ORACLE

Демонстрация технологий безопасности Oracle

Безопасность OCI, WAF, API Gateway, IDaaS, CASB, Identity & Access Management и другое

Олег Файницкий
CISSP, CCSP, OCI OCP, PhD., OEA, Master Principal Sales Consultant
Oracle Identity Management & Cybersecurity

Oracle Online Security Day
22.10.2020

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

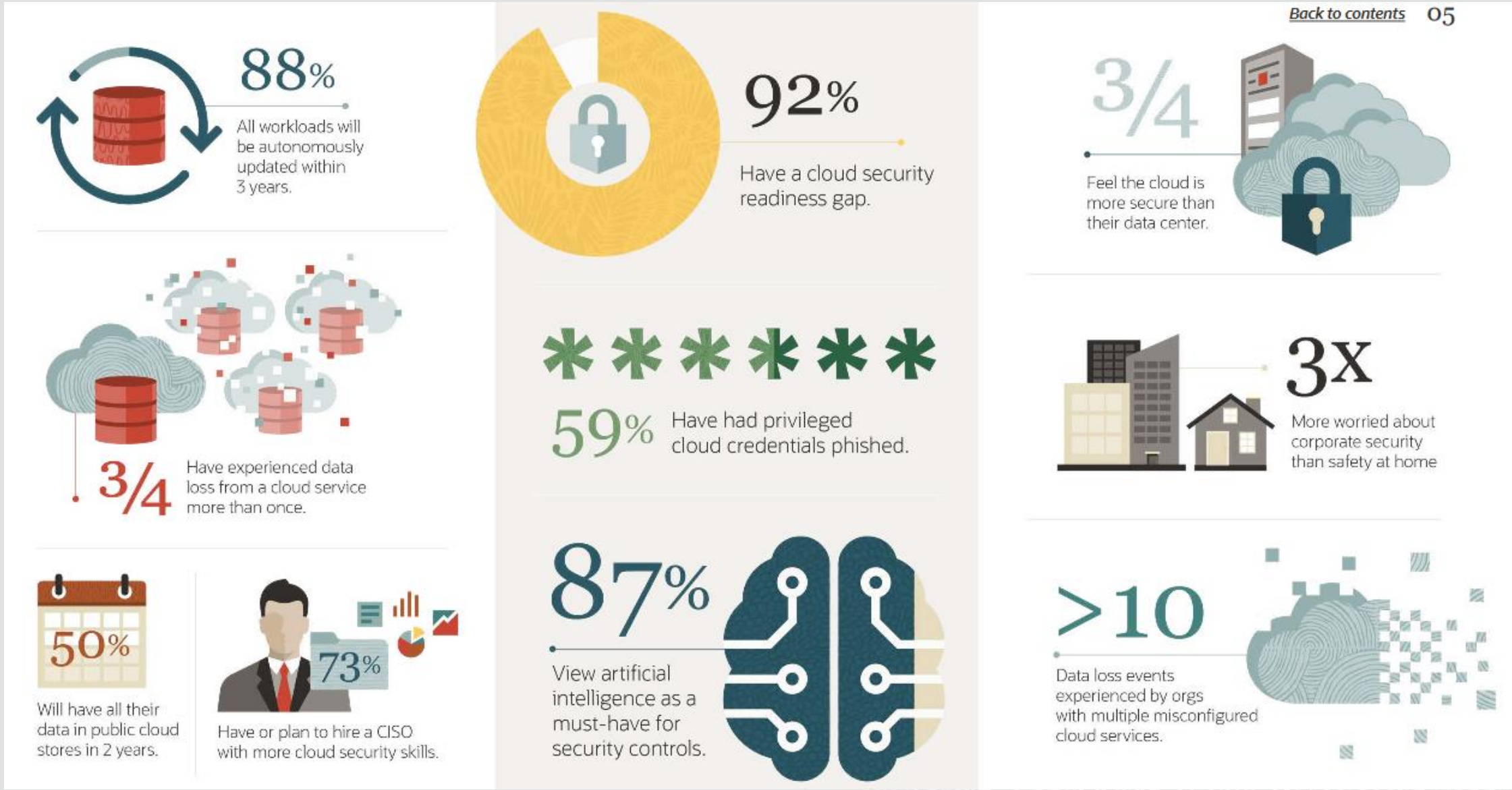
The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Содержание

Безопасность Oracle Cloud Infrastructure 2.0 (OCI)

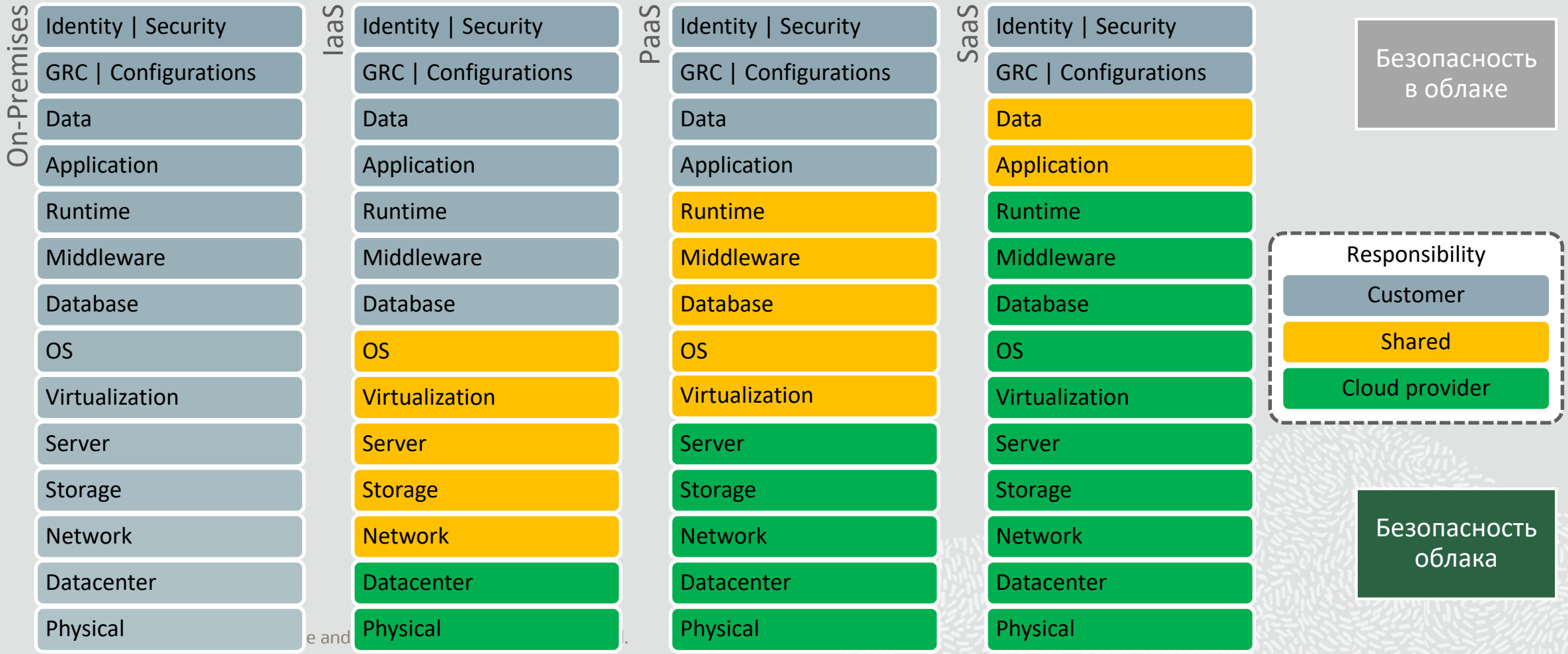
Обзор (15 мин)

Безопаснее ли в облаках? (Oracle & KPMG отчет)

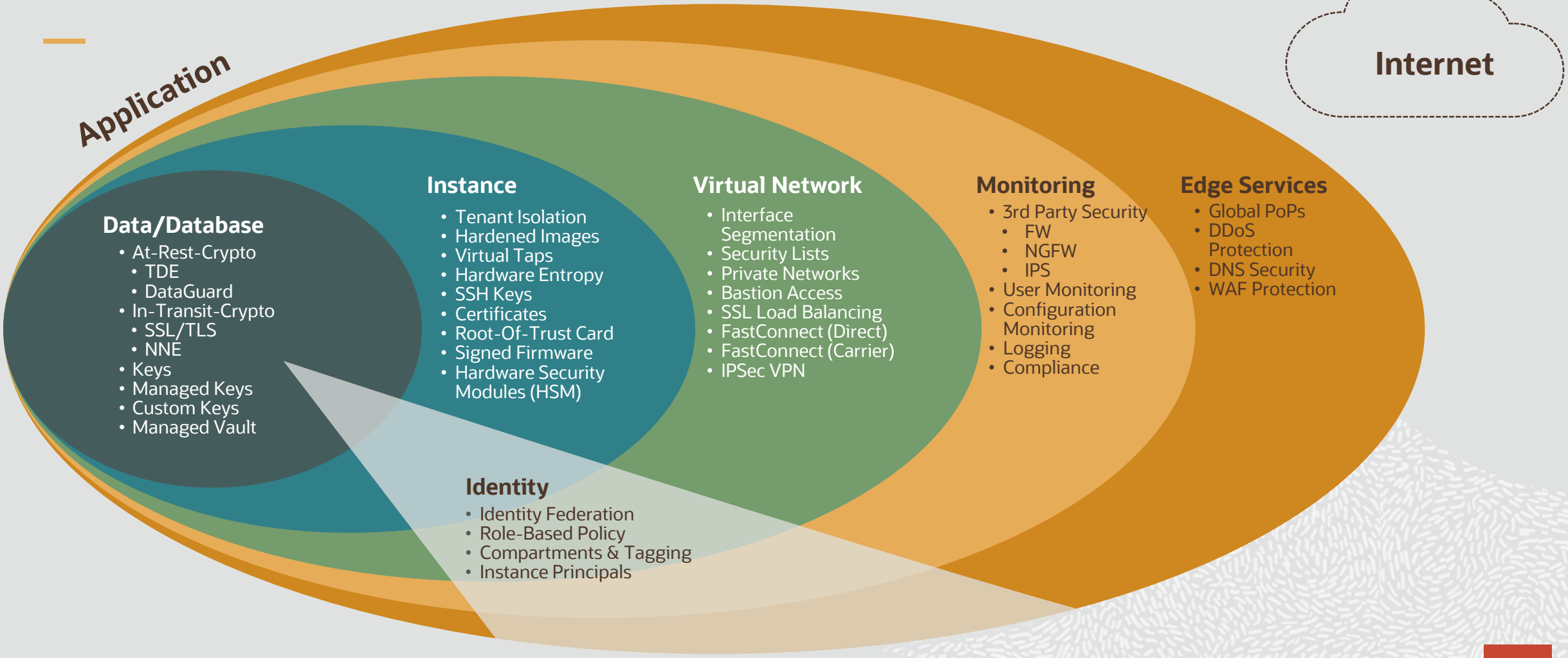


https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf

Разделение ответственности в облаке

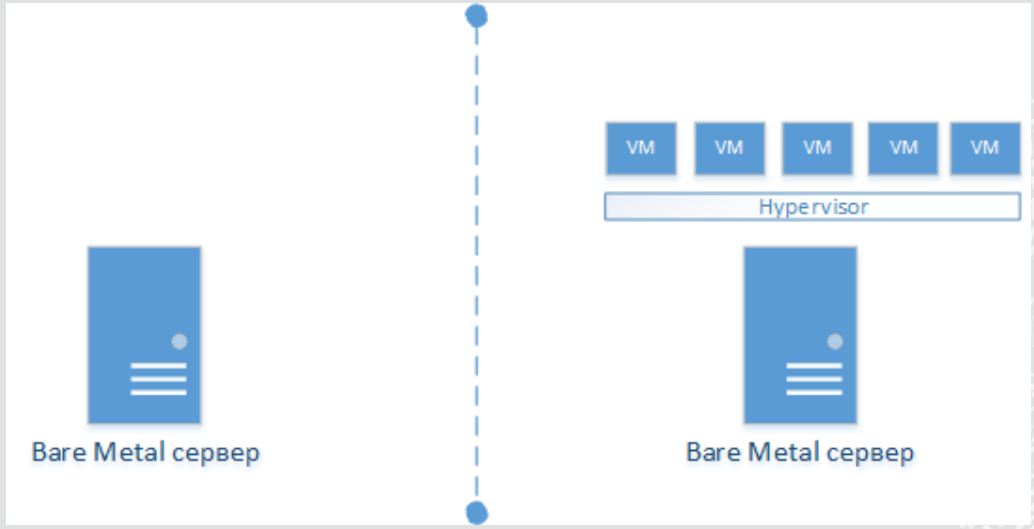


Стратегия облачной безопасности Oracle



Изоляция (Customer Isolation)

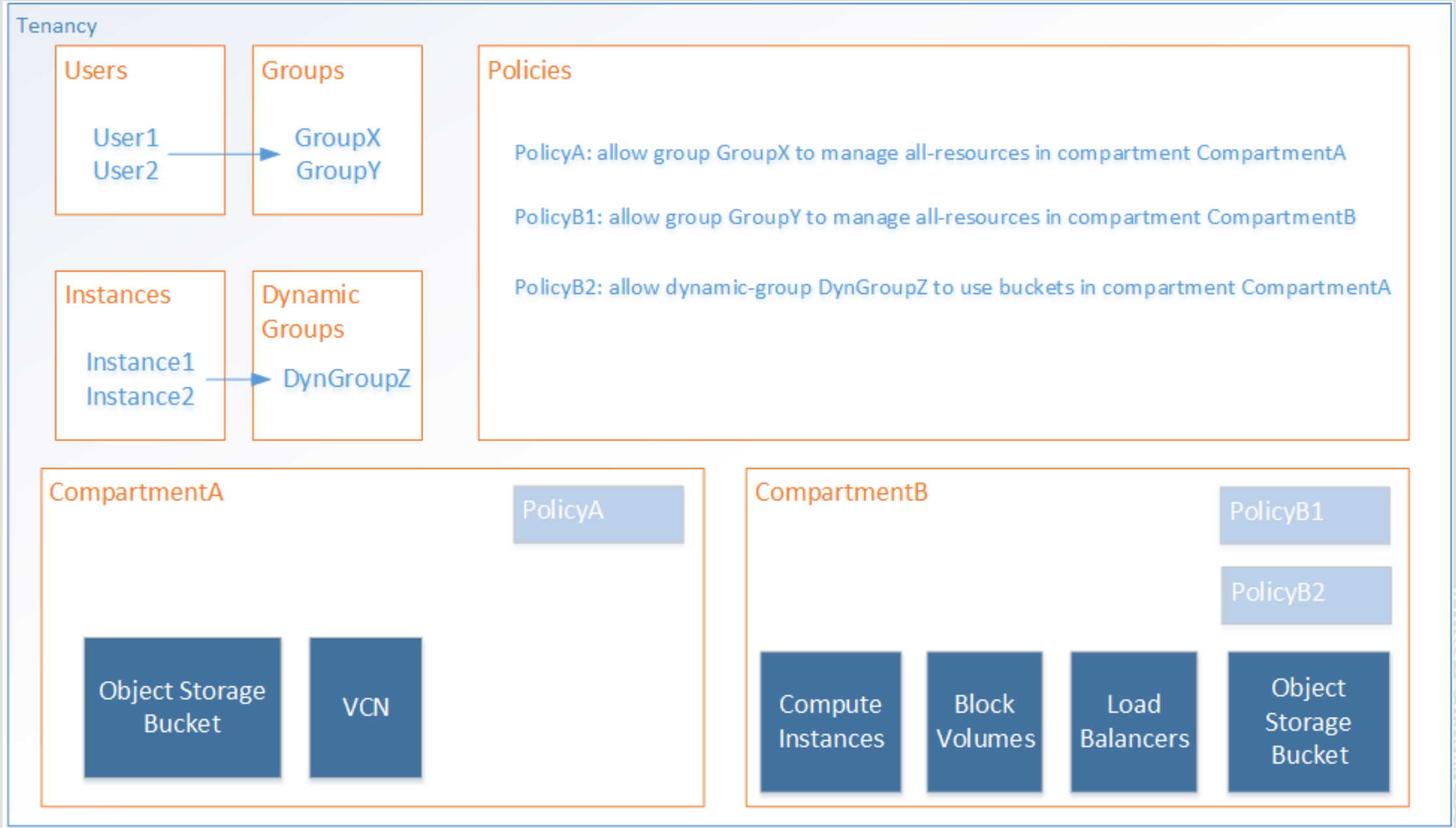
- Два вида изоляции
  - Tenant-level – изоляция от «шумных соседей» и от сотрудников Oracle (Bare Metal Compute, VCN / Subnets, Data-at-rest шифрование)
    - Compute: Bare Metal, Dedicated VM Host
    - VCN различных тенантов изолированы на уровне OSI L3
    - Public / Private подсети, VCN Peering, Security Lists, Network Security Groups
    - Service Gateway для доступа к сервисам OCI из private subnet
  - Resource level – изоляция внутри тенанта (Compartments / IAM policies)



Шифрование данных (Data Encryption)

- Шифрование хранилищ данных
  - Block Storage / Boot Volumes - шифрование At-rest (AES256), ключи автоматически генерируются Oracle или берутся из KMS Vault, In-transit шифрование (возможно для PARAVIRTUALIZED режима)
  - Object Storage – client-side шифрование ключами заказчика, шифрование At-rest (AES256) ключами, управляемыми Oracle (или через Key Management Service), TLS для In-transit
  - File System Storage – шифрование At-rest (AES256) ключами, управляемыми Oracle (или через Key Management Service), In-transit
  - Data Transfer Service – стандартные утилиты Linux dm-crypt и LUKS
- Шифрование на уровне СУБД (ATP, ADW, DB Systems)
  - At-rest – Oracle TDE для файлов СУБД и бэкапов, Key Store / Wallet для мастер-ключа
  - Дополнительное шифрование бэкапов RMAN (опционально), бэкапы помещаются в Object Storage
  - In-transit – шифрование Oracle Net Services (AES, DES, 3DES, RC4)

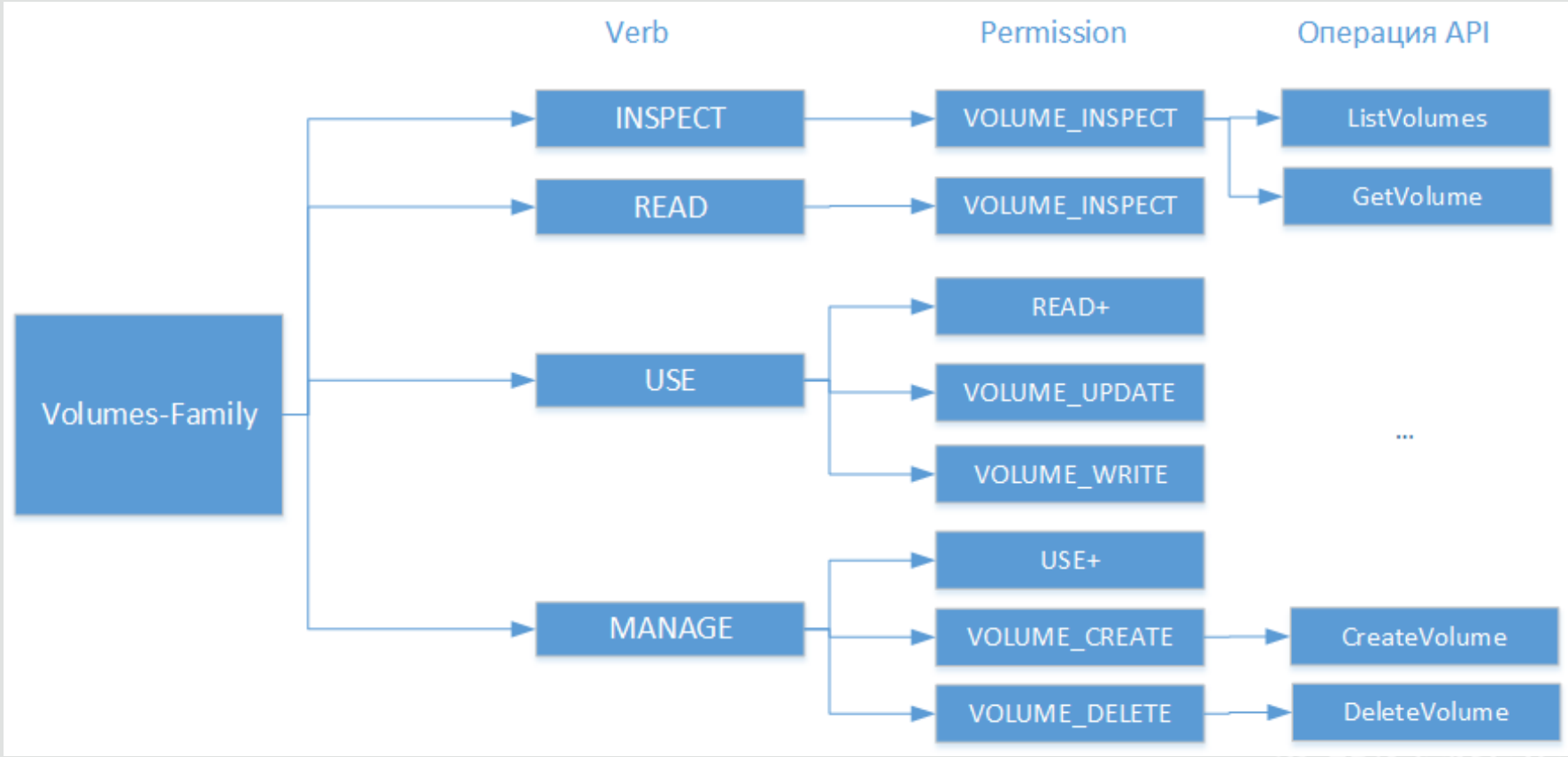
Security Controls: IAM (identity & access mgmt) сервис



Security Controls: Аутентификация

- Имя пользователя / пароль для доступа в OCI консоль
- API Signing Key для доступа к REST API
  - Вызов REST API через TLS1.2
  - Private-ключ располагается только на стороне заказчика, в OCI хранится только Public-ключ
  - Пара ключей RSA 2048-bit
- Пара SSH-ключей для аутентификации в Compute Instance (для Linux)
  - 2048-bit RSA или DSA, 128-bit ECC
- Auth-токены
  - Для интеграции с 3rd party API, которые не поддерживают API signing key
- Multifactor Authentication (MFA)
  - Через мобильное приложение – Oracle Mobile Authenticator, Google Authenticator (TOTP, Push-уведомления)
- Instance Principal – аутентификация для Compute Instance по сертификатам
- Федеративное SSO (в качестве IdP – Identity Cloud Service, Azure AD, любой SAML)

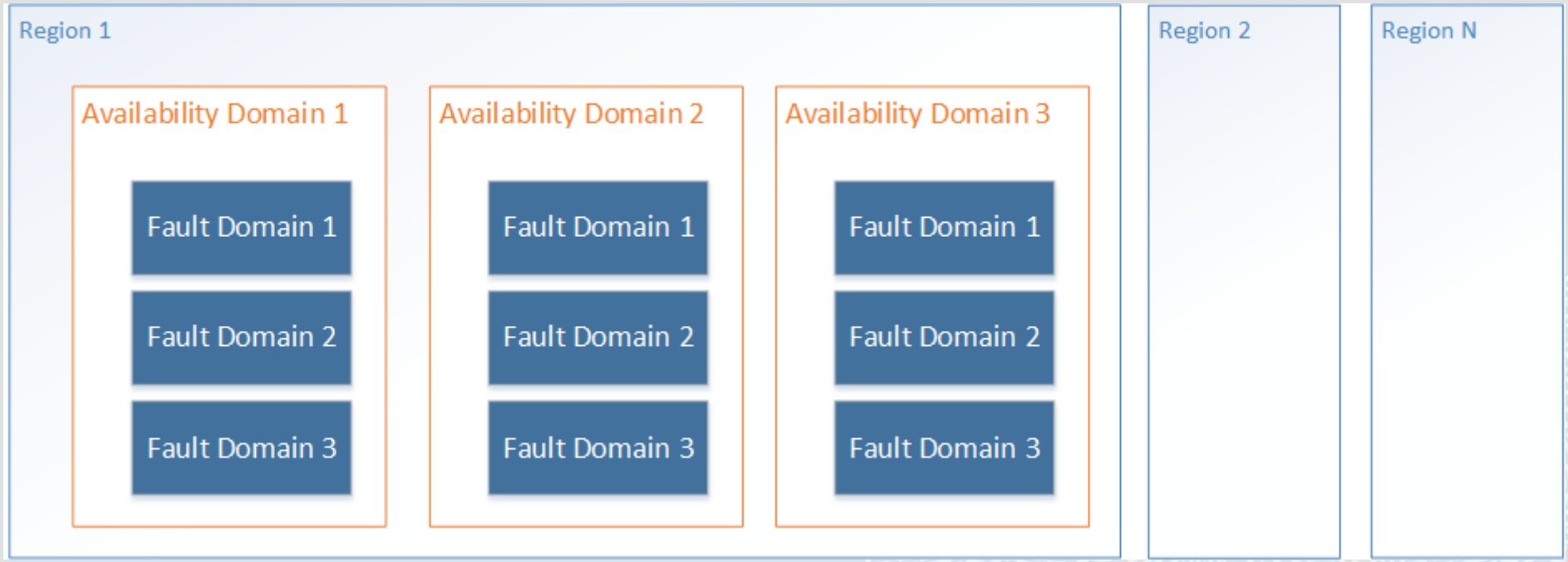
Security Controls: Авторизация



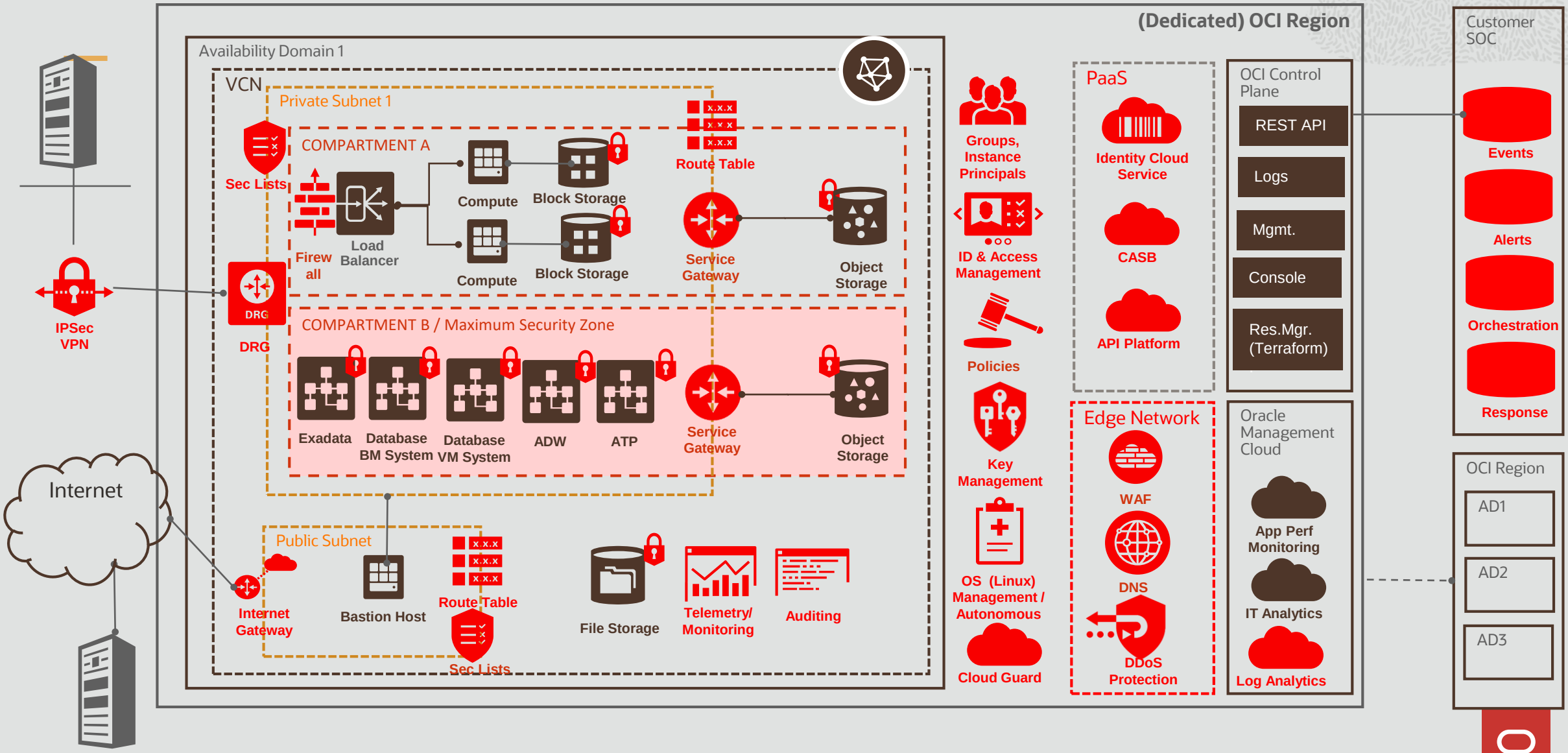
- Ресурсы OCI помещаются в контейнеры – Compartments, доступ к ресурсам внутри контейнера разграничивается IAM-политиками
  - Zero Trust – по умолчанию пользователи не имеют прав
- Политика: Allow <subject> to <verb> <resource-type> in <location> where <conditions>
  - Пример: allow dynamic-group FrontEnd to use load-balancers in compartment ProjectA

Высокая доступность

- 14+ OCI регионов, в каждом регионе – 3 (*) домена доступности (Availability Domain), в каждом домене доступности – три «домена отказа» (Fault Domain)
  - (*) – некоторые регионы временно с одним доменом доступности



OCI Security – все в одном

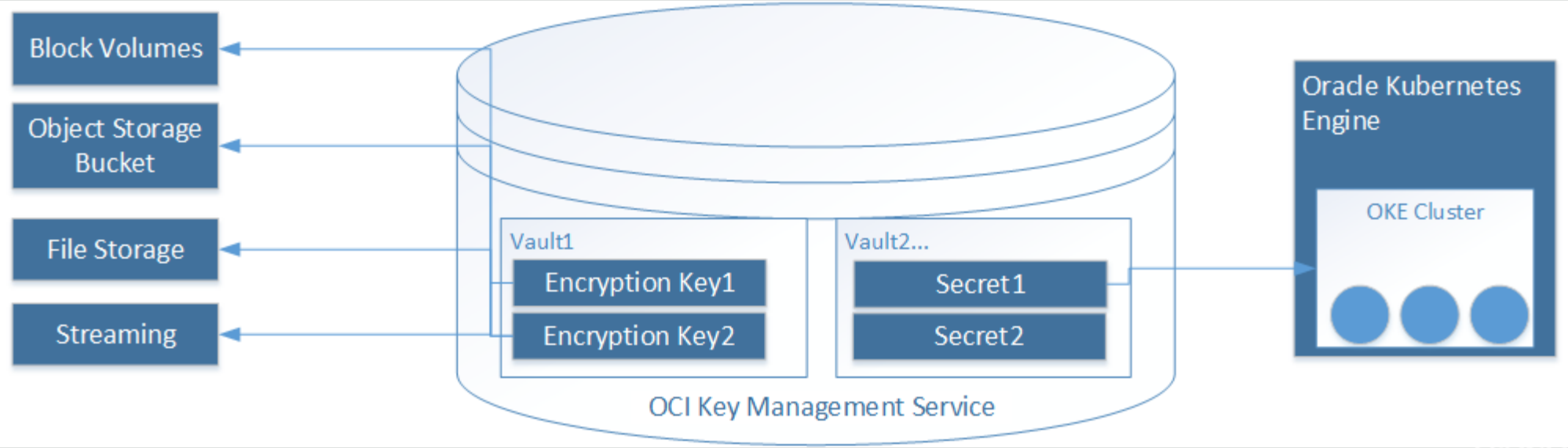


Сервисы безопасности OCI

OCI Web Application Firewall, OCI DNS Zone Management и OCI Key Management, архитектура безопасности типового приложения в OCI, обзор и демо (20 мин)

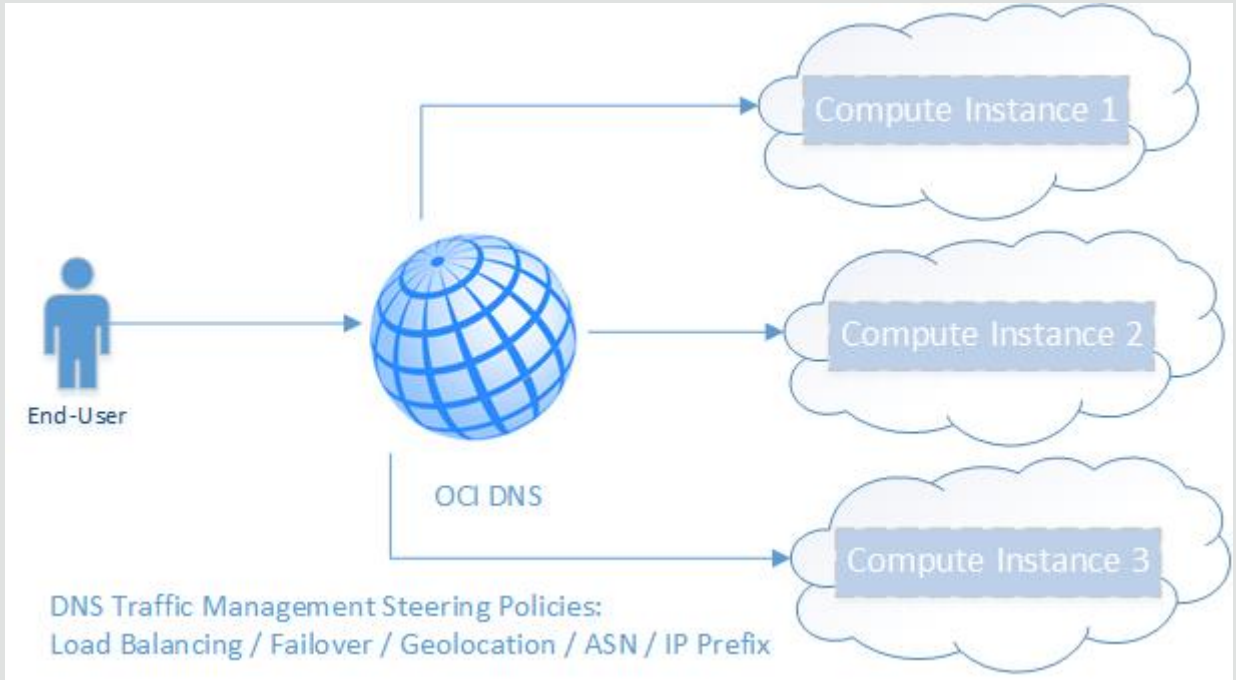
OCI Key Management

- Надежное и безопасное хранилище ключей
  - Управление ключами (create / delete, enable / disable, rotate), циклом жизни ключей (включая автоматическую ротацию)
  - HSM сертифицирован по FIPS 140-2 Security Level 3
  - “Bring your own key” – можно загружать собственные ключи
  - AES 128 / 192 / 256



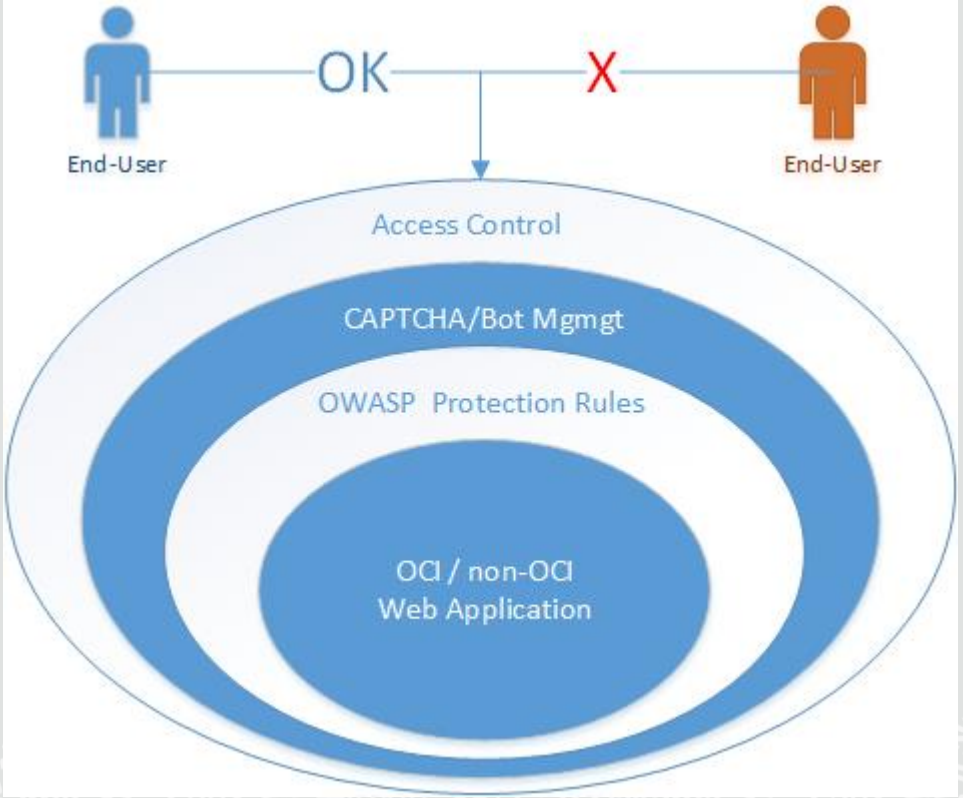
OCI DNS Zone Management

- Высокодоступный DNS сервис
  - Управление зонами и записями DNS
  - Импорт файлов DNS зон
  - Поддержка Secondary DNS
- Перенаправление трафика (DNS Traffic Management Steering Policies)
  - Load Balancing / Failover / Geolocation / ASN / AP Prefix
- Защищенный DNS
  - TSIG (Transaction Signature) – цифровая подпись DNS пакетов для аутентификации в процессе Update'a
- DDOS-защита "always on"
  - От Level 3,4-атак: SYN floods, UDP floods, ICMP floods, NTP Amplification etc



OCI WAF

- Наложенная защита веб-приложений
  - В OCI или в любом другом расположении
- Protection Rules - Защита от типовых атак на веб-приложения (XSS, SQL-инъекции, CSRF, эскалация привилегий
  - >250 правил защиты для веб приложений в соответствии с OWASP
- Level 7 DDOS защита
- Управление ботами
  - Javascript challenge, CAPTCHA
  - Bot whitelisting
- Контроль доступа
  - На основе географического расположения
  - На основе IP адресов, имени домена и т.д.

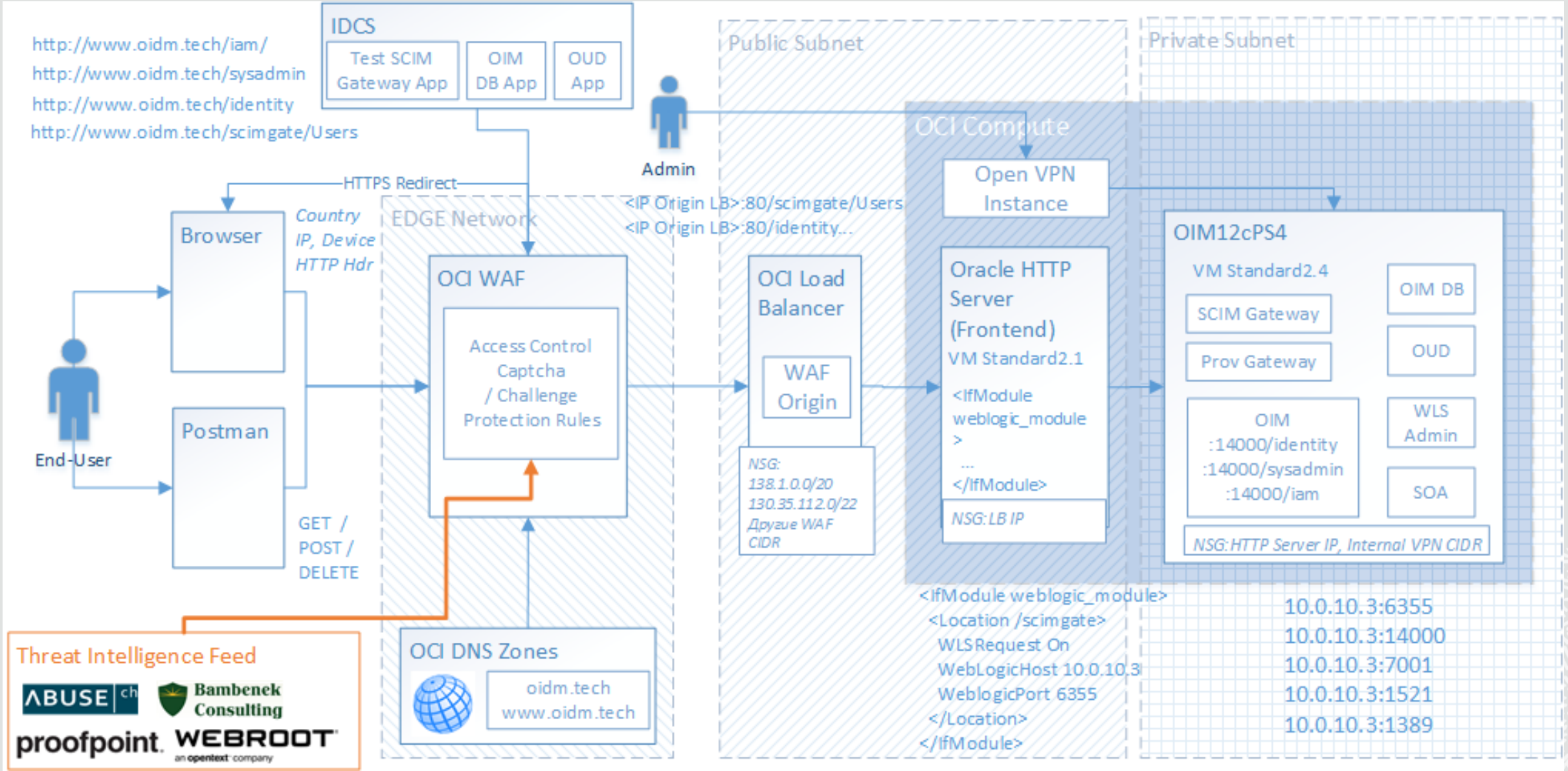


OCI WAF Threat Intelligence

- “плохие” IP поступают из различных источников и обновляются ежедневно
  - ABUSE.ch, Bambenek Computing, BlockList.de, BruteForceBlocker Project, ProofPoint ET Labs, Feodo IP Blocklist, Palevo, Webroot BotNets, Webroot Denial of Service, Webroot Mobile Threats, Webroot Phishing, Webroot Proxy, Webroot Reputation, Webroot Scanners, Webroot Spam Sources, Webroot Tor Proxy, Webroot Web Attacks, Webroot Windows Exploits, ZueS
- Функционал временно доступен через OCI CLI или OCI REST API
  - По умолчанию отключено

```
Type `help` for more info.
oleg_fayni@cloudshell:~ (eu-frankfurt-1)$ oci waas threat-feed list --waas-policy-id ocid1.waaspolicy.oc1..aaaaaaaaxvdvhwzdokbdyueuggihbdog5xm4vzvsejqmpbqintippchgeiya
{
  "data": [
    {
      "action": "OFF",
      "description": "      the IP blocklist includes known ZeuS Command & Control servers (hosts) around the world.\n",
      "key": "be102fee-1340-493b-80ad-fa5ff45a2998",
      "name": "Zeus Tracker"
    },
    {
      "action": "OFF",
      "description": "      is the blacklist of \"bad\" SSL certificates identified by abuse.ch to be associated with malware\n      or botnet activities.\n",
      "key": "65cdfae8-68c7-44aa-b9e6-812a2156eb29",
      "name": "SSL Abuse"
    },
    {
```

Пример архитектуры приложения на OCI

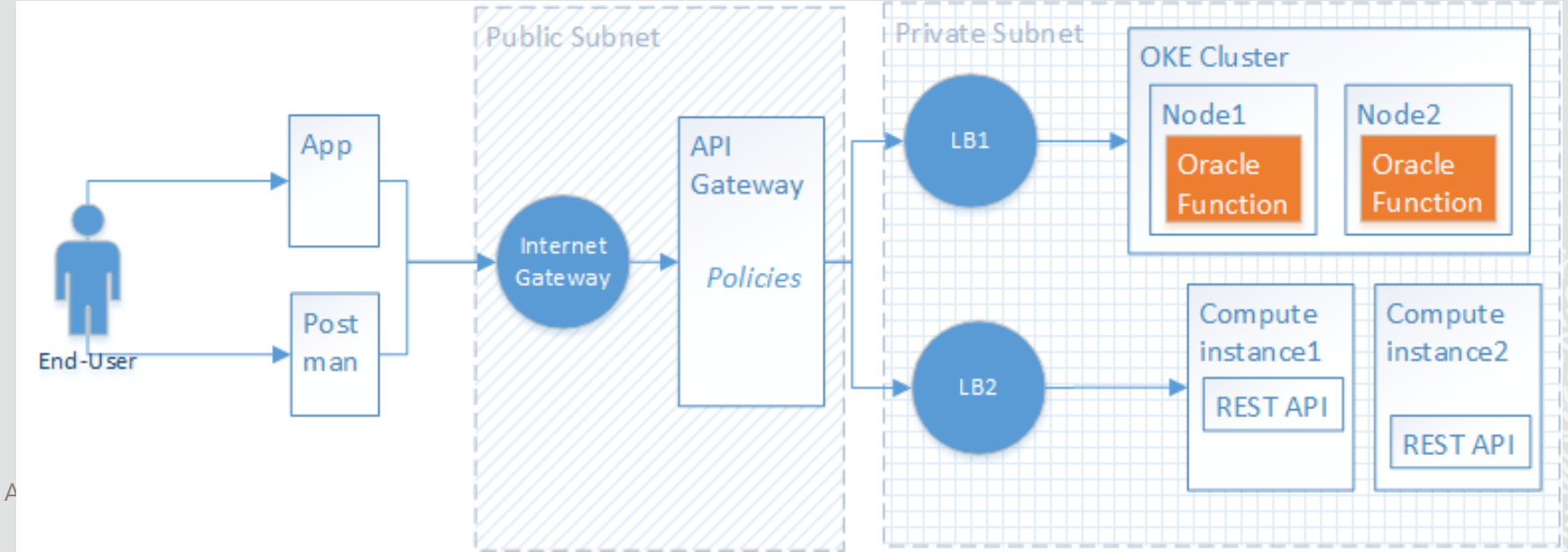


Наложенная защита API при помощи OCI API Gateway

Обзор и демо (15 мин)

OCI API Gateway

- Наложенная защита API, единая «точка входа»
  - Для приложений в OCI или в любом другом расположении
- Аутентификация, авторизация и ограничение запросов
- Валидация API, трансформация запросов и ответов, поддержка CORS (Cross-Origin Resource Sharing)
- Для REST endpoint'ов (например, на Compute Instance или в OKE кластере, или в вас в ЦОД)
- Для Oracle Functions
  - Контейнеры в OKE на основе открытого стандарта FN-project

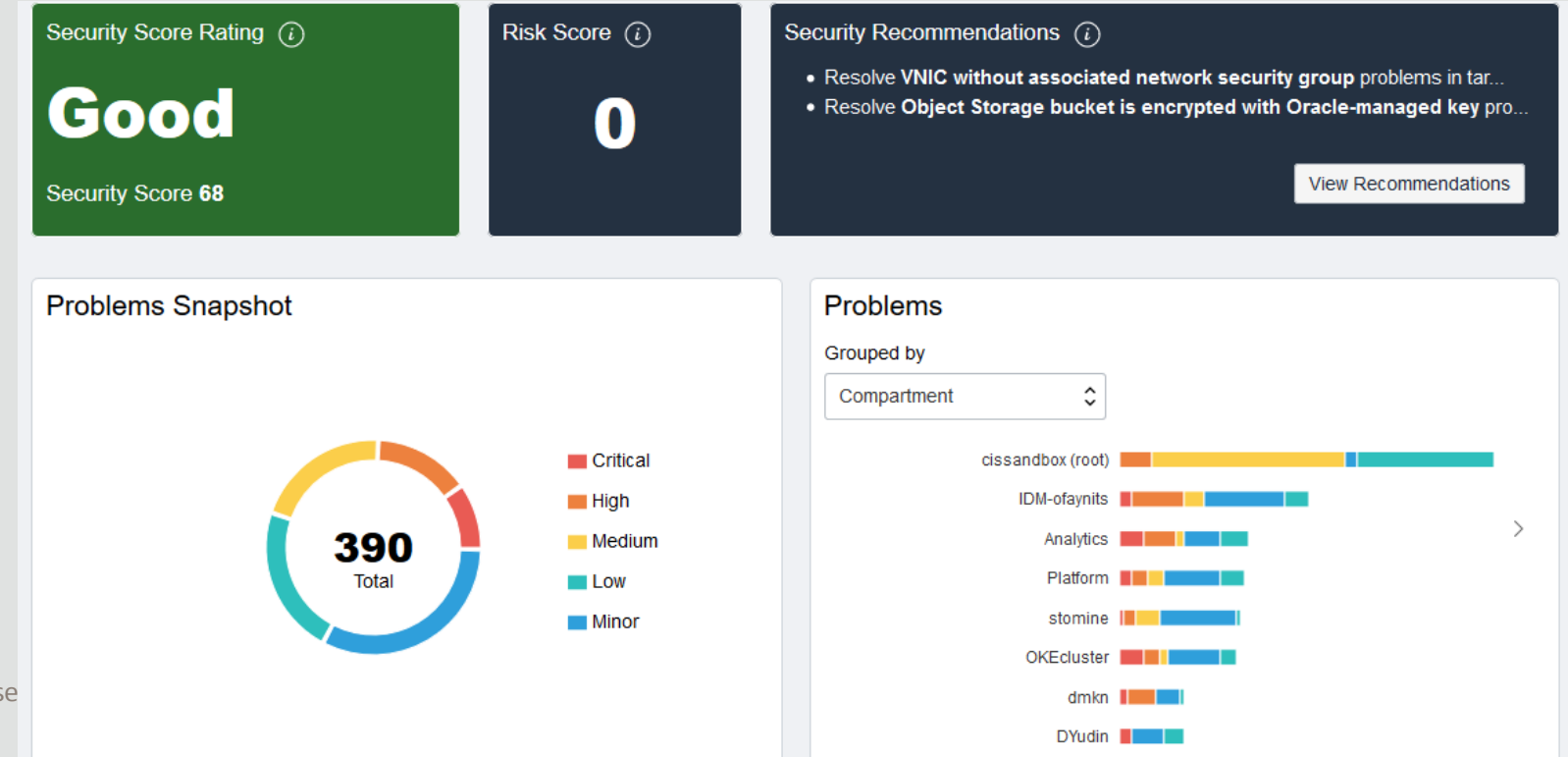


Мониторинг и контроль рисков ИБ в OCI при помощи OCI Cloud Guard и Maximum Security Zones

Обзор и демо (15 мин)

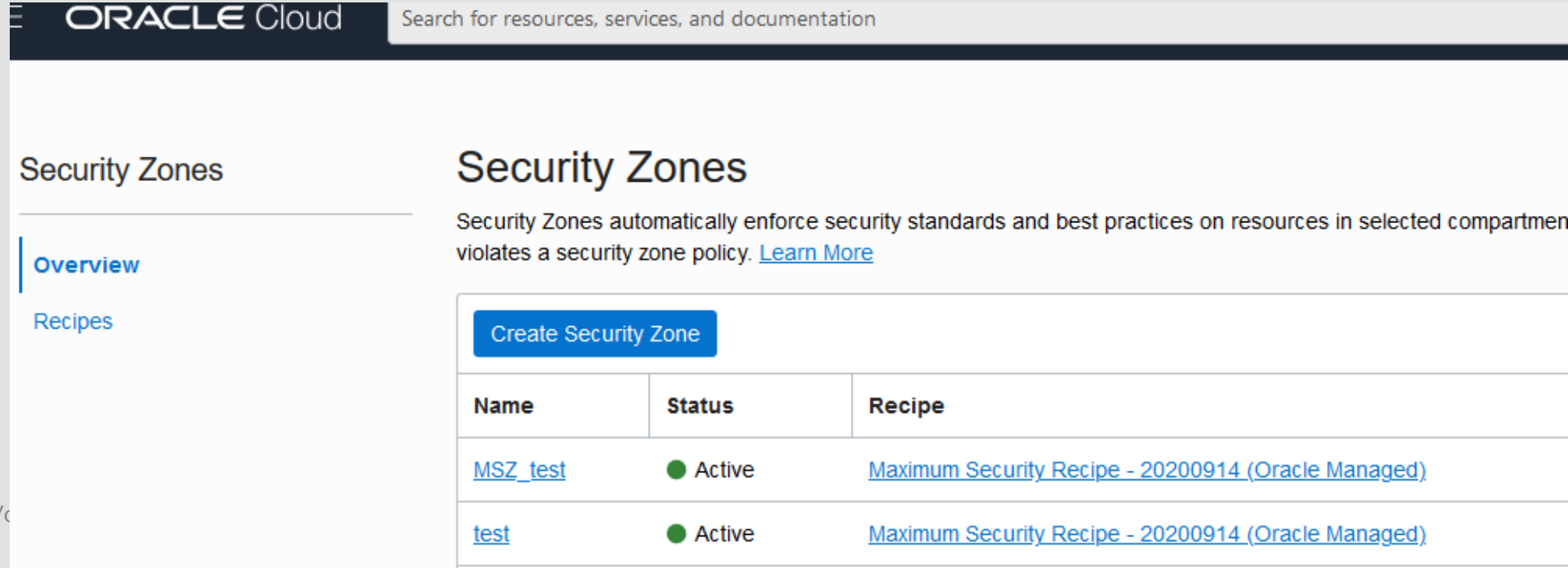
OCI Cloud Guard

- Централизованный мониторинг настроек OCI, а также действий пользователей (элементы UEBA)
- OCI Configuration Detector Recipe (Oracle Managed)
- OCI Activity Detector Recipe (Oracle Managed)
- Оценка состояния риска в OCI инфраструктуре
- Рекомендации по улучшению безопасности в OCI тенанте
- Автоматизация устранения найденных проблем через механизм «респондеров» (responders)



OCI Security Zones

- Автоматизированное применение политик безопасности для бизнес-критичных данных (без возможности отключить)
- Снижение рисков ИБ, связанных с размещением данных в облачной среде
- Встроенная экспертиза («рецепты») по настройкам безопасности OCI
- Безопасности на уровне «отделений» (Compartment-based Security)



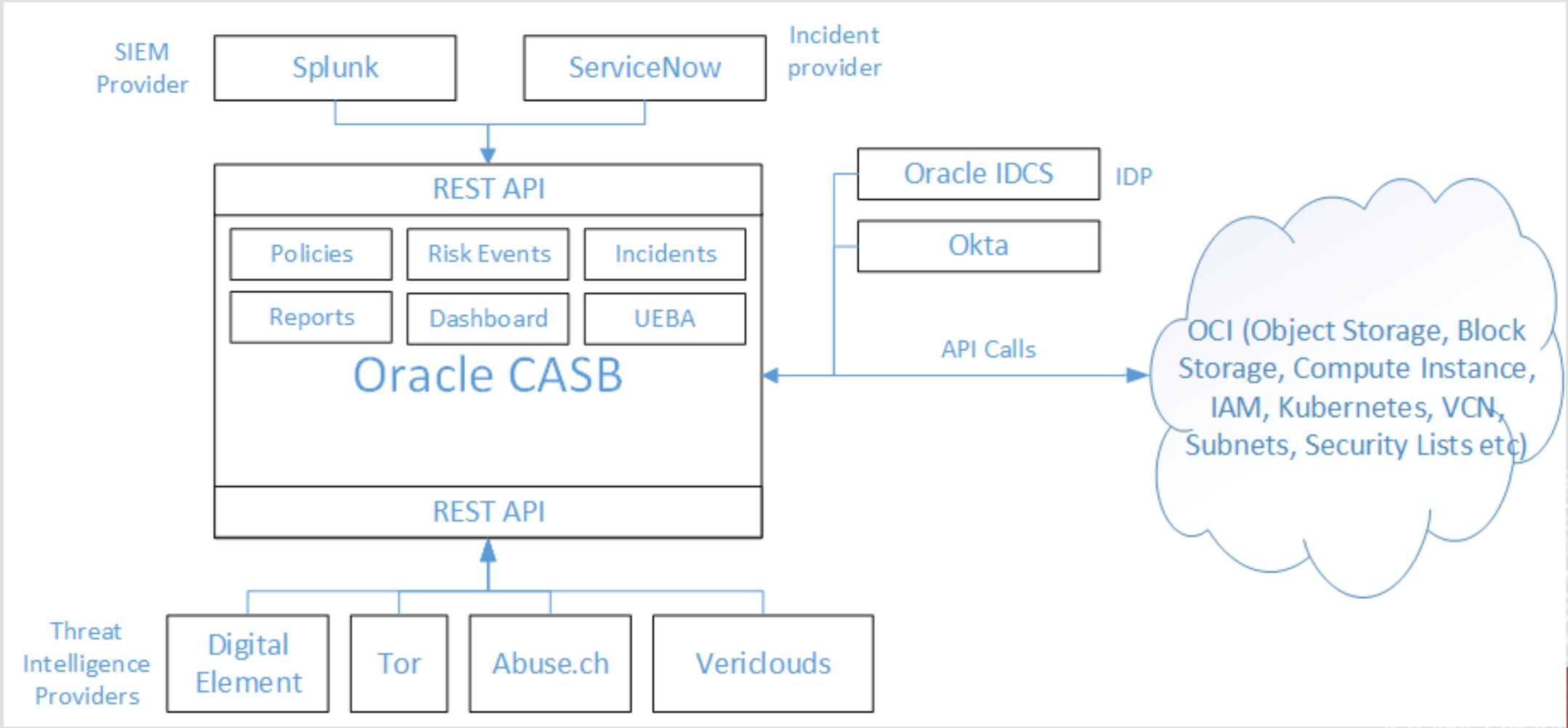
Мониторинг и контроль рисков ИБ в Oracle SaaS, OCI, AWS и Azure с помощью Oracle CASB

Обзор (5 мин)

Oracle CASB Cloud Service 4 OCI & Oracle SaaS (FA)

- Наложенная защита OCI (“Security IN the Cloud”) – повышение прозрачности использования облака для ИБ, мониторинг безопасности для OCI (настроек, действий пользователей внутри OCI)
  - Настраивается на Compartment
- Выявление «риск-событий» на основе предопределенных политик и внешних провайдеров угроз (репутация IP, URL и т.д.)
- Пример – Object Bucket с доступом public
- Формирование инцидентов на основе риск-событий
  - Возможна интеграция с ServiceNow
- Вычисление риска, ассоциированного с поведением конечных пользователей (UEBA) с элементами машинного обучения
- Предопределенные политики, преднастроенные для OCI
- Oracle SaaS – встроенный мониторинг объектов с повышенным риском
- Может также использоваться с другими облачными системами – Oracle SaaS, AWS, Azure и т.д.

Oracle CASB Cloud Service 4 OCI

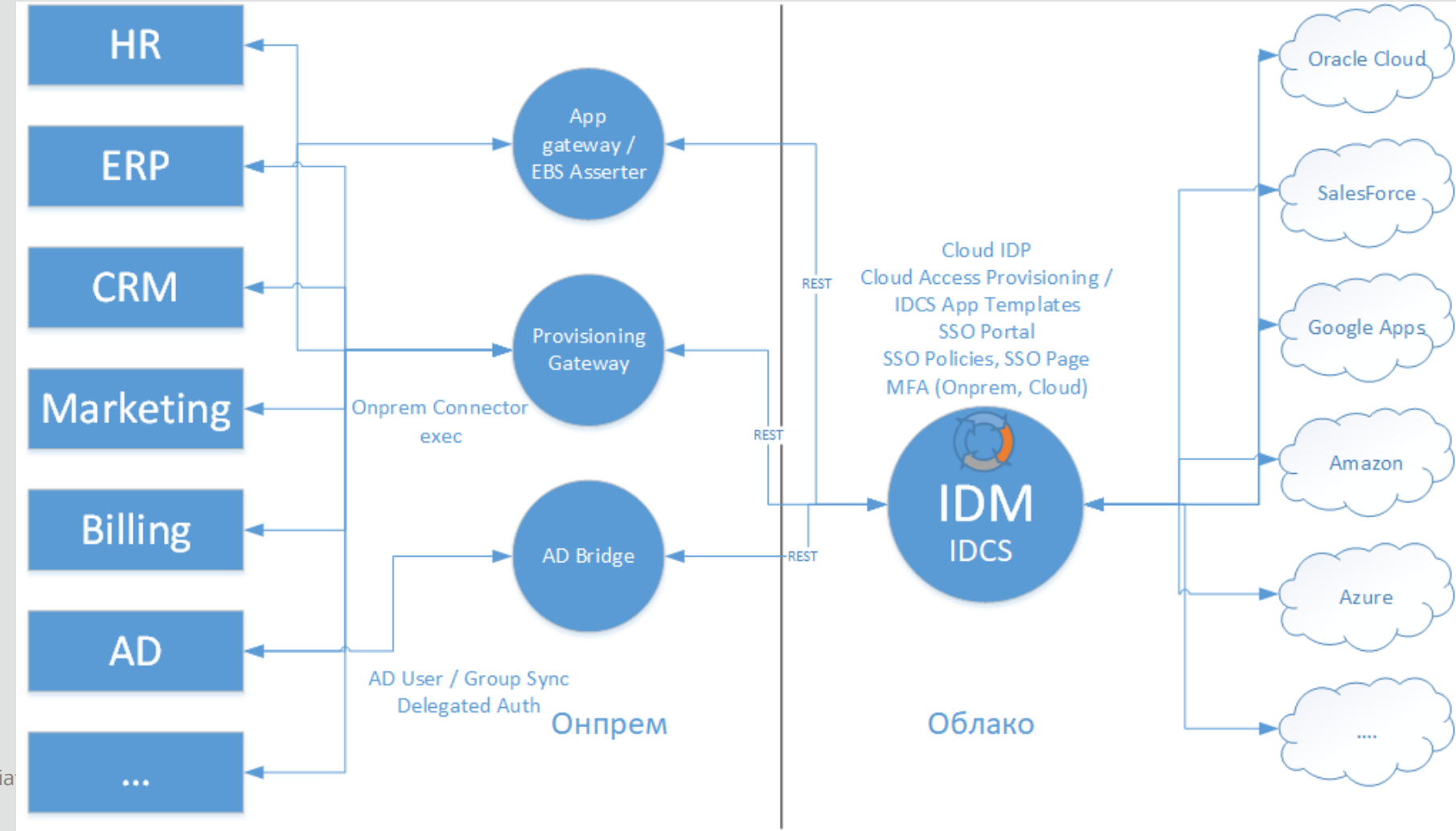


Гибридный IDaaS с Oracle Identity Cloud Service (IDCS), интеграция с онпрем доменом через AD Bridge и с онпрем системами через Provisioning Gateway, SCIM Gateway

Обзор и демо (15 мин)

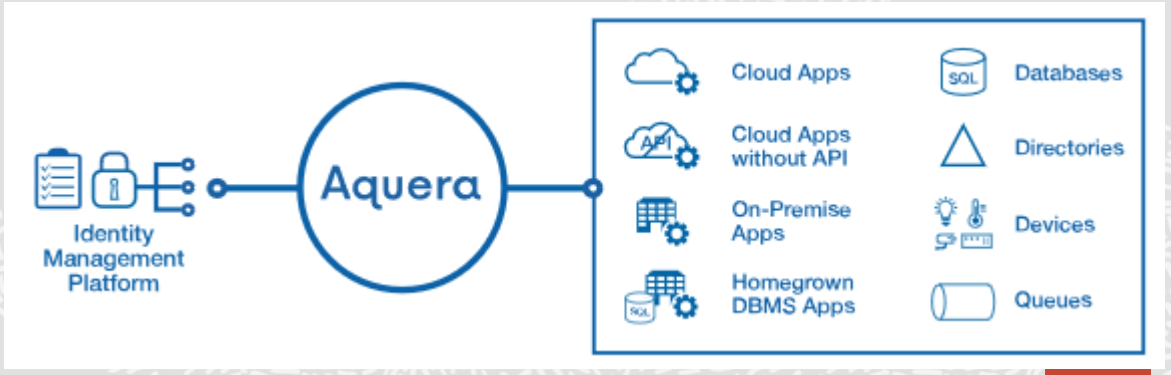
Identity Cloud Service

- Аутентификация. Авторизация, SSO, поддержка SAML, OpenID Connect, OAuth2.0
- Предоставление доступа (Provisioning)
- Поддержка гибридного облака (Prov Gateway, App Gateway, AD Bridge)



IDCS & SCIM Gateways

- SCIM Gateway – приложение, транслирующие REST SCIM в API вызовы интегрируемой системы
- Позволяет подключить через SCIM App Template любые онпрем и облачные системы
- SCIM Gateway для каждой системы, SCIM Gateway – вид коннектора к целевой системе
  - SCIM Gateway на Node.js: https://github.com/oracle/idm-samples/tree/master/idcs-scim-gateway-app
- Возможен вариант - один SCIM Gateway на много систем
- Поддерживаемые 3rd-party SCIM Gateway: Kapstone, Aquera (3000+ apps, onprem & cloud)
  - Позволяют вынести SCIM Gateway в DMZ
  - Нет прямого inbound доступа к приложению



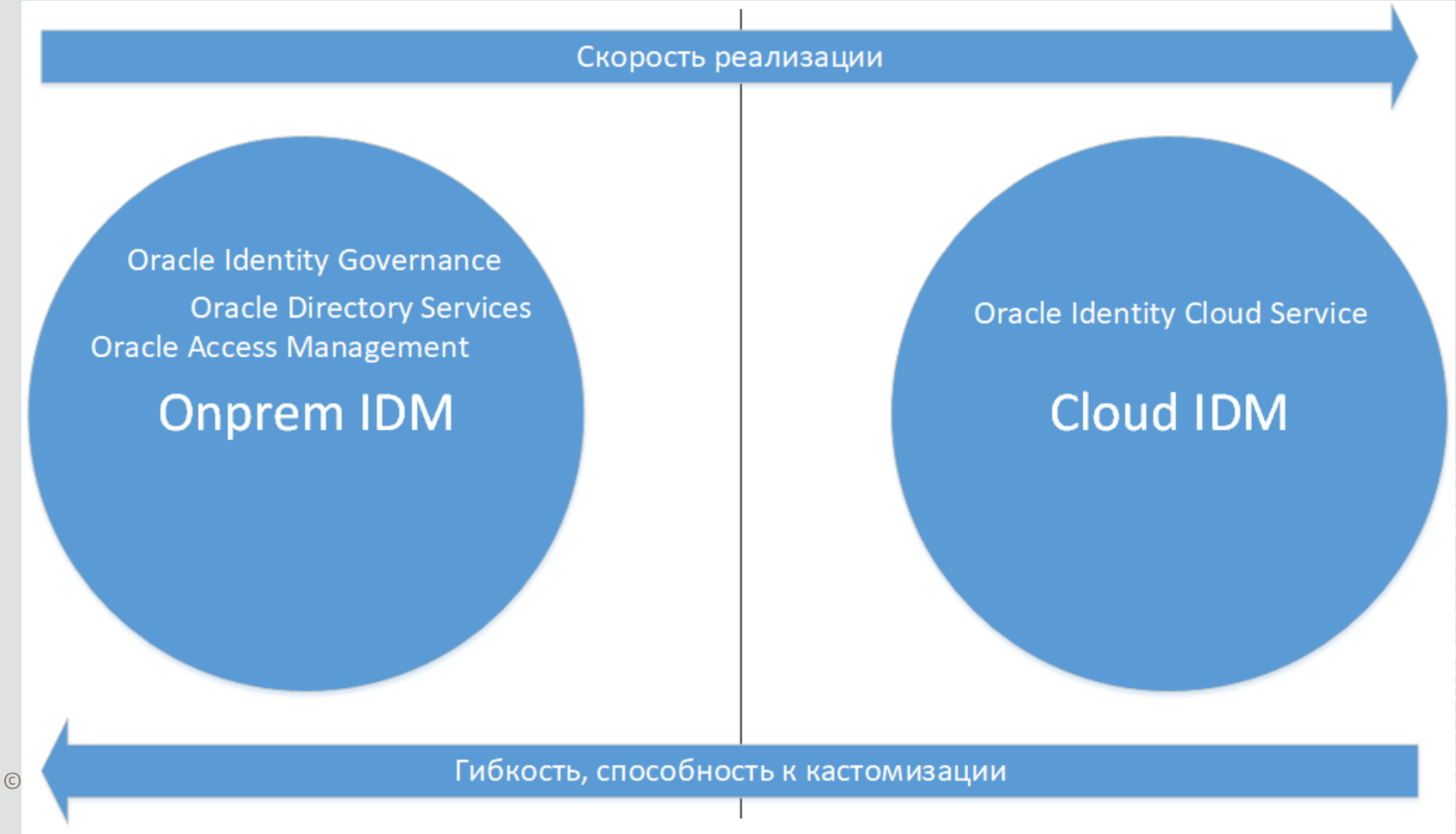
Интеграция IDaaS в бизнес-процессы безопасности (согласование доступа, контроль разделения полномочий, сертификация доступа, управление ролями) через Oracle Identity Governance

Обзор и демо (15 мин)

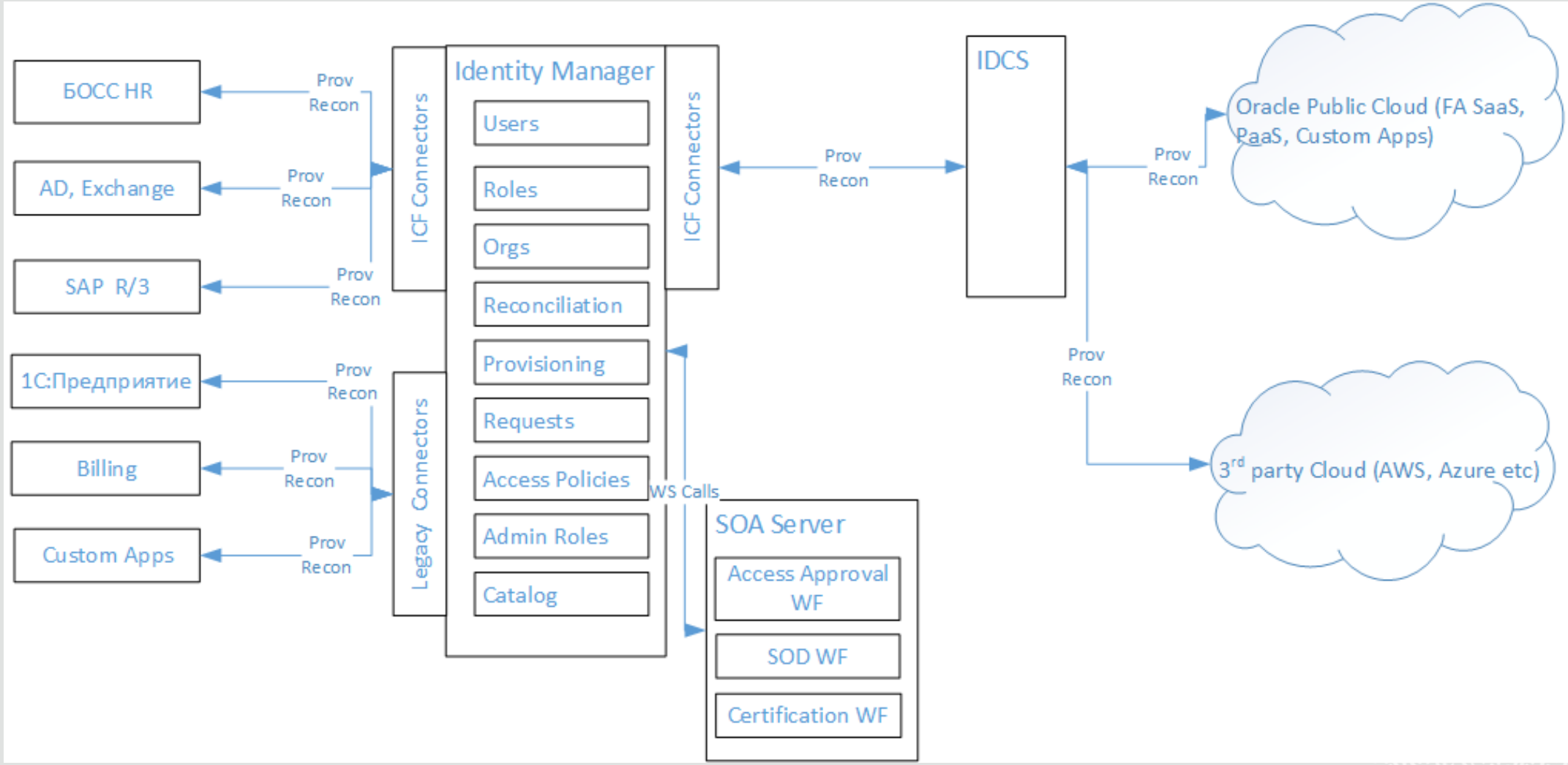
Oracle Identity Governance (Identity Manager)

- Онпрем продукт, но может быть развернут в OCI
- Автоматизация цикла жизни учетной записи конечного пользователя
- Автоматизация цикла жизни роли как набора полномочий
- Интеграция онпрем и облачных систем в бизнес-процессы безопасности компании
  - Запрос доступа / согласование доступа
  - Запрос изменения состава роли / согласование
  - Сертификация доступа (проверка неизбыточности полномочий на периодической основе)
  - Сертификация роли (проверка неизбыточности состава роли на периодической основе)
  - Контроль совместимости полномочий (Segregation Of Duties – SOD) – превентивный и детективный, в контексте доступа пользователя и в контексте роли, интеграция с процессами сертификации через фактор риска
  - Отчетность, оперативная и историческая (с использованием BI Publisher)

Identity Cloud Service vs Identity Governance



Identity Cloud Service & Identity Governance



Разворачивание Oracle Identity & Access Management на OCI как terraform-стека через OCI Resource Manager

Обзор (10 мин)

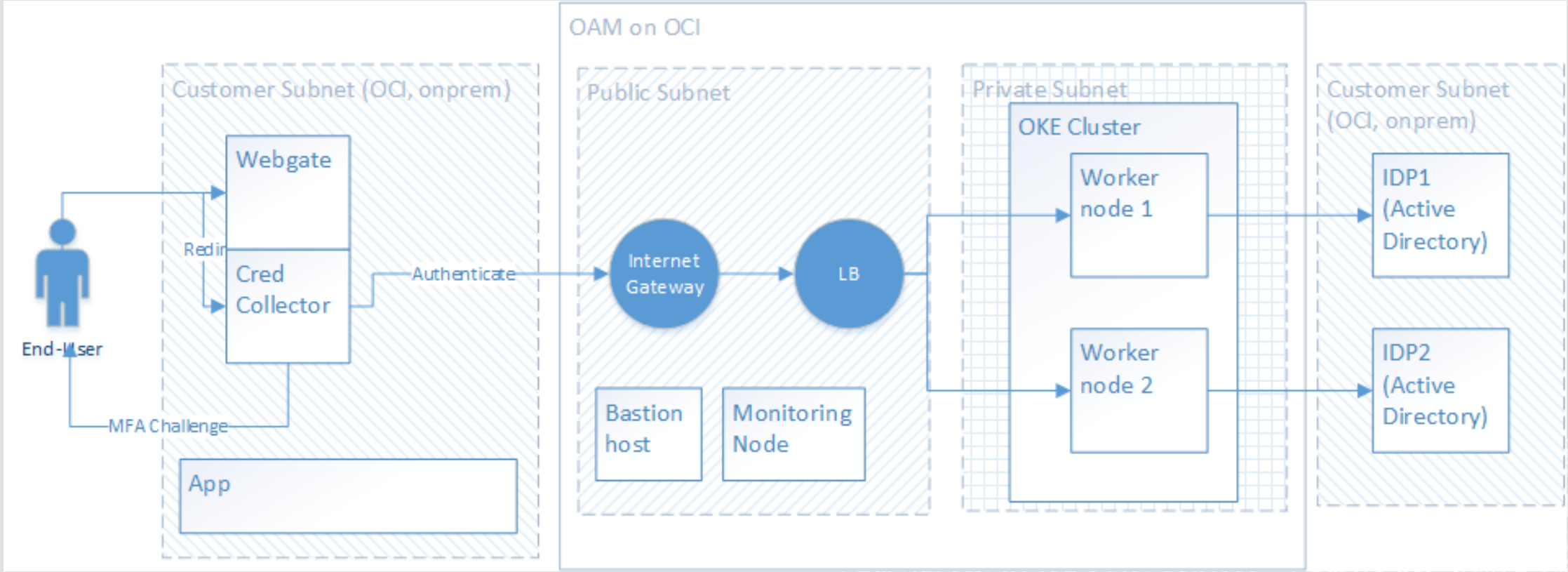
Oracle Access Management

- Онпрем продукт, но может быть развернут в OCI
- Контроль доступа – аутентификация, авторизация
  - Поддержка основных протоколов: SAML, OpenID Connect, OAuth2.0, Kerberos и т.д.
- Многофакторная аутентификация
- WebSSO
- Федеративное SSO
- По умолчанию стандартный и документированный способ защиты многих приложений Oracle:
  - Siebel
  - Oracle e-Business Suite
  - Primavera
  - BI
  - И другие
- Может быть интегрирован с IDCS

OCI Resource Manager

- Terraform – продукт IaaC (Infrastructure as a Code) для автоматизации управления облачными ресурсами
  - Декларативное описание ресурсов, State-файл
  - Локальное и удаленное выполнение команд (например, скрипта установки ПО)
  - С модулем-плагином для OCI
- Запускает основные terraform-команды
  - Plan
  - Apply
  - Destroy
- RM Stack – набор OCI ресурсов, определенные в terraform-формате
- RM Job – terraform-действие (Apply, Plan, Destroy)
- RM Variables – переменные, используемые внутри скриптов terraform
- Terraform-конфигурация может быть загружена и выгружена
- Стэки для разных OCI приложений доступны на OCI Marketplace

Oracle Access Management 12.2.1.4 на OCI



Ресурсы

- Безопасность OCI - https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
- Безопасность OCI (документация) - https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm
- https://www.easyoraidm.ru - Easy ORA IDM проект (блог на тему Oracle Identity Management и Cybersecurity, by Oleg Faynitskiy) - виртуальные тренинги, статьи, FAQ
- https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf - Oracle & KPMG Cloud Thread Report

Спасибо

Oleg Faynitskiy

Oracle CIS, oleg.faynitskiy@oracle.com