Построение архитектуры Zero Trust при помощи технологий ViPNet

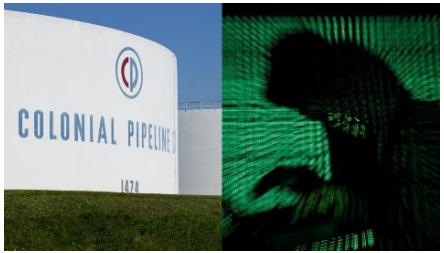
Кирилл Пантелеев

Новости пестрят заголовками об успешных атаках

$ 4,62 млн
Средний ущерб от взлома программ вымогателей

¼ – доля программ вымогателей

Средняя стоимость утечки увеличилась на 10% в годовом исчислении, самый высокий показатель за 7 лет



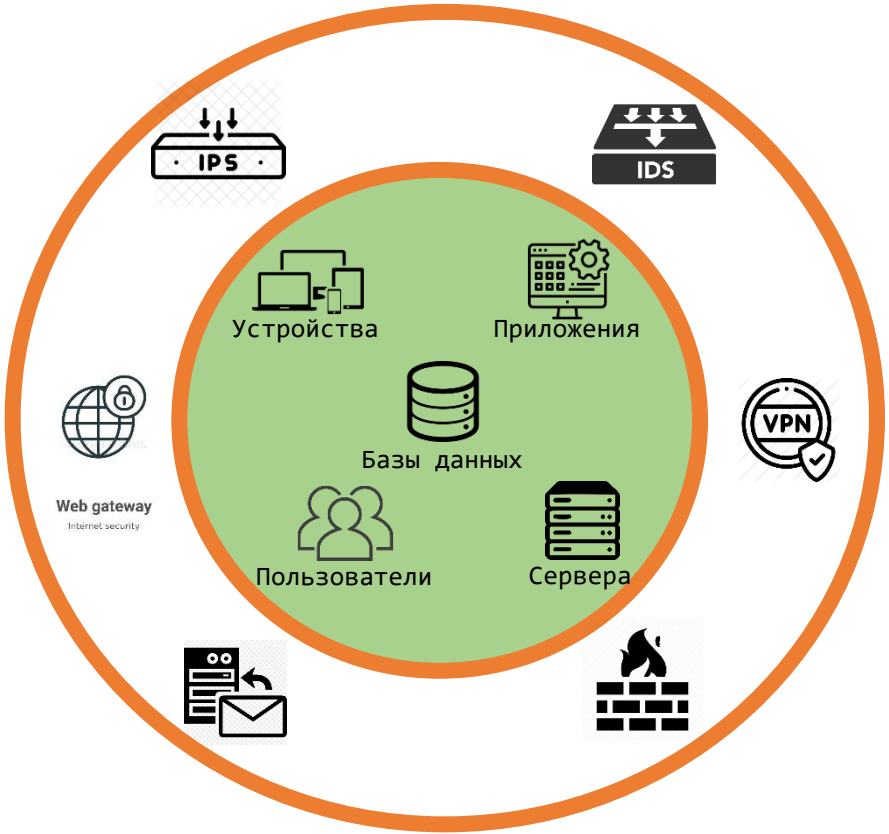
123 млн дол. заработала группировка Revil

*Cost of a Data Breach Report 2021 IBM Security

Мир стремительно меняется, периметр меняется вместе с ним

Работа с облачными сервисами

Выросшая мобильность сотрудников



Соблюдение баланса «безопасность – удобство»

Переход на удаленную работу

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

ТехноФест 2021 infotecs

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

2010

Zero Trust

Аналитиком компании Forrester Джоном Киндервагом предложена концепция Zero Trust.

2014

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).

2017

ZT CARTA и ZTX

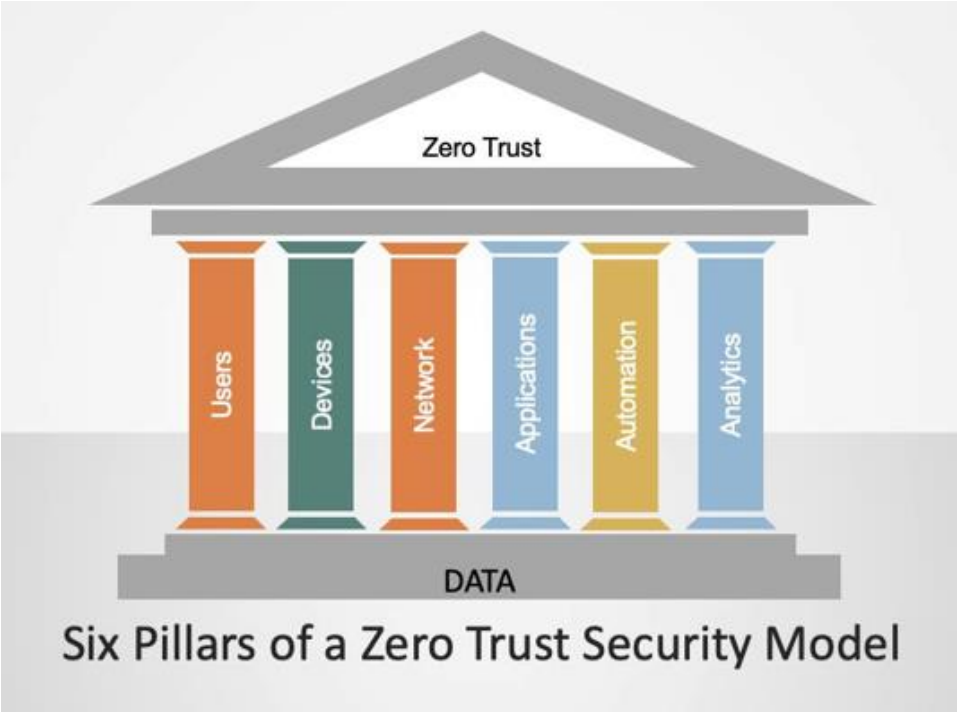
Эксперт Forrester Чейз Каннингэм расширяет концепцию ZT, назвав ее Zero Trust eXtended.
Специалисты Gartner финализируют свою концепцию CARTA.

2021

Генерализация

ИТ индустрия признает термин Zero Trust Architecture как общее название.

Что входит в модель «нулевого доверия»?



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

Zero Trust – это, в первую очередь, цель\стратегия сетевой безопасности, в основе которой лежит набор технологий, которые обеспечивают принцип «никому ничего не доверяй». Архитектуру данной модели можно строить на разных решениях и программных продуктах.

ТЕХНО infotecs 2021 ФЕСТ

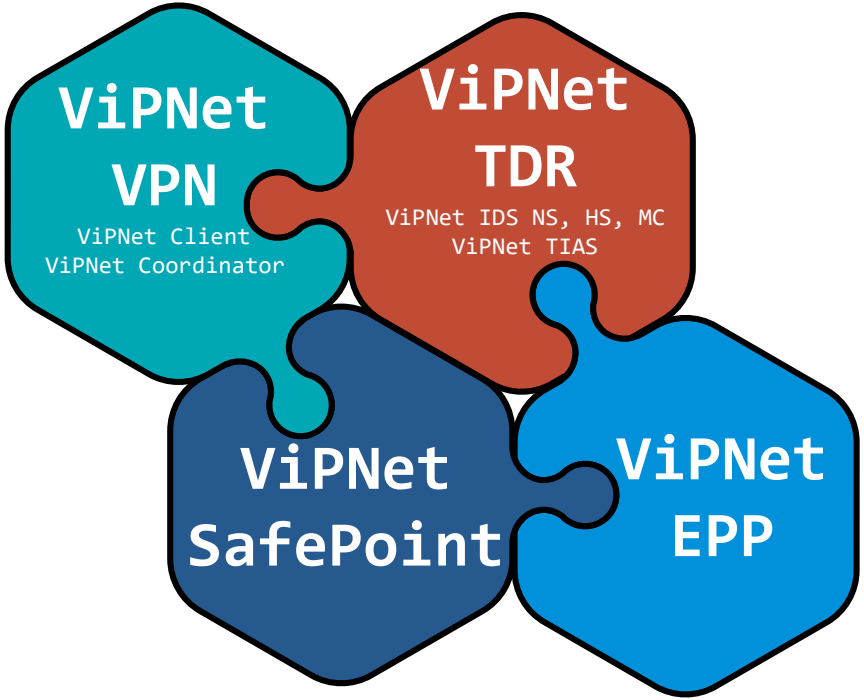
Что предлагаем мы

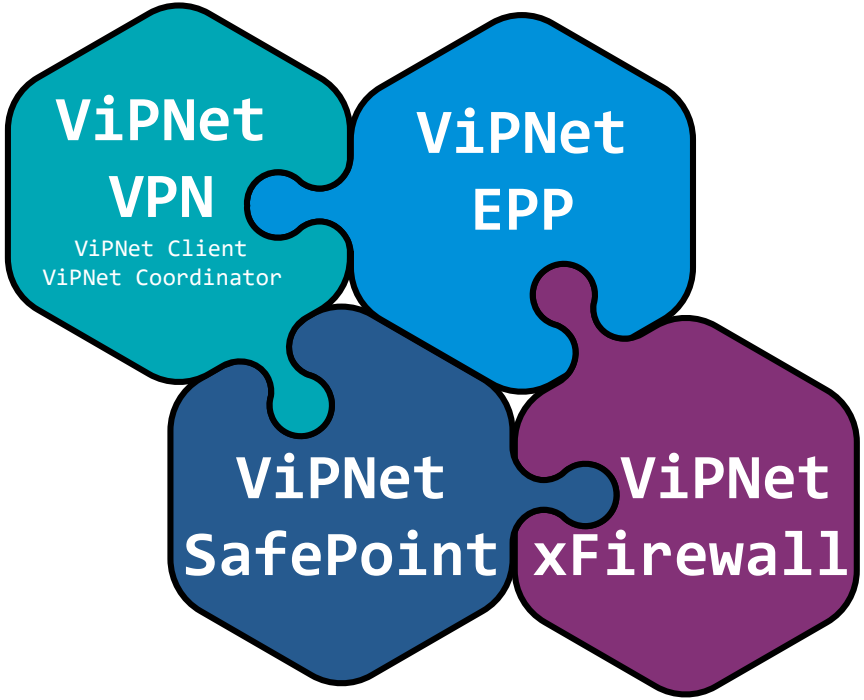
Продукты ИнфоТеКС соответствующие технологиям Архитектуры Zero Trust

ТехноФест infotecs 2021

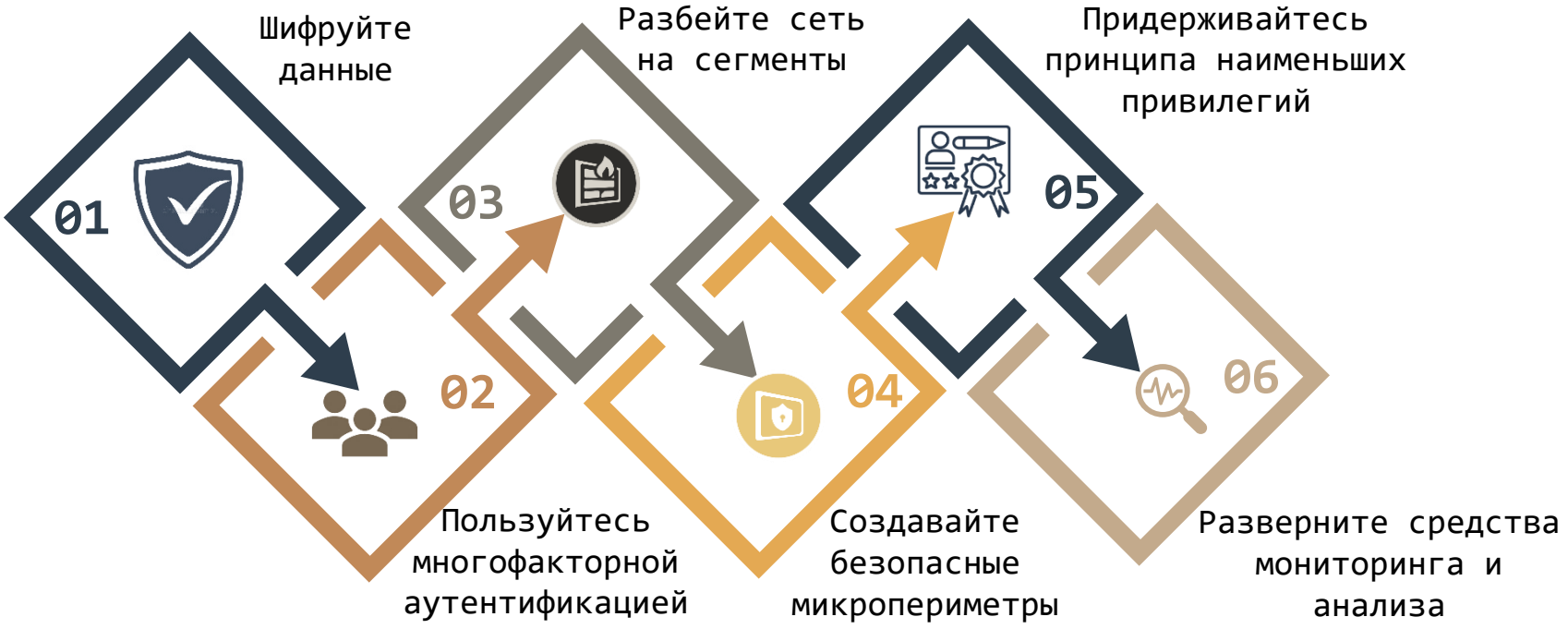
	ViPNet Client	ViPNet Coordinator	ViPNet xFirewall	ViPNet SafePoint	ViPNet EPP	ViPNet TDR
Identity and Access Management (IAM)				☑		
Многофакторная аутентификация (MFA)	☑			☑		
Защита EndPoint (микроперимметры)	☑			☑	☑	
Микросегментация	☑	☑	☑	☑	☑	
Zero Trust Network Access (ZTNA)	☑	☑	☑	☑	☑	
Мониторинг 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
- Потеря актуальности оппортунистических атак

Схемы решения

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

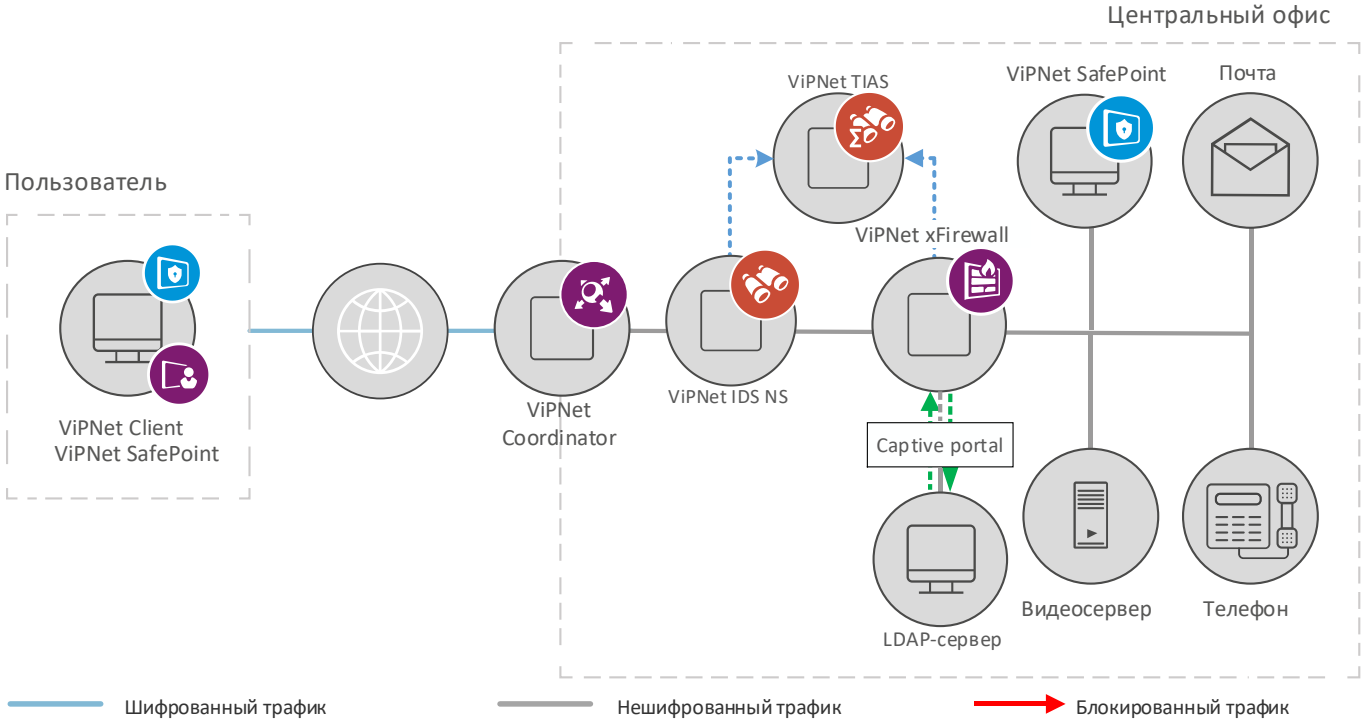
- Сегментация сети
- Комплексная защита от сетевых угроз на всех уровнях
- Безопасное использование персональных устройств в рабочих целях с соблюдением политик безопасности – BYOD (Bring Your Ownn Device)

ViPNet TDR

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

ZTA = VPN+xFirewall +SafePoint+TDR

- ✓ MFA-аутентификация перед подключением
- ✓ Безопасное подключение к сети
- ✓ Защита данных
- ✓ Микросегментация
- ✓ Фильтрация трафика на уровне приложений
- ✓ Аутентификация для подключения к ресурсам
- ✓ Обнаружение и реагирование на угрозы



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)

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

- ✓ MFA-аутентификация перед подключением
- ✓ Безопасное подключение к сети
- ✓ Микросегментация
- ✓ Фильтрация трафика на уровне приложений
- ✓ Аутентификация для подключения к ресурсам
- ✓ Анализ трафика на наличие сетевых атак
- ✓ Регламентированный доступ в Интернет

Создание микропериметра с помощью ViPNet EPP

ViPNet Client

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

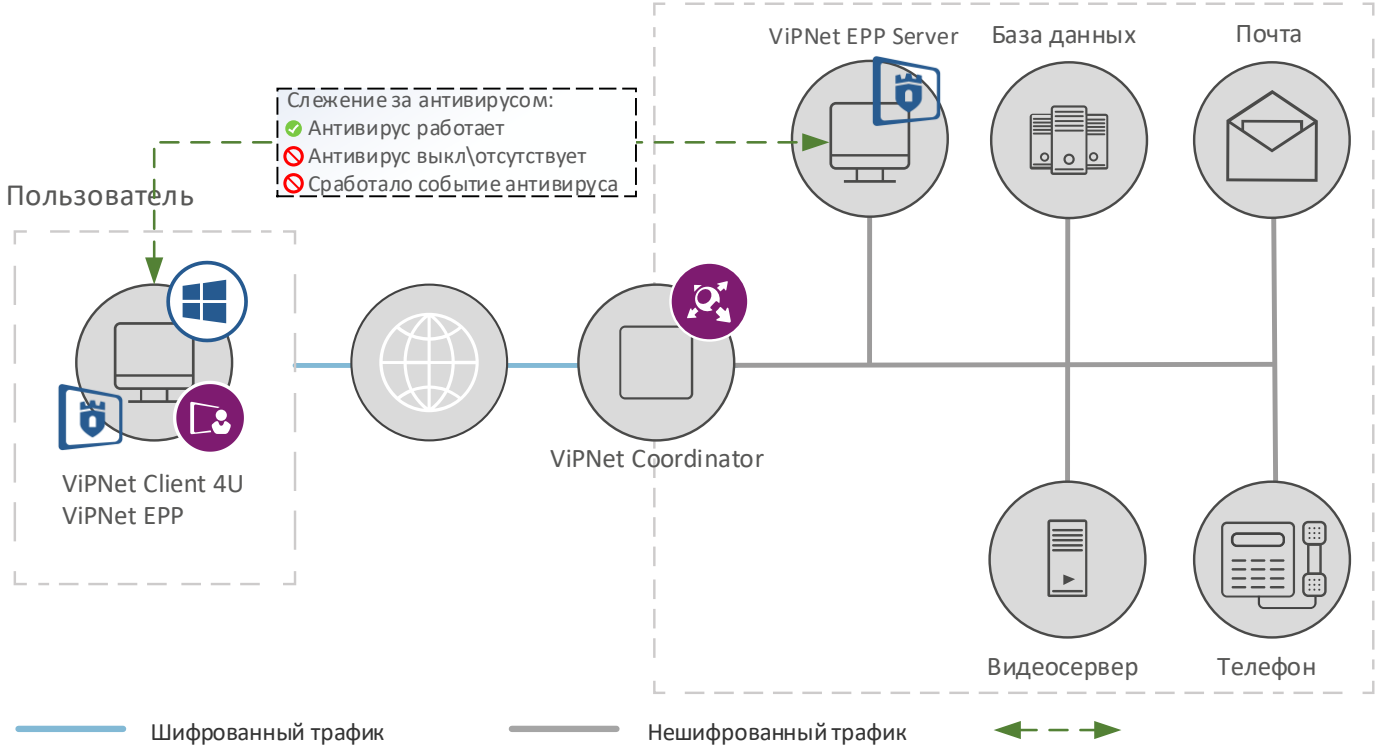
ViPNet Coordinator

- 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

Создание микропериметра с помощью ViPNet EPP



Подведем итог, на чем строится ViPNet Zero Trust Architecture

Защищенное соединение

Построение шифрованного туннеля между узлами защищенной сети **ViPNet Client, ViPNet Coordinator**

Микропериметр

Контроль доступа пользователей к:
- программам
- файлам и документам
- устройствам

Все ПО и службы защищены от изменений **ViPNet SafePoint**
За отслеживание работы антивируса отвечает **ViPNet EndPoint Protectoin**

Микросегментация

ViPNet Client, Coordinator – сегментация сети для обеспечения политик нулевого доверия.
ViPNet xFirewall – разграничение доступа и комплексная защита от сетевых угроз

Мониторинг и аналитика

ViPNet EndPoint Protectoin, ViPNet IDS NS, ViPNet TIAS – защита от внешних угроз, обнаружение и реагирование на неизвестные угрозы

ZTA готова!

ТЕХНО 2021 infotecs Фест

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow