

Стек решений ИнфоТеКС для концепции ZTNA















техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Алексей Данилов
Руководитель направления
Отдел развития продуктов ИнфоТеКС

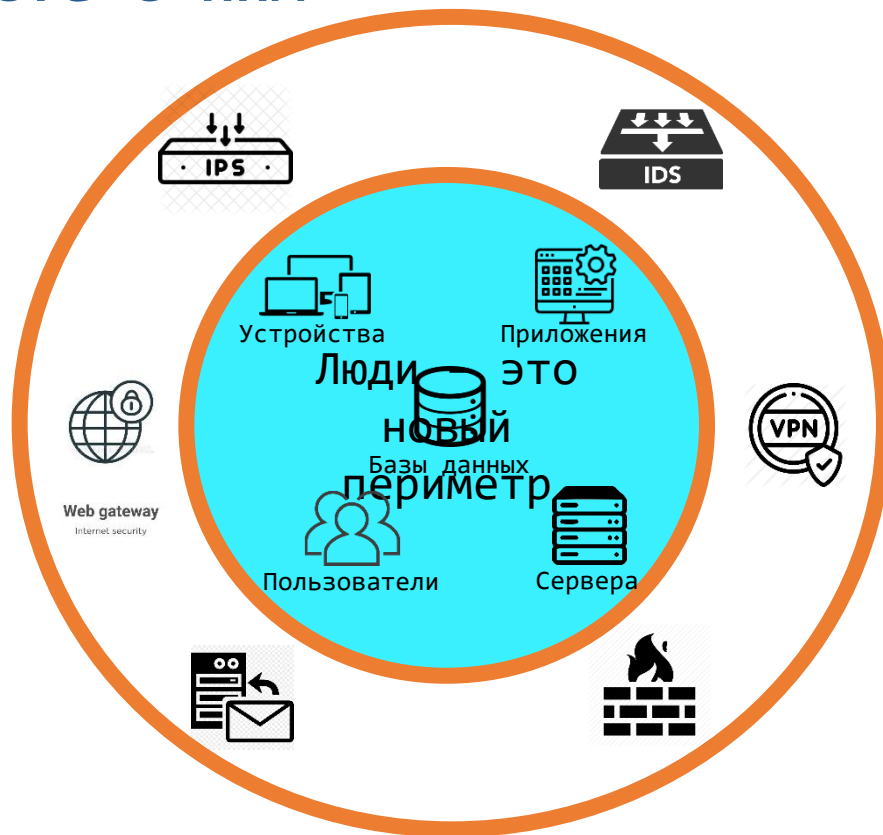
Новости пестрят заголовками об атаках, взломах, утечках...

- ¼ – доля программ вымогателей
- \$ 4,62 млн Средний ущерб от взлома программ вымогателей
- \$ 123 млн заработала группировка Revil

 <p>СМИ: Colonial Pipeline заплатила вымогателям 5 000 000 долларов</p>	 <p>Вымогатели обещают не атаковать медицинские учреждения во время пандемии COVID-19</p>	 <p>Positive Technologies: целевым атакам подвергались треть российских компаний</p>	 <p>Утечка exploits АНБ произошла из-за ошибки, допущенной сотрудником три года назад</p>
 <p>В США введен региональный режим ЧС из-за атаки на трубопроводную компанию Colonial Pipeline</p>	 <p>Около 30% «жертв атаки на SolarWinds» не были клиентами SolarWinds</p>	 <p>Учетные данные SolarWinds были публично доступны на GitHub</p>	 <p>Использование трендовых уязвимостей сокращает время взлома до 45 минут</p>
 <p>Взлом SolarWinds затронул Национальное управление по ядерной безопасности США и компанию Microsoft</p>	 <p>DDoS-вымогатели угрожают австралийским банкам</p>	 <p>Из-за незащищенной БД компании Voxx произошла утечка 26 млн SMS-кодов двухфакторной аутентификации</p>	 <p>Вымогатели стали требовать второй выкуп за удаление похищенных файлов</p>

*Cost of a Data Breach Report 2021 IBM Security

Мир стремительно меняется, периметр меняется вместе с НИМ



Основные причины



Работа с облачными сервисами



Выросшая мобильность сотрудников



Переход на удаленную работу



Попытка соблюсти баланс безопасность/ удобство

Кибератаки вышли на государственный уровень



Sec. 3. Modernizing Federal Government Cybersecurity.

(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

Executive Order on Improving the Nation's Cybersecurity
MAY 12, 2021•PRESIDENTIAL ACTIONS

Он улетел, но обещал вернуться



JUNIPER
NETWORKS



 paloalto®
NETWORKS

Ответ на новые вызовы

Zero Trust (ZT) или «нулевое доверие»
– набор постоянно развивающихся концепций и идей, направленных на принятие точных решений о доступе субъекта к объекту с минимальными привилегиями для каждого запроса доступа.

Краткая история концепции Zero Trust

Zero Trust

Аналитиком компании Forrester Джоном Киндервагом предложена концепция Zero Trust.

2014

ZT CARTA и ZTX

Эксперт Forrester Чейз Каннингэм расширяет концепцию ZT, назвав ее Zero Trust eXtended. Специалисты Gartner финализируют свою концепцию CARTA.

2021

Появление новых подходов

Google публикует описание их подхода к Zero Trust, назвав его BeyondCorp. В Gartner называют свою модель Continuous Adaptive Risk and Trust Assessment (CARTA).

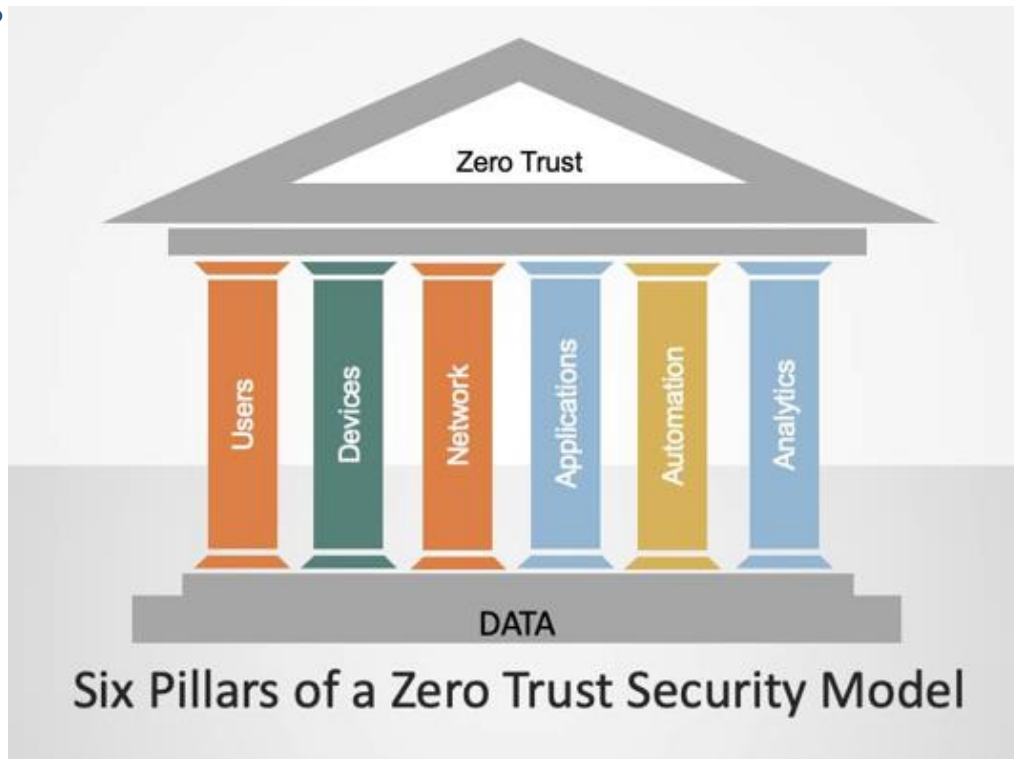
Генерализация

ИТ-индустрия признает термин Zero Trust Architecture как общее название.

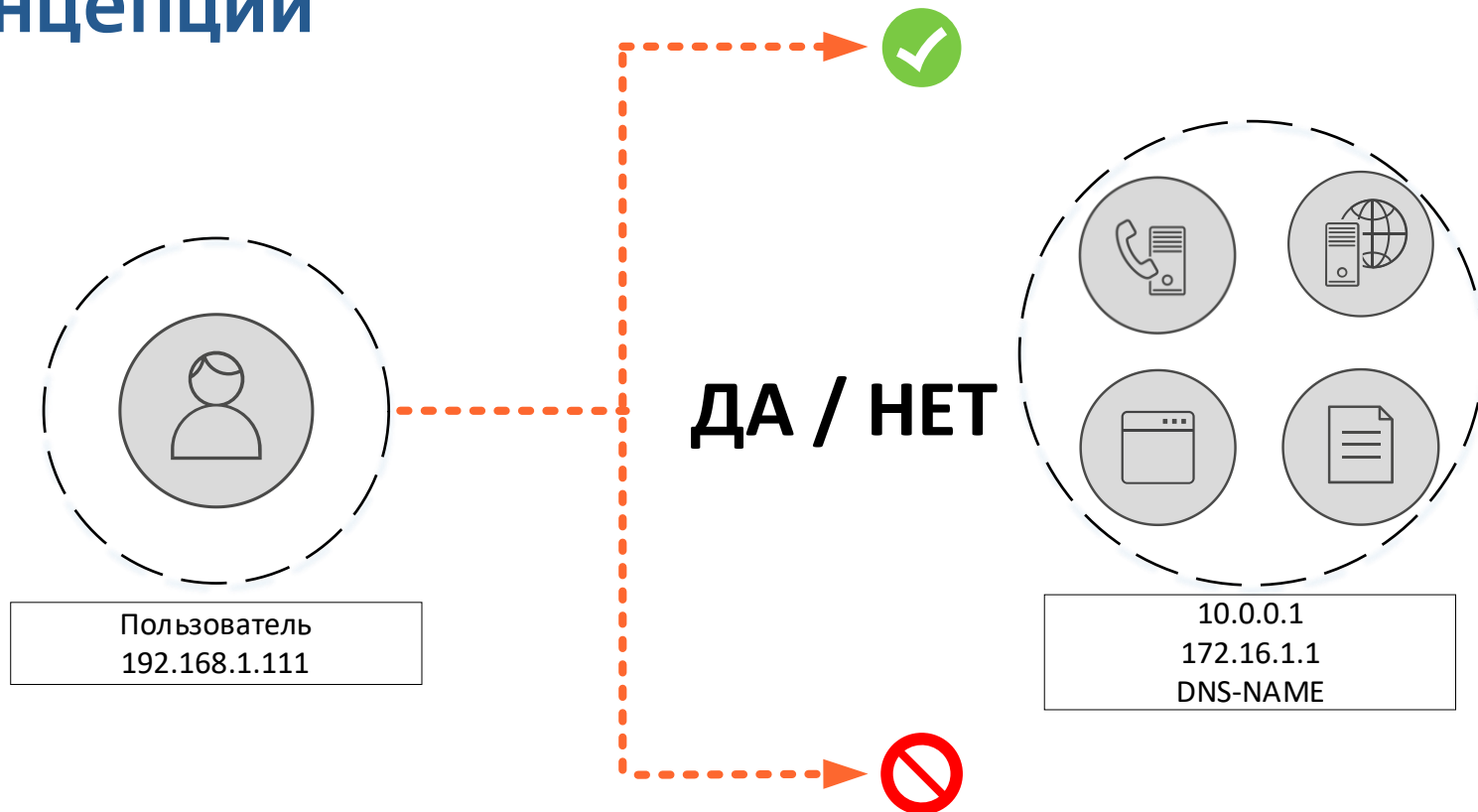
2010

2017

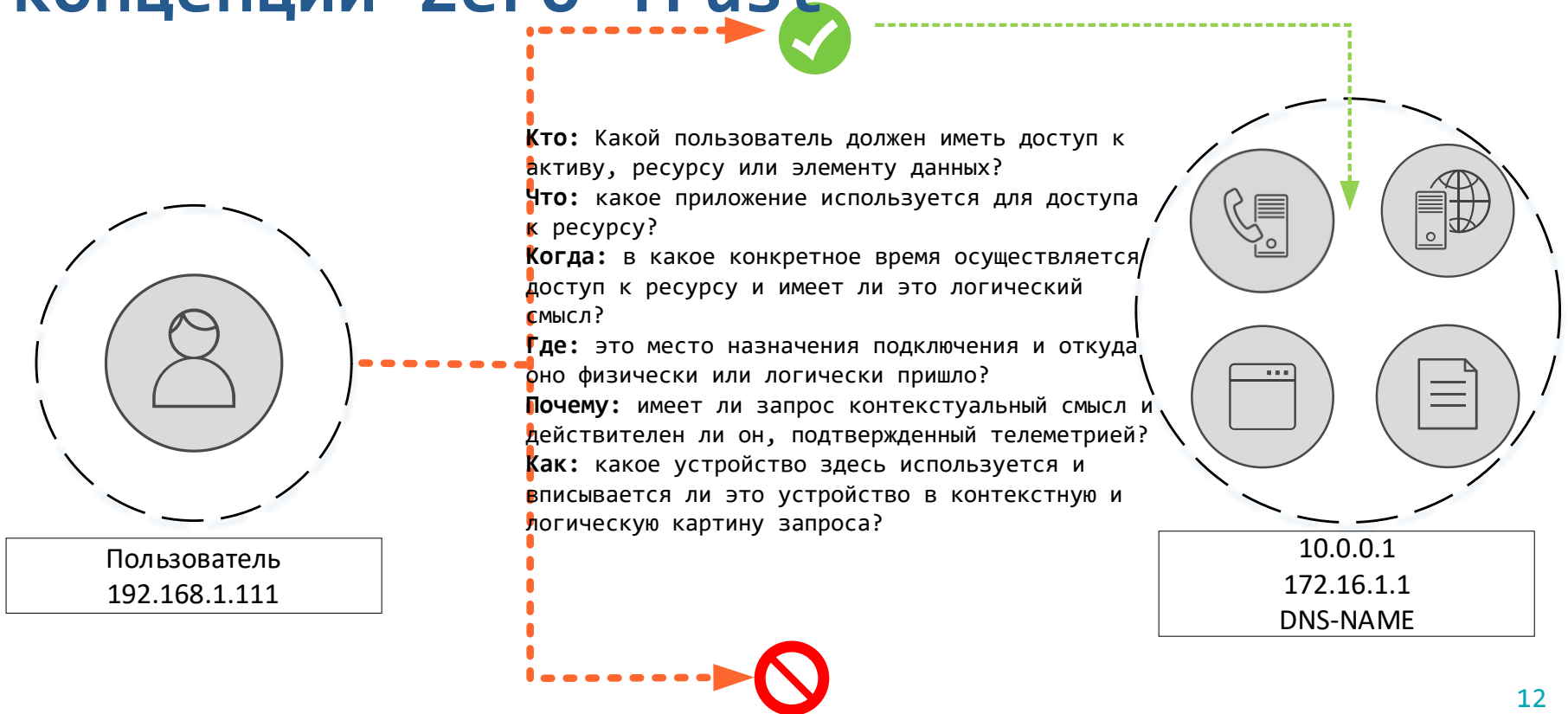
Что входит в модель «нулевого доверия»?



Предоставление доступа в старой концепции



Предоставление доступа в концепции Zero Trust



Технологии, с помощью которых строится архитектура Zero Trust

Для реализации архитектуры с нулевым доверием требуется несколько технологий:

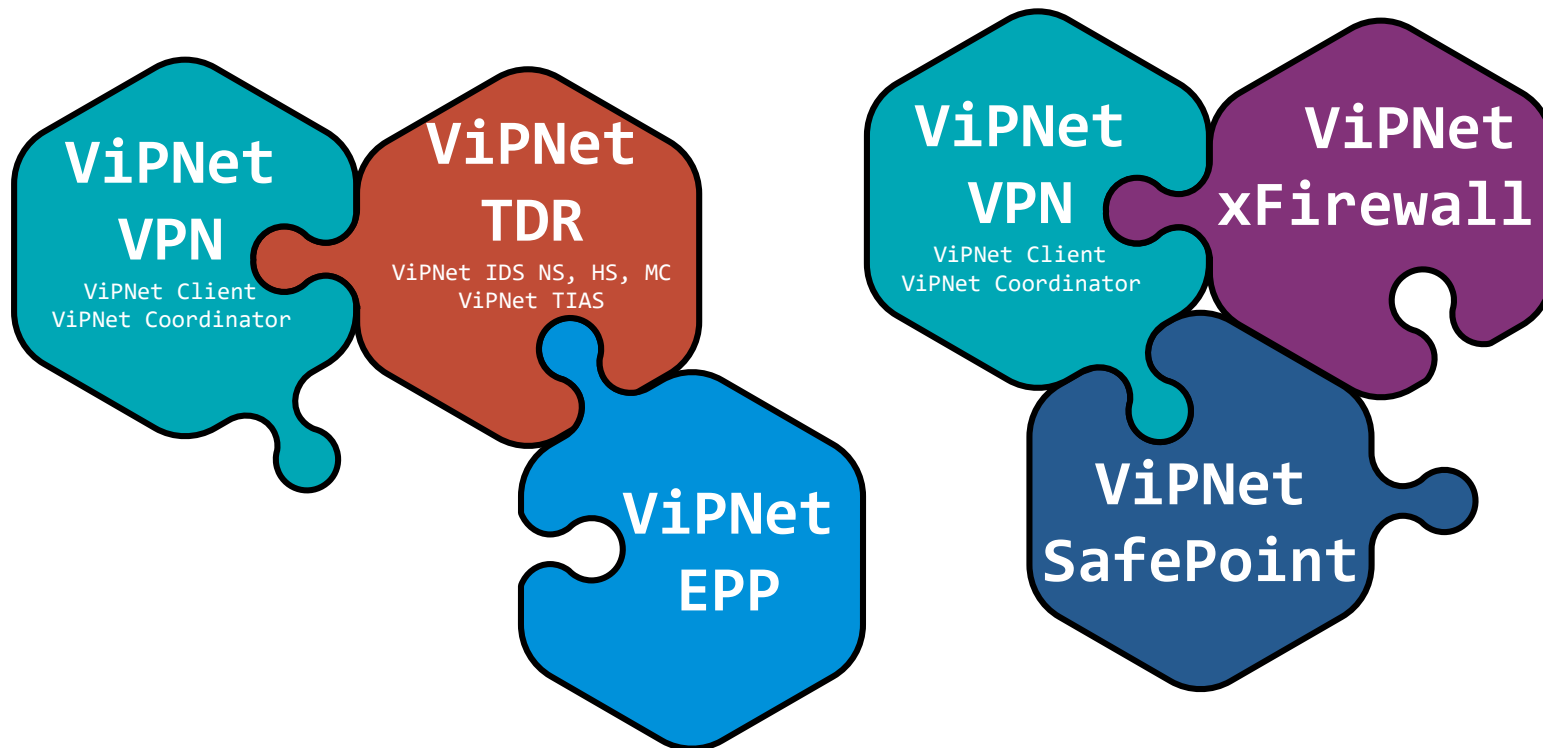
- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Endpoint Protection
- Zero Trust Network Access (ZTNA)
- Microsegmentation
- Visibility and Analytics

Что предлагаем мы

Продукты ИнфоТеКС, соответствующие технологиям Архитектуры Zero Trust

	ViPNet Client	ViPNet Coordinator	ViPNet xFirewall	ViPNet SafePoint	ViPNet EPP	ViPNet TDR
Identity and Access Management (IAM)				✓		
Многофакторная аутентификация (MFA)	✓			✓		
Защита EndPoint (микروпериметры)	✓			✓	✓	
Микросегментация	✓	✓	✓	✓	✓	
Zero Trust Network Access (ZTNA)	✓	✓	✓	✓	✓	
Мониторинг и аналитика			✓	✓	✓	✓

ViPNet Zero Trust как конструктор



Действия для достижения Zero Trust

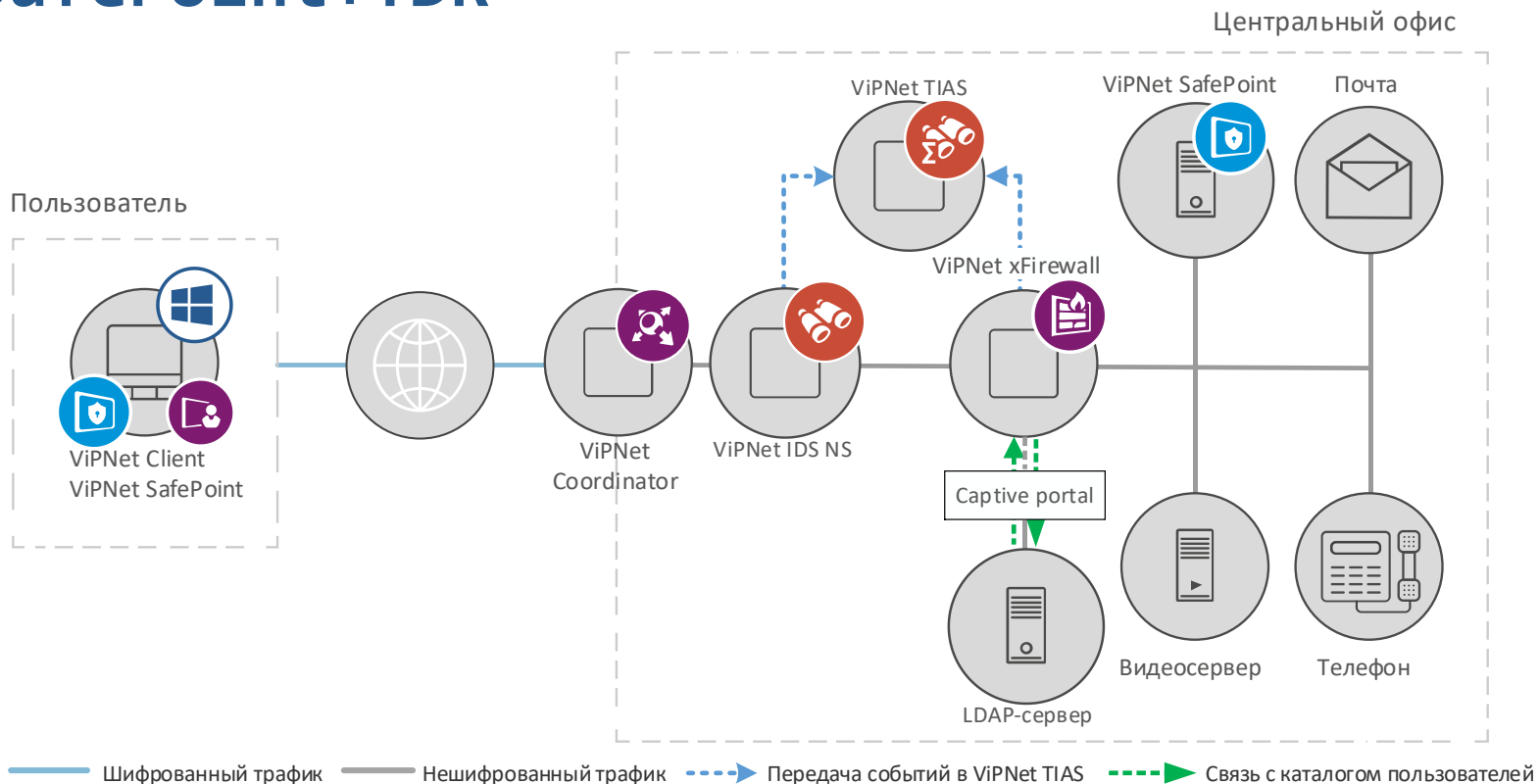


Преимущества подхода Zero Trust

- Максимально усложняет кражу данных
- Уменьшение поверхности атаки
- Помощь в управлении рисками
- Устранение нехватки специалистов по обеспечению безопасности
- Потеря актуальности оппортунистических атак

Схемы решения

ZTA = VPN+xFirewall +SafePoint+TDR



ZTNA = VPN+xFirewall+SafePoint+TDR

ViPNet Client

- Защищенное подключение к корпоративной сети
- MFA – аутентификация перед подключением

ViPNet Coordinator

- Защищенная связь между корпоративной сетью и «пользователями домашнего офиса»
- Сегментация сети
- Несанкционированный доступ и предотвращение атак

ViPNet SafePoint

- Управление идентификацией и доступом (включает интеграцию с Active Directory)
- MFA – аутентификация для всех пользователей
- Безопасные политики для всех пользователей или группы пользователей (какие процессы, службы, программы и файлы могут быть запущены пользователем)

ViPNet xFirewall

- Сегментация сети
- Комплексная защита от сетевых угроз на всех уровнях
- Безопасное использование персональных устройств в рабочих целях с соблюдением политик безопасности – BYOD (Bring Your Own Device)

ViPNet TDR

- Выявление угроз в реальном времени с рекомендацией по их оперативному устранению
- Непрерывный процесс мониторинга угроз информационной безопасности и обнаружения компьютерных атак

Безопасный доступ в Internet с Zero Trust = ViPNet VPN + xFirewall



Безопасный доступ в Internet с Zero Trust = ViPNet VPN + xFirewall

ViPNet Client

- Защищенное подключение к корпоративной сети
- MFA – аутентификация перед подключением

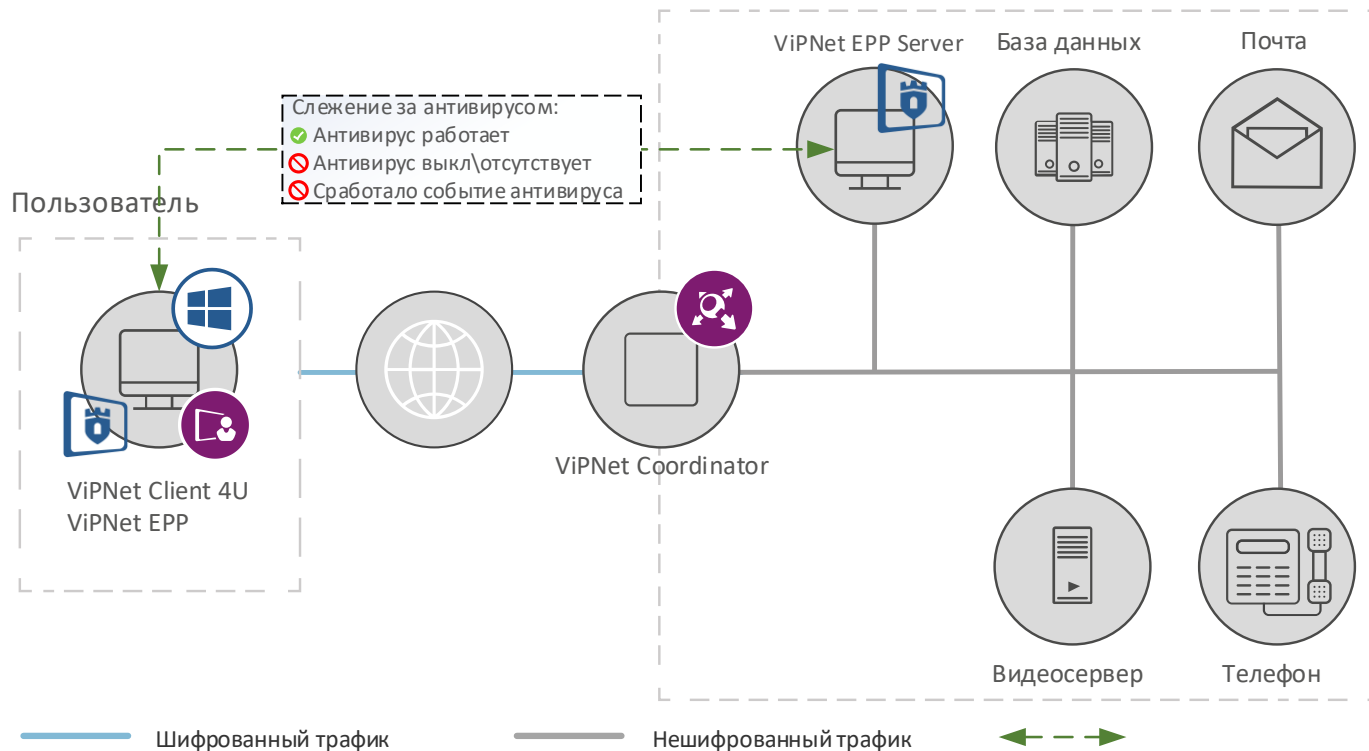
ViPNet Coordinator

- Защищенное соединение между корпоративной сетью и «пользователями домашнего офиса»
- Сегментация сети
- Несанкционированный доступ и предотвращение атак

ViPNet xFirewall

- Сегментация сети
- Комплексная защита от сетевых угроз на всех уровнях
- Безопасное использование персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BYOD (Bring Your Own Device)

Создание микропериметра с помощью ViPNet EPP



Создание микропериметра с помощью ViPNet EPP

ViPNet Client

- Защищенное подключение к корпоративной сети
- MFA – аутентификация перед подключением

ViPNet Coordinator

- Безопасная связь между корпоративной сетью и «пользователями домашнего офиса»
- Сегментация сети
- Несанкционированный доступ и предотвращение атак

ViPNet EPP

- Выявление угроз в реальном времени с рекомендацией по их оперативному устранению
- Фильтрация трафика
- Контроль за состоянием устройства
- Контроль за антивирусом

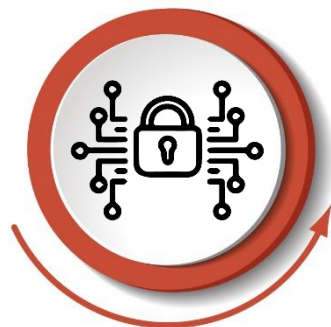
Подведем итог, на чем строится ViPNet Zero Trust Architecture



Защищенное соединение

Построение шифрованного туннеля между узлами защищенной сети

ViPNet Client, ViPNet Coordinator HW/VA



Микропериметр

Контроль доступа пользователей к программам, файлам и документам, устройствам. Всё ПО и службы защищены от изменений. Комплексная защита конечных точек от атак и обнаружение и реагирование на вредоносные действия. Отслеживание работы антивируса

ViPNet EPP, ViPNet SafePoint



Микросегментация

Сегментация сети для обеспечения политик нулевого доверия. Разграничение доступа на прикладном уровне, безопасное подключение BYOD устройств и комплексная защита от сетевых угроз.

ViPNet Client, ViPNet Coordinator HW/VA, ViPNet xFirewall



Мониторинг и аналитика

Защита от внешних угроз, обнаружение и реагирование на неизвестные угрозы

ViPNet EPP, ViPNet IDS NS, ViPNet TIAS



Архитектура Zero Trust готова!


infotecs

Вопросы?

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363