Концепция Zero Trust в цифровом рабочем пространстве

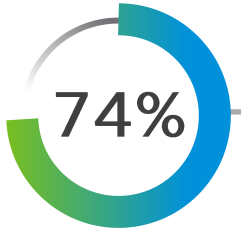
Дима Гарф
Ведущий инженер по решениям EUC
Мария Бочарова
Инженер по решениям VMware Казахстан и Центральная Азия

Ноябрь 2022

Понятие “Рабочее место” претерпело кардинальные изменения

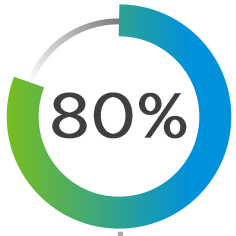
И меняется каждое поколение

Гибридный формат работы никуда не исчезнет



Гибридная модель работы

Компаний используют или планируют внедрить гибридную модель работы.[1]

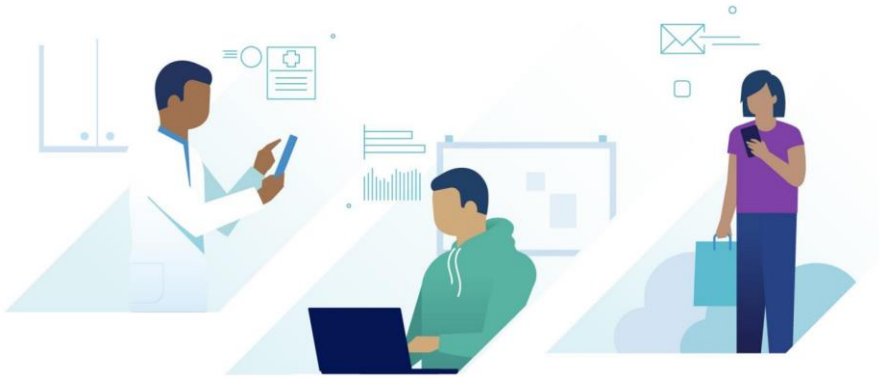


Разнообразие Кадрового резерва

Гибридная работа позволяет компаниям получить **разнообразный кадровый резерв.**[2]

Доступ к цифровым инструментам

Работодатели должны предоставлять **доступ к цифровым инструментам** для возможности удалённой работы.[3]



1. US companies only, Source: Future of Work 2022 Hybrid Work Stats, Zippia
2, 3. Vanson Bourne. “The Virtual Floorplan” October 2021.

Вызовы ИБ при распределении рабочей силы

Отсутствие опыта и высокие риски

Могу ли я доверять данному устройству?

Как я могу обеспечить надежную работу пользователей в удаленных локациях?

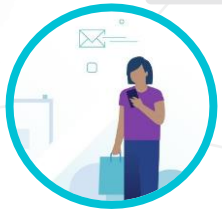
Как я могу эффективно и безопасно поддерживать удаленный доступ?

Как восстановить безопасный доступ?

Как защитить мои данные?

Как поддерживать личные устройства?

Как я могу обеспечить беспрепятственный доступ для повышения производительности?



Реализация концепции безопасного доступа

Защищайте доступ ко всем приложениям с помощью Single-Sign-On

Подтверждайте личность с помощью Мультифакторной Аутентификации(MFA)

Контролируйте доступ с помощью умный полик и проверок на риски

Обеспечьте наименее привилегированный доступ с надежным управлением

Цифровая рабочая область

Виртуализация

Виртуальные приложения
Виртуальные рабочие столы

TS | SBC | RDSH | VDI

Идентификация

Аутентификация
SSO

Мобильность

EMM | MDM |
MAM | MIM

Безопасность

Защита конечных точек
Мобильная защита от угроз

Концепция Zero Trust от точки до точки: Идеально для распределённого рабочего пространства

VMware Anywhere Workspace защищает потоки данных от пользователя/ устройства до приложения

Любой пользователь,
Любое устройство,
Любое местоположение

Zero Trust
Принципы безопасности

Доверие и проверка любого устройства	Непрерывная проверка уровня доступа пользователя	Защищённый доступ к любым приложениям и данным

VMware Horizon 8

Безопасность

- Глубокая экспертиза с Horizon Instant Clone
- Основные критерии безопасности с Horizon NIAP
- Windows Hello для бизнеса
  Предотвращение кейлоггеров
  Предотвращение записи экрана
  Улучшения водяных знаков
  Запись сессий

VMware Horizon®

Пользовательский Опыт

- Blast улучшает визуальное восприятие
- Доступ к персональному хранилищу
- Расширенные улучшения для Microsoft Teams

Безопасность и пользовательский опыт не должны быть компромиссом — оптимизируйте и то, и другое

Unified Endpoint Management (UEM) устраняет разрозненность ИТ и ИБ

Workspace ONE UEM Объединяет инструменты и процессы управления для повышения эффективности ИТ

vmware®

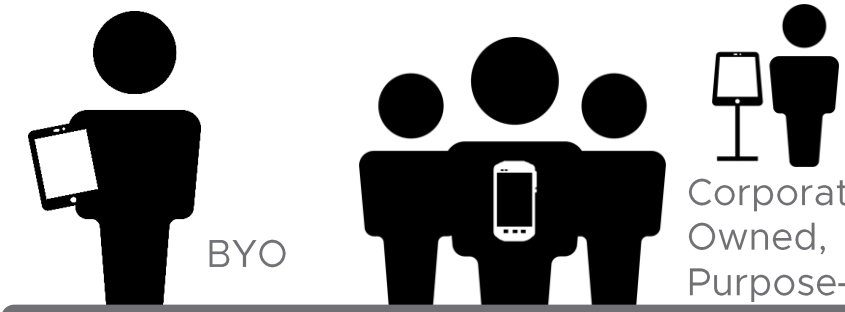
Workspace ONE™

трализованный менеджмент
Сопровождение жизненного цикла устройств
Защита между конечными точками
Интеллектуальная аналитика
Непрерывное обучение

Любое устройство

Desktops, Mobile, Connected 'Things'

Любая платформа



BYO

Corporate-Owned, Purpose-Built

Для любых типов пользователей

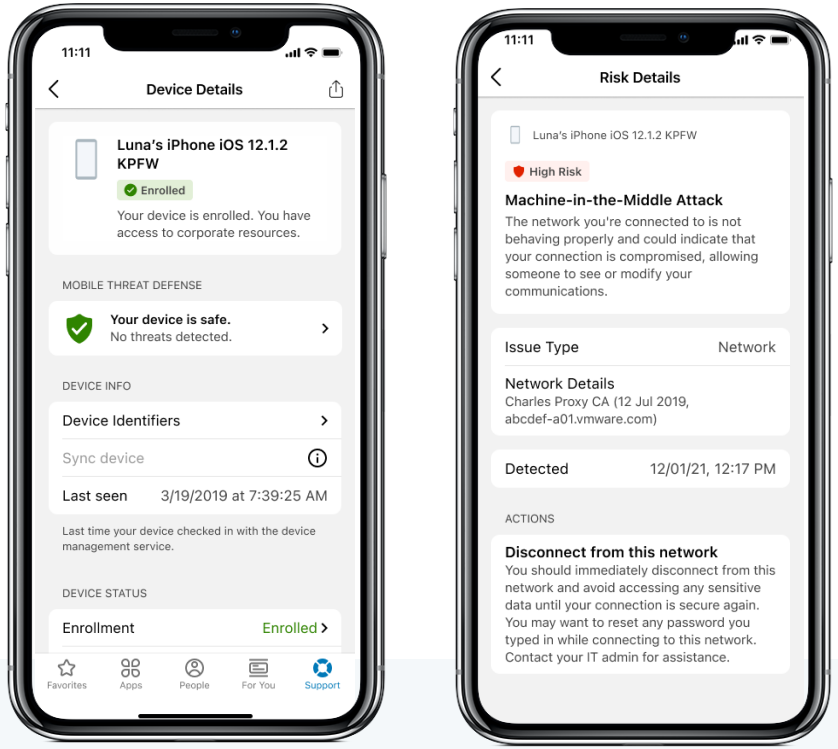
Workspace ONE Защита мобильных устройств

Расширенная безопасность для iOS, Android, и Chrome OS

VMware
Workspace ONE®
Mobile Threat Defense™

Безопасность мобильных устройств адресована:

- Угрозам приложений
- Уязвимости сайтов и контента, раскрытые в результате фишинга
- Угрозам нулевого дня и уязвимостям устройств
- Атаки типа «машина посередине»



Комплексная безопасность на базеLookout.

Автоматизированное и интегрированное управление и безопасность с помощью платформы Workspace ONE

Непрерывный доступ

Оценка контекста для определения доступа

Доверие, основанное на контексте

APP

Identity | Context | Login Risk | User Risk etc.

- MFA enforcement
- Restricted access

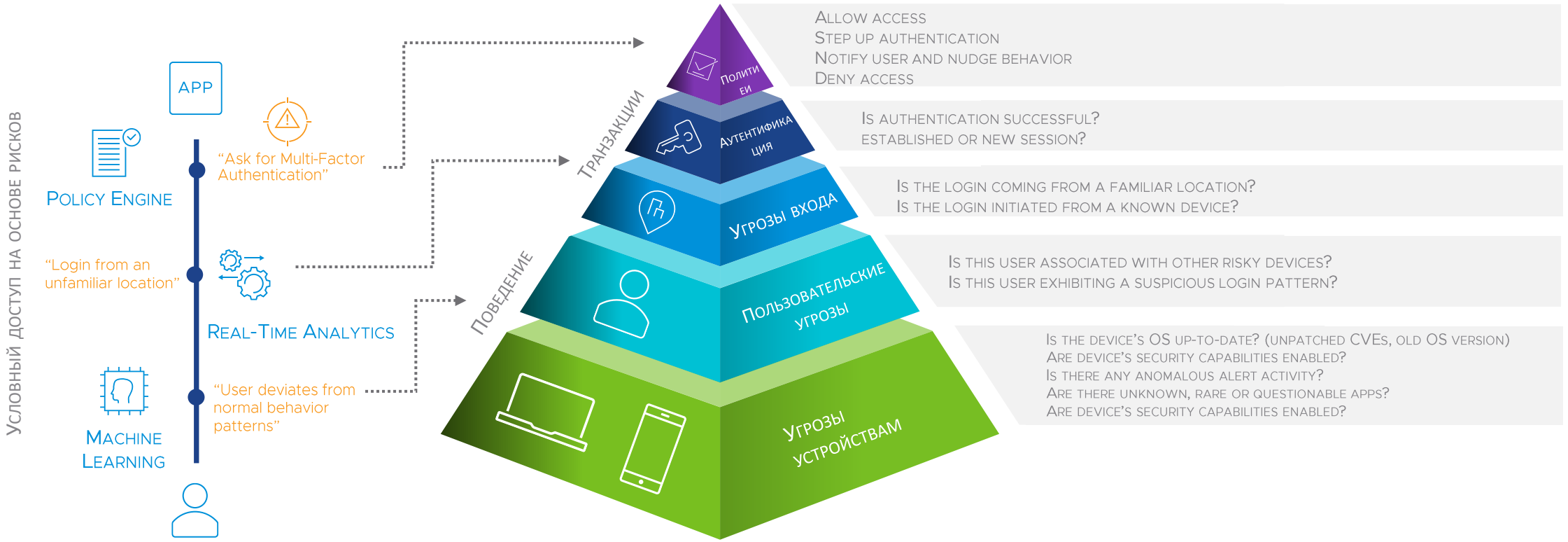
Доверие устройствам

APP

Managed | Jailbroken | Compliant etc.

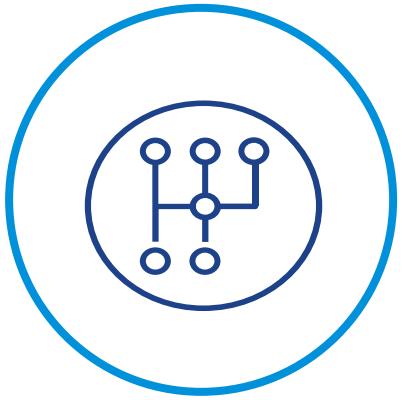
- Blocked
- App specific access
- Restricted access

Динамическая оценка риска

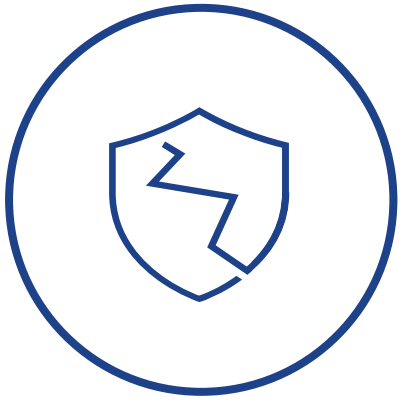


Пароли это проблема!

Слишком много и легко забываются



Проблемы с использованием



Легко украсть, собрать, воспроизвести

“На украденные учетные данные приходится почти 50% сторонних взломов, фишинговых атак, базовых атак на веб-приложения (BWAA) и системных вторжений.”

Source: Verizon Data Breach Investigation Report

Современная аутентификация: Надёжно и безопасно

Bad: Password	**Good:** Password and...	**Better:** Password and...	**Best:** Passwordless
123456	SMS	Authenticator (Push Notifications)	Authenticator (Phone Sign-in)
qwerty	Voice	Software Tokens OTP	Window Hello
password		Hardware Tokens OTP (Preview)	FIDO2 security key
iloveyou			Certificates
Password1			

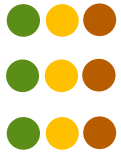
Беспарольная аутентификация в Workspace One Access

[MDM] **Managed** Devices 

[MAM] **Registered** Devices 

Unmanaged Device 

То, что вы ЗНАЕТЕ

1. Login Recovery Codes 
2. Security Questions

То, что у вас ЕСТЬ

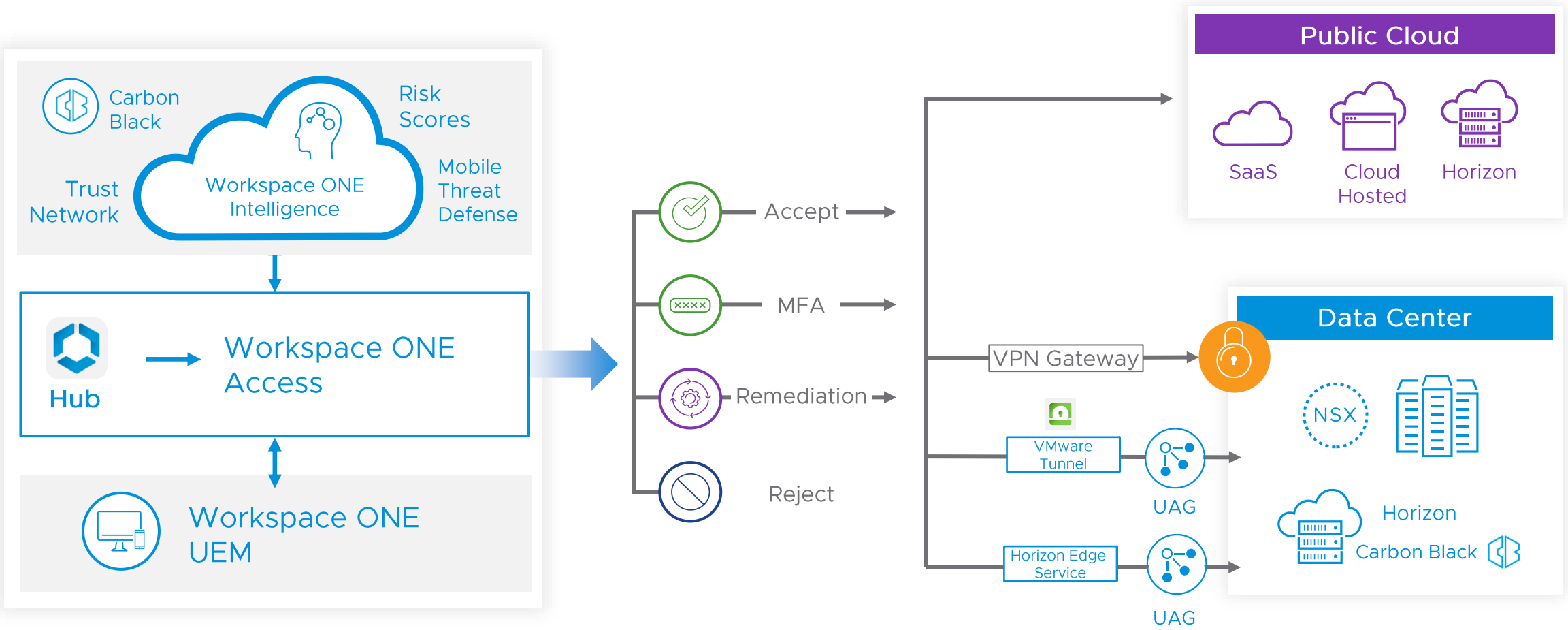
1. Built-in Certificate 
2. External Certificate 
3. UEM Token Auth 
4. Hub Verify Push 
5. Hub Verify TOTP 
6. Access TOTP 
7. Email – Magic Link 
8. FIDO 2 

То, что НУЖНО

1. Biometric FIDO 2 
2. Bluetooth/Access Point Login 

Anywhere Workspace

Обзор платформы Zero Trust



UEM – Unified Endpoint Management
UAG – Universal Access Gateway

Спасибо за внимание!