FORTINET®

VIRTUAL

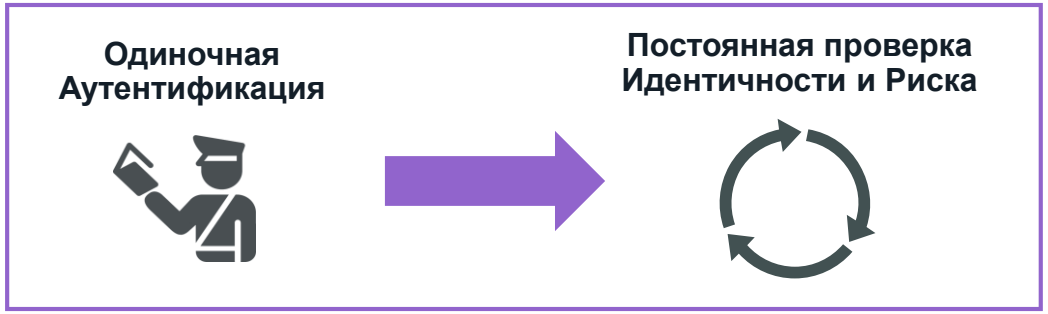
SECURITY DAY

Разрушая мифы об архитектуре безопасности с нулевым доверием

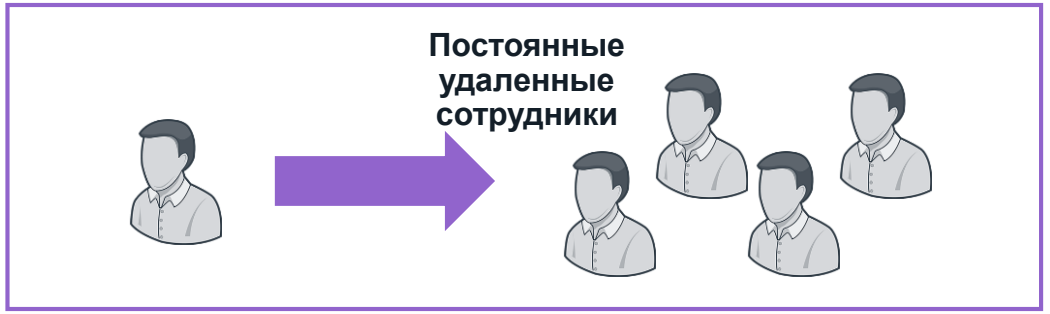
Чингис Талтаев

Системный инженер

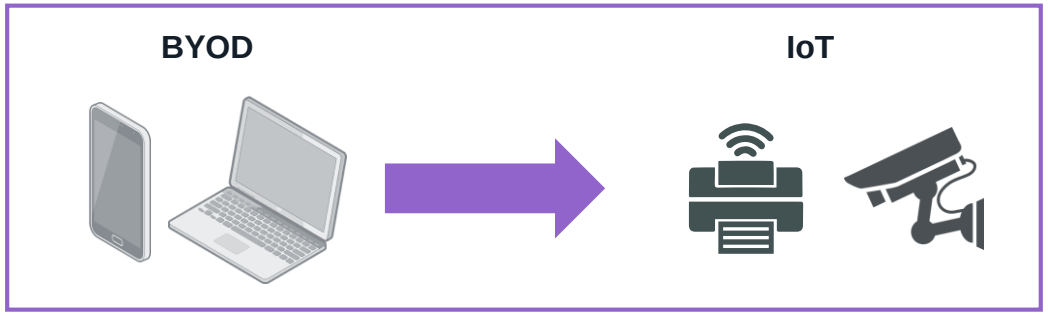
Тренды в развитии сетевого доступа



К 2024г, 70% приложений будет использовать MFA (по сравнению с 10% на сегодняшний момент[1]



С 4% до 30% возрастет доля сотрудников работающих постоянно удаленно к концу 2021[2]



К 2025г, в мире будет **12 МЛРД** установленных устройств IoT[3]

К 2025, в мире будет **3.7 МЛРД** установленных IoT устройств в промышленности, сфере обслуживания и на транспорте[3]

1 Gartner Magic Quadrant for Access Management, 12 August 2019
2 Global Workplace Analytics
3 Gartner. IoT Forecast

FORTINET

Традиционная модель безопасности

Реальность - Злоумышленники умеют развивать атаки внутри доверенной сети

- Традиционная модель защиты сети сфокусирована на защите Периметра
- Внутренние сети:
  - Плоская структура безопасности
  - Доверенная зона с малым количеством проверок и мер сдерживания
  - Слабый мониторинг безопасности, медленная реакция на инциденты ИБ
- Много способов проникнуть в сеть
- Оказавшись внутри сети, Злоумышленник становится частью доверенной зоны безопасности и имеет широкие возможности для горизонтального развития сетевой атаки

Forrester Zero Trust Extended (ZTx)

FORTINET

Мифы о модели безопасности Zero Trust

Миф №1:

Модель Zero Trust применима только к большим компаниям

SMB: В 2020г 54.29% инцидентах ИБ с произошло раскрытие данных*

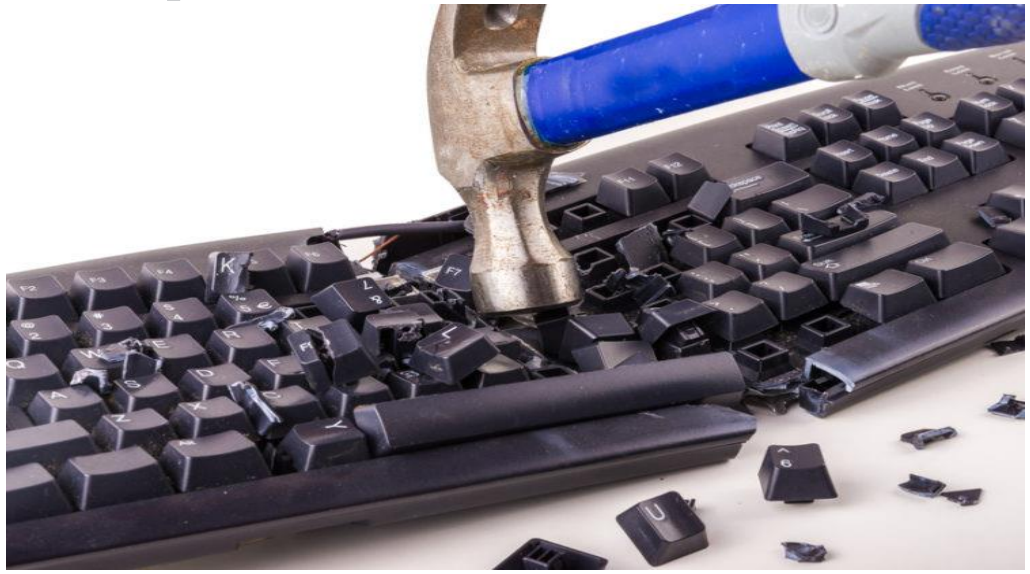
Large: В 2020г в 6.65% инцидентах ИБ произошло раскрытие данных*

Практики Zero Trust применимы для любых компаний независимо от размеров и индустрии

FORTINET

*Источник: Verizon Data Breach Investigations Report (2020)

Мифы о модели безопасности Zero Trust



Миф №2:

Внедрение Zero Trust требует единовременной полной замены существующей сети и средств безопасности

Zero Trust улучшает текущие методы контроля безопасности, концентрируясь на последовательном и пошаговом внедрении без разрушения

Мифы о модели безопасности Zero Trust

Миф №3:

Внедрение Zero Trust порождает культуру недоверия в компании

Zero Trust удаляет «слепые зоны» в отношения доверия, обеспечивая прозрачность доступа пользователей к ресурсам независимо от их расположения, одновременно закрывая «слепые зоны» доверия для злоумышленников

Zero-Trust Network Access

Знание и Контроль за Всеми и Всем внутри и вовне Сети

Обеспечение целостной политики безопасности в Сети, Облаке и вовне Сети

FORTINET

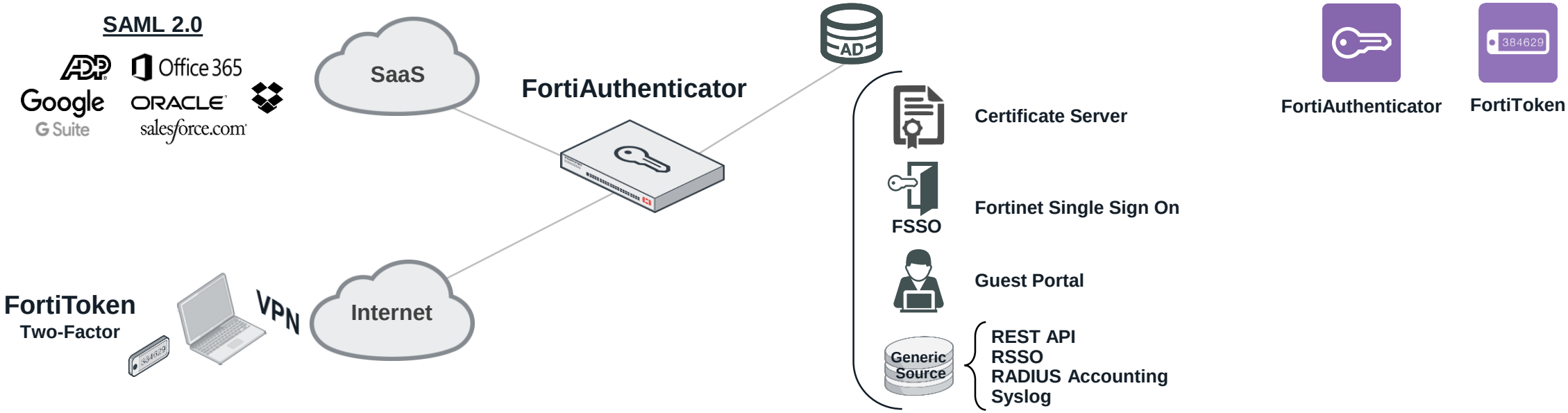
Zero-Trust Network Access

Компоненты

	Контроль, КТО подключен в сеть	Контроль, ЧТО подключено в сеть	Контроль устройств ВНУТРИ и ВОВНЕ сети
Identity Access Management **Аутентификация**	FortiAuthenticator FortiToken		
Network Access Control **Контроль доступа в сеть**		FortiNAC	
Endpoint Access Control **Контроль конечных узлов**			FortiClient Fabric

Zero Trust Network Access - Идентификация пользователей

Необходимо знать, **КТО** подключен к сети

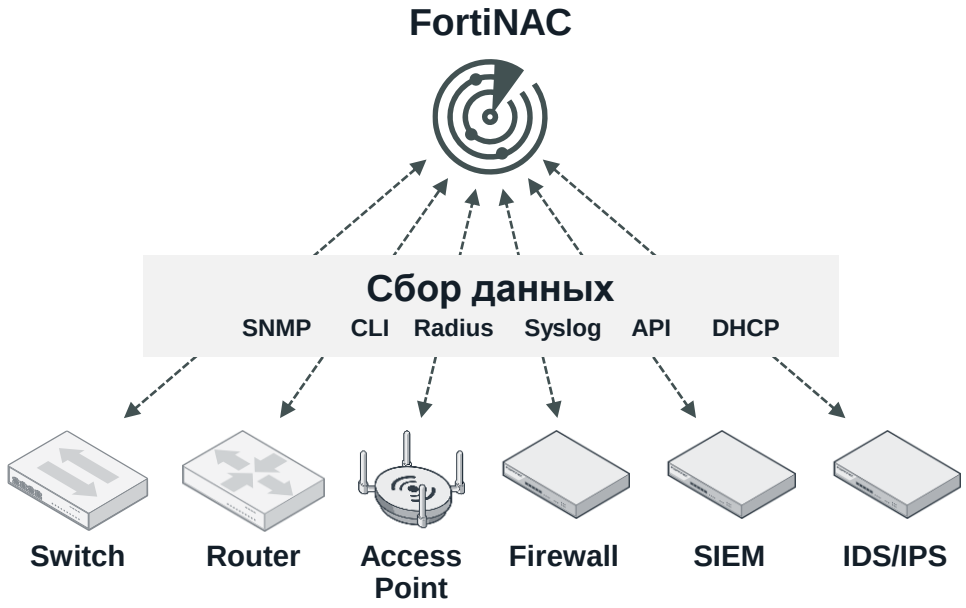


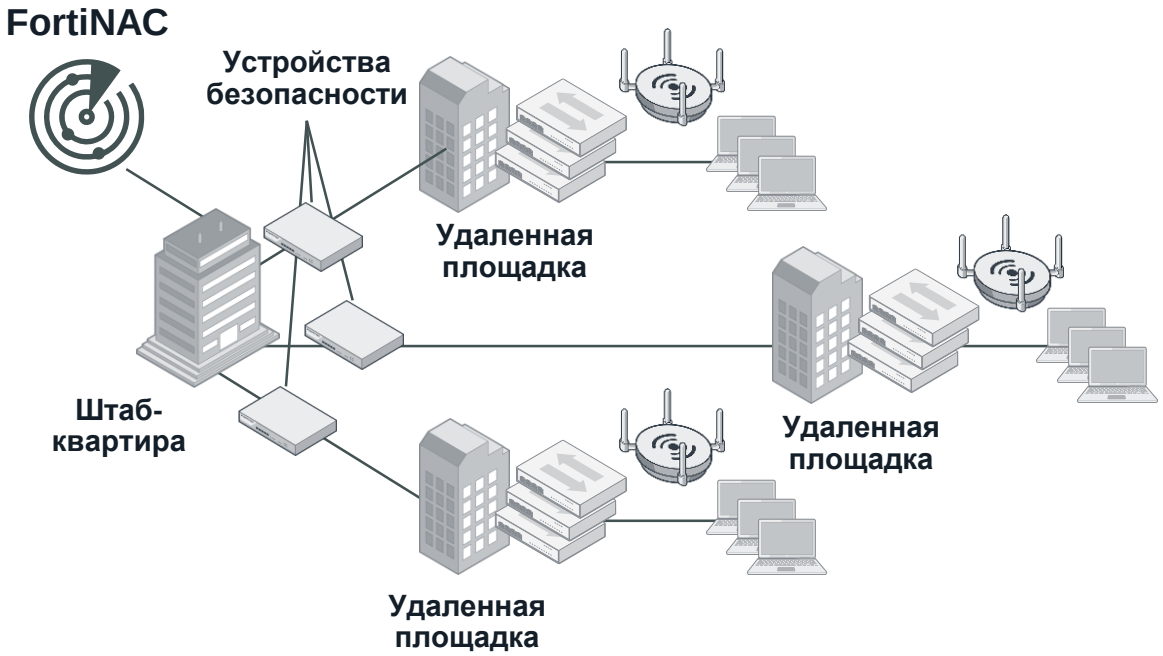
Аутентификация	Ролевой Доступ	Single Sign On
Установить личность / идентичность с помощью логина / пароля, сертификата, и / или ввода дополнительного фактора	Обеспечить информацией от источника аутентификации для использований привилегий	Упростить процесс для пользователя, обеспечив безопасность

Zero Trust Network Access— Контроль подключений устройств

Необходимо знать, **ЧТО** подключено в сеть

FortiNAC





Видимость	Динамический контроль	Непрерывное реагирование
Идентификация устройств, профилирование, поиск уязвимостей	Динамическая микро-сегментация Поддержка сегментации по намерениям	Автоматическое реагирование и оркестрация сети Расширение Security Fabric

Управление рисками до подключения в сеть

Видимость

Местоположение

Пользователь

Устройство

Приложение

Время

Осведомленность

Политики

Соответствие требованиям

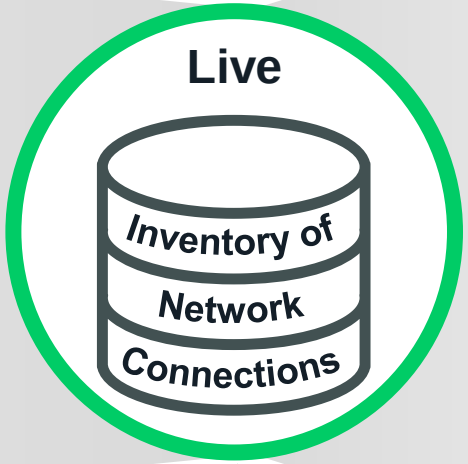
Принудительные меры

Автоматизация

Контроль сетевого доступа

Доверие

Инвентаризация сетевых подключений в реальном времени



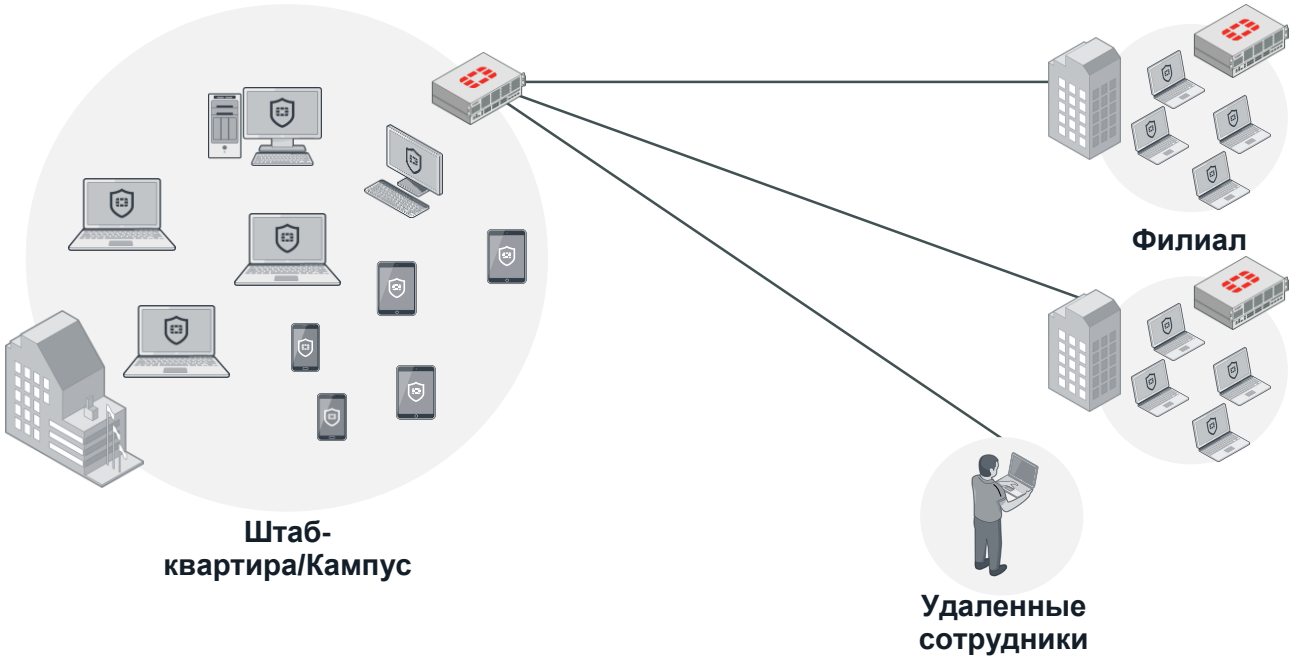
Индикаторы доверия

Управление рисками после подключения в сеть

Zero-Trust Network Access - Защита Устройств

Защита устройств внутри и вовне сети организации

FortiClient
Fabric Agent



Видимость конечных узлов	Контроль Цифровой Гигиены	Безопасный Удаленный Доступ
Сбор телеметрии Статус защиты Установленные приложения	Поиск Уязвимостей Веб Фильтрация Установка Исправлений / Патчей Динамическая Группировка	Динамический Контроль Доступа Организация VPN Single Sign On (SSO)

FORTINET

Ценность модели безопасности Zero-Trust Network Access

ВЫЗОВЫ	ПРЕИМУЩЕСТВА
Слабые и украденные пароли	Усиление безопасности с помощью двухфакторной аутентификации (2FA)
Слабый контроль за устройствами в сети	Автоматизация определения и адаптации к сети пользователей и устройств
Растущая плоскость атаки на IoT	Микросегментация с использованием политик доступа по принципу наименьших привилегий
Видимость и контроль за сотрудниками на удаленном доступе	Сбор телеметрии с устройств вне сети и принудительное применение и исполнение политик безопасности

FORTINET


FORTINET