The bridge to possible

Модель сетевого доступа с нулевым доверием (Zero Trust) на марше

Михаил Кадер, инженер

mkader@cisco.com

Workforce Zero Trust = Удобнее + Безопаснее

Отсутствие пароля

Беспарольная Аутентификация

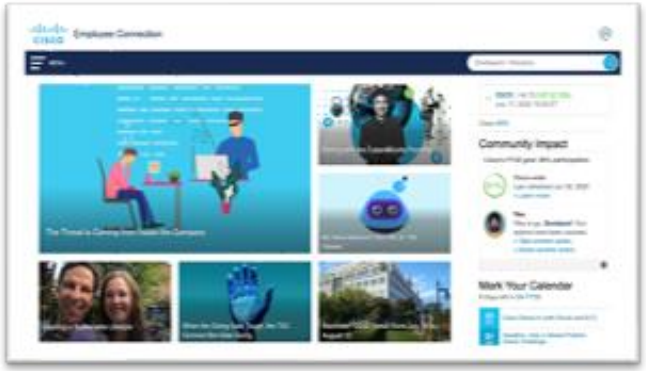
Сертификат устройства

Состояние устройства

MFA

Облачные приложения

Межсетевой экран



Локальные приложения

Без VPN

Обзор Workforce Zero Trust

Чем отличается подход Zero-Trust

Традиционный подход

Доверие основывается на том из какой сети приходит запрос

Как только злоумышленник проникает вовнутрь, он может осуществлять спонтанное перемещение по сети и получать нужный доступ

Безопасность не распространяется на новый облачный периметр, мобильное и гибридное окружения

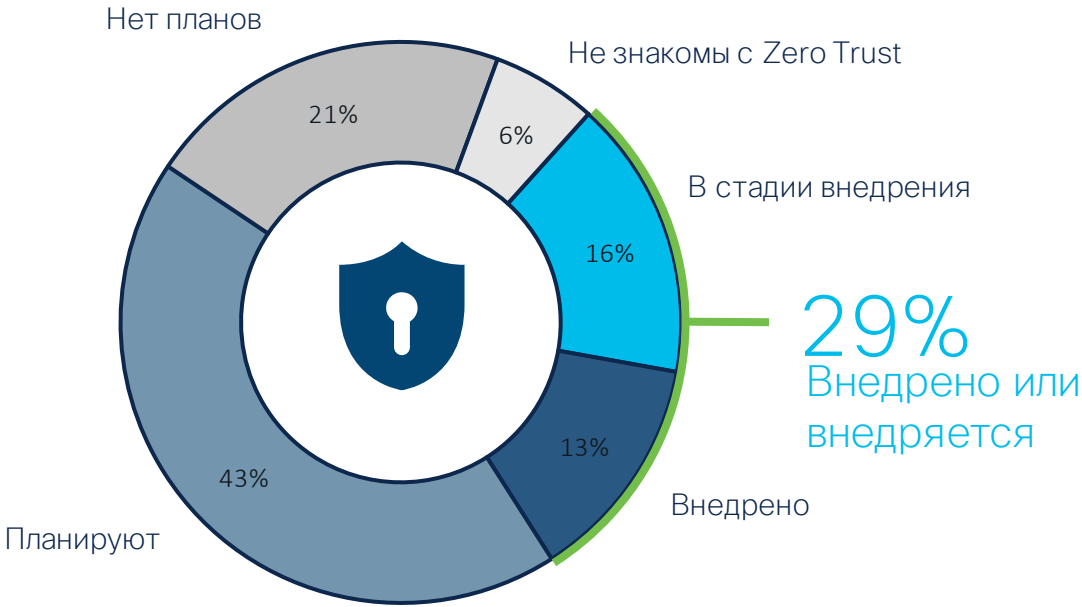
Подход Zero Trust

Доверие устанавливается для каждой попытки подключения, независимо от того откуда пришел запрос

Безопасный доступ в Ваши приложения и сети. Убедиться в том что только нужные пользователи и устройства получают доступ

Расширение доверия с поддержкой современных BYOD, облачных приложений, гибридных окружений и прочего.

73% Организаций Планируют Внедрение Zero Trust



Zero Trust везде!

Workforce

Доступ пользователей и устройств

Пользователь тот за кого себя выдает?

Есть ли у них доступ к нужным приложениям?

Безопасно ли их устройство?

Доверенное ли устройство?

Workload

Доступ к приложениями и сервисам

Какие приложения используются в сети?

Что обращается к приложениям и данным?

Безопасны ли и доверены коммуникации с приложениями?

Workplace

Сетевой доступ

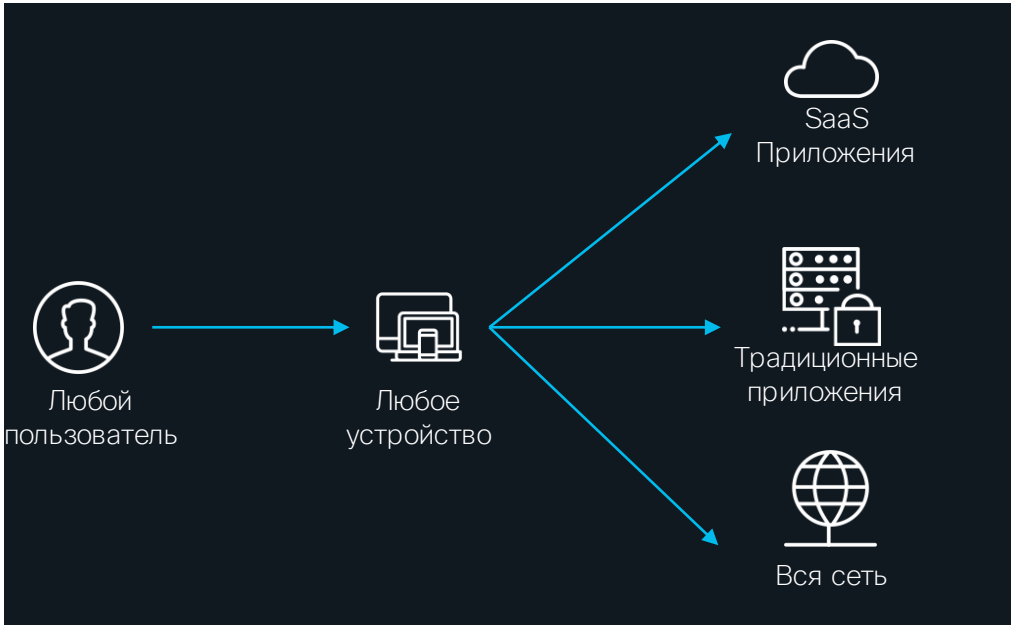
Аутентифицируются ли пользователи и устройства в сети?

Какой доступ они получают?

Безопасны ли эти устройства?

Сетевая сегментация основана на доверии?

Защита пользователя



Доверие пользователю

- ✓ MFA
- ✓ Адаптивный MFA
- ✓ Без пароля

Доверие устройству

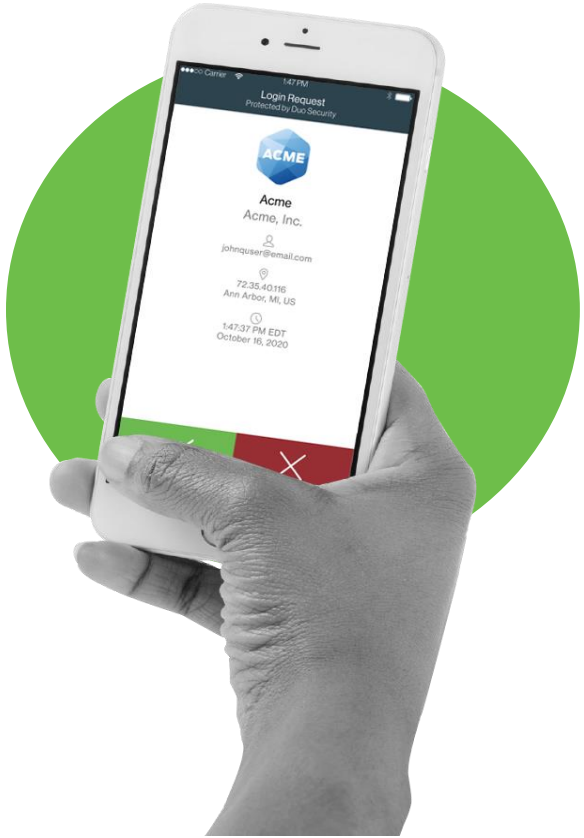
- ✓ PCs и Macs
- ✓ iOS и Android

Безопасный доступ

- ✓ Single Sign-On (SSO)
- ✓ Удаленный доступ без VPN

Удобство для пользователя

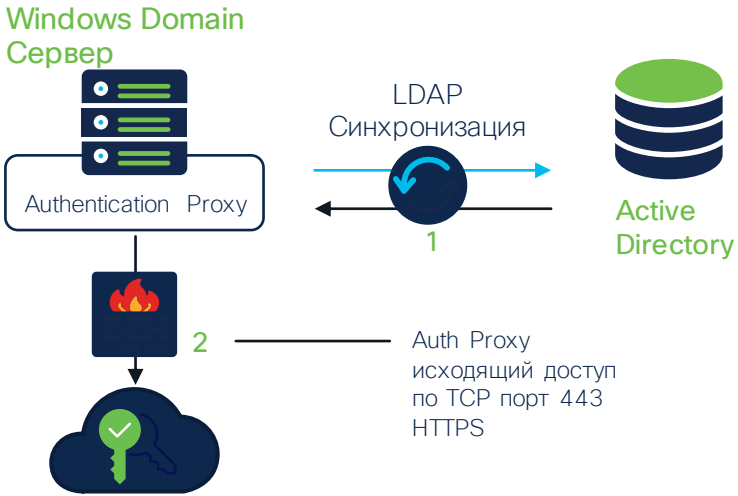
- Мгновенная интеграция всех приложений
- Пользователи сами регистрируются за минуты
- Аутентификация за секунды без ввода кодов



Легкая интеграция пользователей AD, LDAP или Azure

Импортируйте пользователей напрямую в Duo из Azure без локального программного обеспечения

Импорт пользователей через LDAP из AD либо OpenLDAP каталогов. Требуется установка Duo Authentication proxy



Неизменность основной аутентификации

Основное устройство пользователя
Основная Аутентификация
Выполняется Вами.

Ваши Сервера и Приложения
Связь с сервером

Запрос отправляется в MFA

Основной сервис и движок политик всегда в облаке

Вторичное устройство пользователя
Вторичная аутентификация
Пользователь подтверждает логин на своем устройстве

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

Основное устройство пользователя

Успех!

Пользователь получил доступ

Защита любых приложений

Собственные приложения (APIs)

Microsoft Окружение

Облачные сервисы

Unix Устройства (SSH Сессии)

Внутренние приложения (VPNs)

Облачные приложения

Web Приложения

SAML 2.0 Приложения

Интеграция с SSO

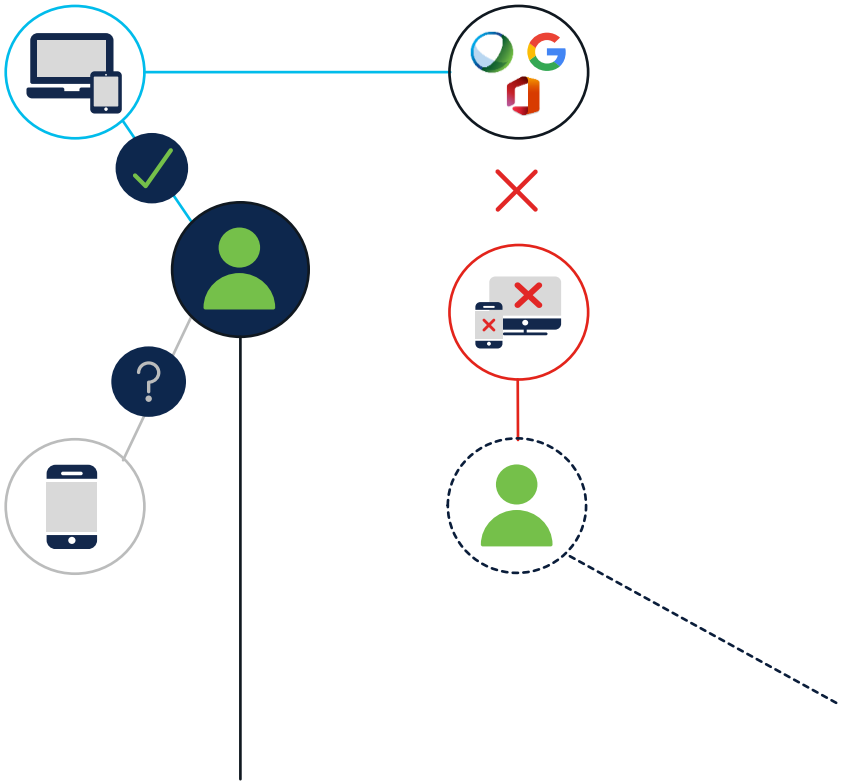
- Получайте простой доступ во все облачные приложения из единого окна
- Внедряйте целостную политику доступа во всех облачных приложениях
- Обезопасить каждое облачное приложение

Поддержка сторонних SSO/IAM

- Нативная интеграция с множеством Identity/SSO платформ
- Обеспечить пользователям целостный опыт работы с единой политикой безопасности во всех приложениях
- Легко получите осведомленность и доверие во всех приложениях

Адаптивные политики

- Создавайте настраиваемые политики безопасности
- Используйте уровни контроля Групповой, Приложения и Глобальный
- Устанавливайте уровень доверия основываясь на пользователях и устройствах



Установление доверия Пользователей и Устройств

Как получить данные об устройствах?

Мобильные Устройства

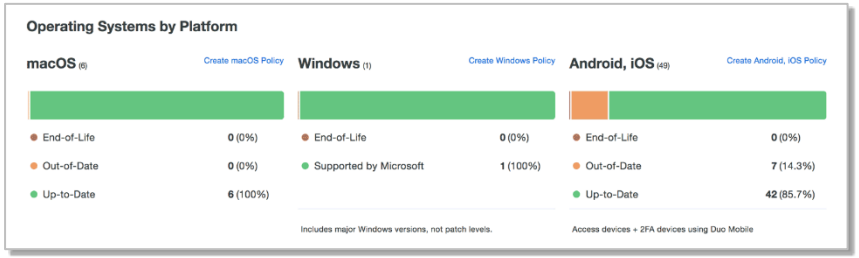
Мобильные браузеры и приложения

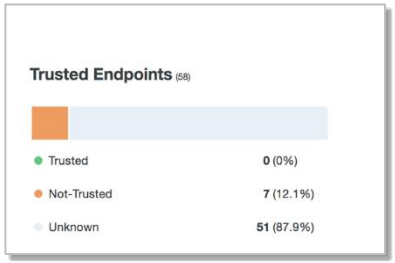
Ноутбуки/Хосты

Браузеры ноутбуков/хостов и приложения

Полная осведомленность

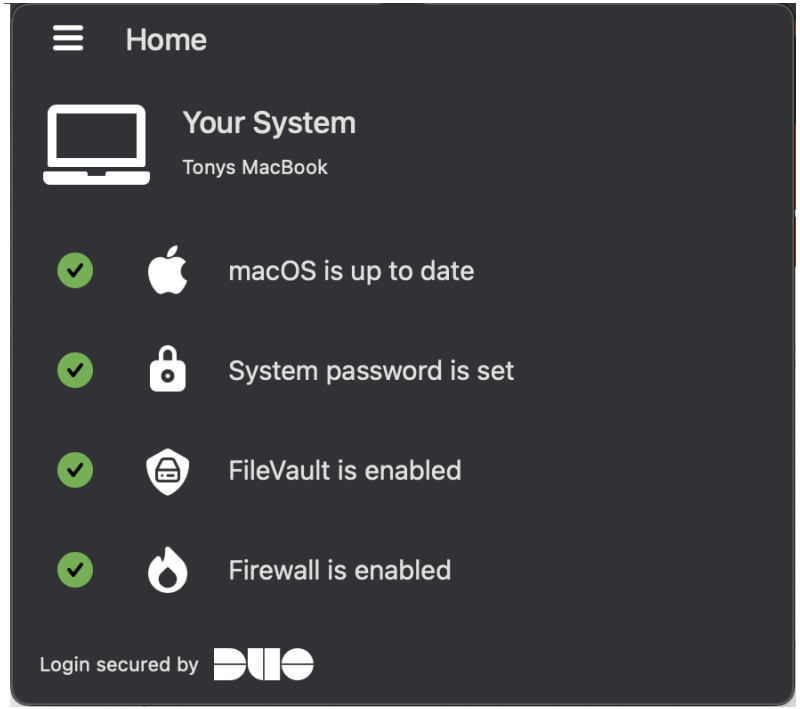
- Получите полную осведомленность о всех Ваших устройствах





Глубокая осведомленность о хостах и ноутбуках

- Оценка безопасности хостов
- Проверка устройств до их логина
- Корпоративное или BYOD устройство
- Поддержка Web приложений
- Windows 10 и MacOS



Отличайте управляемые устройства от BYOD

Mobile

Duo: Приложение Duo Mobile может использоваться для доверия мобильному устройству. (подходит для организаций без MDM)

Нативно: AirWatch, MobileIron, Google G Suite, Sophos

Windows

Нативно: Microsoft AD, Ivanti (Landesk), AMP

Скриптами: Symantec Altiris, Chef, Microsoft SCCM, AirWatch и др.

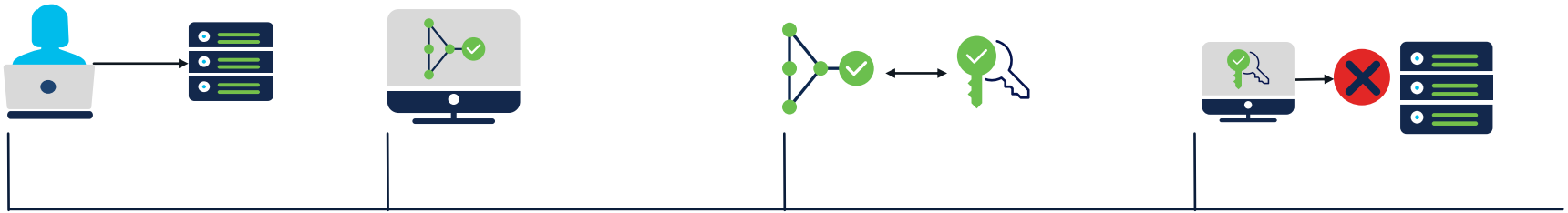
MacOS

Нативно: Jamf, AMP

Скриптами : Symantec Altiris, Chef, Microsoft SCCM, AirWatch и др

Постоянное наблюдение (xDR)

Совместная работа для обеспечения безопасного доступа



Пользователи используют свои устройств для доступа к приложениям

EDR, запущенный на хосте обнаруживает malware

EDR уведомляет MFA об инфекции на устройстве

MFA блокирует доступ устройств в приложения

Zero Trust

	Workforce	Workload	Workplace
			
Кто или Что	Люди и их Устройства (Ноутбук, Планшет, Смартфон)	Приложения, Сервисы, Микросервисы	IT Хосты и Сервера, Internet of Things (IoT) устройства и OT/ICS
Проверка доверия	Доступ к приложениям	Связь с другими системами	Доступ в сеть: Проводной, Беспроводной, и VPN
От	Отовсюду	Локальные, Гибридные и Публичные облака	Локальные, Гибридные и Публичные облака
	Доступ пользователя и устройства	Доступ к сервисам и приложениям	Сетевой доступ

Заключение

Улучшение опыта работы пользователей с Zero Trust

- Подготовьте к гибридной работе с
  - С целостным опытом как для локальной, так и удаленной работы
  - Централизованная и целостная политика безопасности с SASE
- Начните путешествие с Workforce Zero Trust:
  - Включите SSO и MFA для своей организации
  - Внедрите доверие для Пользователя и Устройства
  - Разверните Zero Trust Network Access для популярных и критичных приложений

Workforce

Доступ пользователей и устройств

Пользователь тот за кого себя выдает?

Есть ли у них доступ к нужным приложениям?

Безопасно ли их устройство?

Доверенное ли устройство?

The bridge to possible

Спасибо!