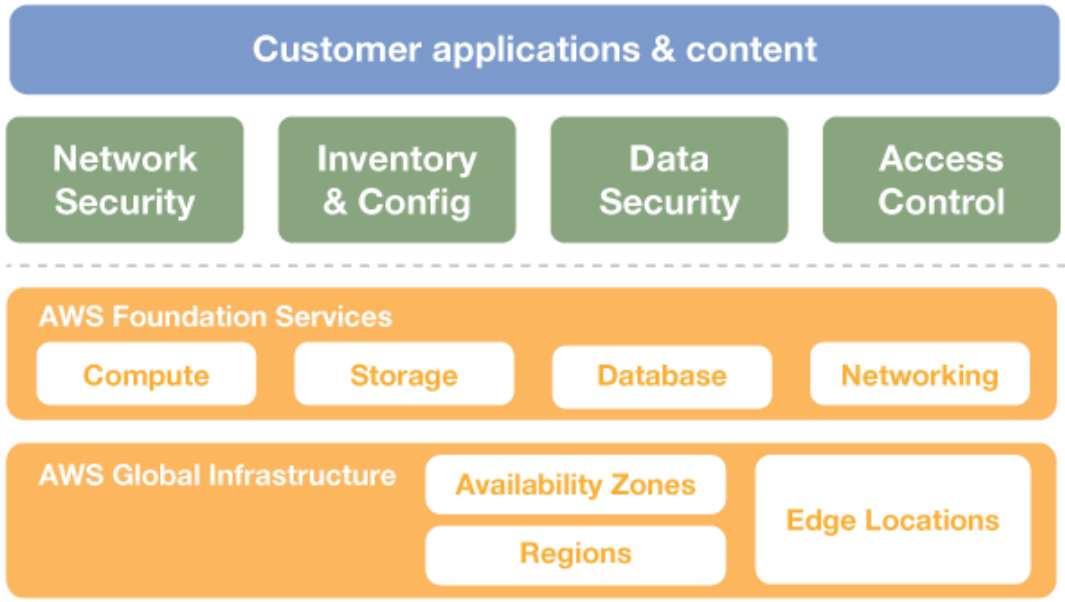
Customer account-only support page warns of "ability to decrypt encrypted data."

Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server

Ответственность в модели разделяемой безопасности



Понимание общей ответственности



You define your controls **'in'** the Cloud

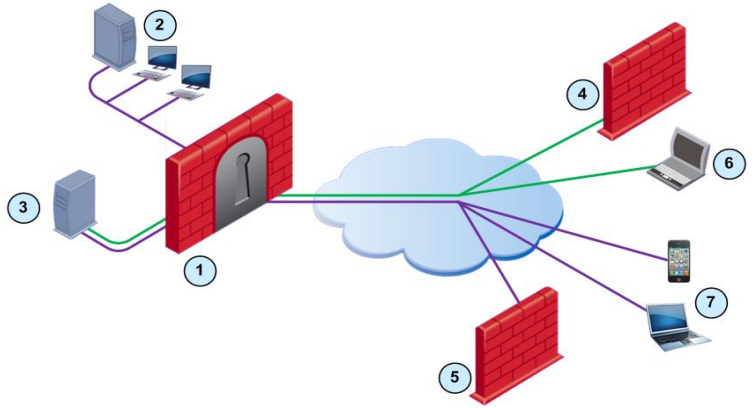
AWS takes care of the security **'of'** the Cloud

- Ошибка в настройках произойдет специально или неумышленно
- Незашифрованные данные могут попасть в Сеть, это опасно
- Следите за администраторами
- Следите за публичным доступом, группами, параметрами доступа, ключами и изменением конфигурационных настроек

CASB – "Caz-bee? Хм…"

- "Cloud Access Security Broker"
- Термин появился с подачи Гартнера 2012
- "Broker" – подразумевает переход между чем-то, некоторую абстракцию, некоторые шлюзы

Cloud Access Security Brokers – Какими они бывают?



- **Perimeter/Agent-centric**
  - Основной фокус на Исполнении, Предотвращении & Контроле Доступа
  - Проверка пакетов & DLP
  - Не простое развертывание
  - Проблемы, связанные с производительностью, масштабированием, задержкой и «глубиной»,

- **API-centric**
  - Основной фокус на обнаружение, Анализ & Управление
  - Бесшовная интеграция с приложениями
  - Быстрое развертывание
  - Отсутствие влияния на производительность или пользователя
  - *Обычно не применяется для DLP*

Oracle CASB Cloud Service

Безопасный доступ

Безопасная работа

Найти

- Теневые и скрытые IT ресурсы
- Оценка риска
- Показатели скомпрометированности

Обеспечить безопасность

- Данные
- Соблюдение требований
- Обеспечение безопасных настроек
- Интеллектуальный поиск угроз

Проконтролировать

- Активность
- Конфигурации
- Транзакции
- Контент
- Политики

Отреагировать

- Автоматический ответ на инцидент
- Интеграция с системами управления ИТ-услугами (ITSM)

Обеспечение облачной безопасности

Мои бизнес-критические приложения требуют мониторинга безопасности и соответствия требованиям!

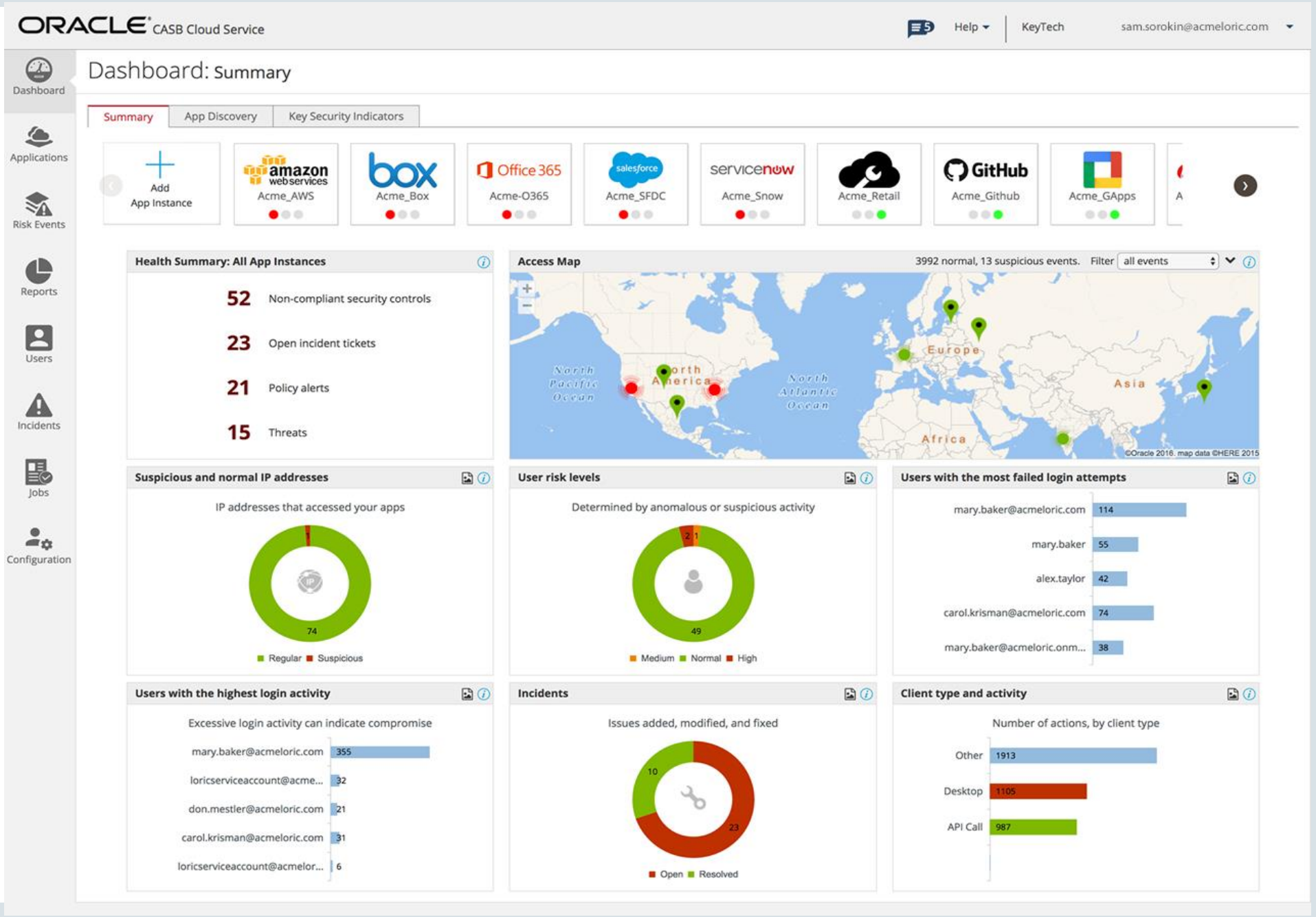
amazon web services · Office 365 · salesforce · Google Apps · Microsoft Azure · okta · servicenow · rackspace · box · GitHub · ORACLE

- Включая Oracle HCM, ERP, CX

Я хочу видеть все используемые сотрудниками облачные приложения! (Shadow IT)

ORACLE

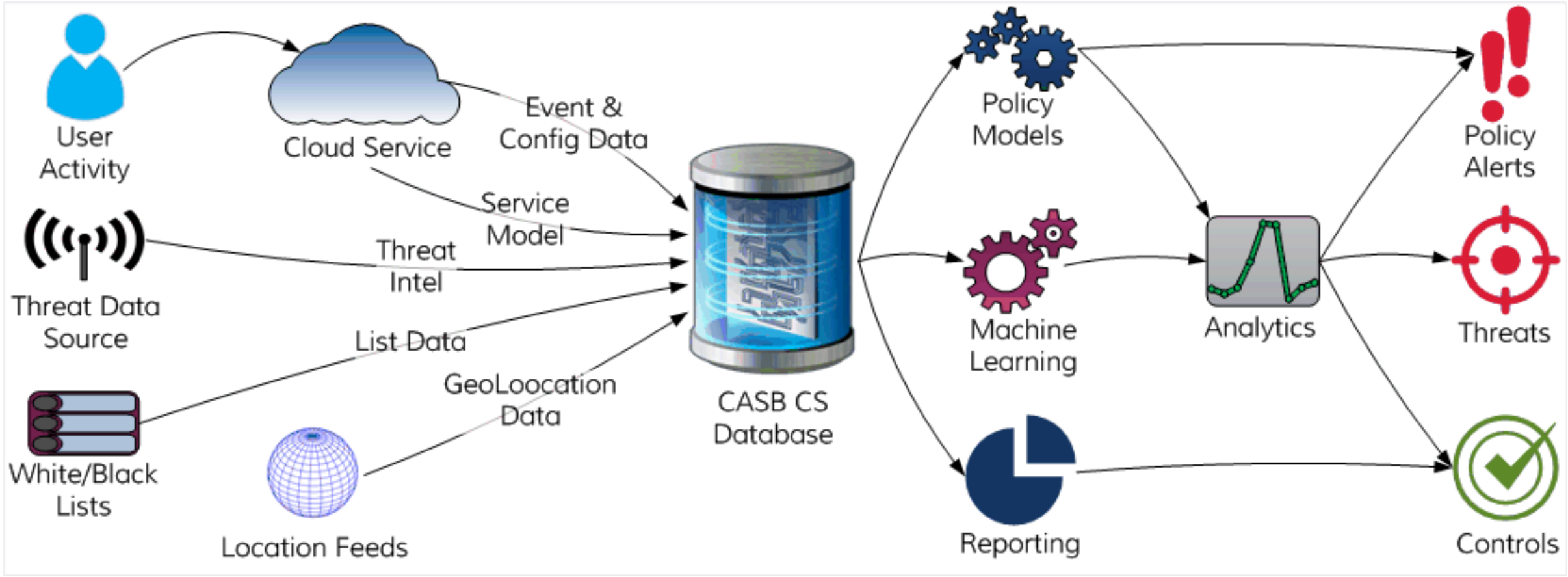
Oracle CASB



Oracle CASB – схема работы

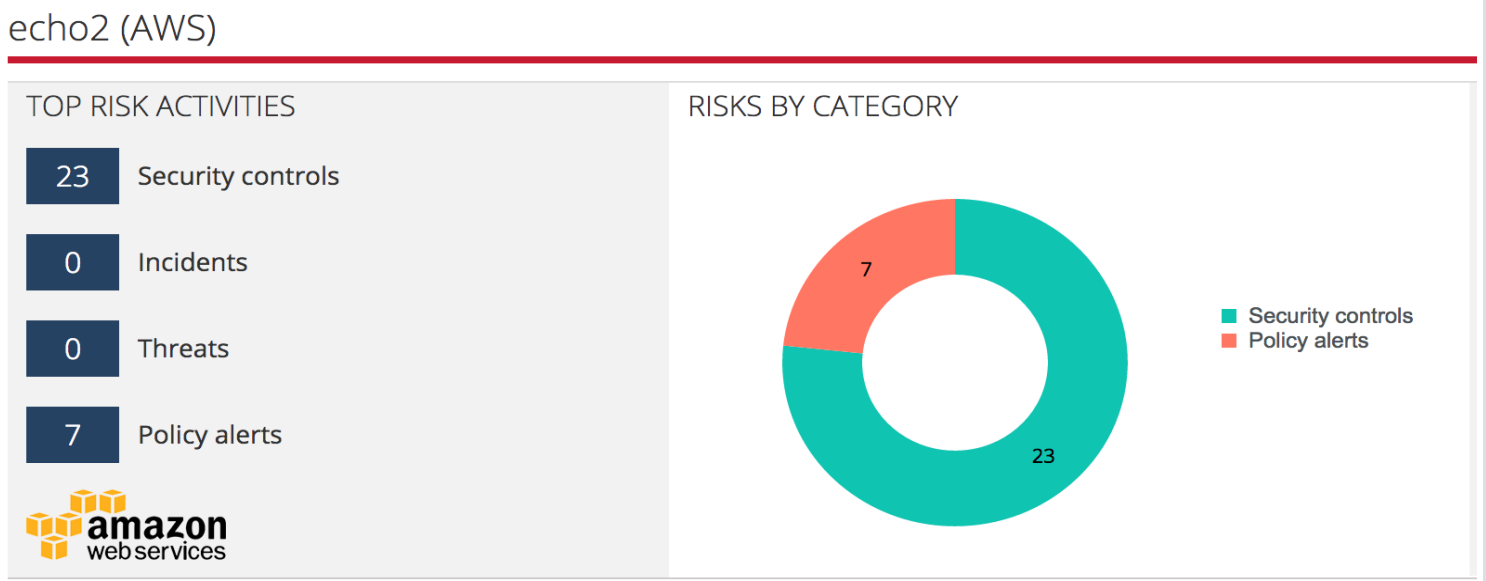
Security-as-a-Service: Без оборудования/ Без ПО/ Без агентов = Быстрое развертывание

CASB CS – диаграмма потоков данных



Оценка риска – три типа контролируемых событий

- Настройки безопасности
- Угрозы
- Нарушение политик



Оценка риска – Настройки безопасности

- Определенные в CASB проверки настроек безопасности
- Часто логические настройки или одиночные значения
  - "SSL enabled"
  - "Password Minimum Length"
- CASB отслеживает «отклонение" от базовых настроек

Оценка риска - Угрозы

- Два типа
  - UBA генерирует предупреждение "Anomalous Behavior"
  - Интеллектуальный анализ угроз генерирует предупреждение "Suspicious Behavior"
- "CASB автоматически обнаруживает странное поведение и предупреждает специалиста безопасности "

Оценка риска – Нарушение политик

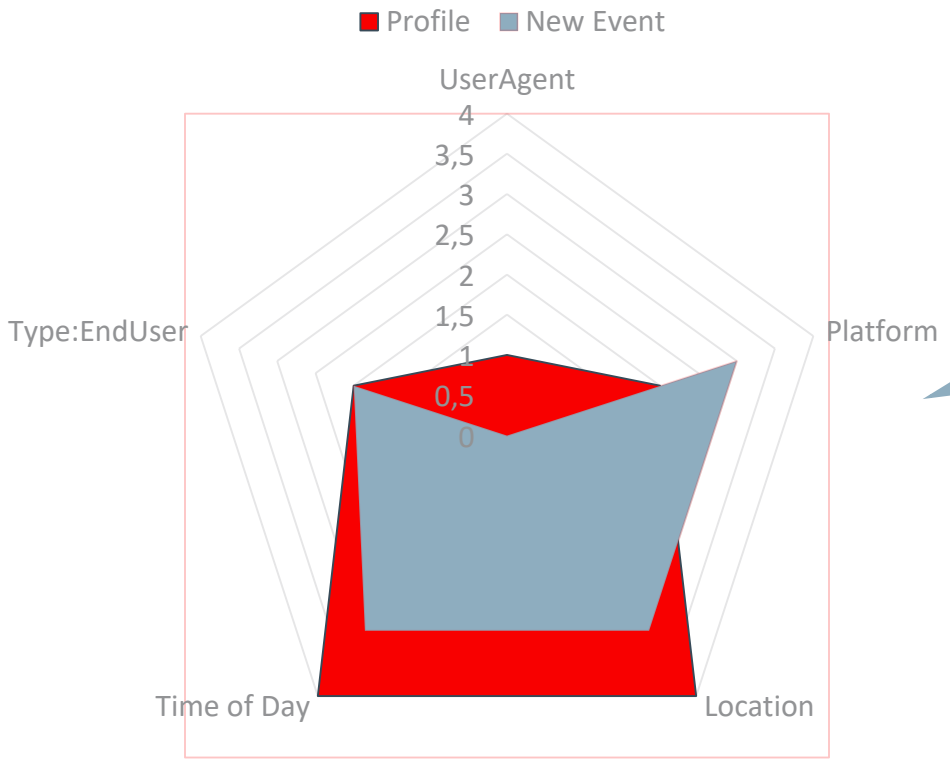
- Основанные на правилах, определенные и настроенные для каждого клиента
- Есть преднастроенные, рекомендованные “лучшими практиками”
- “ Я могу сказать CASB, о чем именно меня нужно предупреждать “

Примеры событий безопасности

- **Настройки безопасности(Security control)**
  - Password policies
  - Permissive network settings
  - Weak resource configurations
- **Нарушение политик (Policy alert)**
  - Resource type (Instance, User, File, Key, Object, etc.)
  - Resource instance (name, regex)
  - User/group inclusion/exclusion
  - Conditions (tags, IP, devices)
  - Free-form conditions
- **Пользователь (Anomalous activity)**
  - Credential hijack risks
  - Session hijack risks
  - Network access exposure
  - Rogue users
  - Brute force attempts
  - Excessive logins/attempts
  - Aberrant downloads/reads
  - Disproportionate sessions
  - Atypical usage (e.g. unusual API access attempts)

Схема работы машинного обучения – «Угрозы нет»

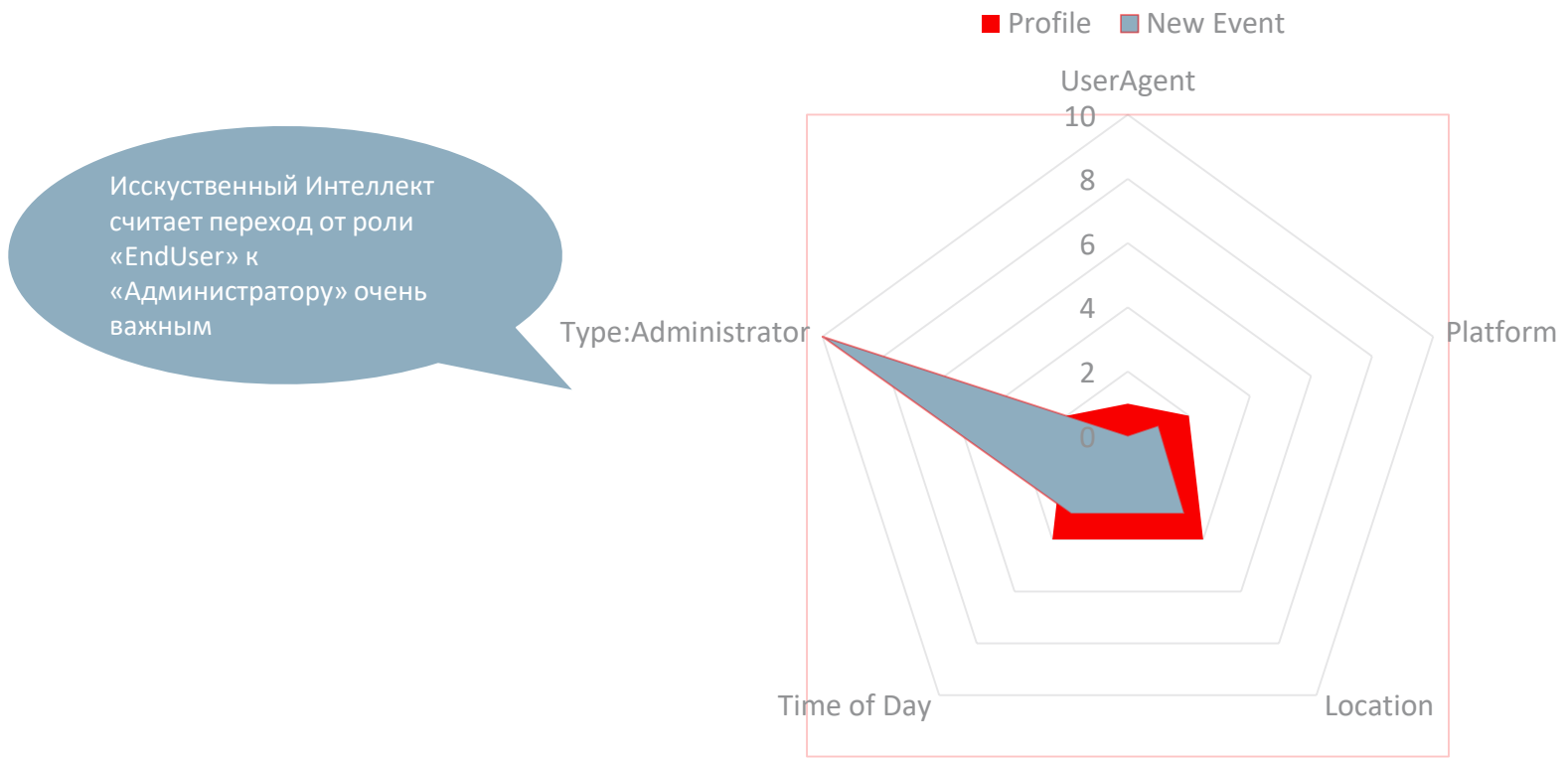
Machine Learning определяет форму с использованием весового коэффицента по оси



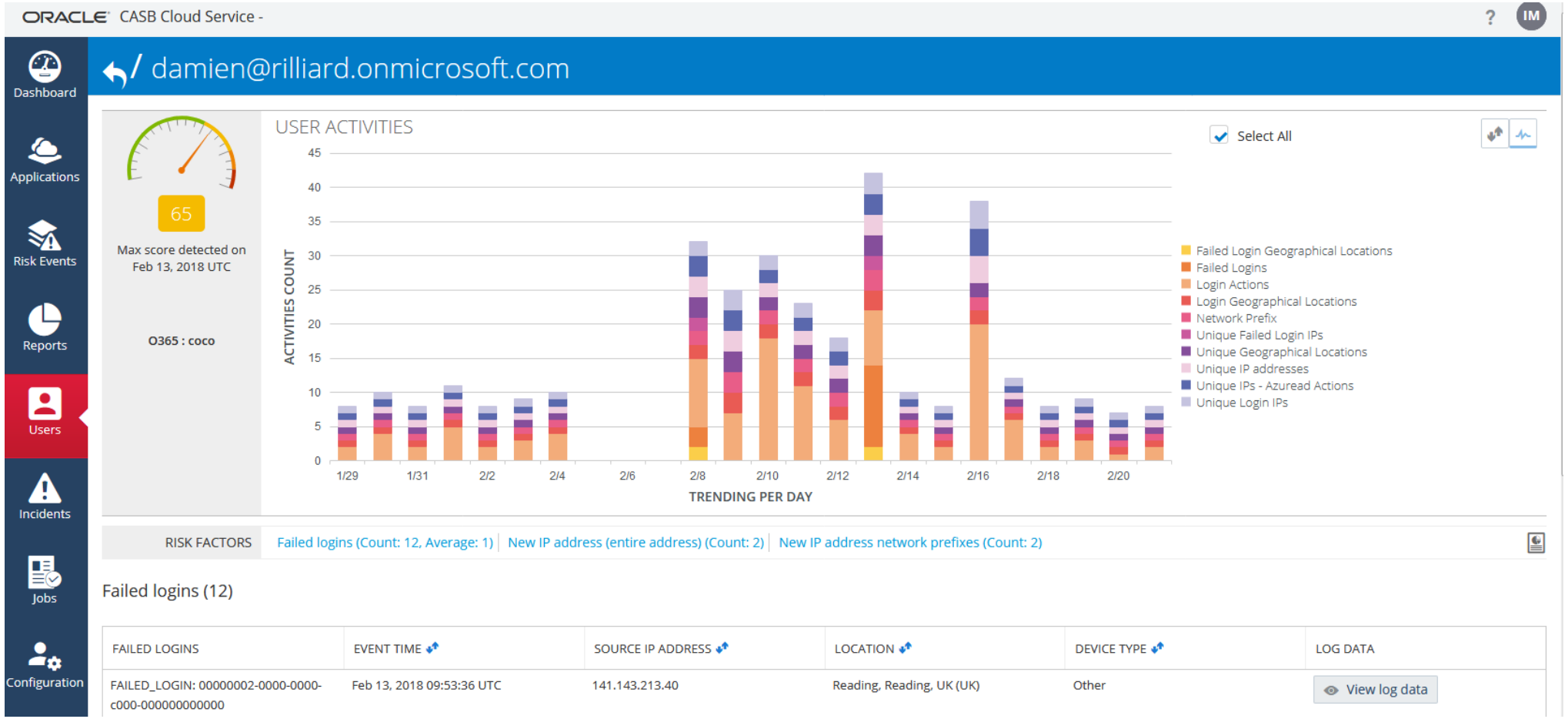
Исскуственный Интеллект не считает, что изменение «Платформы» очень важно. Пользователь просто использовал свой телефон.

Схема работы машинного обучения – «Угроза»

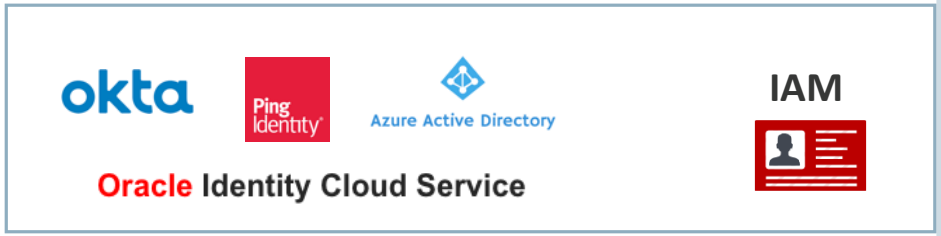
Machine Learning определяет форму с использованием весового коэффицента по оси



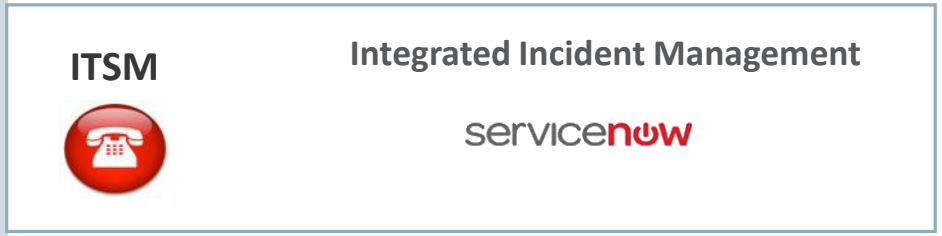
Машинное обучение – пример из жизни

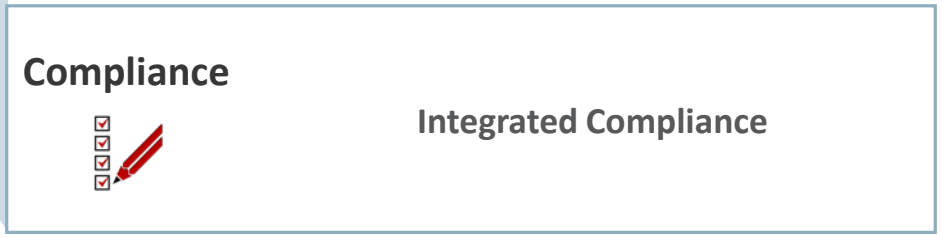


Oracle CASB и възможности интеграции



Oracle CASB Cloud Service





Oracle’s Cloud Security - компоненты


ORACLE®