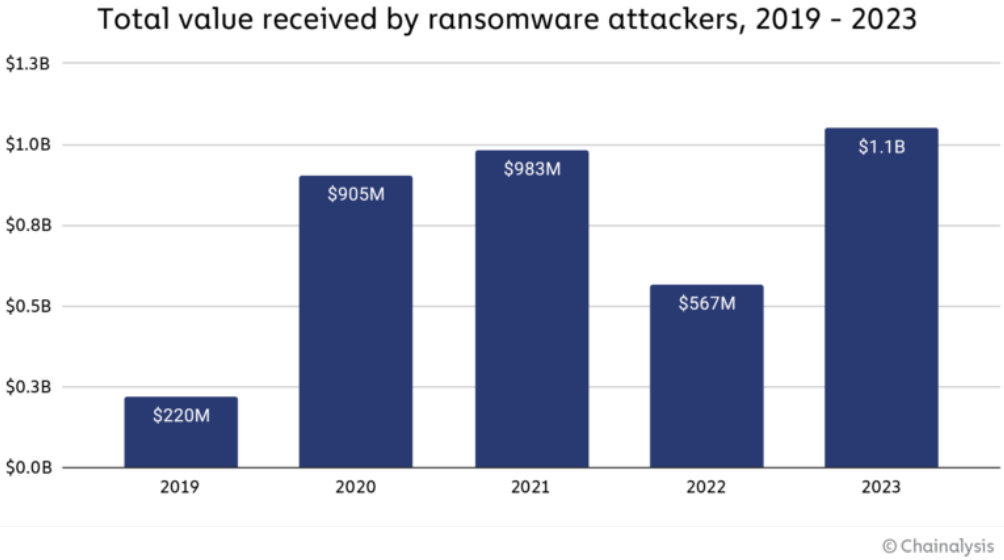
Стек решений ИнфоТеКС для концепции ZTNA

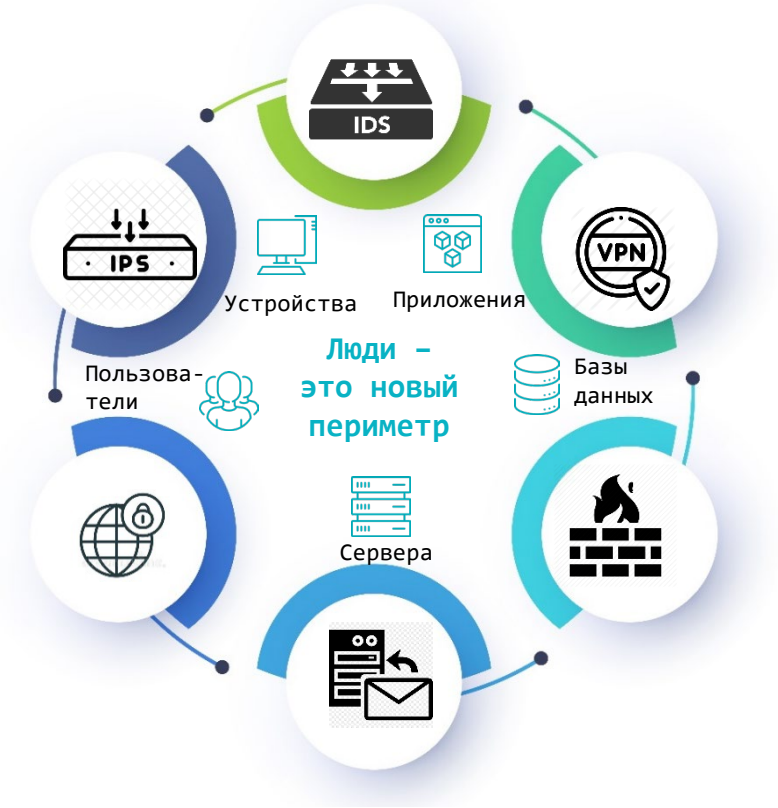
Алексей Данилов

Новости пестрят заголовками о доходах от атак



- Почти 80% выплат вымогателям составляет 1 млн $
- Ransomware, APT – ориентир крупные компании
- Ransomware as a Service (RaaS) – ориентир небольшие организации

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

Barracuda

paloalto NETWORKS

ТЕХНО infotecs 2024 ФЕСТ

ОТВЕТ НА НОВЫЕ ВЫЗОВЫ

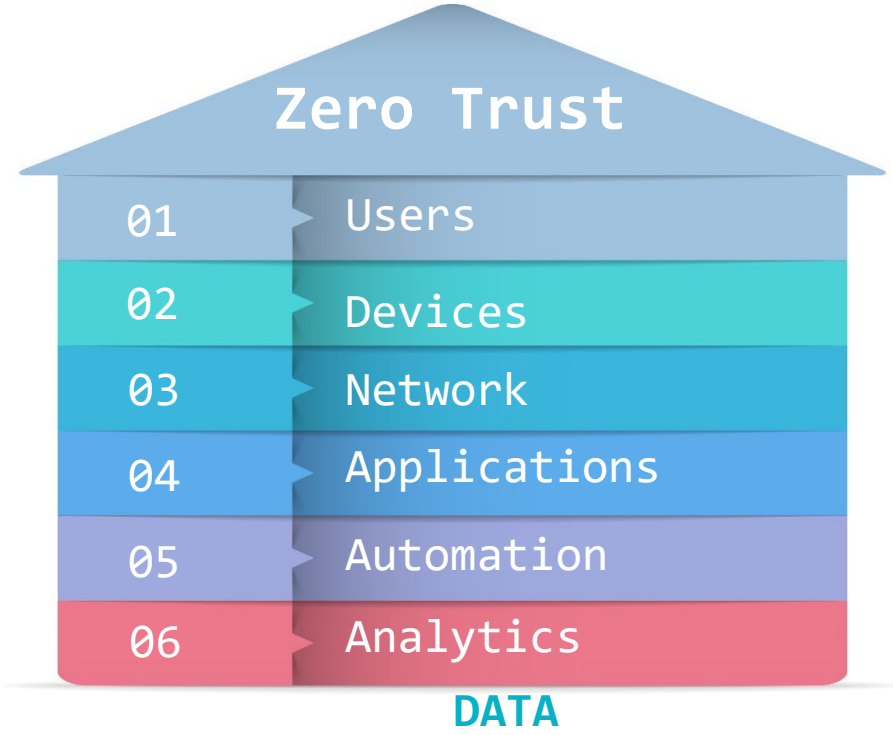
«Старый новый год»

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.

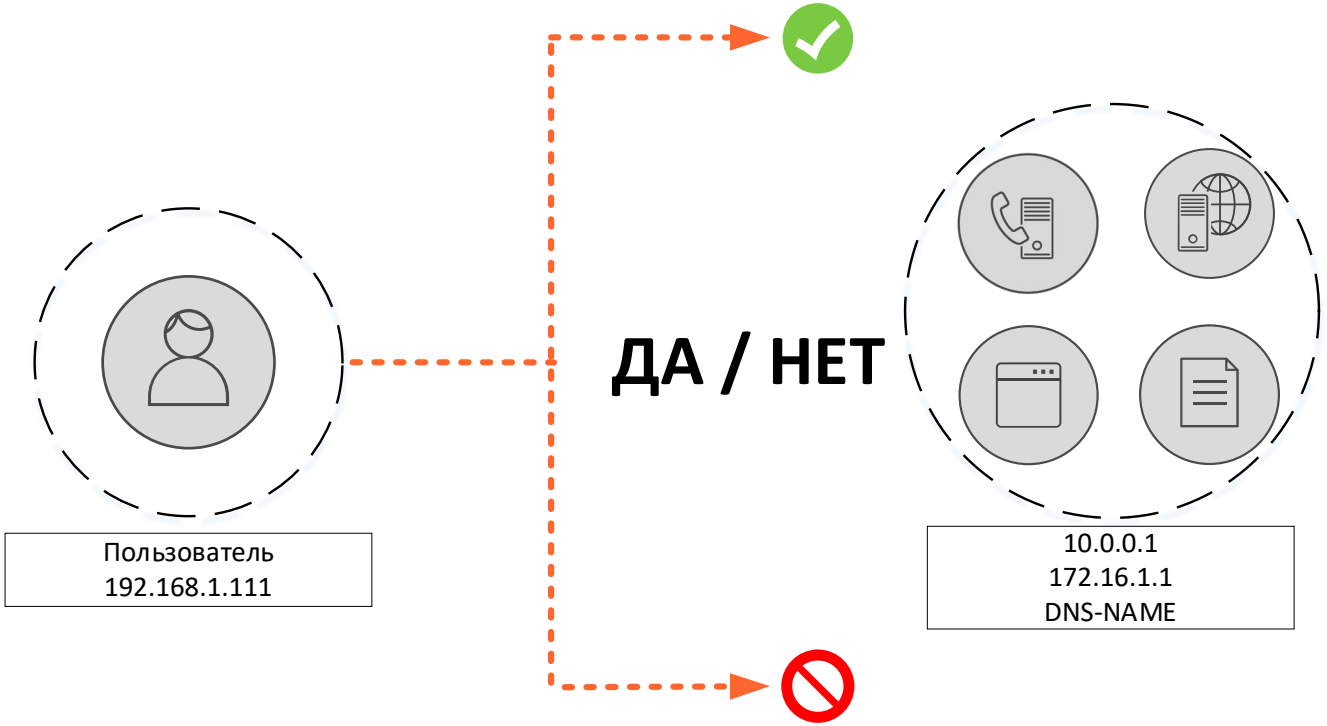
Краткая история концепции Zero Trust

Что входит в модель «нулевого доверия»?

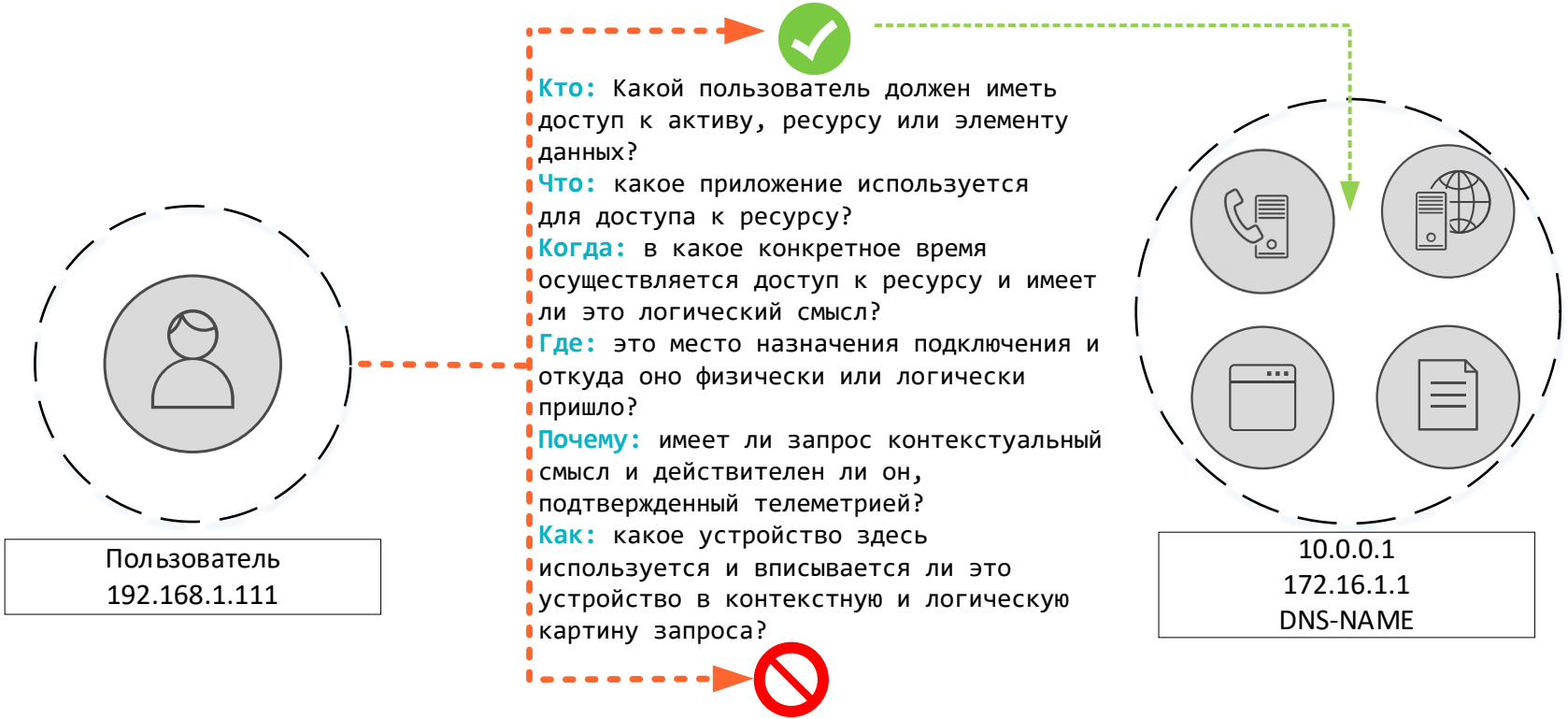
Six Pillars
a Zero Trust
Security Model



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:

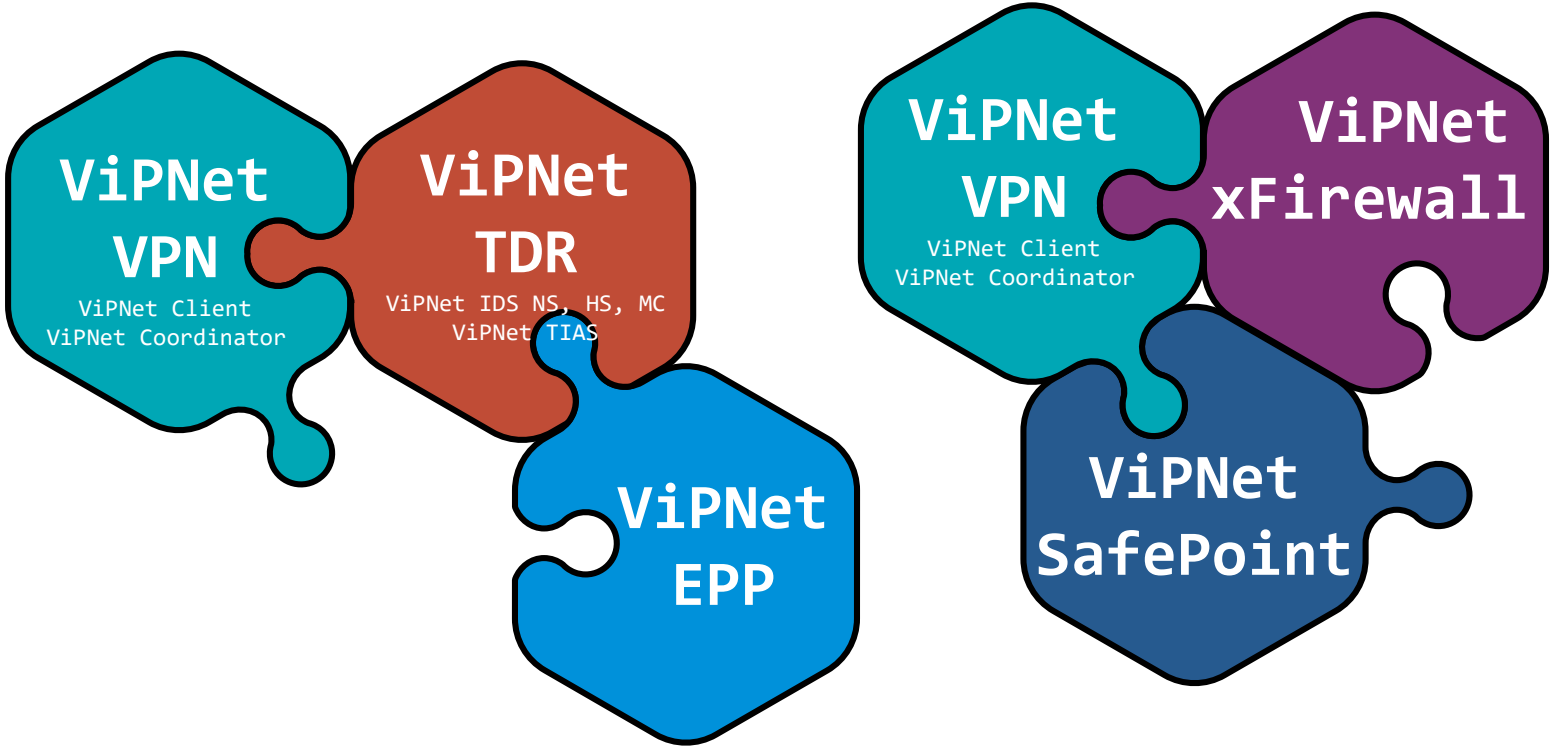
- Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Endpoint Protection
- Zero Trust Network Access (ZTNA)
- Microsegmentation
- Visibility and Analytics

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 (микроперимметры)	☑			☑	☑	
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

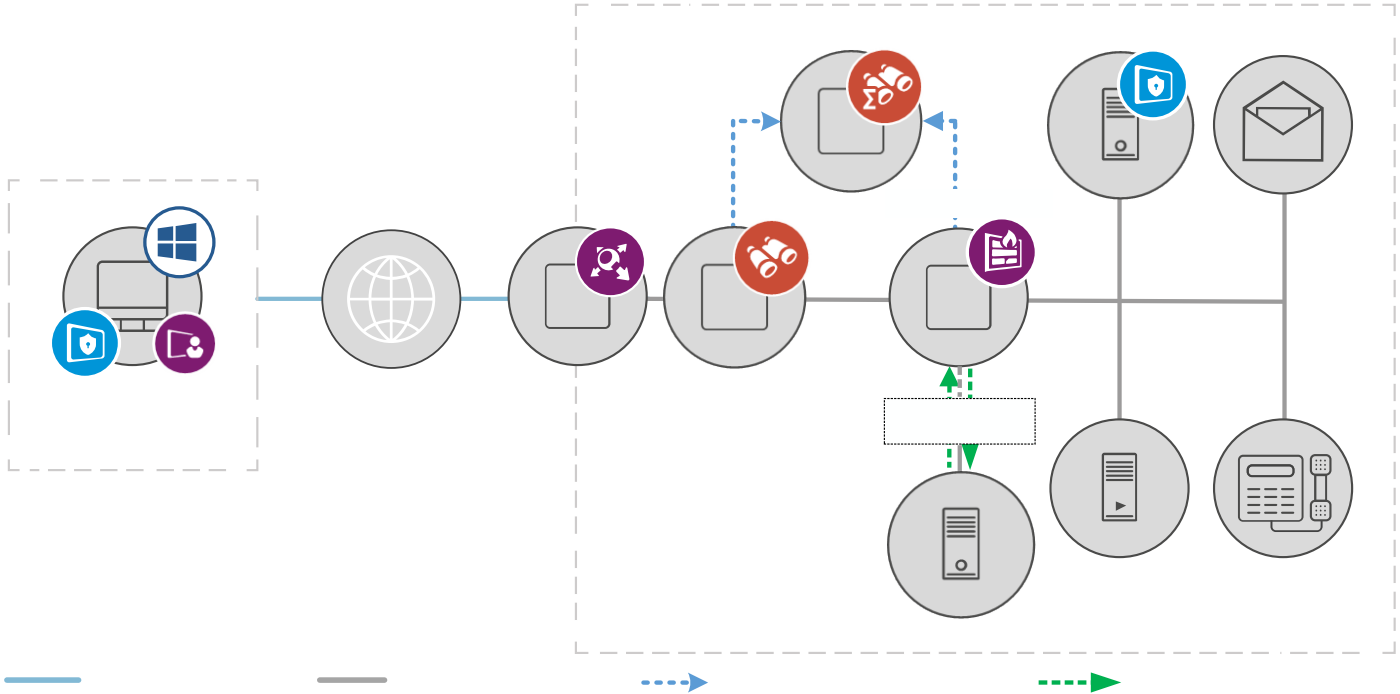
Устранение нехватки специалистов по обеспечению безопасности

Потеря актуальности оппортунистических атак

ТЕХНО infotecs 2024 ФЕСТ

СХЕМЫ РЕШЕНИЯ

ZTA = VPN+xFirewall +SafePoint+TDR



ZTNA = VPN+xFirewall+SafePoint+TDR

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

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

ZTNA = VPN+xFirewall+SafePoint+TDR

- 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)

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

ZTNA = VPN+xFirewall+SafePoint+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

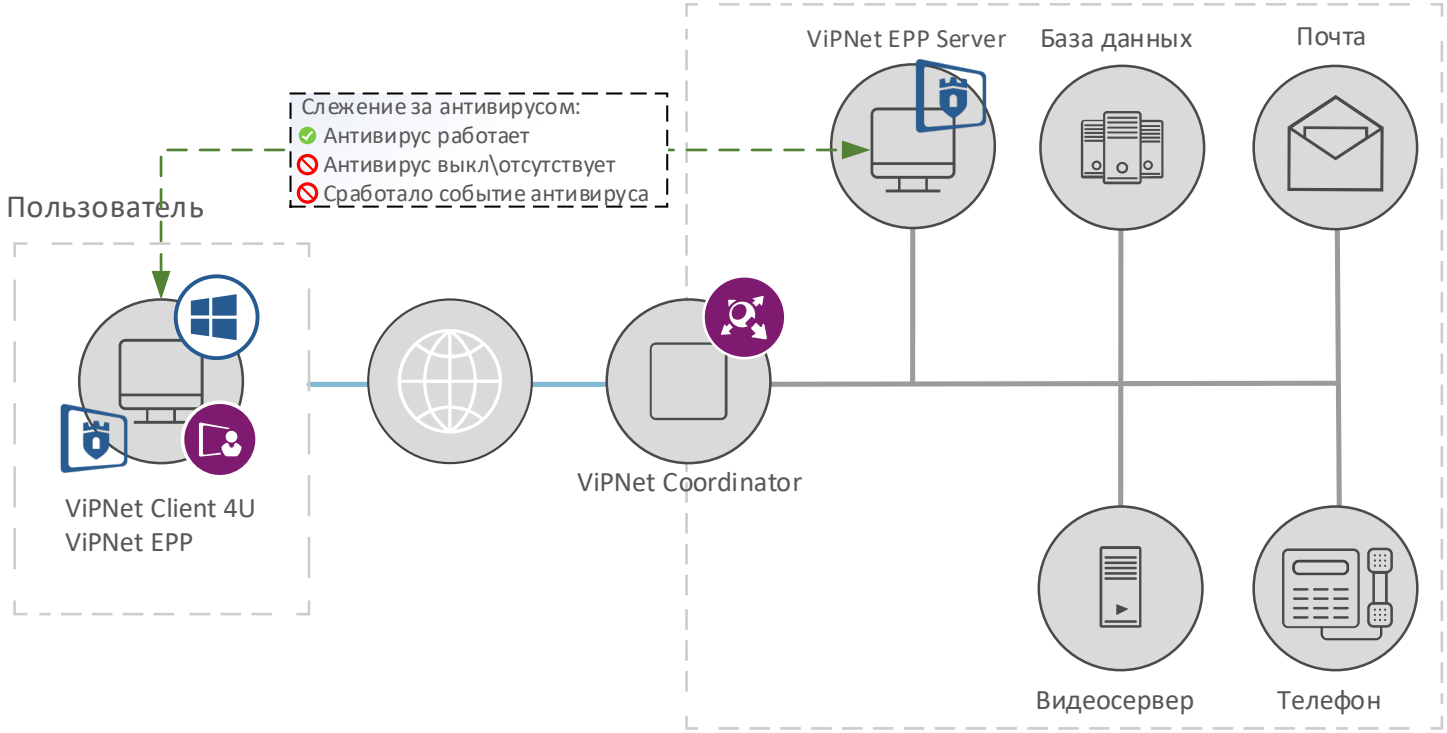
- Защищенное подключение к корпоративной сети
- MFA – аутентификация перед подключением

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

Безопасный доступ в Internet с Zero Trust = ViPNet VPN + 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

ТЕХНО infotecs 2024 ФЕСТ

ViPNet Client

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

ViPNet Coordi-nator

- 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

Архитектра Zero Trust готова!

ТЕХНО 2024 infotecs ФЕСТ

Вопросы?

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363