

Кадыков Иван
руководитель продуктового направления



ViPNet EndPoint Protection

сертифицированная система комплексной
защиты рабочих станций и серверов



Свершилось

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4666

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
22 марта 2023 г.

Выдан: 22 марта 2023 г.
Действителен до: 22 марта 2028 г.

Настоящий сертификат удостоверяет, что изделие **ViPNet EndPoint Protection**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, реализующим функции межсетевого экрана и системы обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа В четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности ФРКЕ.00238-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00238-01 30 01.

Сертификат выдан на основании технического заключения от 21.02.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией АНО «Институт инженерной физики» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 03.03.2023, оформленного органом по сертификации ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.А001).

Заявитель: АО «ИнфоТеКС»

Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29

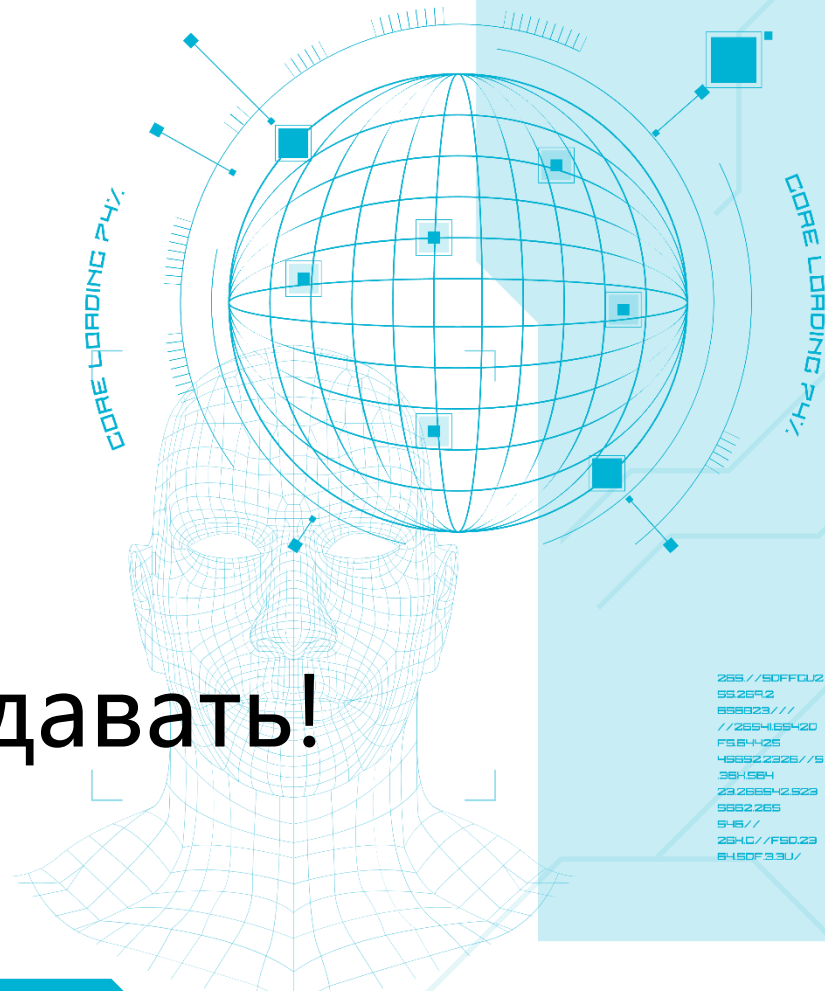
Телефон: (495) 737-6192

Долгожданный сертификат!

- Межсетевой экран тип В класс 4
- Система обнаружения вторжений У4
- 4 класс ТДБ

Сертифицирована версия 1.5.1

Все!
А теперь продавать!



2SS // 80FFCQ2
SS 26R2
858823 ///
// 265465420
FS 64-26
46652 2326 // 5
364584
23 266542 523
662 266
8-6 //
264C // F60.23
8-450F 33U /

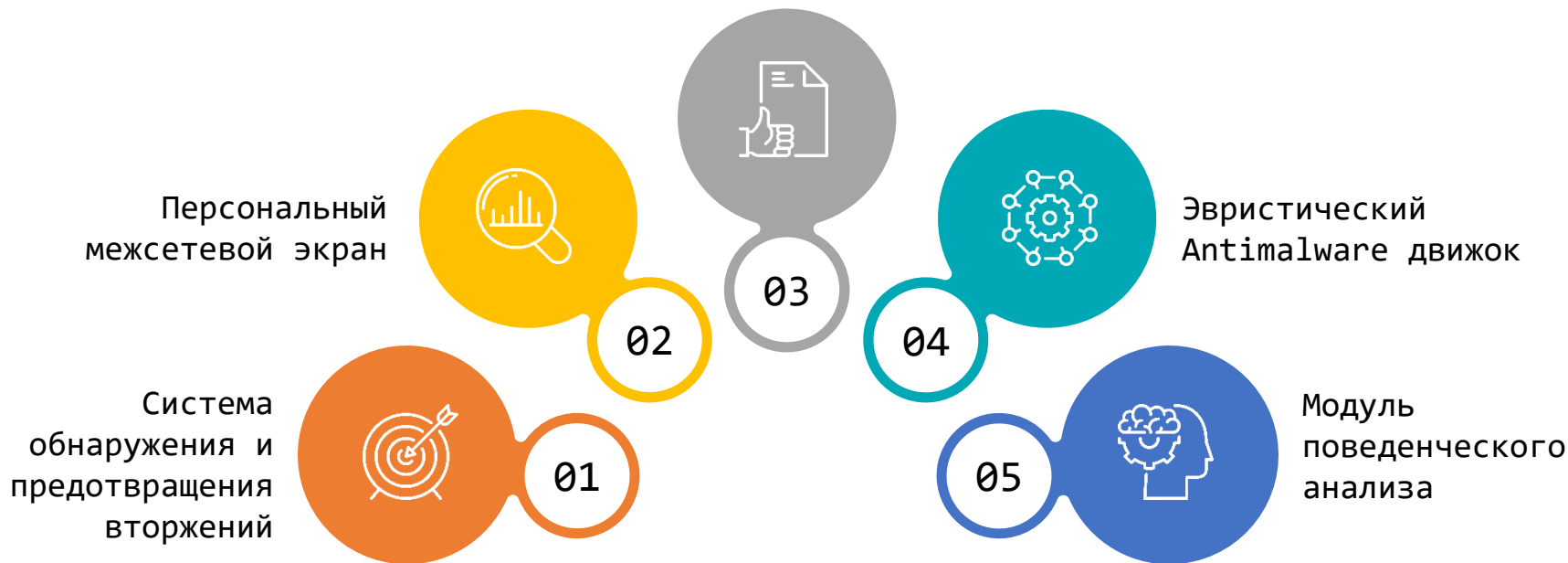


VIPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых», «бесфайловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия

Защитные механизмы

Контроль приложений



Обнаружение и предотвращение атак

Используем:

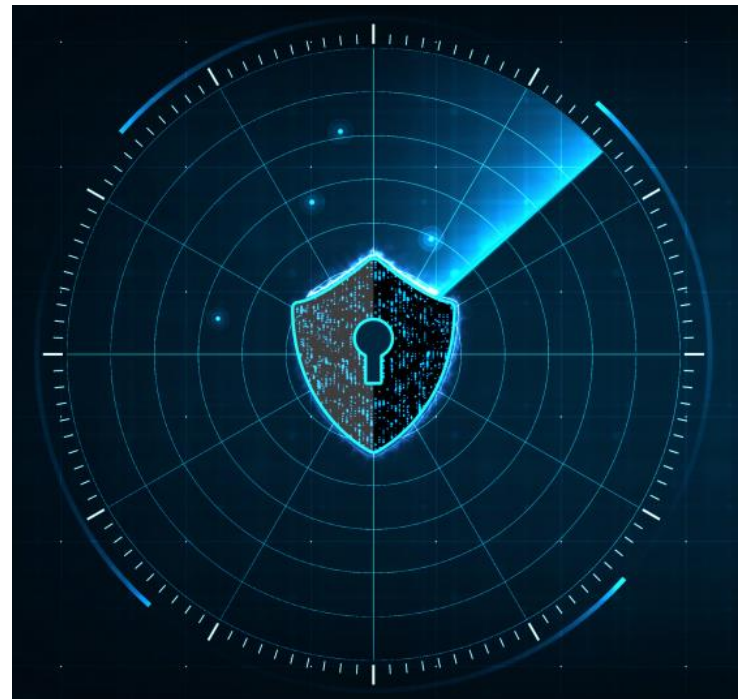
- Эвристический анализ
- Сигнатурный анализ

Следим за:

- Системными журналами Windows
- Журналами и логами приложений
- Изменениями в файловой системе и реестре
- Сетевым трафиком

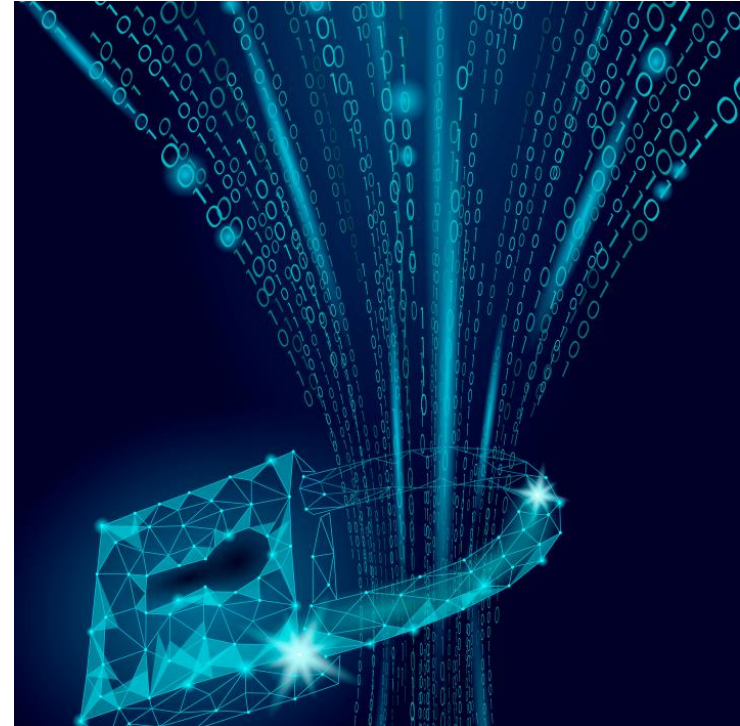
Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты



Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие преднастроенных фильтров
- Создание фильтров для определенных групп хостов
- Создание правил фильтрации из журнала трафика



Контроль приложений

- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений



Эвристический Antimalware движок

- Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда
- Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения
- Модель постоянно обновляется в рамках подписки на БРП



Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения.

Выявляем различного рода аномалии, например:

- Аномальный вход в систему
- Аномалия в создании процесса
- Аномалия в создании задачи планировщику
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.

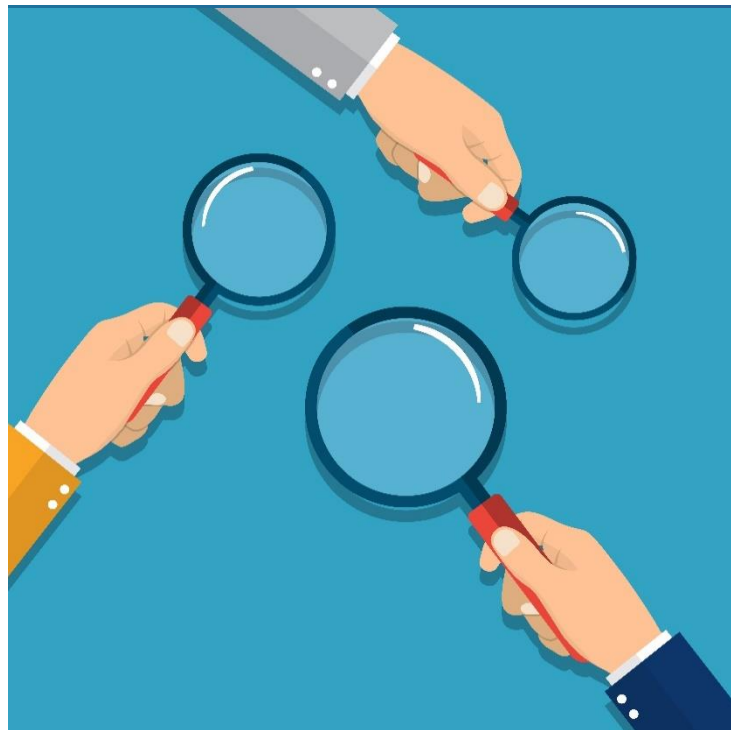


Обнаружение и предотвращение бесфайловых атак

Расширение возможностей модуля обнаружения и предотвращения вторжений

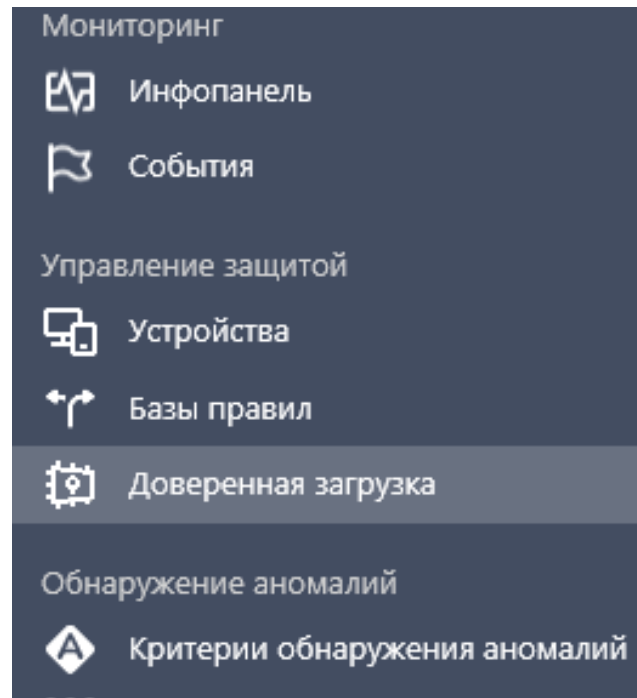
Отслеживаем техники Keylogging и Process injection

- Credential API Hooking (T1056.004)
- Process Hollowing (T1055.012)
- Process Doppelganging (T1055.013)
- Dynamic-link library injection (T1055.001)
- Portable Executable Injection (T1055.002)



Ещё одна «приятная» особенность!

- Теперь для управления ViPNet SafeBoot 2.1, 3.0 и далее можно (нужно) использовать ViPNet EndPoint Protection.
- В версии 1.5.1 функциональность аналогична ViPNet SafeBoot MC
- Начиная с версии 1.6 добавятся:
 - Обновление SafeBoot в сети
 - установка корневых сертификатов (если аутентификация по сертификату на токене)
 - Управление пользователями (создание/изменение/удаление)



Управление ViPNet SafeBoot

ViPNet EndPoint Protection Server

Администратор

Мониторинг

Инфопанель

События

Управление защитой

Устройства

Базы правил

Доверенная загрузка

Обнаружение аномалий

Критерии обнаружения аномалий

Поведенческий анализ

AntiMalware

Сервис

Журналы

Доверенная загрузка

Устройства

Лицензии

Введите название устройства

Выбрано 0

Выгрузить журнал аудита

Активировать лицензию

Наименование	Состояние	Версия SafeBoot	Лицензия
↑ Все устройства > Офис			
☐ astra	Не в сети	Не установлен	Не распределена
☐ DESKTOP-4FTK2QK	В сети	2.0.0.22	Не распределена

☒ Передача событий в ViPNet TIAS

Уровни передаваемых событий

Минимальный уровень событий: Информационное ▼

Типы правил

- ☒ Обнаружение вторжений
 - ☒ Правила обнаружения локальных атак
 - ☒ Правила обнаружения сетевых атак
 - ☒ Выполняемые команды
 - ☒ Обнаружение установки ПО
 - ☒ Мониторинг файлов
 - ☒ Статус пакетов обновления Windows
 - ☒ Получение контрольных сумм файлов
- ☒ Персональный межсетевой экран
- ☒ Контроль приложений
- ☒ Предотвращение вторжений

Сервер ViPNet TIAS

Адрес сервера ViPNet TIAS: 10.0.24.164 Порт: 34222

Отправить тестовое сообщение

Идентификатор ViPNet EPP Сервера: f1dc75da-3131-499c-88ac-a6963694068b



Интеграция с ViPNet TIAS

Другие варианты передачи данных

- электронная почта
- по syslog в формате cef

Передача данных

Электронная почта Active Directory Syslog TIAS

☐ Использовать рассылку по электронной почте

Настройки отправки оповещений

Период отправки сообщений (минут):

Адрес отправителя:

Почтовый сервер

Почтовый сервер: Порт:

☒ Использовать SSL/TLS

Авторизация

Имя пользователя:

Пароль:

Проверить настройки

Передача данных

Электронная почта Active Directory Syslog TIAS

☒ Передача событий в Syslog

Уровни передаваемых событий

Минимальный уровень событий:

Поддерживаемые ОС

Сервер и агент

- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Только Агент

- Astra Linux Special Edition 1.6 и 1.7
- РЕД ОС 7.3 / 7.3.1
- Альт Рабочая станция 8 СП
- Debian 11 (64-разрядная)
- CentOS 7.5 (64-разрядная)



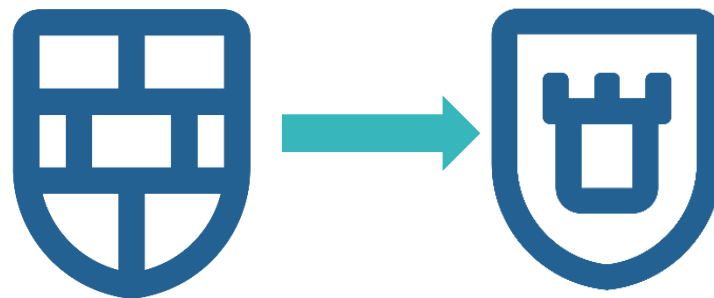
Полезная информация



Замена ViPNet Personal Firewall 4.5

Причины:

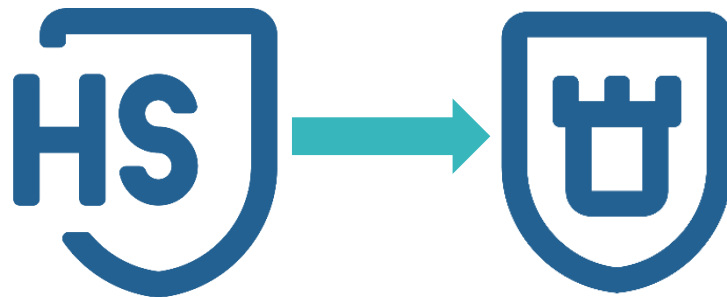
- ViPNet Personal Firewall находится на поддержке
- ViPNet Personal Firewall не поддерживает последние версии отечественных Linux
- Исключена поддержка ОС Windows
- Нет централизованного управления



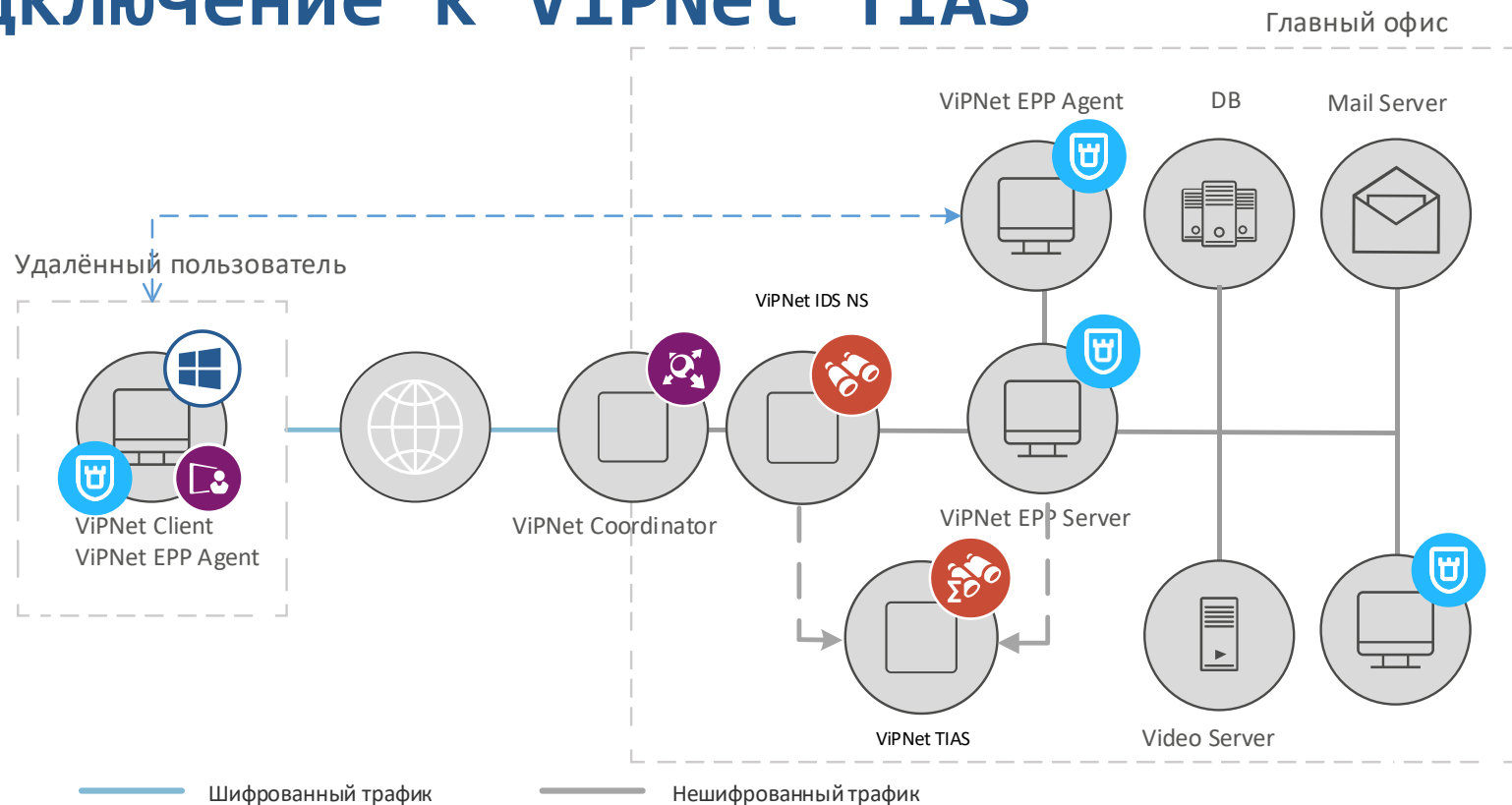
Замена ViPNet IDS HS

Причины:

- ViPNet IDS HS находится на поддержке
- ViPNet IDS HS не поддерживает последние версии отечественных Linux
- Нет возможности предотвращения и реагирования на атаки



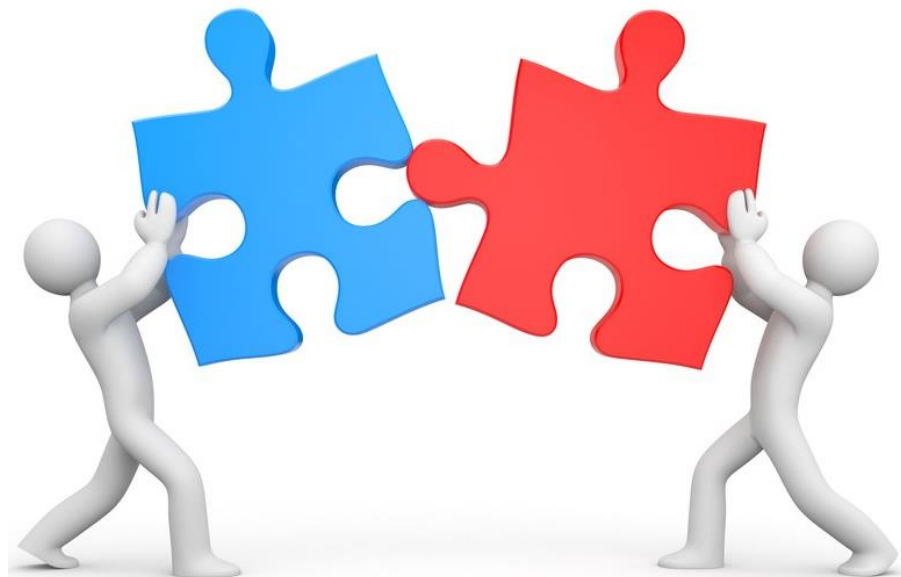
Замена ViPNet IDS HS и подключение к ViPNet TIAS



А если есть сторонний антивирус?

Сторонний антивирус – это ещё один эшелон защиты. VipNet EPP никак не конфликтует с антивирусами, а с некоторыми, даже «дружит»:

- Kaspersky Endpoint Security
- Dr.Web Desktop Security Suite



Интеграция с VipNet Client 4U и ZTNA

Возможность управления фильтрами защищённой сети на хосте, через локальную консоль VipNet EndPoint Protection

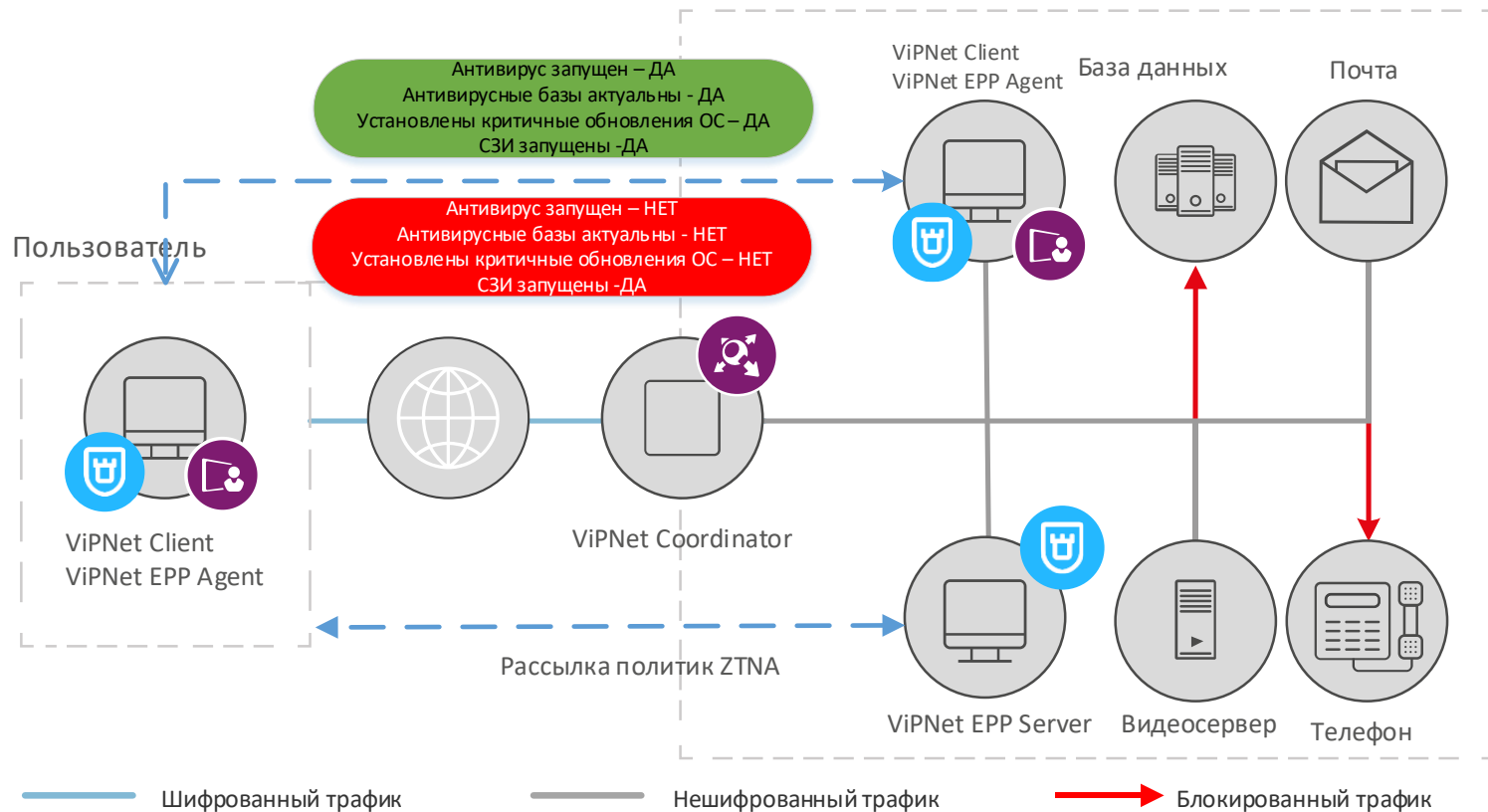
Организация ZTNA-политик:

- Проверка хоста на наличие определённого ПО, полученных обновлений ПО и антивирусных баз и т.д.
- Блокировка защищенной сети на устройстве при несоответствии устройства политикам ZTNA, информирование пользователя об этом

РЕЛИЗ в сентябре 2023



Вариант ZTNA – схематично



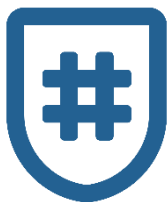
Раз уж заговорили о будущем – что ещё будет?

- Реализация сервера под Linux
- Расширение возможностей по управлению ViPNet SafeBoot
- Модуль Safebrowsing
- Реализация SSL-инспекции на хосте
- Внедрение новых методик определения бесфайловых атак
- Прочие улучшения



Вместо заключения

Защиты хоста сертифицированными продуктами ViPNet



ViPNet SafeBoot



ViPNet Client 4U

Доверие
к платформе
и обеспечение
доверенной
загрузки ОС

Разграничение
доступа
и защита
данных

Обеспечение
защищенных
коммуникаций

Защита
от внешних
атак
и угроз



ViPNet SafePoint



ViPNet EndPoint
Protection

Эпилог – «на партнёрке в 2016»



3

Пришло время



4

ИнфоТеКС и EndPoint Protection.

5

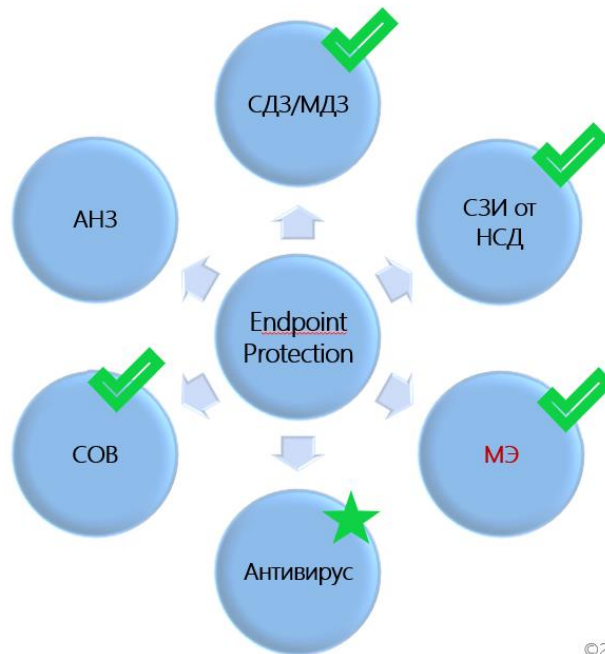
Endpoint Protection - это



6

Основной драйвер

Endpoint Protection - это



©2016, ОАО «ИнфоТеКС».



Ответы на вопросы

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363





Спасибо за внимание!

При поддержке



m[≡]rlion

AXOFT

РУТОКЕН
КОМПАНИЯ ПРАКТИВ

