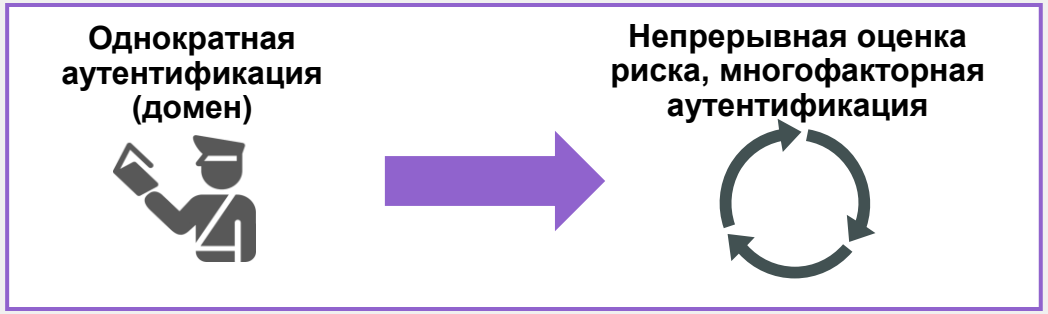
Архитектура сетевой безопасности с нулевым доверием (ZTNA)

FortiOS 7.0

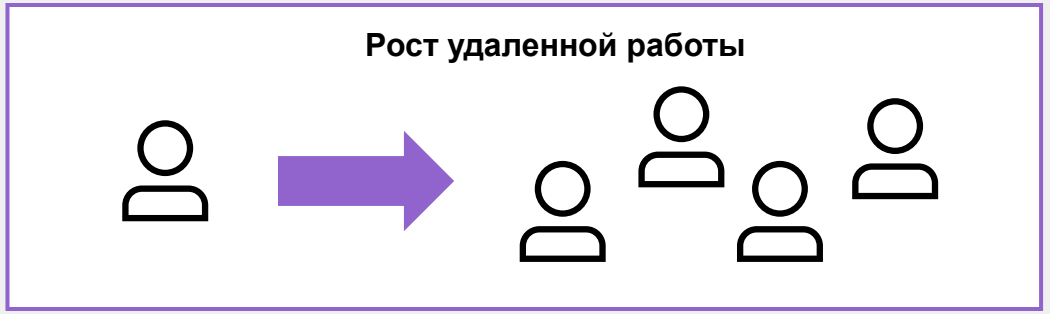
13/08/2021

Андрей Терехов, инженер

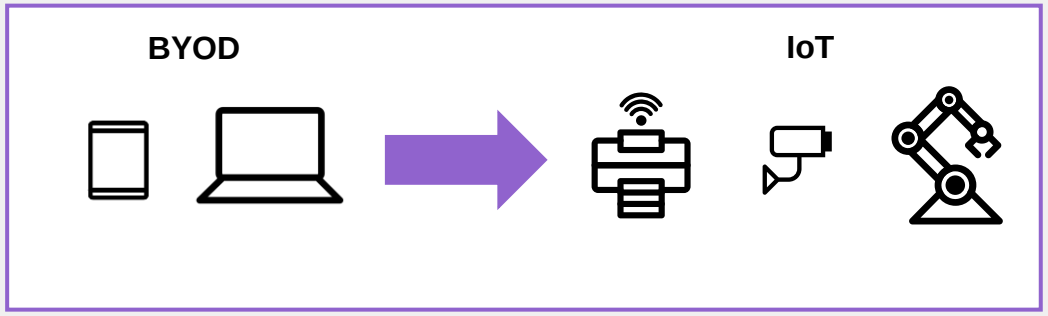
Тренды сетевого доступа в организациях



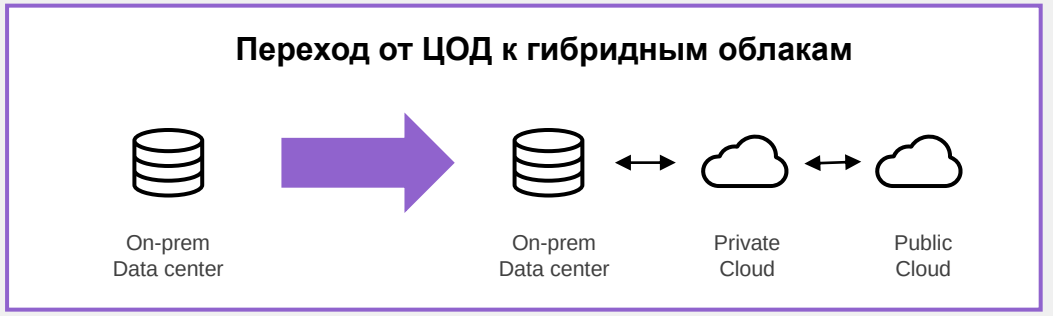
К 2024, 70% доступа к приложениям будет использовать многофакторную аутентификацию (10% на сегодня)[1]



К концу 2021, 30% рабочей силы перейдёт на постоянную удаленную работу[2]



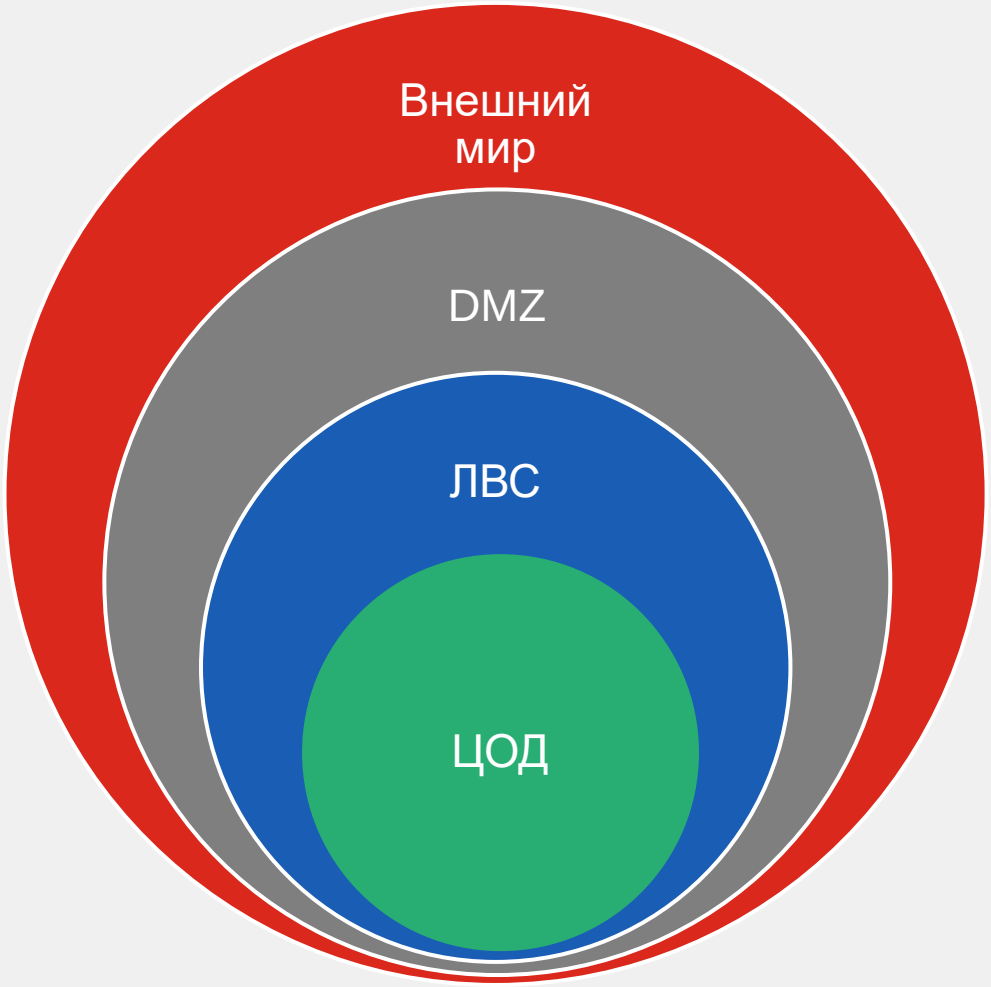
К 2025, в мире будет 12 **миллиардов** функционирующих IoT устройств[3]



Большинство организаций так или иначе использует облачные сервисы, что делает сценарии гибридной инфраструктуры всё более актуальными[4]

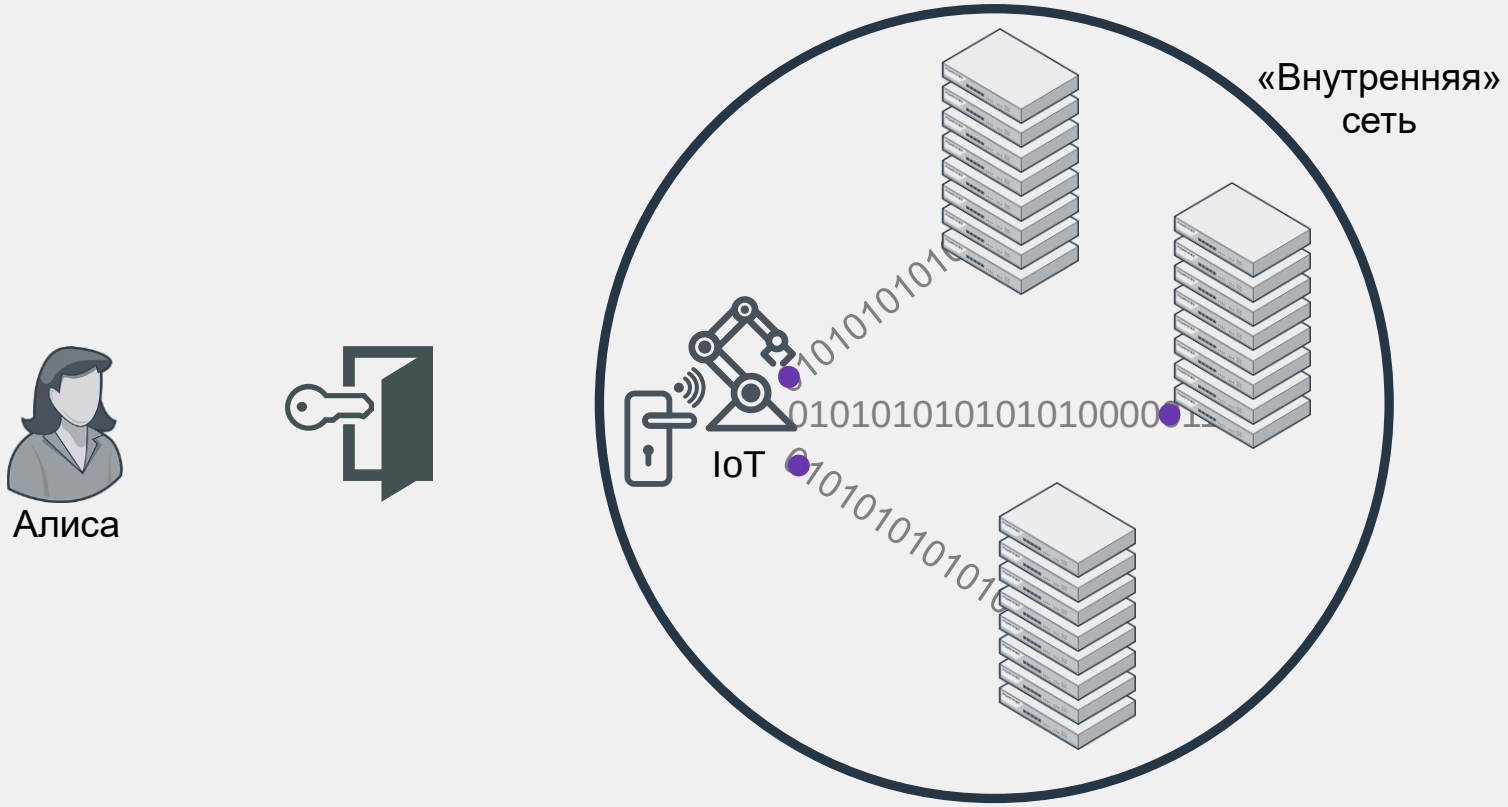
1 Gartner Magic Quadrant for Access Management, 12 August 2019
2 Global Workplace Analytics
3 Gartner IoT Forecast
4 Gartner Magic Quadrant for Public Cloud Managed Services, 4 May 2020

Меняются архитектуры



Проблема доверия на основе локации

Предполагаемое доверие несет риск



Принципы нулевого доверия

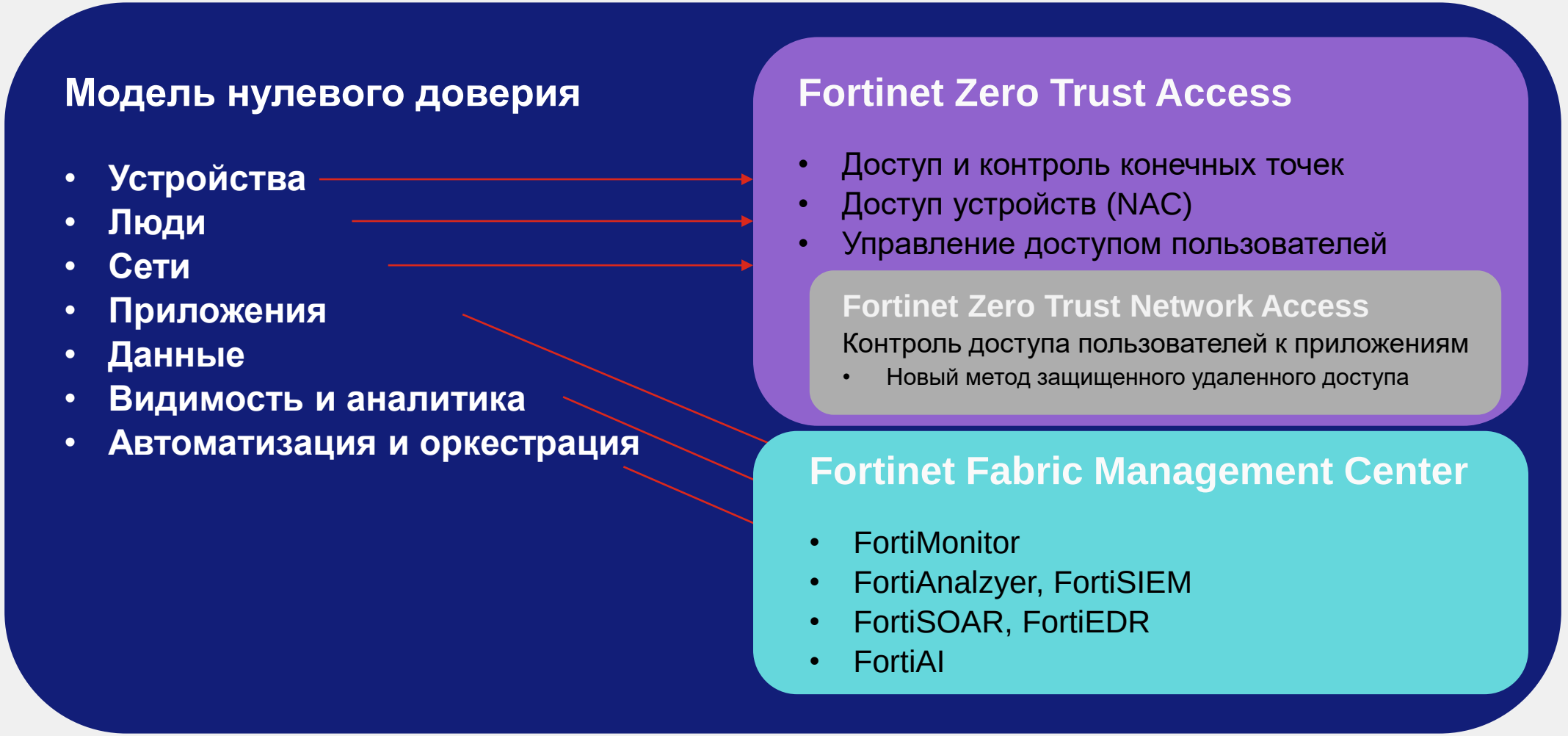
Для пользователей и устройств

- Проверка
  - Аутентификация и проверка – на повторяющейся основе

- Предоставление минимального доступа
  - Сегментация сети на небольшие легко контролируемые зоны
  - Контроль доступа к приложениям, данным, ресурсам
  - Минимизация привелегий в соответствии с ролью или необходимостью

- Предположение о компрометации
  - Проектирование с учётом возможного проникновения злоумышленников
  - Больше нет доверенных зон (например, офисная сеть)

Решения Fortinet в контексте модели нулевого доверия



Fortinet Security Fabric

Широта

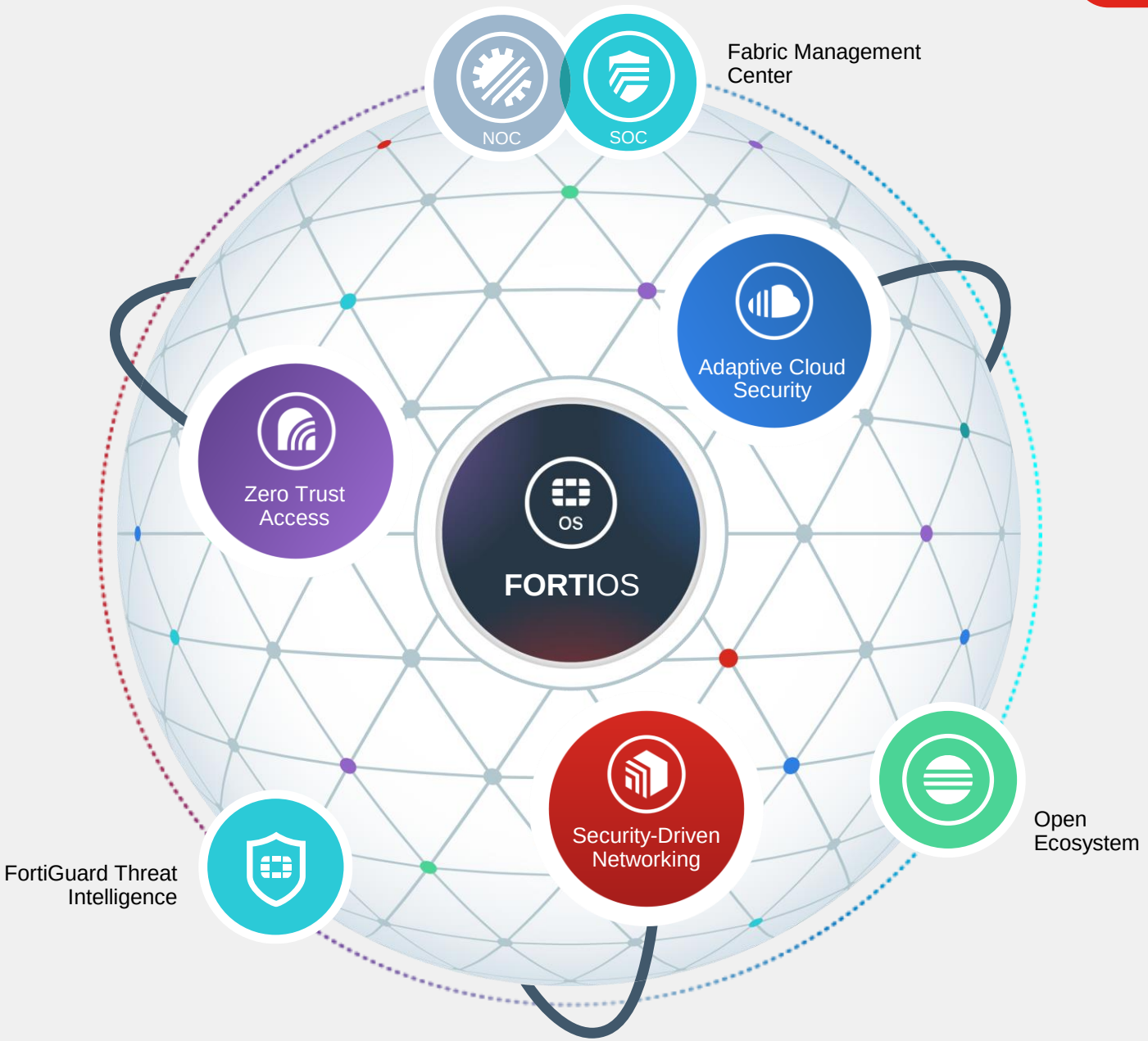
видимость и защита всей поверхности цифровой атаки для лучшего управления рисками

Интеграция

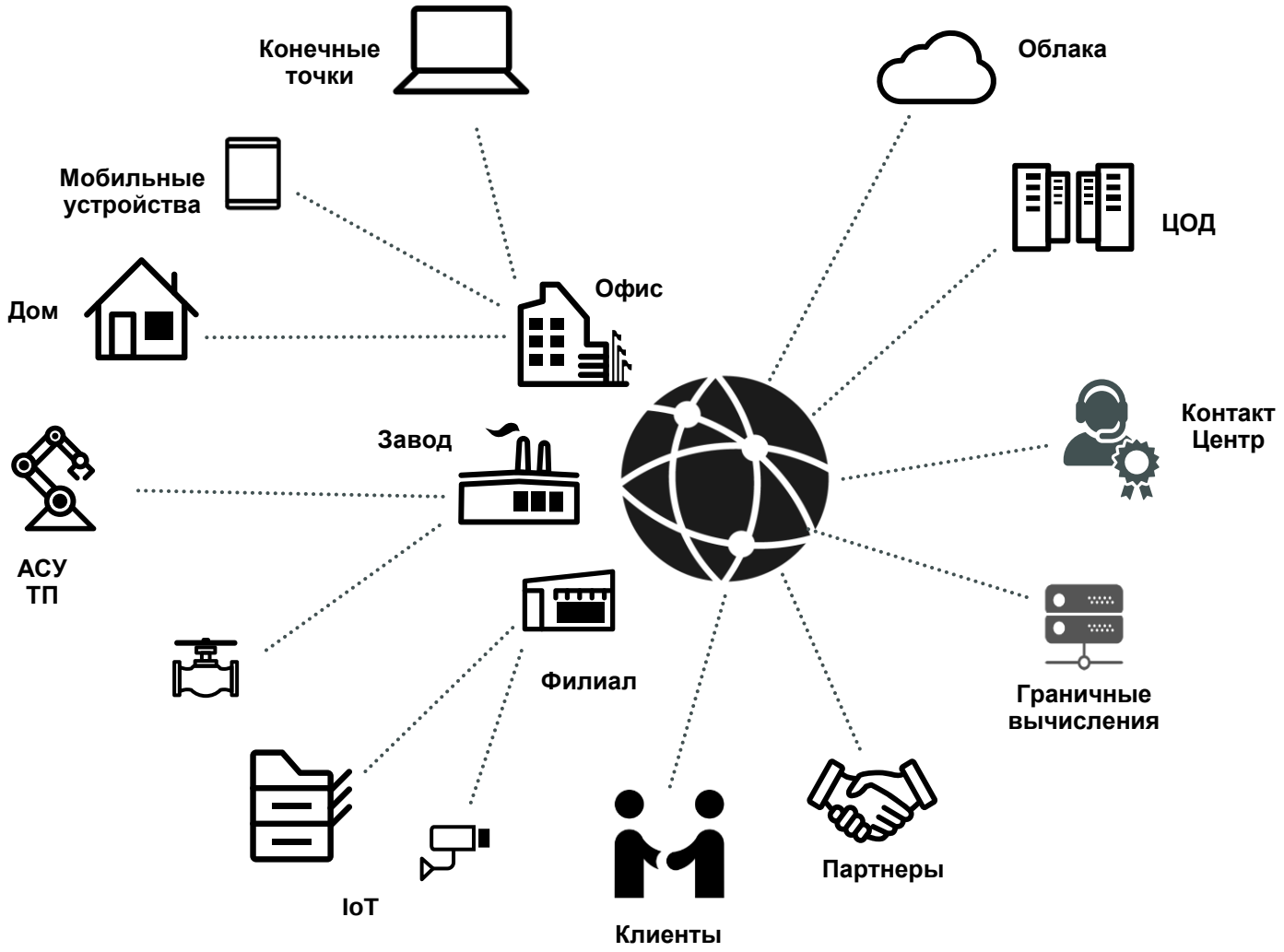
решение, которое снижает сложность управления и делится информацией об угрозах

Автоматизация

самовосстанавливающиеся сети с безопасностью на основе искусственного интеллекта для быстрой и эффективной работы



Zero Trust Access – Доступ с нулевым доверием



Знание и контроль всего и всех внутри и вне сети

Обеспечивает консистентную политику безопасности по всей сети, в облаках и за пределами сети

Zero Trust Network Access

До 2021

Zero Trust Access

Доступ пользователей и устройств

Управление доступом пользователей

Аутентификация

VPN туннели

Удаленный доступ

Контроль доступа к сети (NAC)

Сетевой доступ

В 2021 (с 7.0)

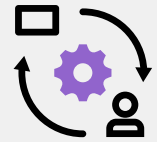
Zero Trust Access

Доступ пользователей и устройств

Управление доступом пользователей

Аутентификация

Доступ к сети с нулевым доверием (ZTNA)

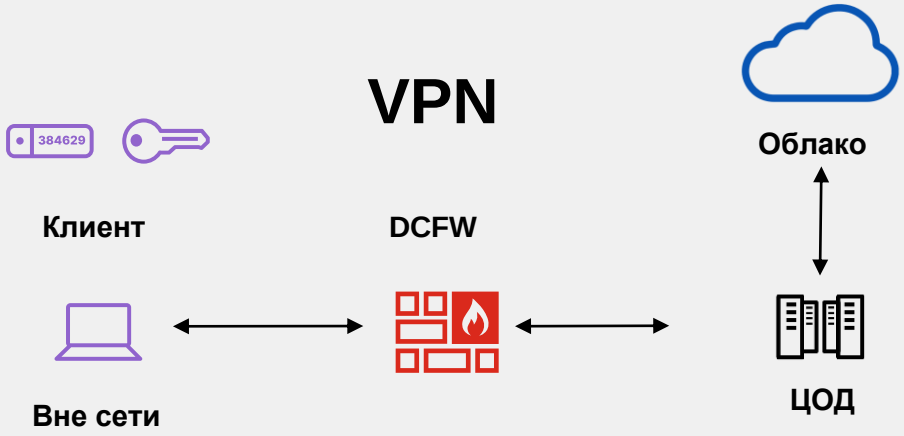


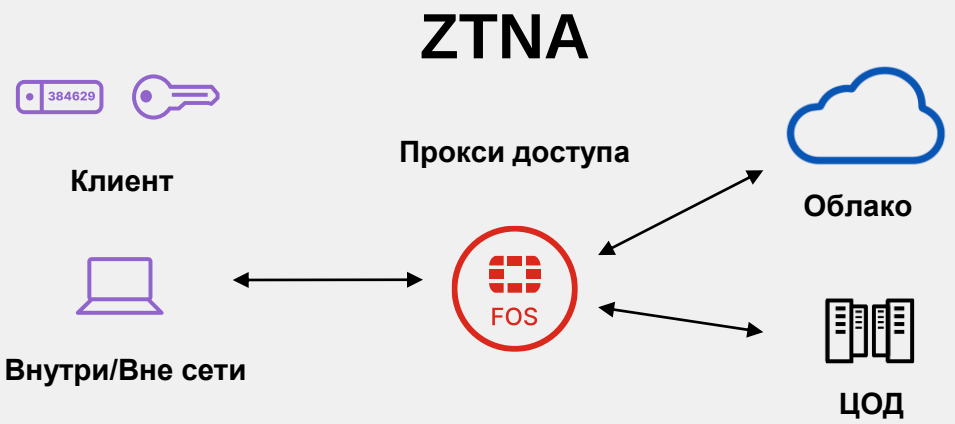
Удаленный доступ

Контроль доступа к сети (NAC)

Сетевой доступ

От традиционных VPN к ZTNA - эволюция



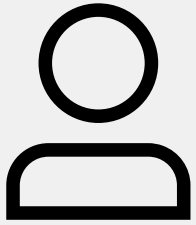


- Однократная проверка доверия
- Доступ ко всей внутренней сети
- Общий набор правил

- Повторяющаяся проверка доверия
- Доступ только к выбранным приложениям
- Набор правил на основе контекста

ZTNA – предпосылки для организаций

Удаленная работа из любой точки



Одинаковый доступ вне зависимости от локации пользователя

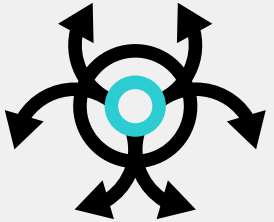
Удобство для пользователей

Переход к облачным сервисам

Предоставление доступа вне зависимости от локации приложения

Гибкое администрирование

Атаки Программ-шифровальщиков



Гранулярный доступ к приложениям

Снижение поверхности атаки

Удаленная работа с возможностями офисной

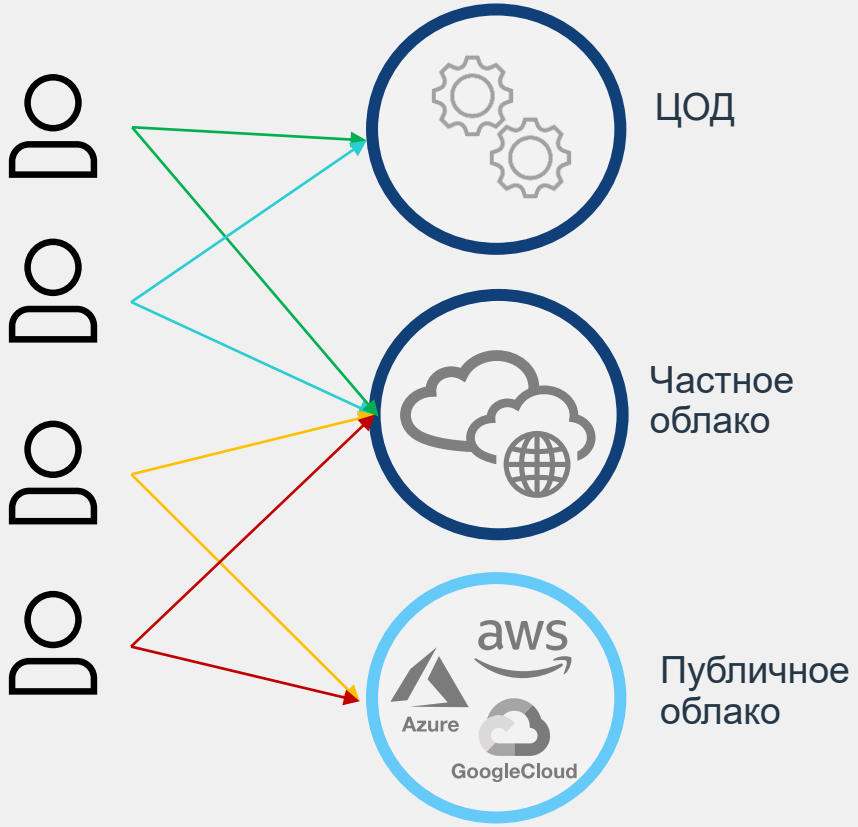
Повышение удобства

- Доступ изнутри или за пределами офиса
- Автоматические защищенные туннели к приложениям
- Поддержка единого входа (SSO)
- Не нужно знать, где находится приложение

Поддержка перехода к облакам

Контроль доступа к гибридной облачной инфраструктуре

- Приложения могут находиться где угодно
- Единое управление шлюзами доступа в собственной инфраструктуре и в облаках
- Группы пользователей обеспечивают быструю и простую настройку
  - Возможна гранулярная донастройка

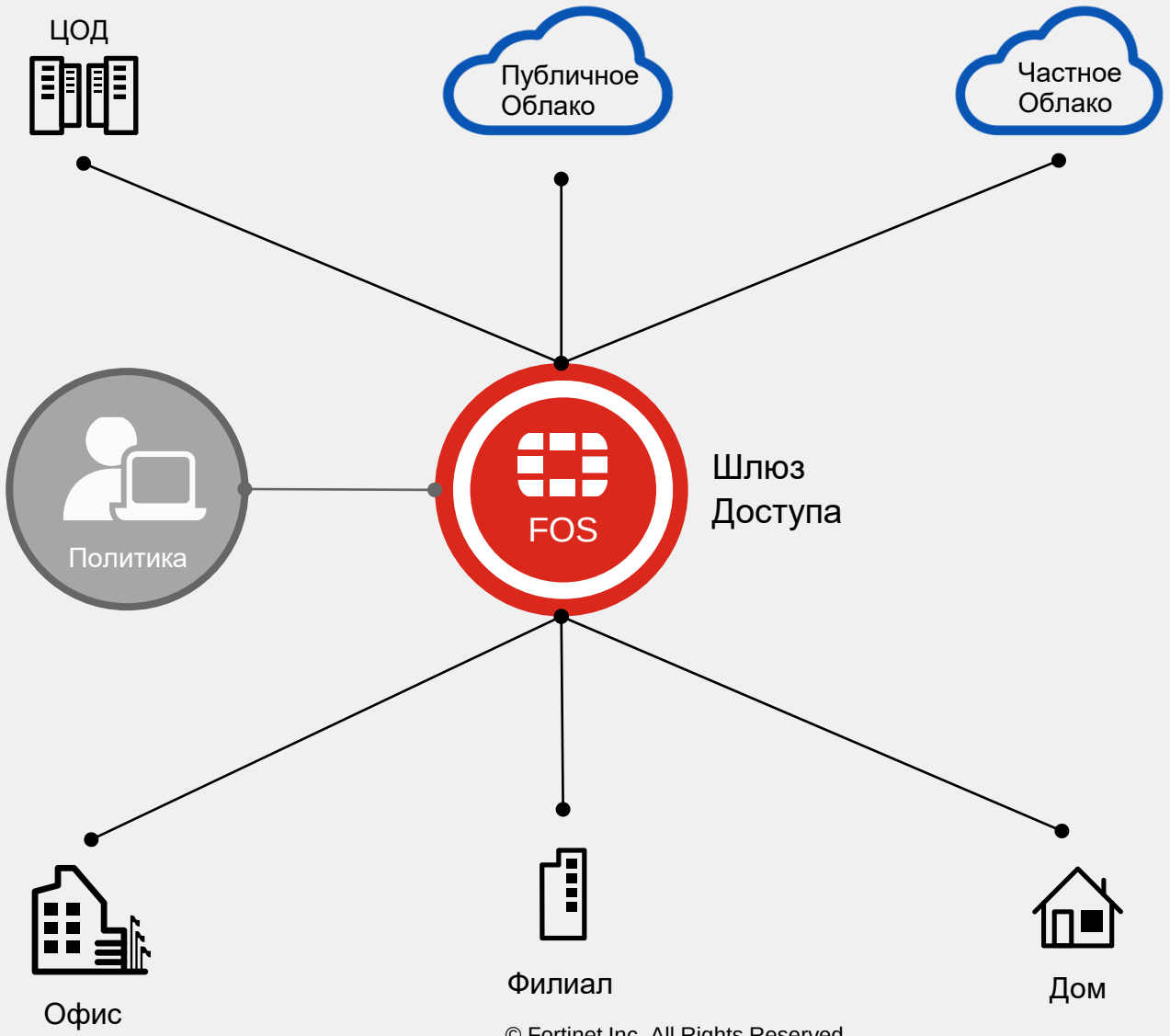


Снижение поверхности атаки

Гранулярный контроль доступа к приложениям

- Учётная запись аутентифицируется при каждом соединении 
- Многофакторная аутентификация и единый вход 
- Идентификация устройства при каждом соединении 
- Оценка соответствия устройства при каждом соединении 
- Доступ пользователей только к необходимым приложениям 
- Инфраструктура скрыта от Интернет за шлюзом доступа 

ZTNA – гибкая архитектура

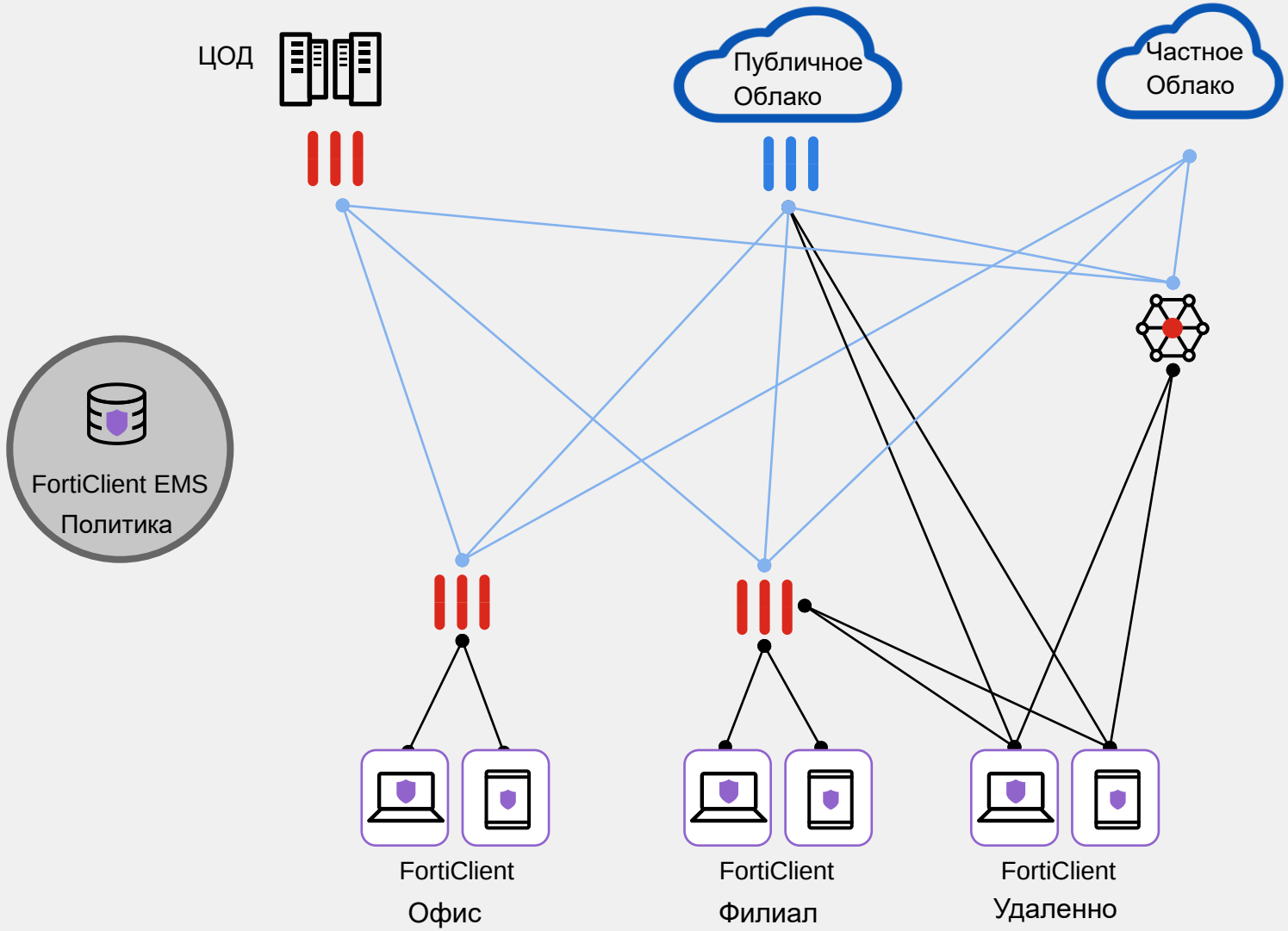


Где бы ни было приложение

Аутентификация пользователя, идентификация устройства и оценка соответствия требованиям при каждом доступе

Где бы ни был пользователь

ZTNA – автоматические защищенные соединения

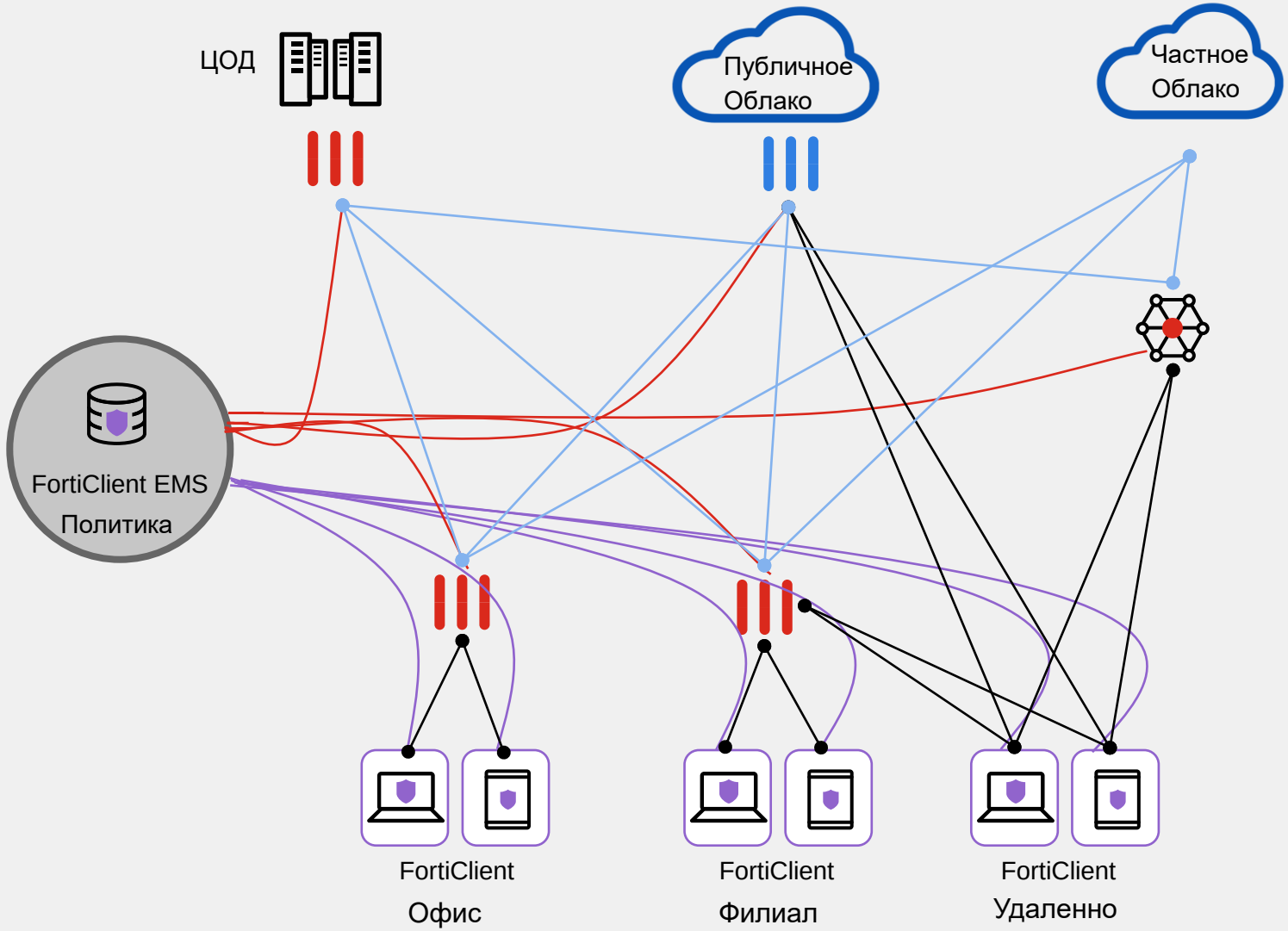


Опора на существующую инфраструктуру

Последовательные переоценка и применение политики

Автоматически устанавливаемые защищенные туннели по протоколу HTTPS

ZTNA Процесс работы



ZTNA Телеметрия

Security Fabric

Аутентификация и проверка устройства

Доступ

ZTNA от Fortinet

Из чего состоит решение? Из существующих компонентов Security Fabric

Ключевые элементы

FortiGate

FortiClient / FortiClient EMS

- FortiGate – строит защищенные туннели, поддерживает таблицу доступа групп к приложениям (FortiOS 7.0)
- FortiClient EMS – настраивает агенты ZTNA в FortiClient для защищенного доступа с использованием FortiGate (FortiClient 7.0)

- Решение для аутентификации
  - FortiAuthenticator, FortiToken или любое стороннее решение, поддерживаемое Security Fabric

Преимущества ZTNA от Fortinet

Наиболее полная реализация с защитой инвестиций

- Опора на существующие инвестиции в шлюзы
  - Большинство решений ZTNA доставляются только из облака и дорого стоят в пересчёте на всех сотрудников организации
  - ZTNA от Fortinet доступно на любых шлюзах FortiGate начиная с FortiOS 7.0
  - Это позволяет дополнительно использовать SD-WAN и SD-Branch
- Высокий уровень защиты
  - Все сессии доступа инспектируют FortiGate на предмет угроз
  - Инспекция происходит вне зависимости от расположения пользователей и приложений
- Не требует дополнительного лицензирования
  - Требуется только FortiClient EMS и FortiGate
  - Доступно в FortiGate «из коробки» (аналогично SD-WAN)

Эволюция VPN туннелей

Реализация принципов нулевого доверия в удаленном доступе

- Повторяющаяся проверка
  - Проверка пользователя при каждом новом запросе
  - Проверка устройства при каждом новом запросе
- Гранулярный контроль
  - Доступ предоставляется к определенному приложению
  - Не требуется предоставлять широкий VPN доступ
- Повышение удобства для пользователей
  - Автоматическое построение туннелей при доступе к приложениям
  - Не требуется дополнительных действий, подключение из офиса и удаленно происходит одинаково

Ценность решения

Повышение защищенности

Снижение риска	Реализуется с помощью
Учётных записей	Посессионная аутентификация
Устройств	Посессионная оценка соответствия
Пересылки данных	Автоматические шифрованные туннели
Обработки данных	Автоматические шифрованные туннели
Доступа к приложениям	Доступ через шлюз

Повышение удобства пользователей

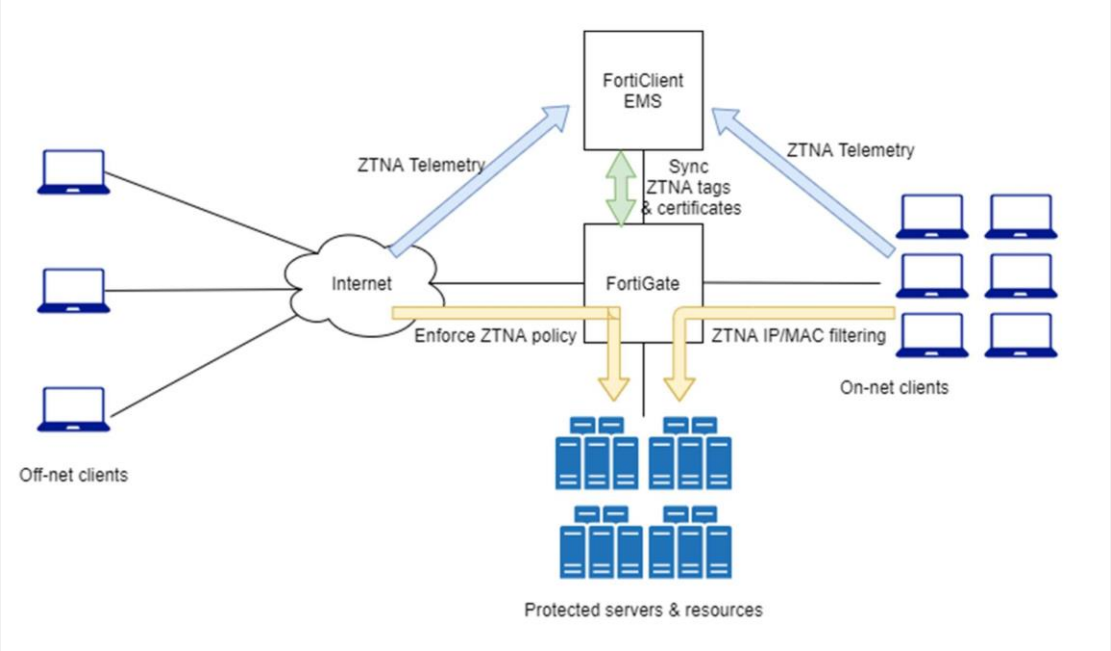
Улучшение	Реализуется с помощью
Упрощение доступа	Автоматические шифрованные туннели
	Единый вход (SSO)
	Гибкость размещения приложений
	Консистентная политика (одинаково внутри и вне сети)

Приглашаем на семинары

25 августа – оффлайн семинар (Hands-On Lab) для партнёров: Zero Trust Network Access Advanced HOL

26 августа – оффлайн семинар (Hands-On Lab) для заказчиков: Zero Trust Network Access Advanced HOL

26 августа – онлайн семинар (Fast Track) для заказчиков: Fortinet Teleworker Solution Engineered for Remote and Secure Productivity with ZTNA



Ссылки для регистрации будут высланы после вебинара


FORTINET