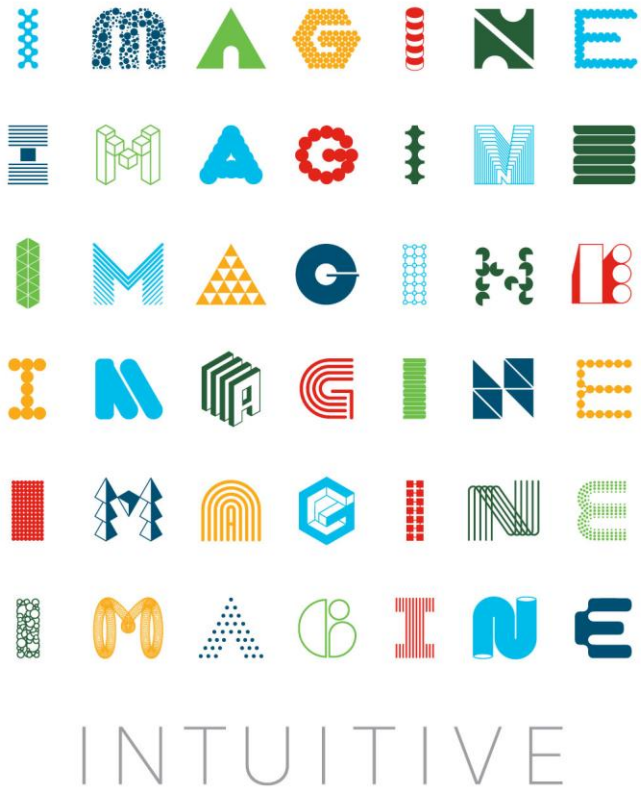
Эволюция систем управления идентификационной информацией

Алексей Лукацкий
Бизнес-консультант по безопасности



Как вы аутентифицируете своих пользователей?

Традиционная аутентификация

Пользователь

Каталог / директория

Интернет /
внутренние ресурсы

Проблема традиционной аутентификации

81%

инцидентов используют украденные или слабые пароли

Компрометация учетных записей остается основным риском. Токены и одноразовые пароли не всегда дружественны к пользователю

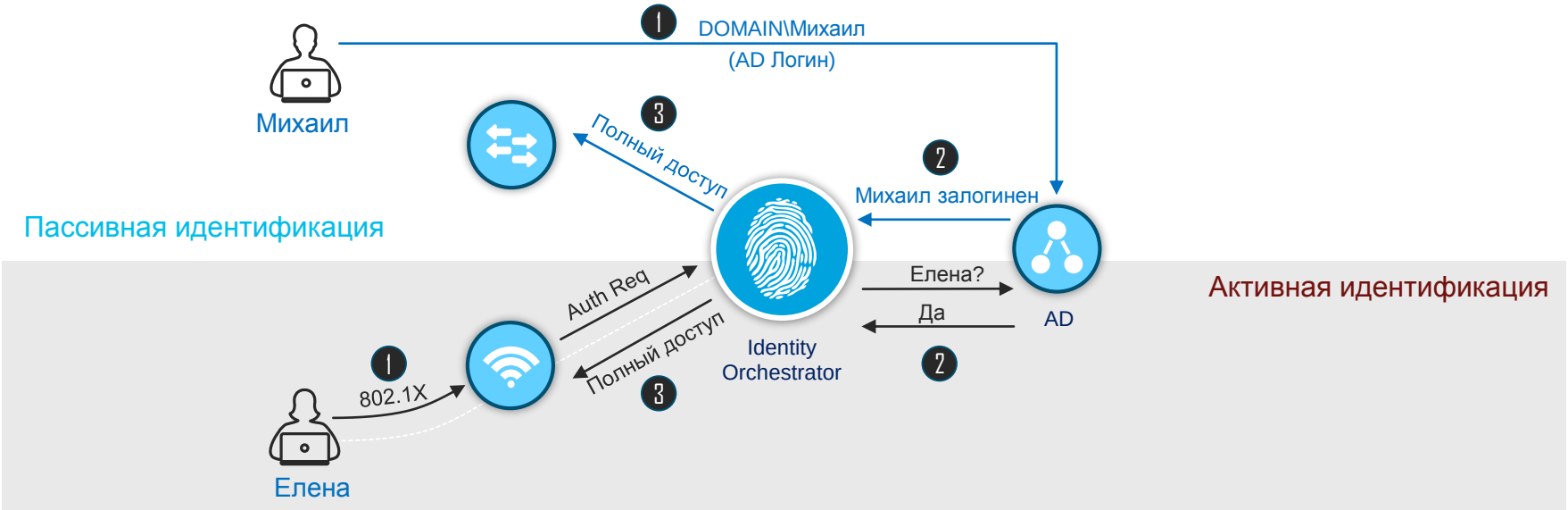
Источник: Verizon 2018 Data Breach Investigations Report

Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации

А если у вас есть устройства, но нет пользователей?

Аутентификация на базе адреса устройства



Пассивная идентификация

Мапинг IP-Пользователь получается пассивно через AD **WMI события**, AD Агенты, **Syslog**, **SPAN** сессии и другое.

Активная идентификация

Мапинг IP-Пользователь получается через активное взаимодействие с ISE клиента по средством **802.1X**, **Web authentication**, **Remote access VPN**, и др.

802.1x усиливает возможности по аутентификации устройств за счет сертификатов PKI

Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств

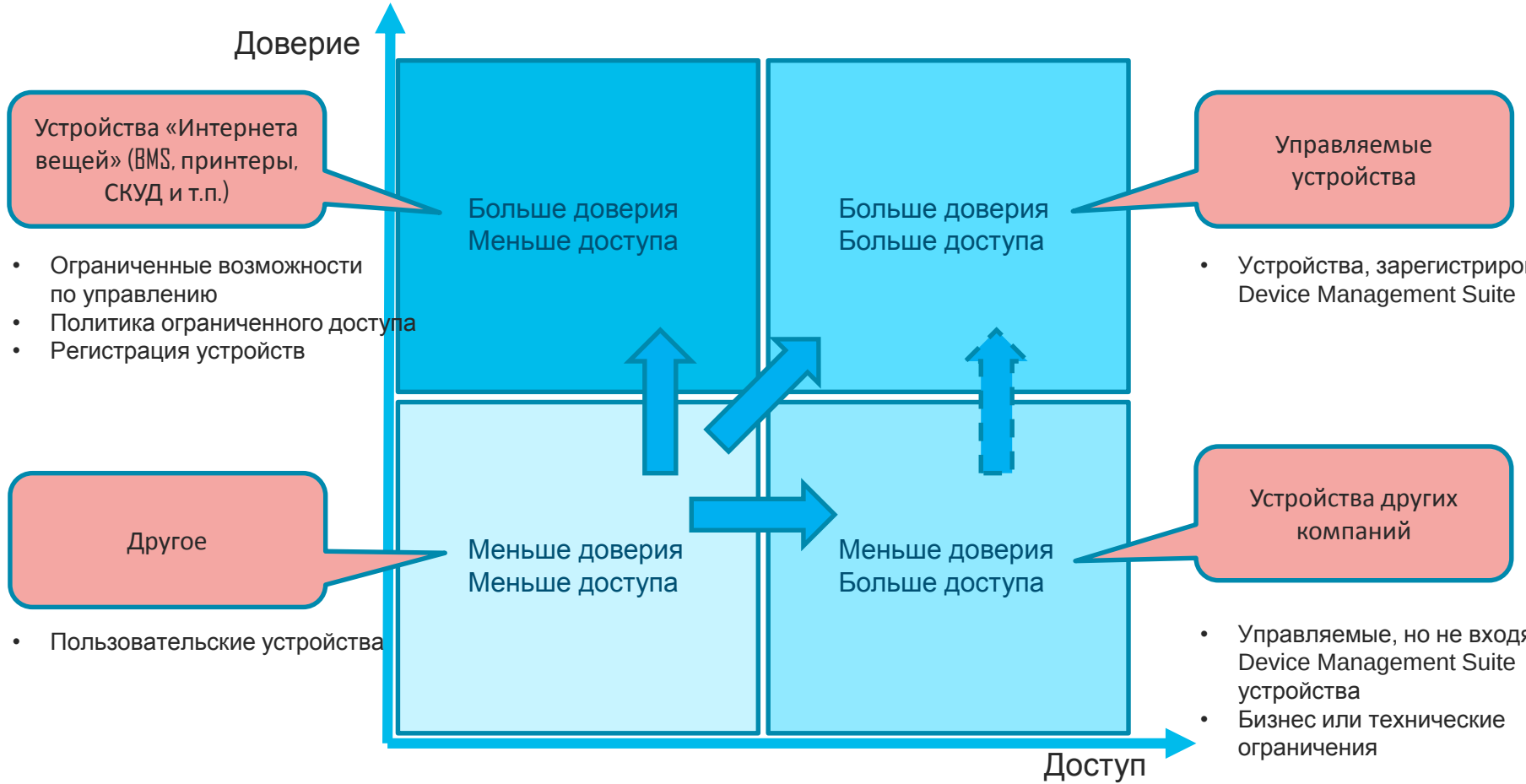
Что вы будете делать, если пользователь прошел аутентификацию на зараженном устройстве?

Часто сотрудники приносят личные и зараженные устройства

90% опрошенных организаций не вполне представляют себе, какие устройства находятся в их сети

75% компаний подтвердили, что их мобильные устройства были атакованы вредоносным ПО за последние 12 месяцев

Разные устройства имеют разные привилегии



- Ограниченные возможности по управлению
- Политика ограниченного доступа
- Регистрация устройств

- Устройства, зарегистрированные Device Management Suite

- Пользовательские устройства

- Управляемые, но не входящие в Device Management Suite устройства
- Бизнес или технические ограничения

Надо добавить к IP контекст доступа

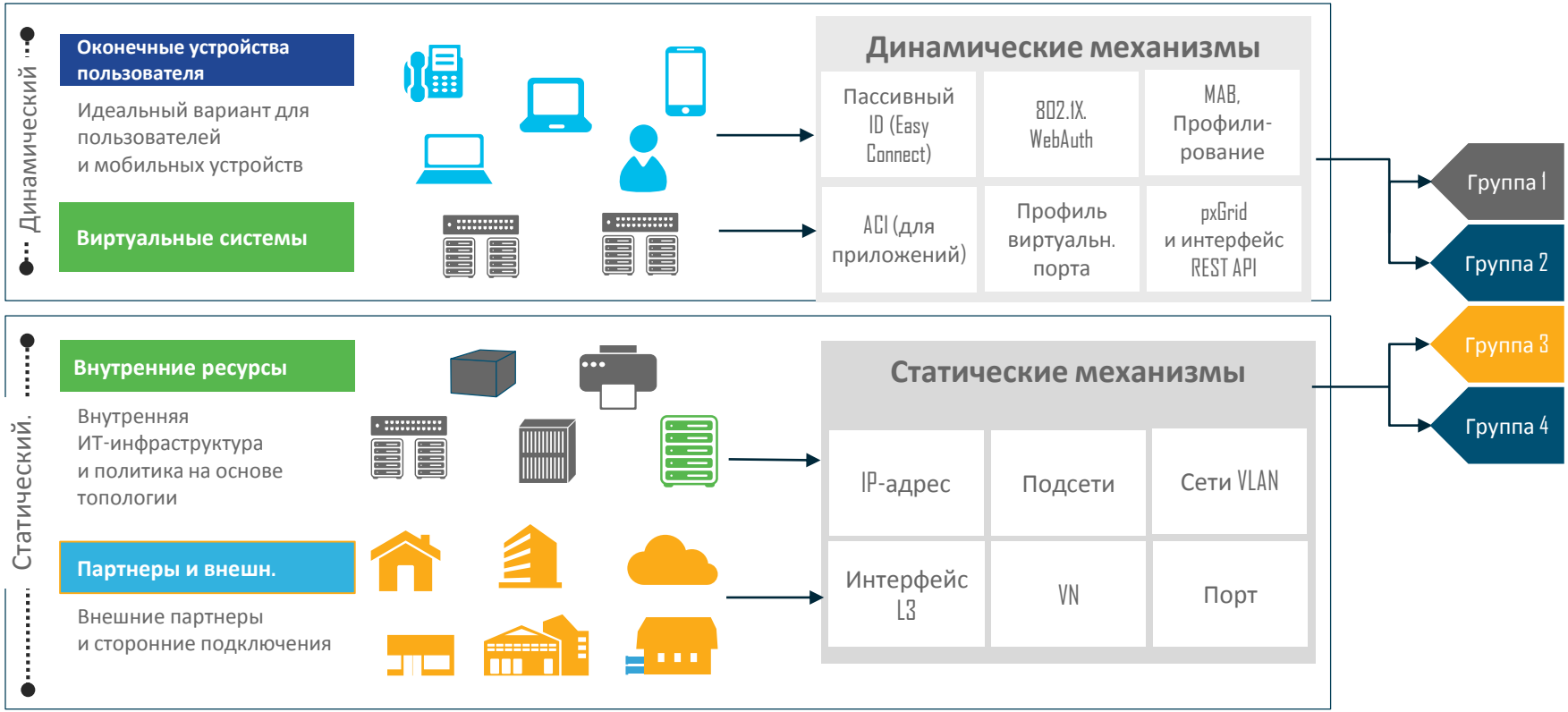
НЕИЗВЕСТНО

Отсутствие контекста		Богатый контекст
IP АДРЕС: 192.168.2.101		Алексей Лукацкий (СОТРУДНИК)
НЕИЗВЕСТНО		MACOS WORKSTATION
НЕИЗВЕСТНО		ЗДАНИЕ-4-ЭТАЖ-3
НЕИЗВЕСТНО		13:30 AM MSK ИЮН 21
НЕИЗВЕСТНО		БЕСПРОВОДНАЯ СЕТЬ
НЕИЗВЕСТНО		НЕТ УГРОЗ / УЯЗВИМОСТЕЙ

ИЗВЕСТНО

РЕЗУЛЬТАТ	РЕЗУЛЬТАТ
ДОСТУП К IP (ЛЮБОЕ УСТРОЙСТВО / ПОЛЬЗОВАТЕЛЬ)	РОЛЕВОЙ ДОСТУП

Добавляем контекст к классификации / аутентификации



Где размещается метка безопасности?

Централизованное управление с помощью оркестратора NAC

Централизованное решение для автоматизации контекстно-задаваемых политик доступа к сетевым ресурсам и обмена контекстом

Пример использования контекста в политике доступа: расширяем обычную идентификацию

Кто? Известные пользователи (Сотрудники, продавцы, HR) Неизвестные пользователи (Гости)	**Что?** Идентификатор устройства Классификация устройств (профиль) Состояние устройства (posture)	**Как?** Проводное подключение Беспроводное подключение VPN-подключение
Где / куда / откуда? Географическое местоположение Департамент / отдел SSID / Порт коммутатора	**Когда?** Дата Время	**Другие?** Пользовательские атрибуты Статус устройства / пользователя Используемые приложения

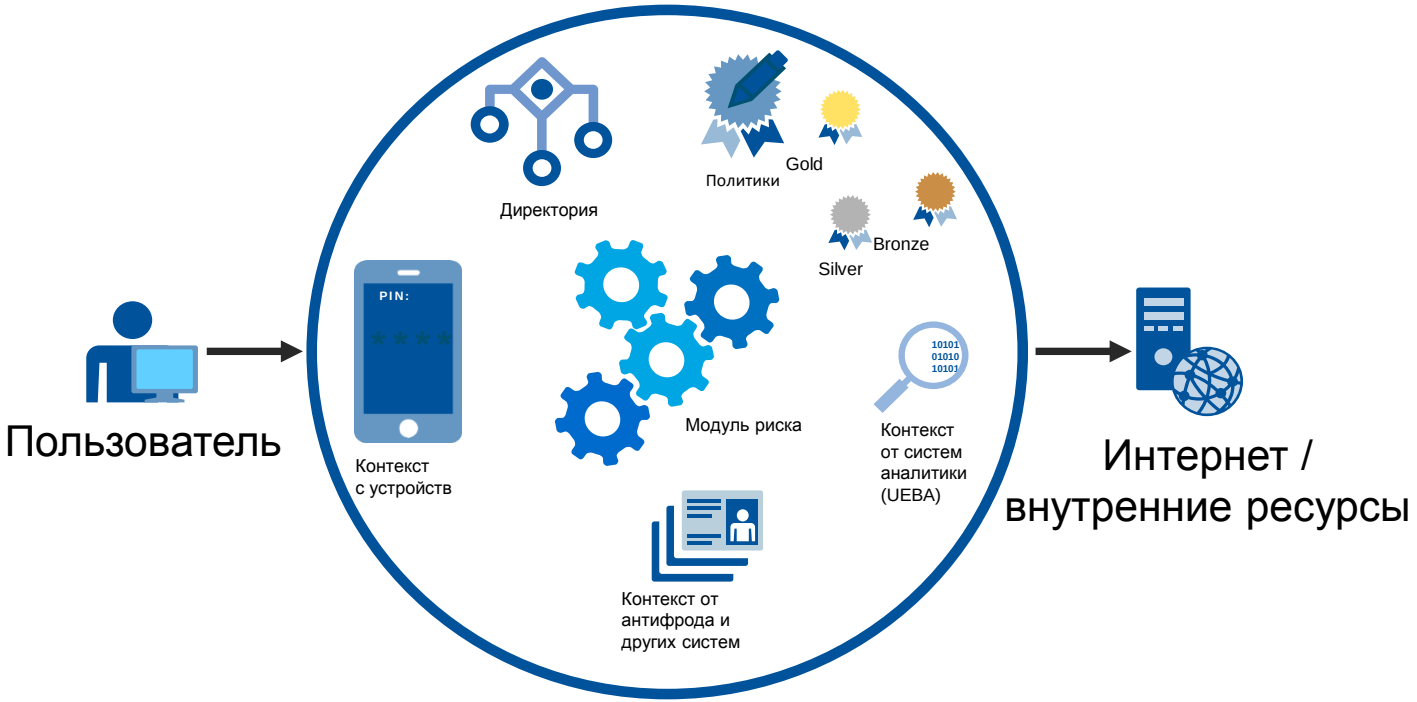
Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей

Дискретность проверок

Уязвимостей
Прав доступа

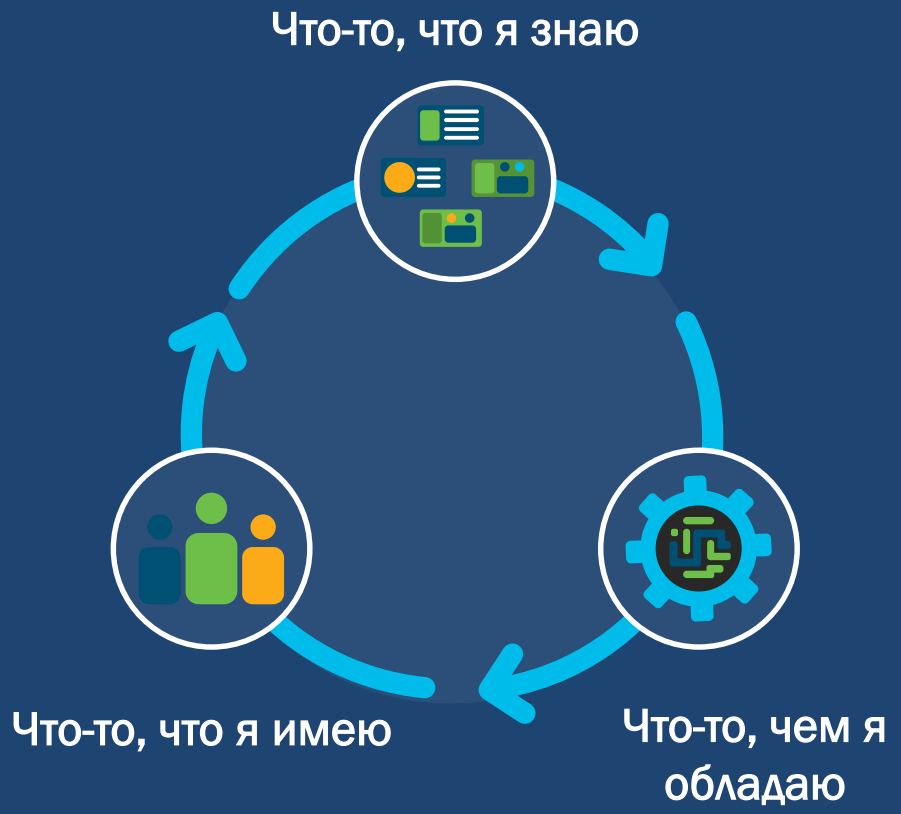
Можно еще добавить непрерывный анализ (ML, UEBA и т.п.)



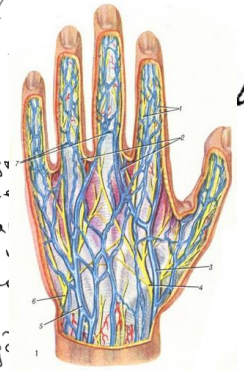
Рекомендации

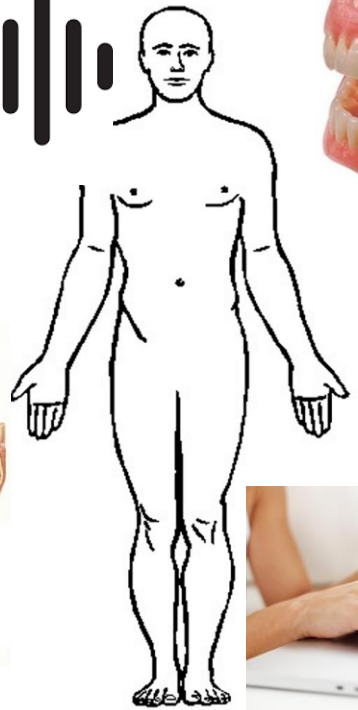
- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей
- Добавление непрерывного анализа с помощью различных систем аналитики, UEBA, антифрода и т.п.

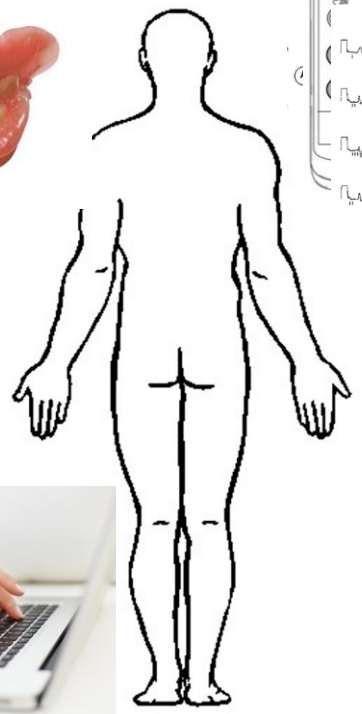
Вспомним основы

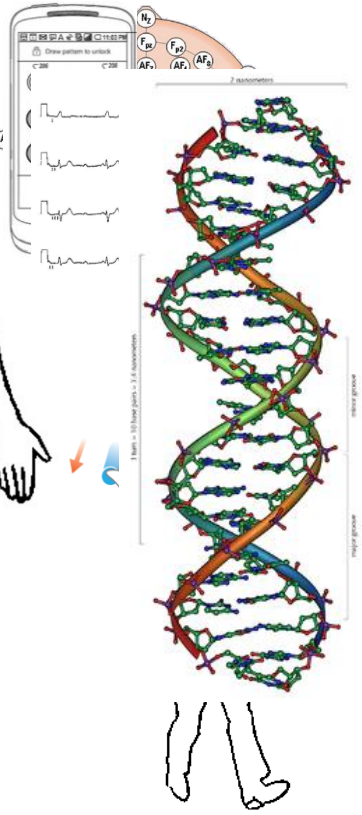


Что можно добавить к паролю?



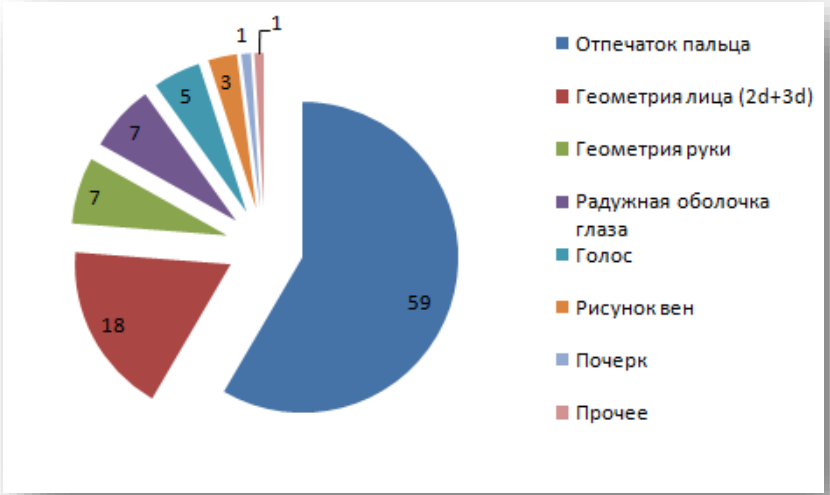






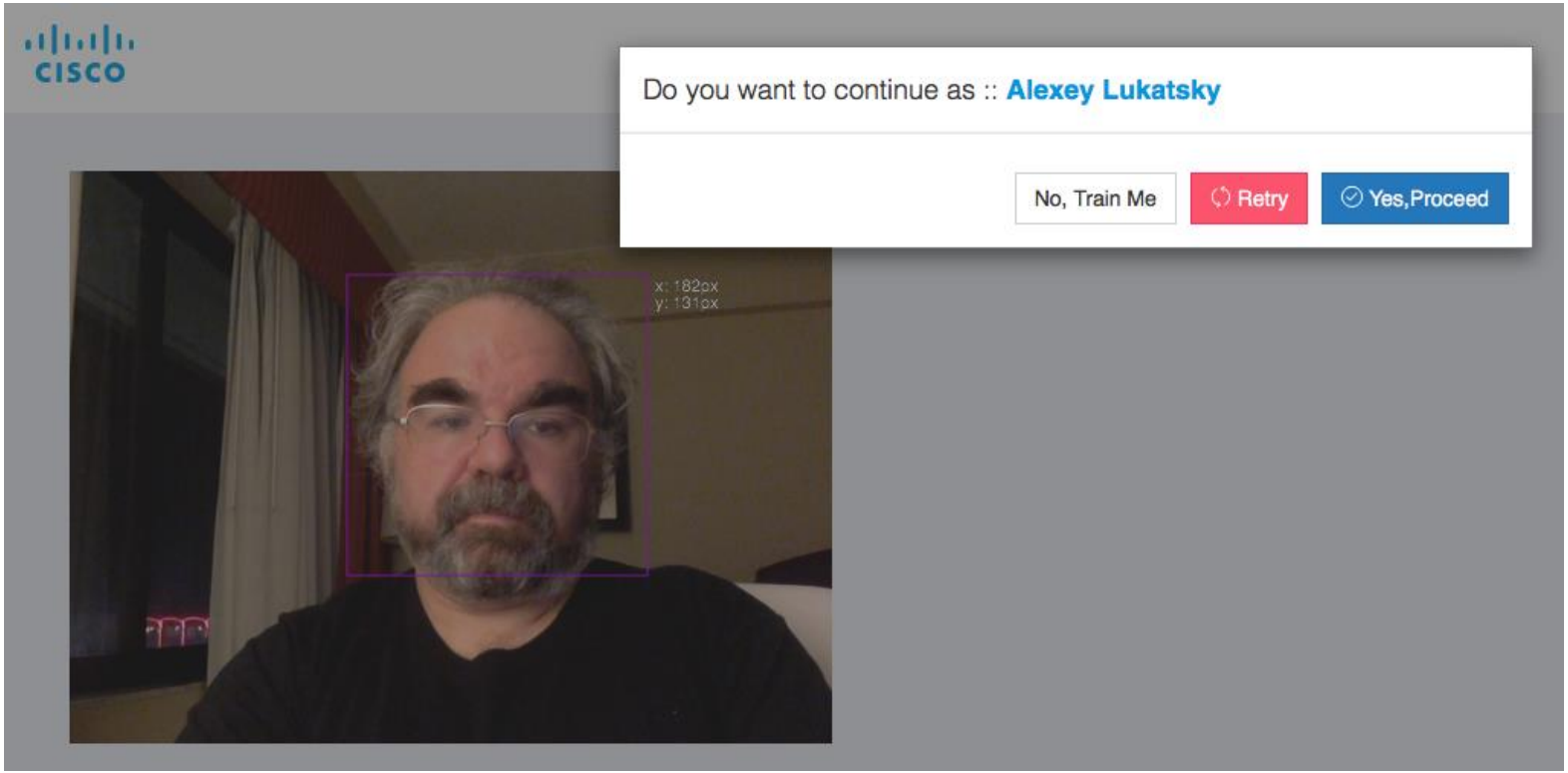
Что обычно применятся организациями?

- Голос
- Геометрия руки
- Геометрия лица
- Отпечатки пальцев
- Строение сосудов кисти (рисунок вен)



В зависимости от точки аутентификации (банкомат, смартфон, Web-сайт, клиент-банк, Call Center и др.) применяются статические или динамические характеристики

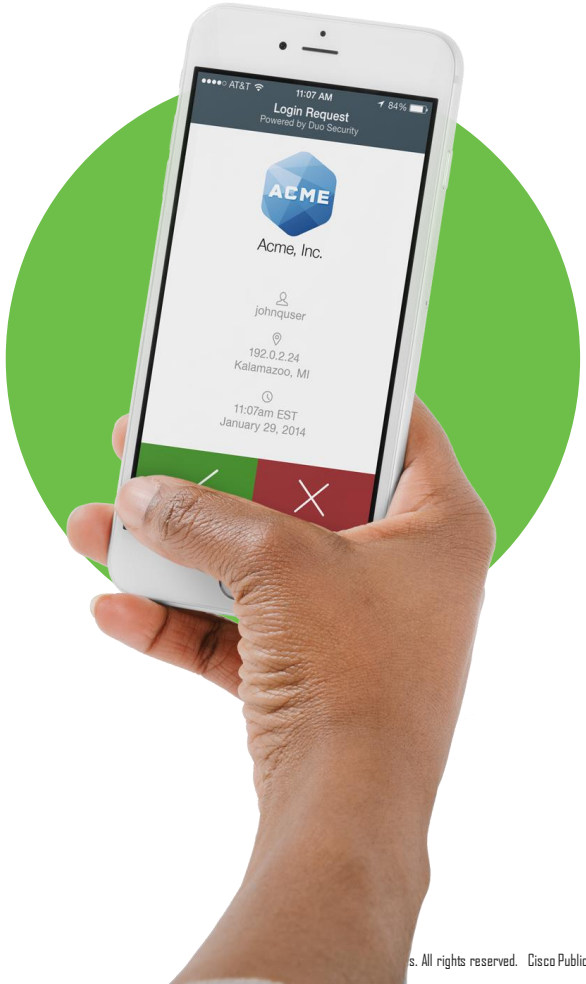
Бета-проект: непрерывная верификация



Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей
- Добавление непрерывного анализа с помощью различных систем аналитики, UEBA, антифрода и т.п.
- Дополнение биометрической идентификацией

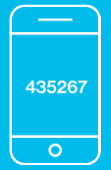
Что-то, что вы знаете
Что-то, что вы имеете
Что-то, чем вы обладаете
Что-то, что вы делаете
Что-то, что вы потеряли
Что-то, что вы забыли
Что-то, что вы нашли
Что-то, что вы видели
Что-то, где вы были
Что-то, что вы создали
Что-то, что вы уничтожили
Что-то, что вы пожертвовали
Что-то, что вы украли
Что-то, что ....



Широкий спектр опций для многофакторной аутентификации

- Разные опции для разных приложений и разных пользователей
- Множественность выбора опций для удобства и гибкости пользователей

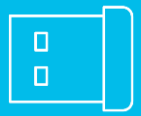
Push



Soft Token

SMS

Звонок



U2F

Носимые гаджеты

Биометрия

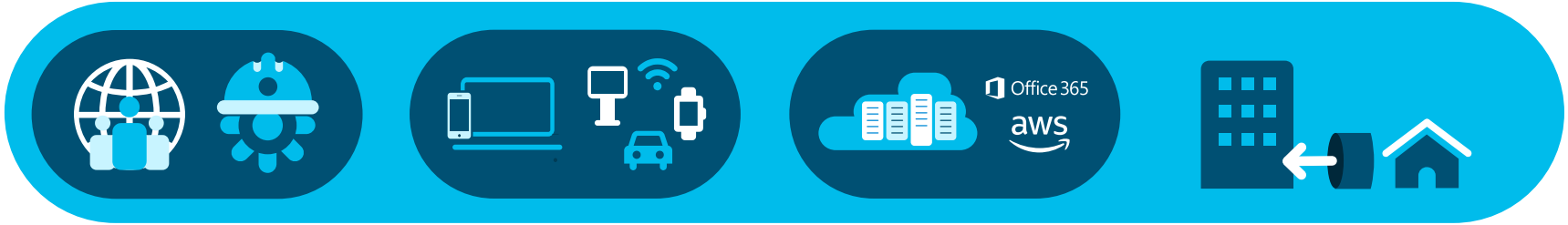
Аппаратные токены

Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей
- Добавление непрерывного анализа с помощью различных систем аналитики, UEBA, антифрода и т.п.
- Дополнение биометрической идентификацией
- Дополнение многофакторной аутентификацией

От частного к общему

В современных предприятиях данным, приложениям и пользователям разрешено перемещаться между…



Любыми пользователями

- Сотрудники
- Контрактники
- Партнеры

Любыми устройствами

- Корпоративные
- Собственные
- IoT

Любыми приложениями

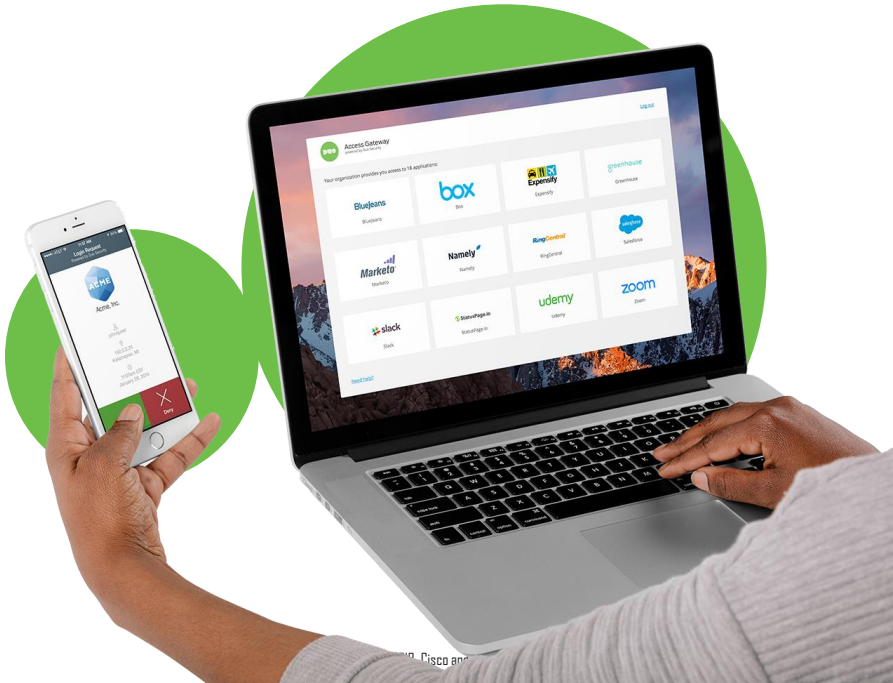
- ЦОД
- Мультиоблако
- SaaS

В любых местах

- Внутри сети
- Через VPN
- Вне сети

Изменение ИТ-ландшафта

В современном мире у нас меняются задачи для систем идентификации



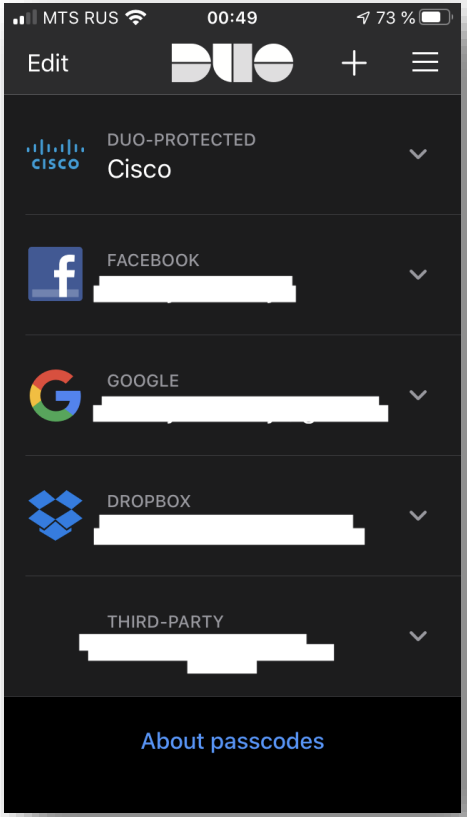
Расширение задач для систем идентификации






Круг пользователей	Системы управления	Управляемые объекты	Управление политиками	Механизмы исполнения	Целевые системы
•Сотрудники •Контрактники •Партнеры •Заказчики •Устройства •Боты •Вещи •Привилегирован-ные учетные записи •Производители	•HR-системы •Облачные приложения •Портал регистрации клиентов •Системы управления ПК •Системы RPA •Системы управления вендорами	•Identities •Entitlements •Privileged entitlements •Application metadata •Data classification •Risk metadata •Credentials •Relationship mapping •User preferences •User consent	•Правила •Роли •Workflows •GRC •Политики приложений	•IGA-коннекторы •SCIM •SaaS-delivered IAM •RPA •ITSSM	**On-Premises:** •Базы данных •Директории •Файлшары •Бизнес-приложения **Облачные:** •Базы данных •Директории •Облачные файлшары •Контейнеры •SaaS-приложения

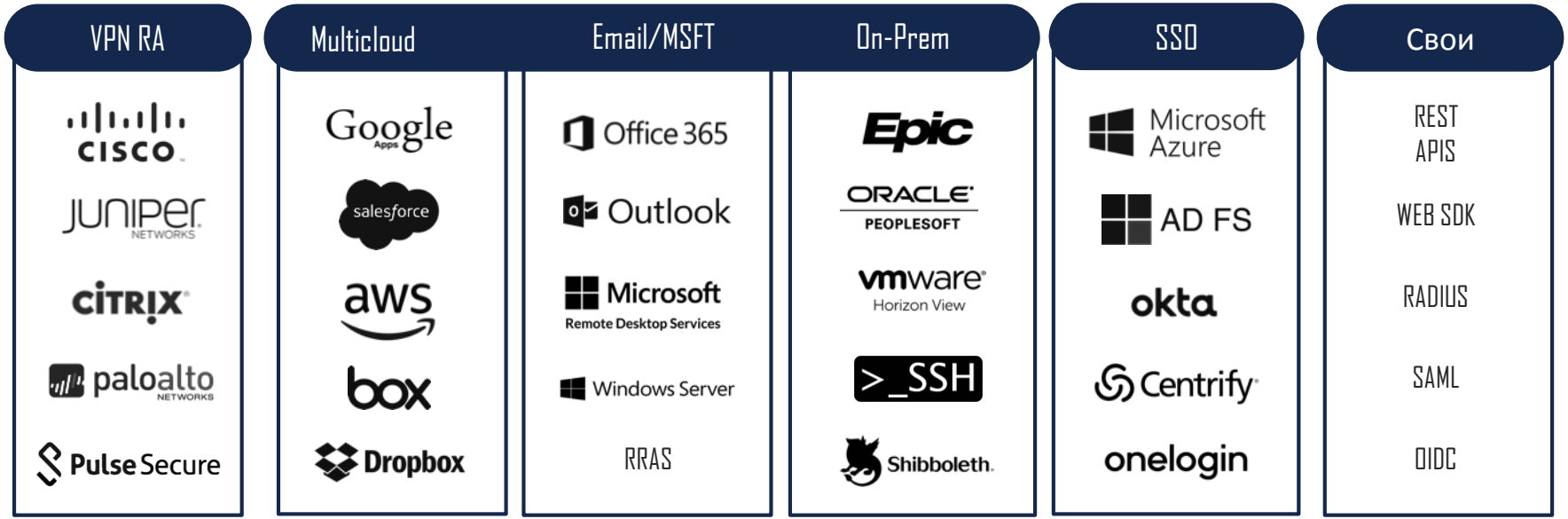
Как проходит аутентификация в разных приложениях?



Разные приложения – единая аутентификация

Начните отсюда

Затем расширяйте



Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей
- Добавление непрерывного анализа с помощью различных систем аналитики, UEBA, антифрода и т.п.
- Дополнение биометрической идентификацией
- Дополнение многофакторной аутентификацией
- Оцените перспективы применения разных приложений, включая облачные и для удаленного доступа

Если у вас есть удаленный доступ и доступ к облачным сервисам

Основное устройство

Основная аутентификация

Пользователь и устройство аутентифицируются с помощью стандартных механизмов

Ваши сервера и приложения

Коммуникации с серверами

Интеграция с внешним провайдером Identity (не видят вашего пароля)

Запрос к IdP

Ключевые компоненты размещаются в облаке

Вторичное устройство

Вторичная аутентификация

- Push
- Mobile Passcode
- Phone, SMS
- HOTP Token
- U2F/WebAuthN
- Bypass

Основное устройство

Успех!

Можно выстраивать цепочку провайдеров Identity

SAML-провайдеры

- Shibboleth
- Microsoft AD FS
- Microsoft Azure AD
- G Suite (Google)
- Okta
- OneLogin
- SecureAuth
- Bitium
- CA SSO
- Radiant Logic
- F5
- Juniper
- Oracle
- И другие

Почему IdP не видит пароля

Протокол SAML 2.0 широко используется тысячами приложений, в том числе и в облаках

Однажды установив доверие между SP и IdP, запросы и ответы SAML 2.0 используются для верификации и обмена пользовательскими учетными записями с приложениями

SAML federation верифицирует состояние аутентификации пользователя, используя специальные токены (пароли не передаются)

Web-браузер

Service Provider (SP)

Identity Provider (IdP)

1) Иван обращается к Salesforce URL

2) Salesforce посылает запрос на аутентификацию IdP

3) Верификация Ивана ИЛИ запрос на аутентификацию

4) Ивана браузер DAG SSO URL

5) Иван аутентифицируется

6) DAG переправляет браузер Ивана к Salesforce для предоставления доступа с помощью токена

7) Иван получает доступ к Salesforce

Протоколы идентификации бывают разные и они тоже эволюционируют

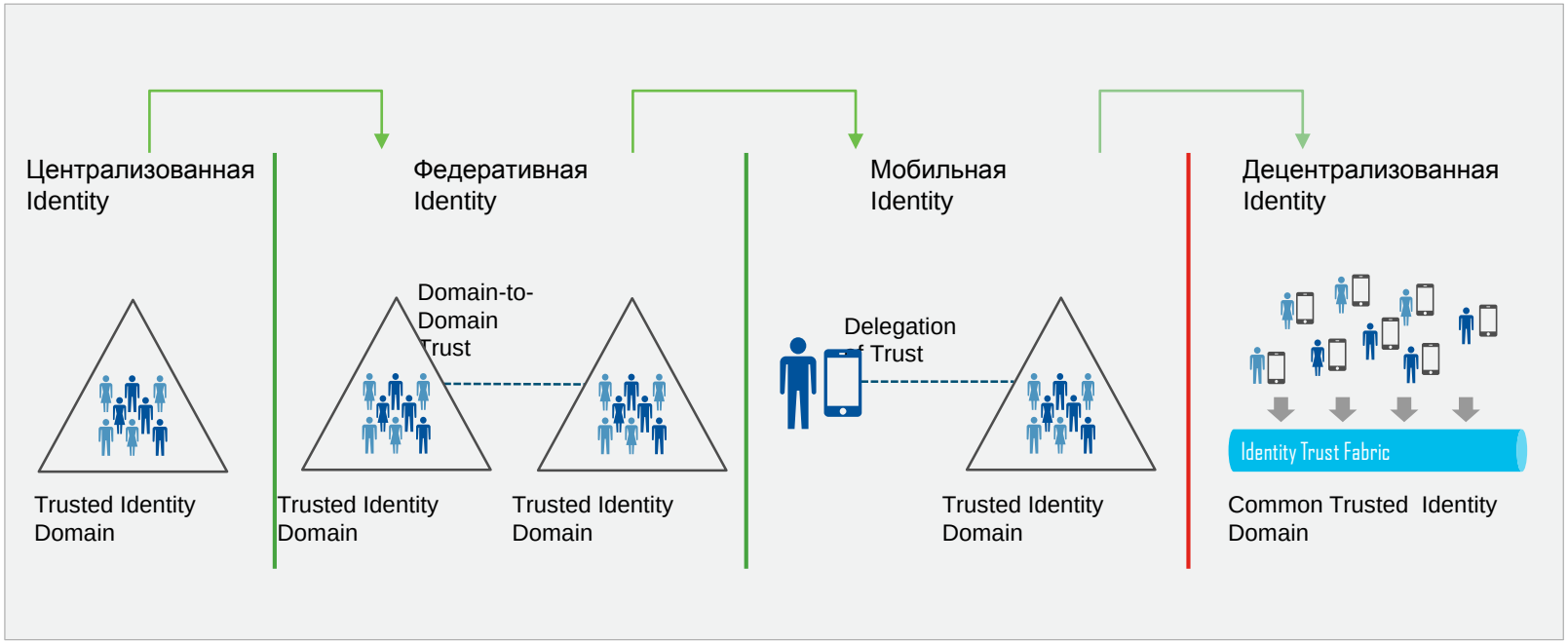
				
Windows Hello for Business	**FIDO протоколы**	**Phone-as-a-Token аутентификация**	**Биометрическая аутентификация**	**Сертификаты и Smart Cards**
•Аутентфикация через Active Directory и Azure AD •Устройства Windows 10 •Распознавание лица, отпечатков пальцев, локальные PIN и ключи безопасности FIDO2	•UAF •WebAuthn •CTAP2 •Локальная биометрическая аутентификация •Ключи безопасности FIDO2	•Мобильный push и мобильный OTP с локальной биометрической аутентификацией	•Лицо, голос, радужка глаза, отпечатки пальцев и геометрия лица •Встроенная в устройство или проприетарная •Локальная или централизованная архитектура	•Smart cards и другие аппаратные токены •Аутентификация по сертификатам для VPN и Wi-Fi •VPN, Wi-Fi, web и email доступ с управляемых устройств

Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей
- Добавление непрерывного анализа с помощью различных систем аналитики, UEBA, антифрода и т.п.
- Дополнение биометрической идентификацией
- Дополнение многофакторной аутентификацией
- Оцените перспективы применения разных приложений, включая облачные и для удаленного доступа
- Дополните системой облачной MFA

Куда это все развивается?

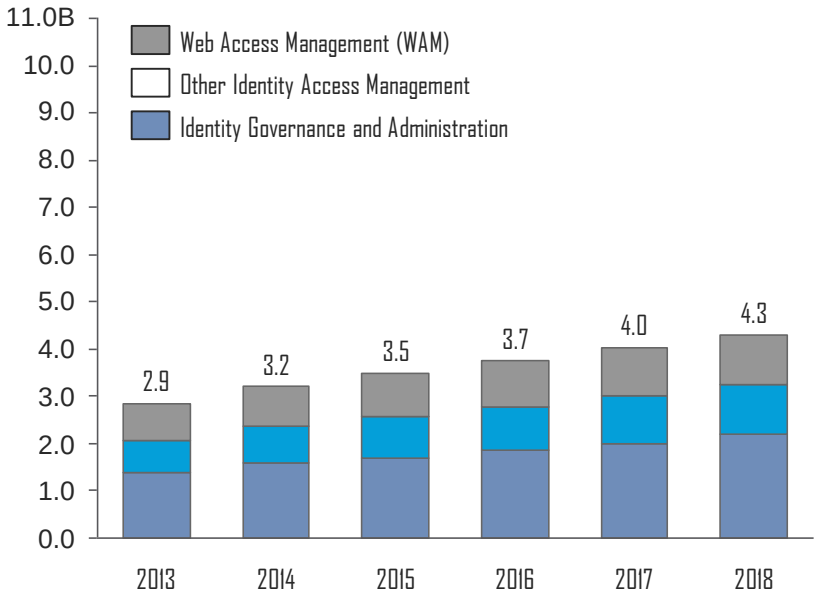
А теперь… блокчейн



Digital Identity

- Digital identity входит в топ дискуссий на последних Blockchain Summit
  - Государственные регистрации и и нотариальные сервисы
  - Управление web-доступом
  - Реестры цифровых прав
- Предложение использовать блокчейн для улучшения биометрической системы идентификации в Индии

Размер рынка Digital Identity ($млрд)



Source: Gartner , CSTG research

Целостная цифровая идентичность

ПРОБЛЕМА

- **> 1 миллиарда людей не имеют никакого официально признаваемого идентификатора**
- **Без идентификации они части невидны, не могут голосовать, не получают медпомощи, образования, финансов и т.п.**
- **Без аккуратных данных о популяции, частные и госорганизации не могут предоставлять сервисы людям**

РЕШЕНИЕ БЛОКЧЕЙН

- **Взаимодействует между блокчейнами**, облаками и организациями, собирая воедино и оцифровывая идентификационные данные, которые часто находятся на разных континентах (GocID, медзаписи, пенсионные записи и т.д.)
- **Предоставляет людям** на платформе возможность **прямого согласия** на то, кто имеет доступ к их данным, а также когда и с кем стоит делиться этой информацией
- **Предоставляет возможность организациям** точно **обслуживать людей** на основе записей в блокчейне

СЕТЬ БЛОКЧЕЙН

- Государство
- Министерство здравоохранения
- Национальное бюро регистраций
- Избирательные комиссии
- Работа с беженцами
- ООН

УРОВНИ ЦЕННОСТИ

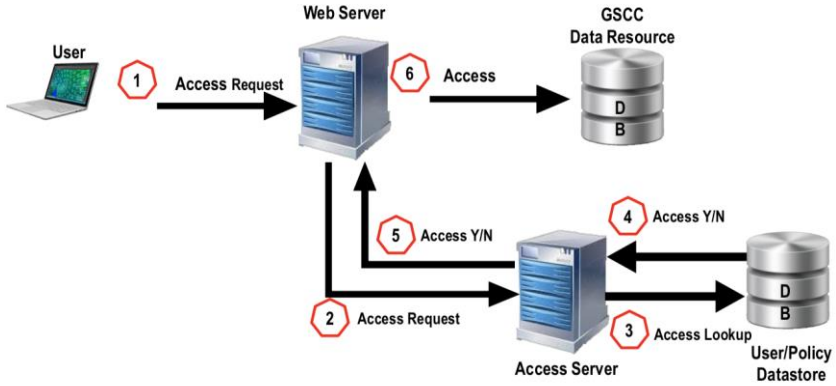
- Расширение возможности людей с идентификацией
- Экономические возможности
- Глобальное развитие

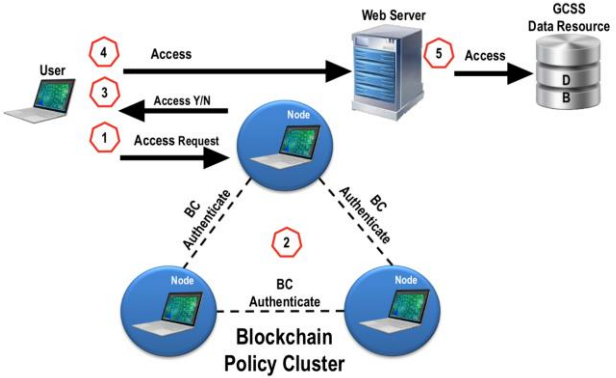
https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/

Реальные кейсы с блокчейном в Identity

- Эстонское правительство на базе решений Guardtime
- BlockVault – децентрализованный менеджер паролей
- Civic – отказ от паролей, имен, 3rd-аутентификаторов или физических токенов
- REMME – защита от атак за счет MFA пользователей и устройств. SSL-сертификаты на блокчейне
- CertCoin – PKI на блокчейне
- А также Sovrin, Evernym, Alastria, uPort…

Академия морской пехоты ВМФ США применяет блокчейн для доступа к системе управления поставками





На базе Oracle Access Management

67% всех запросов на доступ связаны с проверками прав доступа

Полученные преимущества

- Децентрализованная аутентификация пользователей
- Потенциальное снижение сетевой загрузки
- Не требуется ДМЗ
- Нет централизованного дорогостоящего web-сервера и хранилища
- Потенциальный рост доступности для удаленных пользователей
- Реализация политики на уровне алгоритма

Маркетинговый хайп

- Разные реализации имеют разную функциональность
- Часто сложно отделить маркетинг от реальности
- По-прежнему масштабируемость остается проблемой и направлением активных исследований
- Блокчейн более сложен и ему не хватает прозрачности и аудируемости традиционных технологий
- Отсутствие общих стандартов и правил

В ИБ блокчейн пока
не столь распространен

Вернемся на землю и подведем итоги

Рекомендации

- Правильно выбирать пароли пользователям
- Правильно управлять паролями внутри организации
- Использовать 802.1x для аутентификации устройств
- Добавление контекста для расширенной идентификации и аутентификации устройств и пользователей
- Добавление непрерывного анализа с помощью различных систем аналитики, UEBA, антифрода и т.п.
- Дополнение биометрической идентификацией
- Дополнение многофакторной аутентификацией
- Оцените перспективы применения разных приложений, включая облачные и для удаленного доступа
- Дополните системой облачной MFA

У меня нет времени смотреть на новые решения по ИБ – мне с угрозами бороться надо!

Рекомендации

Через неделю

- ❑ Оцените ваши текущие задачи, требующие идентификации пользователей, устройств и приложений
- ❑ Составьте перечень требований к системе идентификации

Через 30 дней

- ❑ Составьте перечень потенциальных поставщиков нужного решения
- ❑ Запланируйте пилотный проект с выбранным вами решением

Через 180 дней

- ❑ Оцените первые результаты пилота решения
- ❑ Запланируйте его развитие на всю организаци/

Спасибо за внимание!

alukatsk@cisco.com