Обзор продуктов линейки ViPNet EndPoint Security

Свежий взгляд на классические подходы к защите Endpoint

Кадыков Иван
Руководитель продуктового направления

ТЕХНО infotecs 2022 ФЕСТ

Пролог

Рынок защиты рабочих станций многогранен

Все поддается структуризации

Классический Endpoint Protection	• знаем, что ищем (антивирус). Блокируем, что знаем (МЭ + HIPS), контролируем подключение устройств
Next Generation Endpoint Protection	• классический Endpoint + модули по обнаружению и противодействию современным угрозам (ransomware, fileless-атаки, never-before-seen attacks) – Sandbox, Appcontrol, Memory Protection…
Endpoint Detection & Response	• NG EPP + возможность расследования инцидента и формирование реакции на инцидент (forensic)

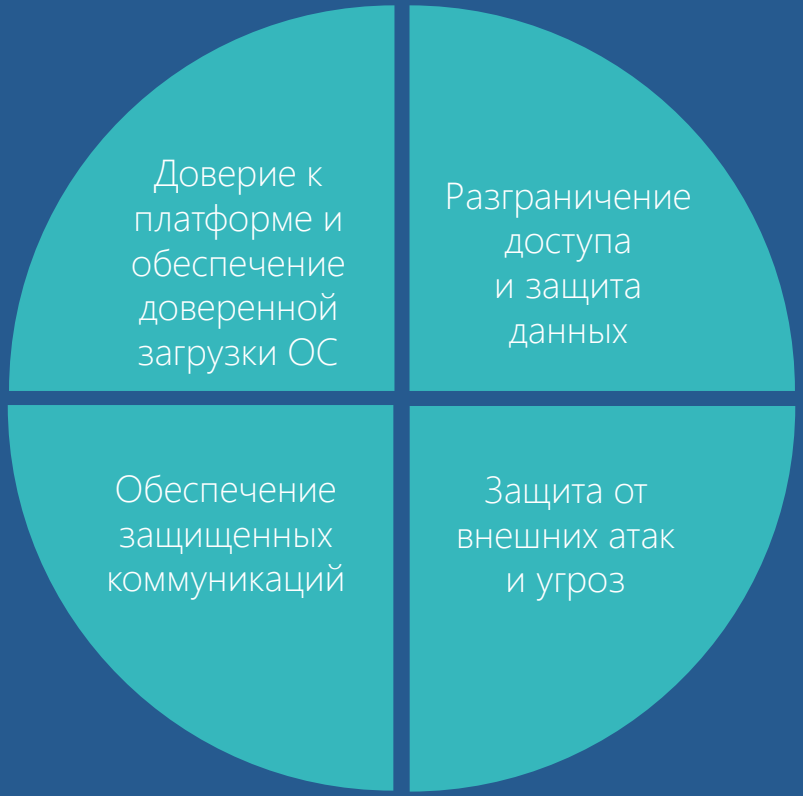
«Российский Endpoint»

Средство защиты
от несанкционированного доступа

«Конечные устройства» — главная цель

Растущее количество атак и недоверенных аппаратных компонент

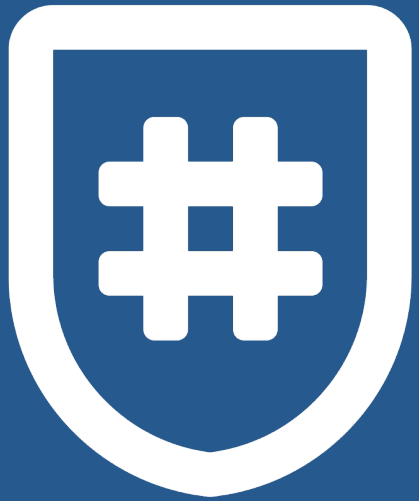
Пользователь - внутренний нарушитель, низкий уровень опыта



Удаленная работа, проведение приватных разговоров

Malware, Ransomeware, Fileless & Never-seen-before attacks

ViPNet SafeBoot



ViPNet SafeBoot

Высокотехнологичный программный модуль доверенной загрузки, устанавливаемый в UEFI BIOS различных производителей. Предназначен для защиты компьютеров и серверов (в т.ч. и серверов виртуализации) от современных угроз НСД, связанных с загрузкой ОС и атак на сам BIOS.

Решаемые задачи ViPNet SafeBoot

Организация доверенной загрузки

Контроль целостности

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS

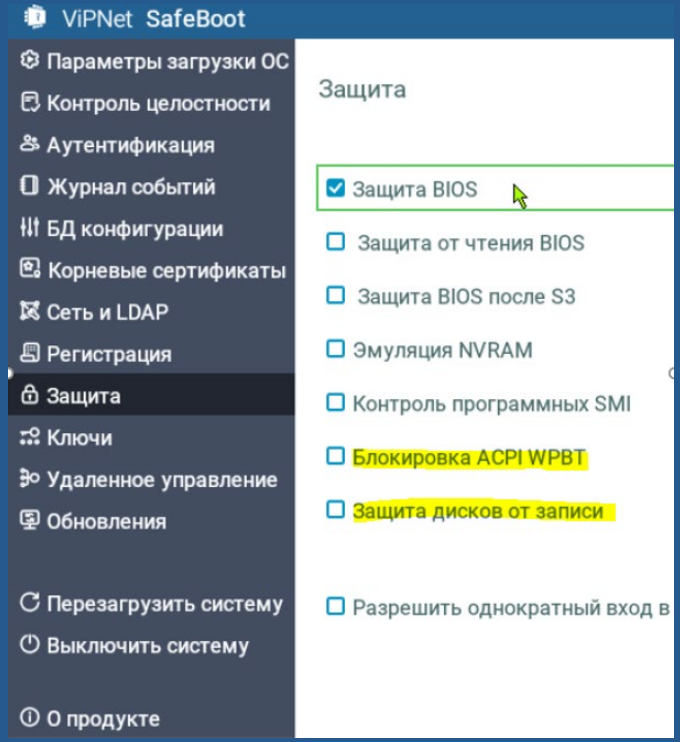
Разграничение доступа

- Двухфакторная аутентификация
- Авторизация в AD/LDAP

Релиз 2.1. Сертифицированная версия

- Защита от malware в UEFI BIOS
- Активация защиты на платформах AMD
- Поддержка токена Rutoken S
- Поддержка работы со считывателями смарт-карт — ACR38, JCR721, ASEDrive IIIe
- Поддержка SSO для входа в операционную систему и ViPNet SafePoint v.1.2
- Поддержка сенсорных экранов, реализация сенсорной клавиатуры под UEFI
- Базовая поддержка ARM-архитектуры

Защита от Malware



Как действует malware?

- запись файлов malware из UEFI на диск посредством встроенного (собственного) драйвера файловой системы
- использование технологии Windows Platform Binary Table (WPBT)

Сертифицировано

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3823

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
14 ноября 2017 г.

Выдан: 14 ноября 2017 г.
Действителен до: 14 ноября 2020 г.
Срок действия продлён до: 14 ноября 2025 г.

Настоящий сертификат удостоверяет, что **программный комплекс «Программный модуль доверенной загрузки ViPNet SafeBoot»**, разработанный и производимый АО «ИнфоТеКС», является программным средством доверенной загрузки, 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 2 уровню доверия, «Требования к средствам доверенной загрузки «(ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты. ИТ.СДЗ.УБ2.ПЗ» (ФСТЭК России, 2013) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00180-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 28.07.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), экспертного заключения от 12.10.2017, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технического заключения от 16.04.2021, оформленного испытательной лабораторией ООО «ЦБИ», и экспертного заключения от 28.05.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «ИнфоТеКС»
Адрес: 127083, г. Москва, ул. Мишина, д. 56, стр. 2, эт. 2, помещение IX, комната 29
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Сертифицирован по :

- Требованиям к средствам доверенной загрузки уровня базовой системы ввода-вывода 2 класса
- Требованиям по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий по 2 уровню доверия

Задачи и потребности — Compliance

- Задача: соответствие требованиям ФСТЭК России по защите ИСПДн, ГИС, АСУ ТП и КИИ — выполнение полного комплекса мер по защите.
- Необходимость использования прописана в мерах защиты по первому и второму классу:
  - В ИСПДн и ГИС — УПД.17
  - В АСУ ТП и КИИ — УПД.3

Банк угроз

ТЕХНО infotecs 2022 ФЕСТ

29 угроз

в полной или косвенной мере
относящиеся к угрозам BIOS/UEFI BIOS

Угроза	Угроза
УБИ.004: Угроза аппаратного сброса пароля BIOS	УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS	УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.008: Угроза восстановления аутентификационной информации	УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.006: Угроза внедрения кода или данных	УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.108: Угроза ошибки обновления гипервизора
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS	УБИ.121: Угроза повреждения системного реестра
УБИ.018: Угроза загрузки нештатной операционной системы	УБИ.123: Угроза подбора пароля BIOS
УБИ.023: Угроза изменения компонентов системы	УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера	УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	УБИ.144: Угроза программного сброса пароля BIOS
УБИ.032: Угроза использования поддельных цифровых подписей BIOS	УБИ.145: Угроза пропуска проверки целостности программного обеспечения
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS	УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS	УБИ.152: Угроза удаления аутентификационной информации
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS	УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
	УБИ.179: Угроза несанкционированной модификации защищаемой информации

Зловреды, атаки, уязвимости…

ТЕХНО infotecs 2022 ФЕСТ

2016

Cr4sh/**PeiBackdoor**

PEI stage backdoor for UEFI compatible firmware

PeiBackdoor – один из первых «зловредов» для UEFI.

2018

LOJAX

First UEFI rootkit found in the wild, courtesy of the Sednit group

Lojax – первый rootkit найденный сотрудниками компании ESET в «дикой среде».

2020

MosaicRegressor: Lurking in the Shadows of UEFI

MosaicRegressor – bootkit найденный сотрудниками «Лаборатории Касперского», предназначенный для шпионажа.

BootHole – уязвимость в загрузчике.

2021

ESPecter – bootkit предназначенный для целевых атак и шпионажа (найден сотрудниками ESET).

2022

MoonBounce позволяет изменить цепочку выполнения команд в UEFI BIOS и осуществить внедрение вредоносного кода, который запуститься при старте машины.
CosmicStrand - руткит находится в образах прошивок материнских плат Gigabyte и Asus , использующих чипсет H81 – 26.07.2022
Уязвимости в подписанных загрузчиках Microsoft – CVE-2022-34301(-34302, - 34303) - 15.07.2022

ViPNet SafeBoot 3.0

- Выпущен ViPNet SafeBoot 3.0, который будет сертифицироваться в двух исполнениях:
  - Исполнение 1. «Локальный» ViPNet SafeBoot – без механизмов удалённого управления, подключения к LDAP – в ФСБ России и в ФСТЭК России
  - Исполнение 2. «Сетевой» ViPNet SafeBoot – с механизмами удалённого управления – только в ФСТЭК России
- Дополнительно реализовано:
  - Доверенная загрузка ОС по сети
  - Формирование отчёта о настройках продукта
  - Поддержка токена Guardant ID версии 2
  - Поддержка ALD PRO (Astra Linux)
  - Поддержка работы на бездисковых станциях

ТЕХНОФЕСТ infotecs 2022

ViPNet SafePoint

ViPNet SafePoint

Средство защиты информации от несанкционированного доступа, устанавливаемое на рабочие станции и сервера, предназначенное для мандатного и дискреционного разграничения доступа к критически важной информации.

Реализована разграничительная (пользователя к объектам) и разделительная (между пользователями) политика доступа, основанная на автоматической разметке создаваемых файлов.

С чего начинается защита от НСД?

Своих пользователей надо знать
«в лицо», поэтому:

- **Идентификация и аутентификация пользователей**
- выполняется собственными механизмами

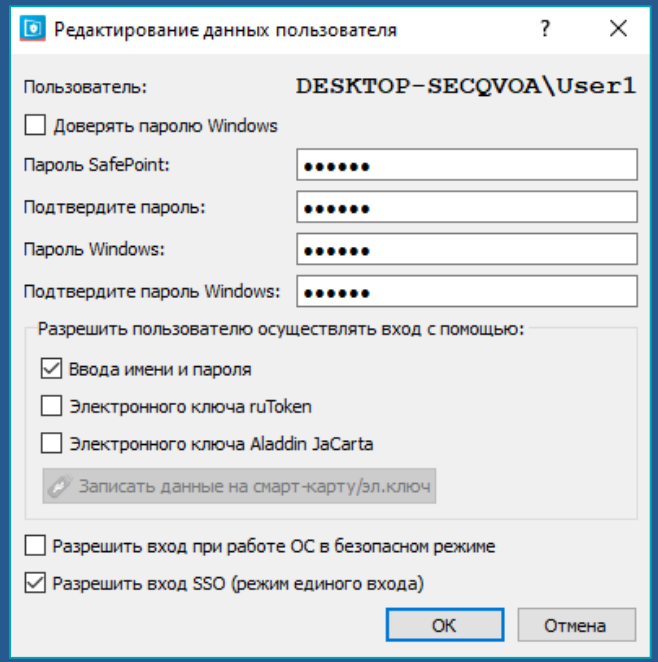
Используем комбинации:

- Логин и пароль
- Логин и идентификатор

SSO (единый вход) для SafeBoot и SafePoint

- В интерфейс SafePoint при добавлении/изменении пользователя добавлен дополнительный флаг:
- «Разрешить вход SSO (режим единого входа)»
- Флаг является индивидуальным для каждого пользователя.

- Поддерживаемые версии
- ViPNet SafeBoot 2.1
- ViPNet SafeBoot 3.0



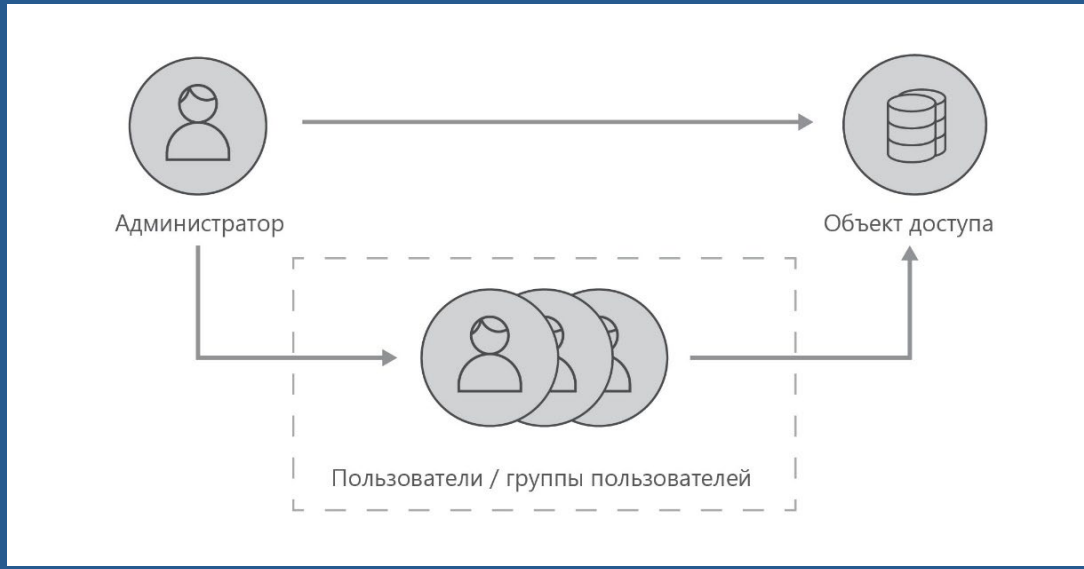
Создание разграничительных политик для пользователя

- После прохождения идентификации и аутентификации, необходимо чтобы пользователь:
  - Работал только с тем ПО, которое разрешено
  - Мог работать только с теми файлами/документами, для которых хватает прав(полномочий)
  - В системе запускались, только разрешенные процессы
  - Не модифицировал(-ись) важные модули

Разграничение доступа

Дискреционный контроль доступа к

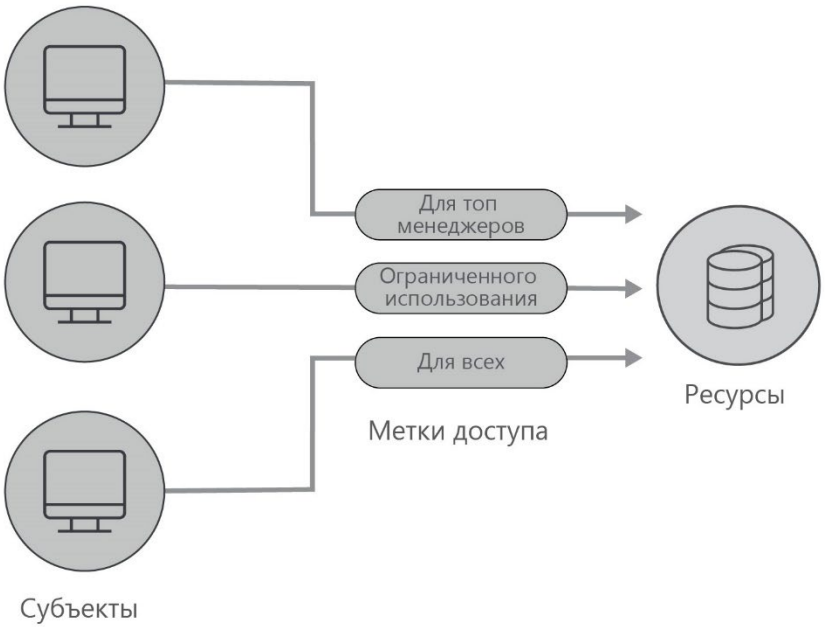
- файловой системе (вкл. сменные)
- прямому доступу к диску
- реестру
- принтерам
- службам
- устройствам
- буфер обмена
- виртуальным машинам



Интересный кейс

- В Windows найдена уязвимость CVE-2021-41379
- Выявлена специалистами из Cisco Talos
- «Повышение привилегий в Microsoft Windows»
- 22.11.2021 выложен эксплоит на GitHub
- Один их вариантов эксплуатации – использование списка управления дискреционным доступом (DACL) в Microsoft Edge Elevation Service

ViPNet SafePoint использует свою дискреционную модель доступа, запрещает запуск того, что создано или изменено пользователем(элемент ЗПС).

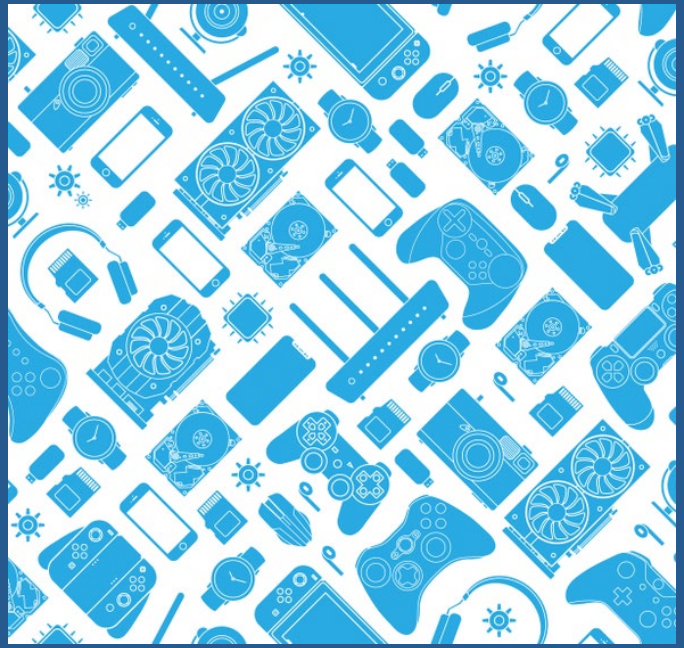


Мандатный контроль доступа пользователей и процессов

Разграничительная политика
на основе меток безопасности

Замкнутая программная среда и контроль времени работы

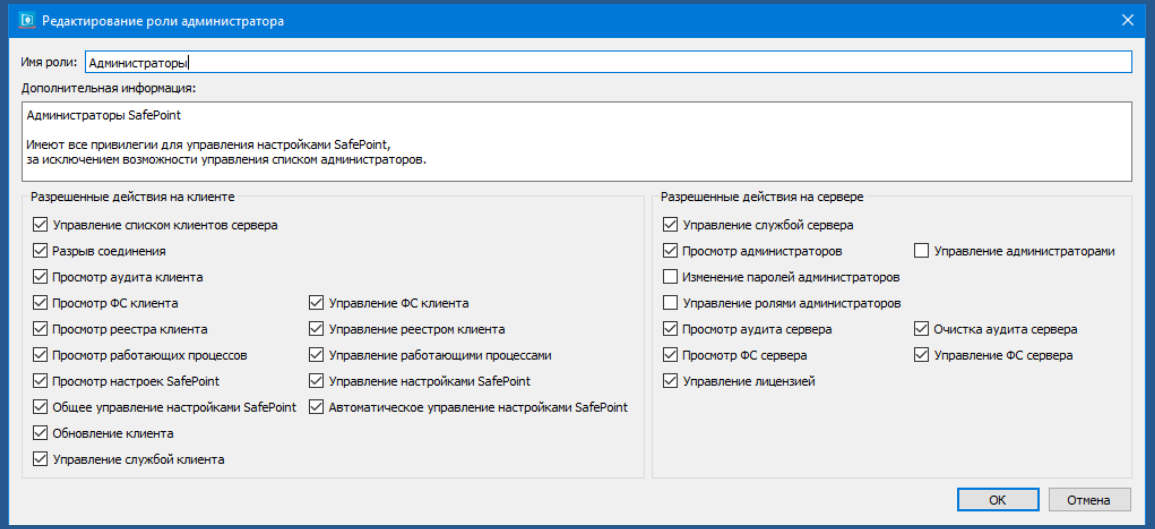
Контроль устройств



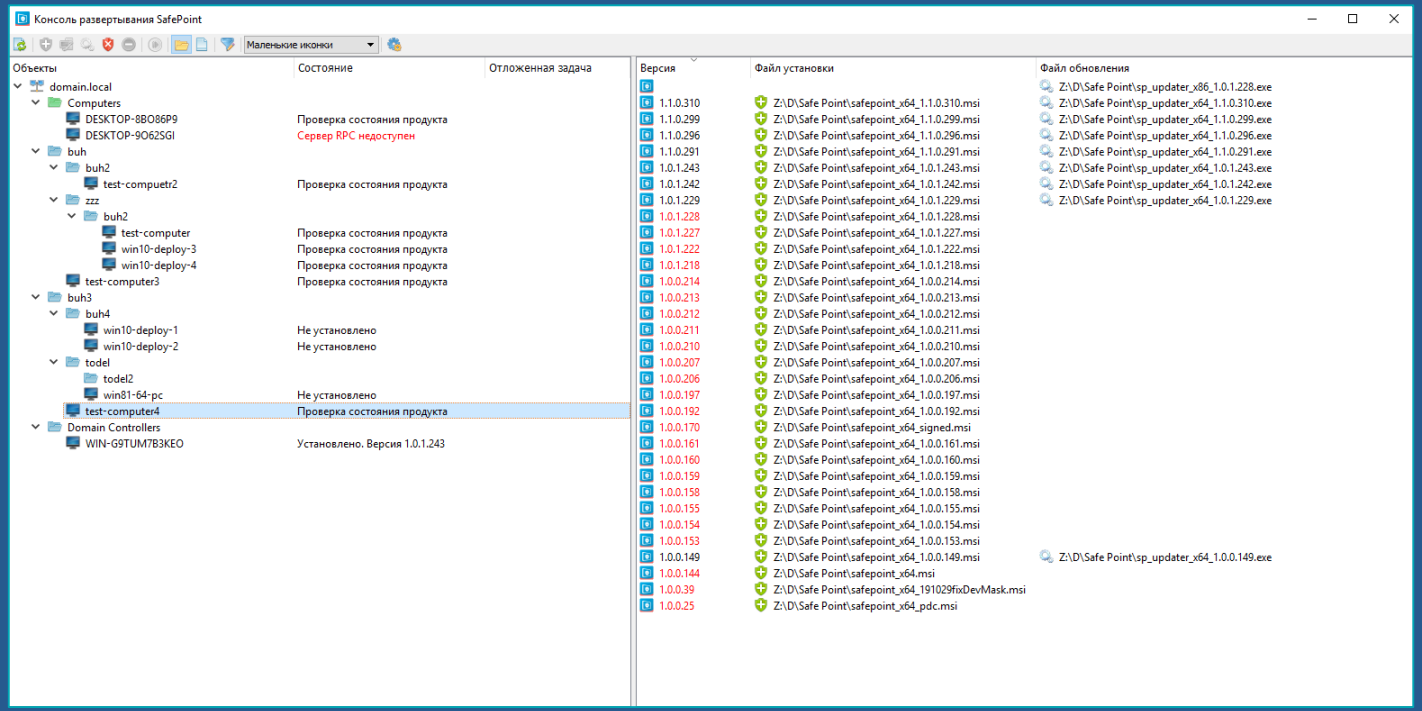
- Контроль и разграничение доступа к подключаемым внешним устройствам
- Разграничение доступа к принтерам

Ограничение действий администраторов

- Реализация настраиваемых ограничений в действиях администраторов – в части управления пользователями в Active Directory
- Делегирование административных полномочий (полных прав/части прав)



Централизованная установка и обновление продукта



Решаемые задачи (дополнительные возможности)

- Защита от внедрения и выполнения вредоносных программ и кода
- Защита от атак на повышение привилегий
- Защита данных от атак на уязвимости системного ПО
- Защита от инсайдеров
- Защита данных от атак на уязвимости прикладного ПО

СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4468

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
18 октября 2021 г.

Выдан: 18 октября 2021 г.
Действителен до: 18 октября 2026 г.

Настоящий сертификат удостоверяет, что **изделие «ViPNet SafePoint»**, разработанное и производимое АО «ИнфоТеКС», является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, 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 средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014), «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по **5** классу защищенности и задании по безопасности ФРКЕ.00240-01 98 01 при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00240-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 15.07.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 05.10.2021, 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

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

ТЕХНО 2022 infotecs ФЕСТ

Сертифицировано

- 5 класс защищенности СВТ
- 4 класс защиты СКН (ИТ.СКН.П4.ПЗ)
- 4 класс ТДБ

ViPNet EndPoint Protection

ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия. Ключевыми модулями системы являются персональный межсетевой экран, система обнаружения и предотвращения вторжений, а также 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

ТехноФест 2022 infotecs

ViPNet EndPoint Protection версия 1.5

Новые защитные механизмы

Новый модуль

Поведенческого анализа (Behavioral analysis)

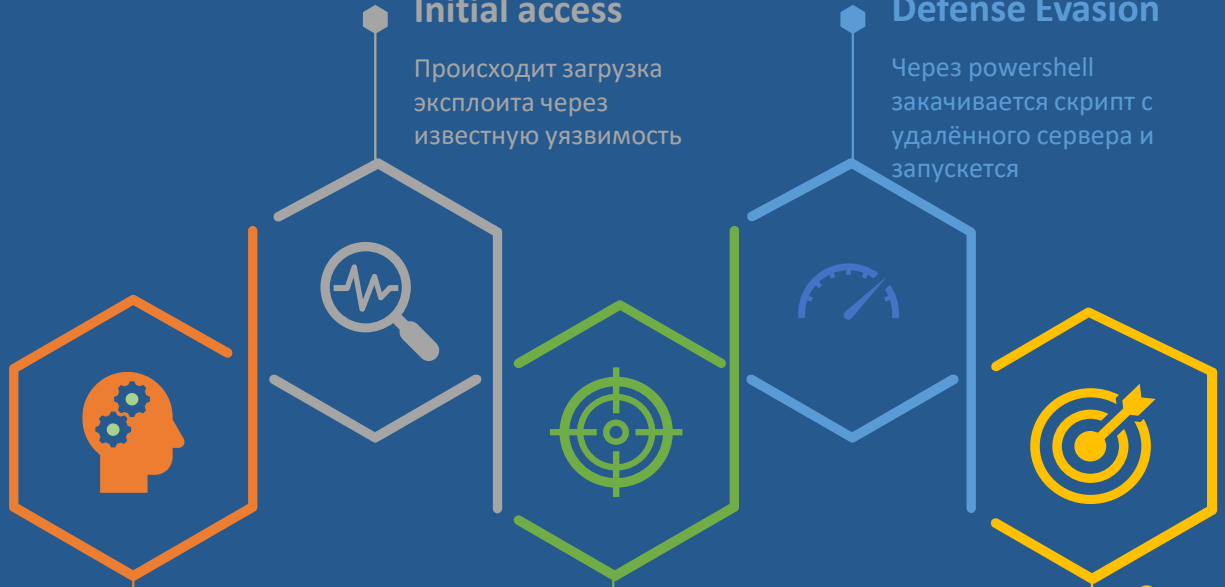
- Выявление аномального поведения (запуска/остановки) системных утилит
- Эвристический движок antimalware

Расширение функциональности HIPS

- Обнаружение и предотвращение бесфайловых атак
- 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)

Как «действует» бесфайловая атака

ТЕХНО 2022 infotecs ФЕСТ



Initial access

Посетил ссылку, открыл почтовое вложение

Initial access

Происходит загрузка эксплоита через известную уязвимость

Execution

Эксплоит запускает powershell в оперативной памяти

Defense Evasion

Через powershell закачивается скрипт с удалённого сервера и запускется

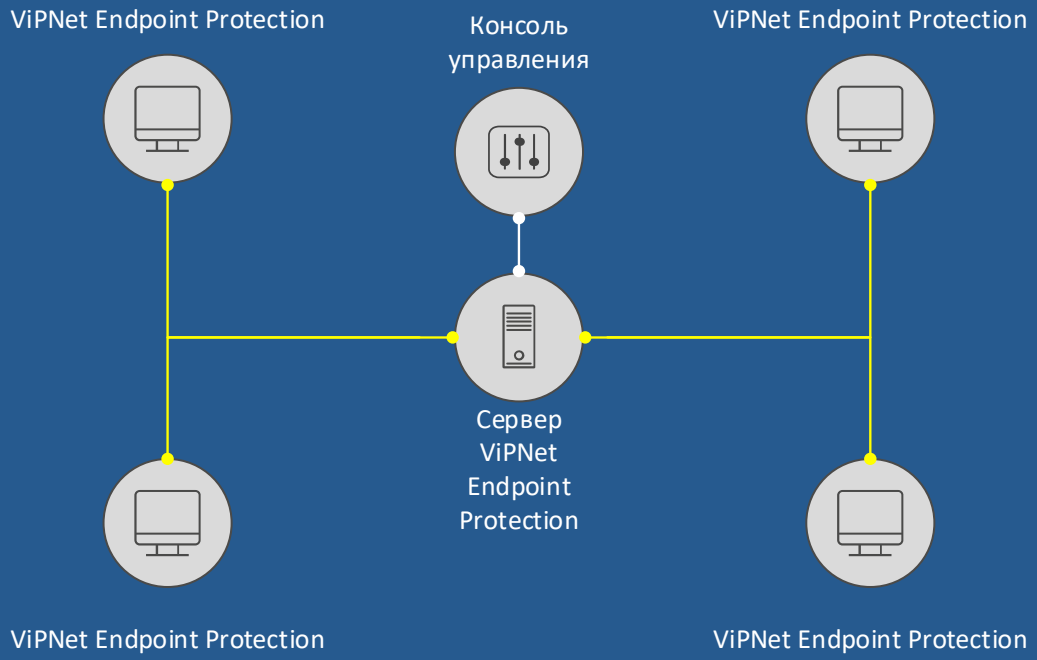
Command and control

Эксплоит располагается в памяти для «плохих дел»

Поддержка Linux

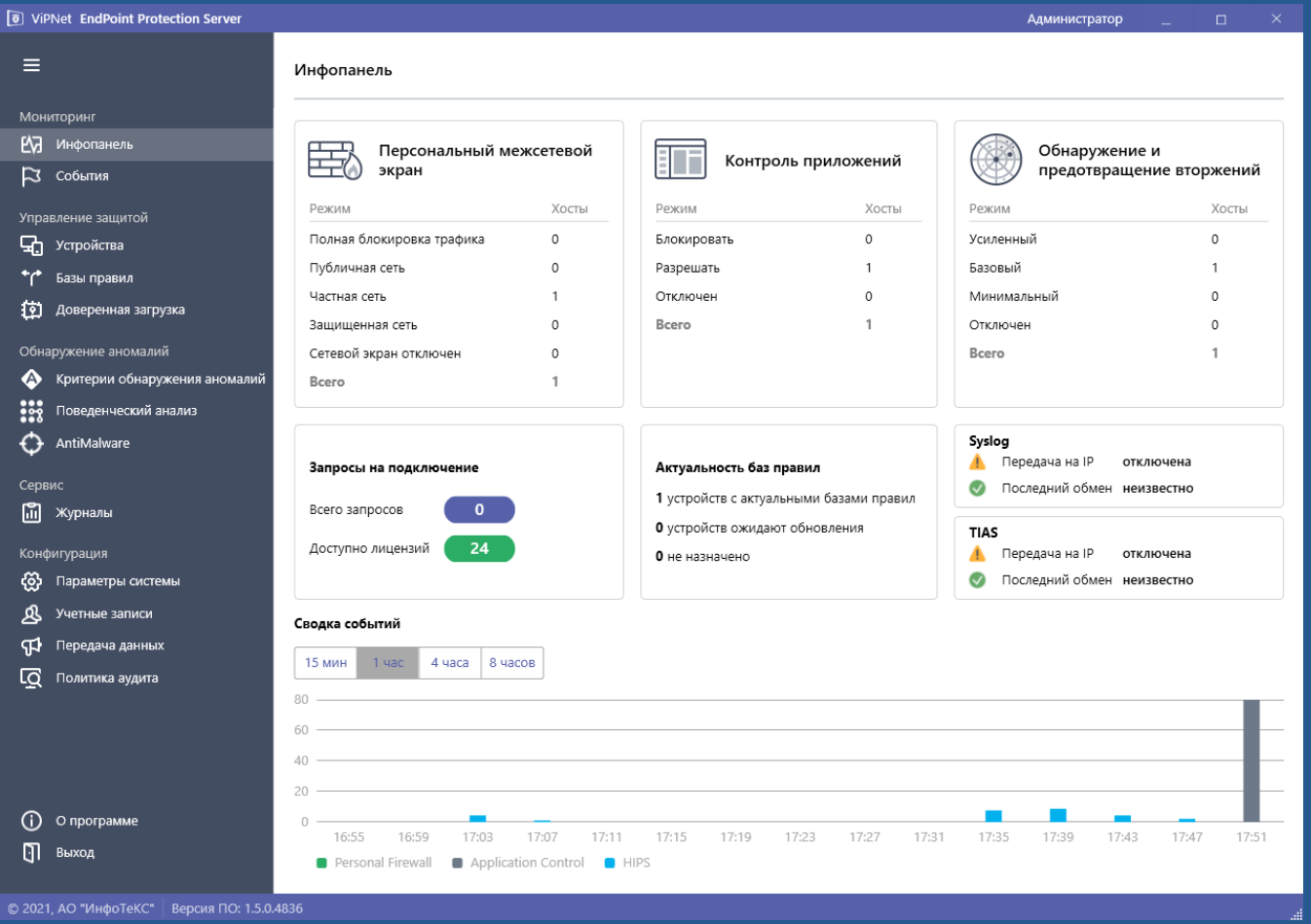
Реализован ViPNet EndPoint Protection агент под следующие операционные системы:

- Astra Linux Special Edition «Смоленск» 1.6.
- РЕД ОС 7.2.
- Альт Рабочая станция 8 СП

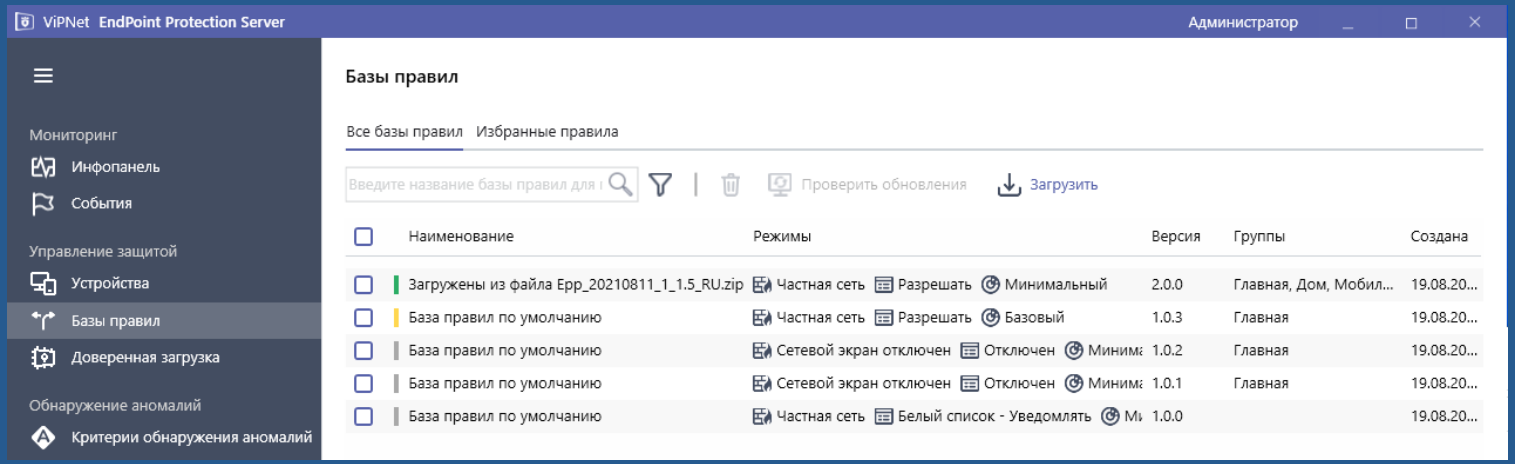


Архитектура ViPNet EndPoint Protection

- Клиент
- Сервер
- Консоль управления



Консоль управления сервером

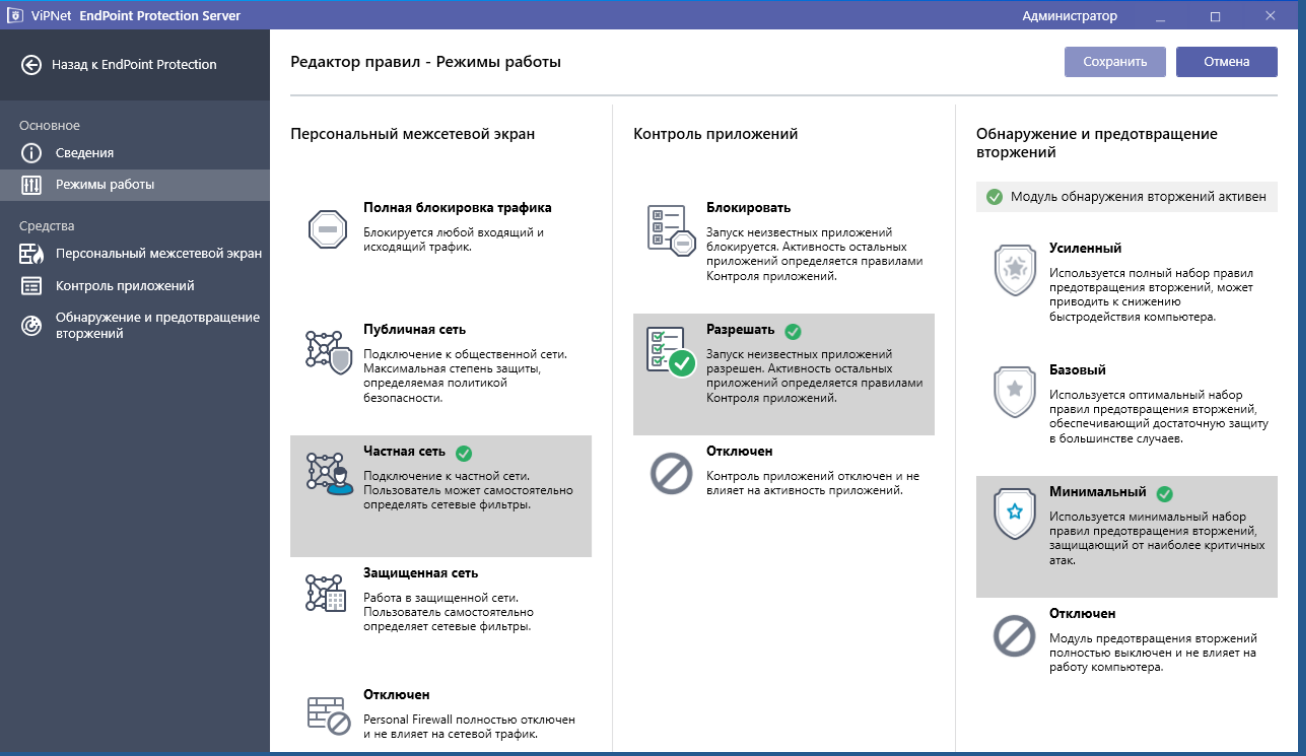


Работаем по правилам!

EndPoint Protection работает по БРП

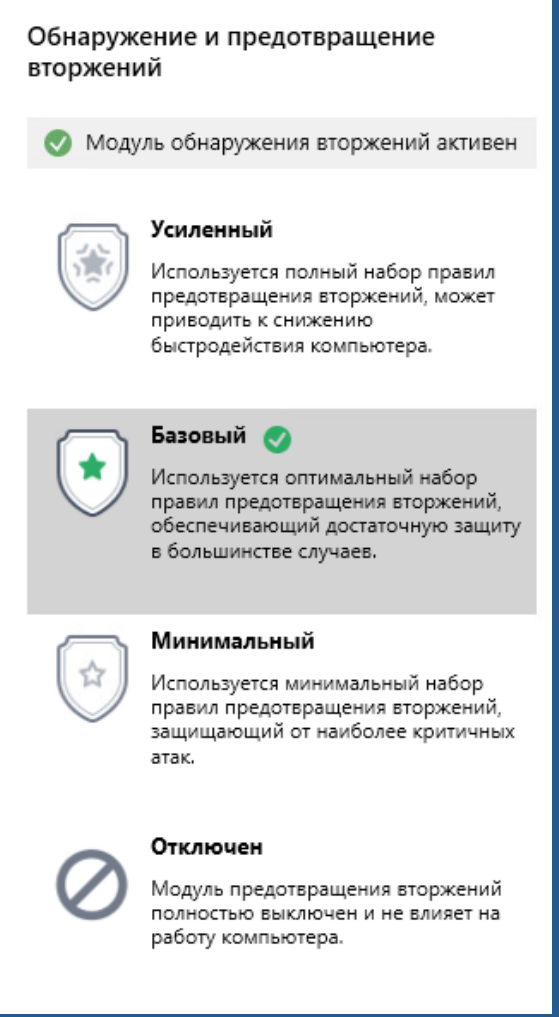
Состоит из:

- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Черного и Белого списка
- Эвристический движок Anti-malware
- Движок обнаружения аномального поведения системных утилит



Настройки модулей – Режимы работы

Администратор может использовать предоставленные нами режимы работы модулей или сам настроить режимы работы модулей



Обнаружение и предотвращение вторжений

Обнаружение вторжений активно всегда.

Механизмы работы схожи с ViPNet IDS HS:

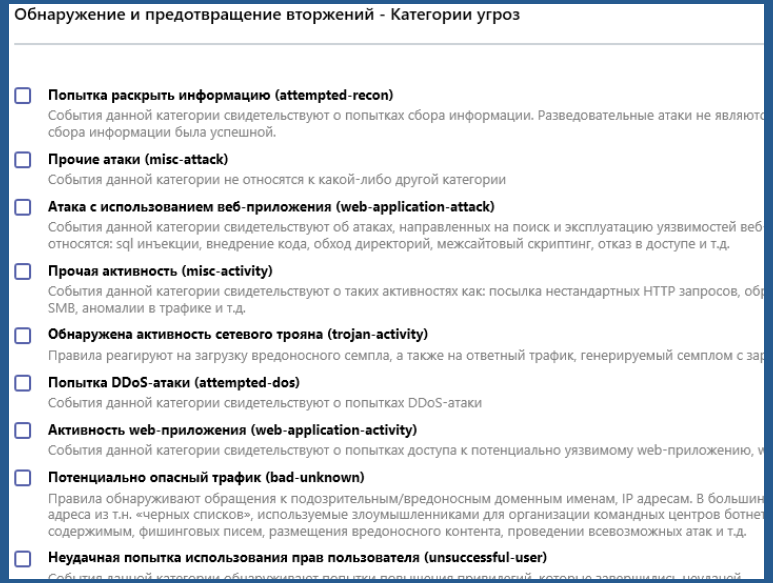
- Загрузили БРП
- Назначили на группу агентов
- Агенты, получив БРП, мониторят события в соответствии с заданными политиками аудита

Предотвращение вторжений — имеется несколько уровней защиты — Усиленный, Базовый, Минимальный (разрабатывали совместно с ПМ)

Предотвращение вторжений

ТЕХНО infotecs 2022 Фест

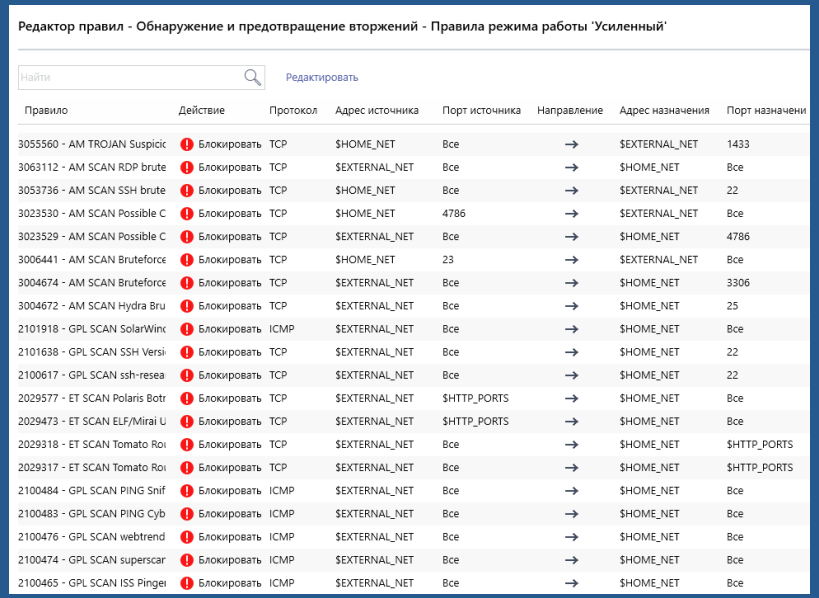
По категориям угроз



Обнаружение и предотвращение вторжений - Категории угроз

- **Попытка раскрыть информацию (attempted-recon)**
  События данной категории свидетельствуют о попытках сбора информации. Разведовательные атаки не являются
  сбора информации была успешной.
- **Прочие атаки (misc-attack)**
  События данной категории не относятся к какой-либо другой категории
- **Атака с использованием веб-приложения (web-application-attack)**
  События данной категории свидетельствуют об атаках, направленных на поиск и эксплуатацию уязвимостей веб
  относятся: sql инъекции, внедрение кода, обход директорий, межсайтовый скриптинг, отказ в доступе и т.д.
- **Прочая активность (misc-activity)**
  События данной категории свидетельствуют о таких активностях как: посылка нестандартных HTTP запросов, обр
  SMB, аномалии в трафике и т.д.
- **Обнаружена активность сетевого трояна (trojan-activity)**
  Правила реагируют на загрузку вредоносного семпла, а также на ответный трафик, генерируемый семплом с зар
- **Попытка DDoS-атаки (attempted-dos)**
  События данной категории свидетельствуют о попытках DDoS-атаки
- **Активность web-приложения (web-application-activity)**
  События данной категории свидетельствуют о попытках доступа к потенциально уязвимому web-приложению, w
- **Потенциально опасный трафик (bad-unknown)**
  Правила обнаруживают обращения к подозрительным/вредоносным доменным именам, IP адресам. В большин
  адреса из т.н. «черных списков», используемые злоумышленниками для организации командных центров ботнет
  содержимым, фишинговых писем, размещения вредоносного контента, проведении всевозможных атак и т.д.
- **Неудачная попытка использования прав пользователя (unsuccessful-user)**
  События данной категории обнаруживают попытки повышения привилегий, которые завершились неудачей

По правилам

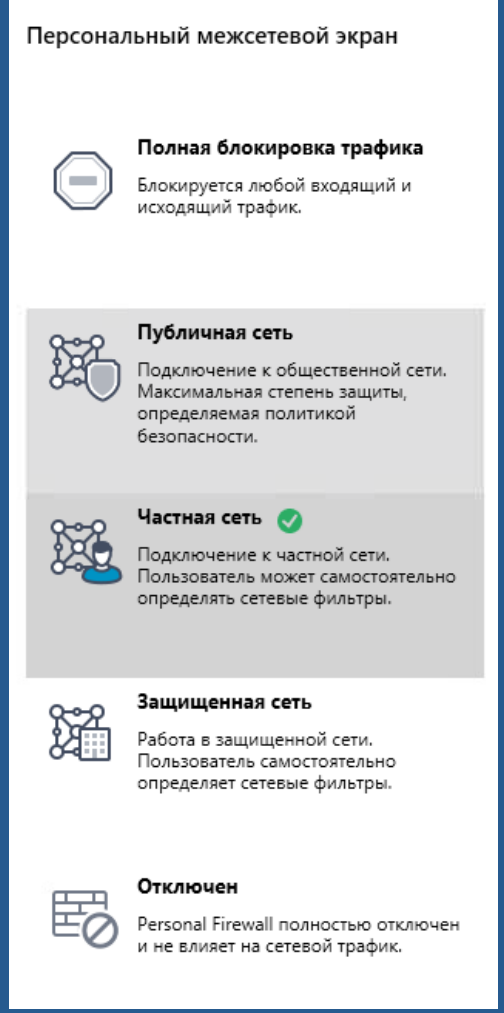


Редактор правил - Обнаружение и предотвращение вторжений - Правила режима работы 'Усиленный'

Найти

Редактировать

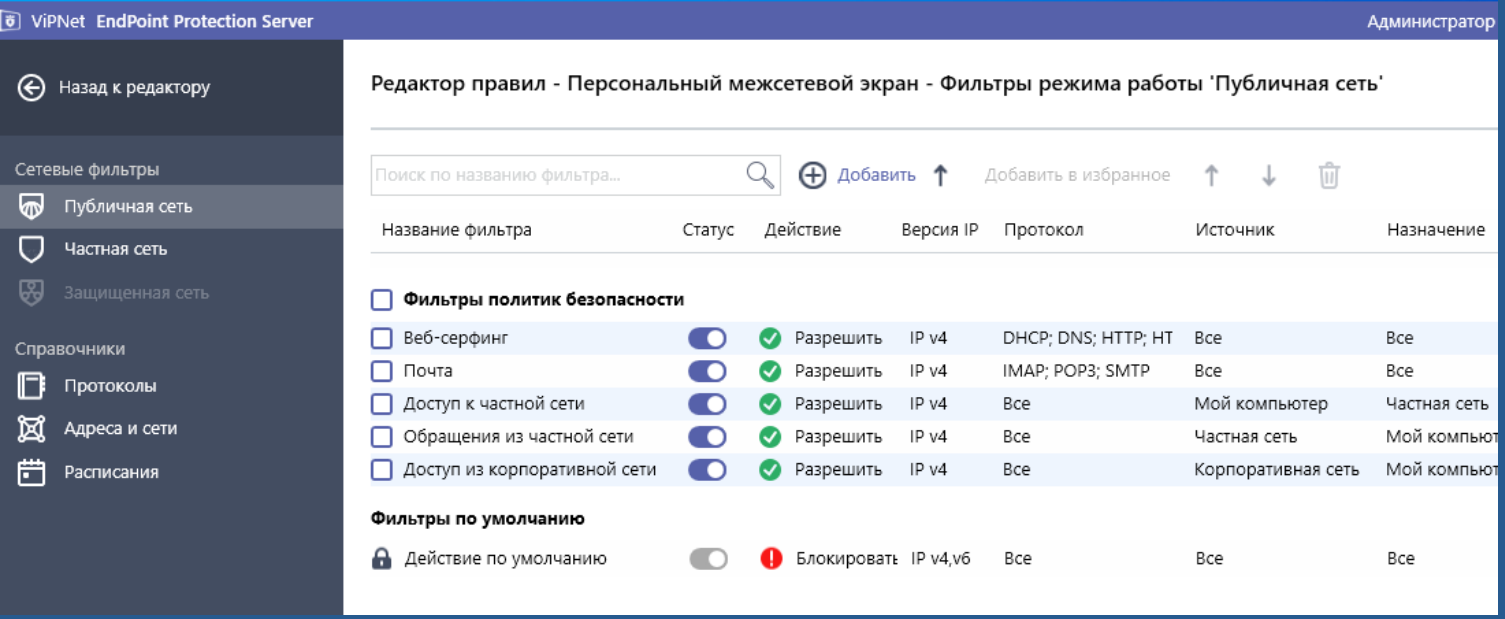
Правило	Действие	Протокол	Адрес источника	Порт источника	Направление	Адрес назначения	Порт назначени
3055560 - AM TROJAN Suspicic	Блокировать	TCP	$HOME_NET	Все	→	$EXTERNAL_NET	1433
3063112 - AM SCAN RDP brute	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	Все
3053736 - AM SCAN SSH brute	Блокировать	TCP	$HOME_NET	Все	→	$EXTERNAL_NET	22
3023530 - AM SCAN Possible C	Блокировать	TCP	$HOME_NET	4786	→	$EXTERNAL_NET	Все
3023529 - AM SCAN Possible C	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	4786
3006441 - AM SCAN Bruteforce	Блокировать	TCP	$HOME_NET	23	→	$EXTERNAL_NET	Все
3004674 - AM SCAN Bruteforce	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	3306
3004672 - AM SCAN Hydra Bru	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	25
2101918 - GPL SCAN SolarWinc	Блокировать	ICMP	$EXTERNAL_NET	Все	→	$HOME_NET	Все
2101638 - GPL SCAN SSH Versi	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	22
2100617 - GPL SCAN ssh-resea	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	22
2029577 - ET SCAN Polaris Botr	Блокировать	TCP	$EXTERNAL_NET	$HTTP_PORTS	→	$HOME_NET	Все
2029473 - ET SCAN ELF/Mirai U	Блокировать	TCP	$EXTERNAL_NET	$HTTP_PORTS	→	$HOME_NET	Все
2029318 - ET SCAN Tomato Ro	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	$HTTP_PORTS
2029317 - ET SCAN Tomato Ro	Блокировать	TCP	$EXTERNAL_NET	Все	→	$HOME_NET	$HTTP_PORTS
2100484 - GPL SCAN PING Snif	Блокировать	ICMP	$EXTERNAL_NET	Все	→	$HOME_NET	Все
2100483 - GPL SCAN PING Cyb	Блокировать	ICMP	$EXTERNAL_NET	Все	→	$HOME_NET	Все
2100476 - GPL SCAN webtrend	Блокировать	ICMP	$EXTERNAL_NET	Все	→	$HOME_NET	Все
2100474 - GPL SCAN superscar	Блокировать	ICMP	$EXTERNAL_NET	Все	→	$HOME_NET	Все
2100465 - GPL SCAN ISS Pinge	Блокировать	ICMP	$EXTERNAL_NET	Все	→	$HOME_NET	Все



Межсетевой экран

Несколько режимов работы с преднастроенными фильтрами от производителя

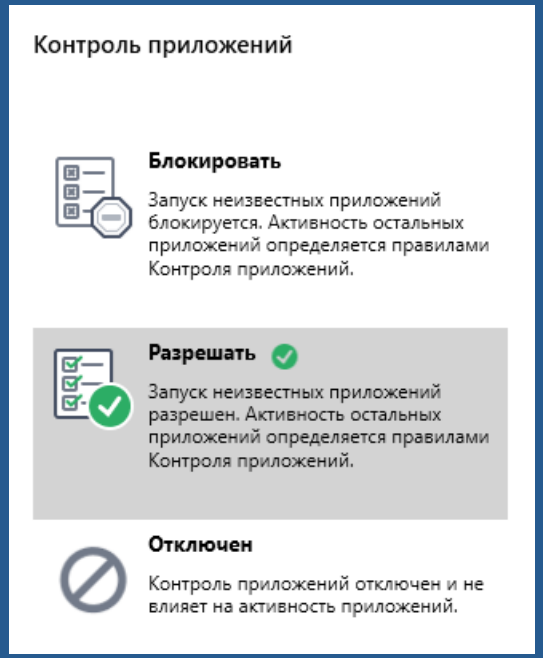
Администратор имеет возможность добавлять/изменять/удалять фильтры в режимах работы «Частная» и «Публичная сеть»



ТЕХНО 2022 infotecs Фест

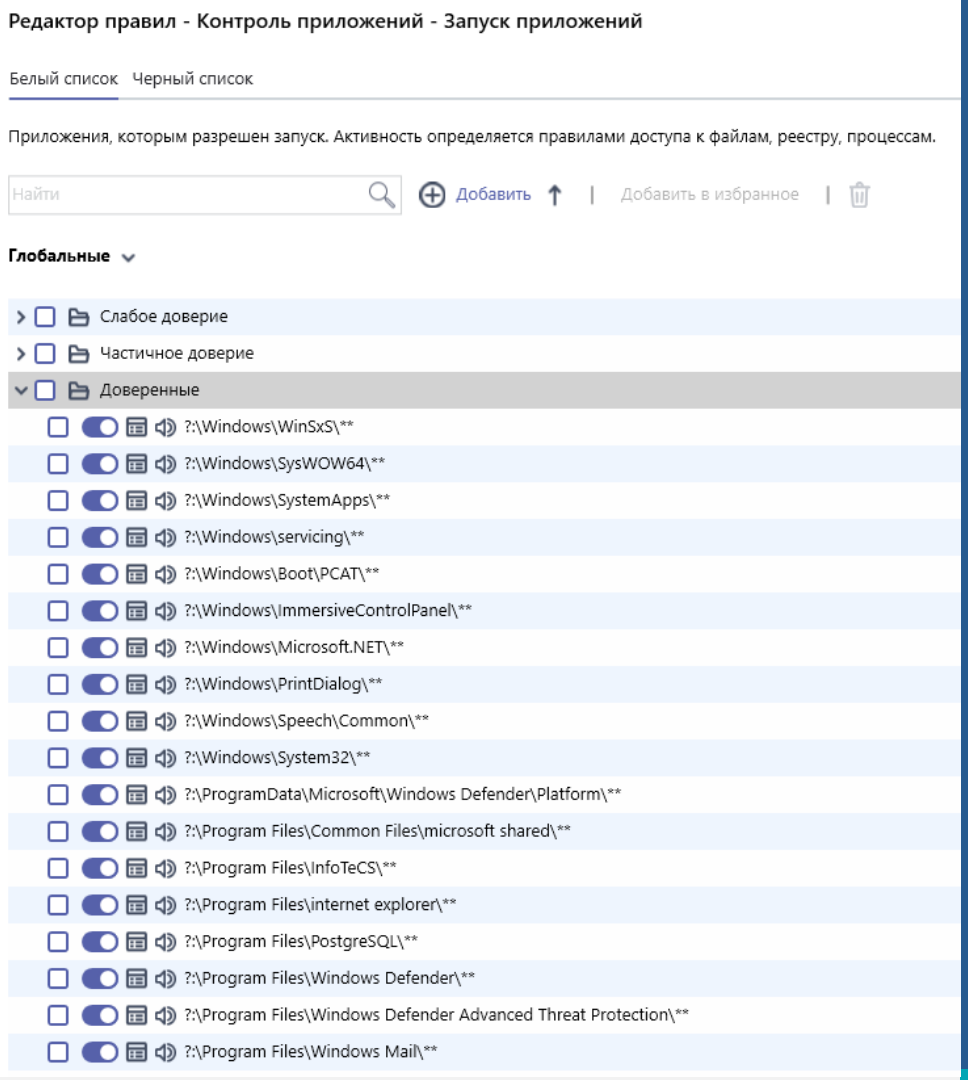
Межсетевой экран

Создание фильтров аналогично PFW, но т.к. это делается на сервере, имеется возможность рассылки на группы агентов с модулем персонального межсетевого экранирования



Контроль приложений

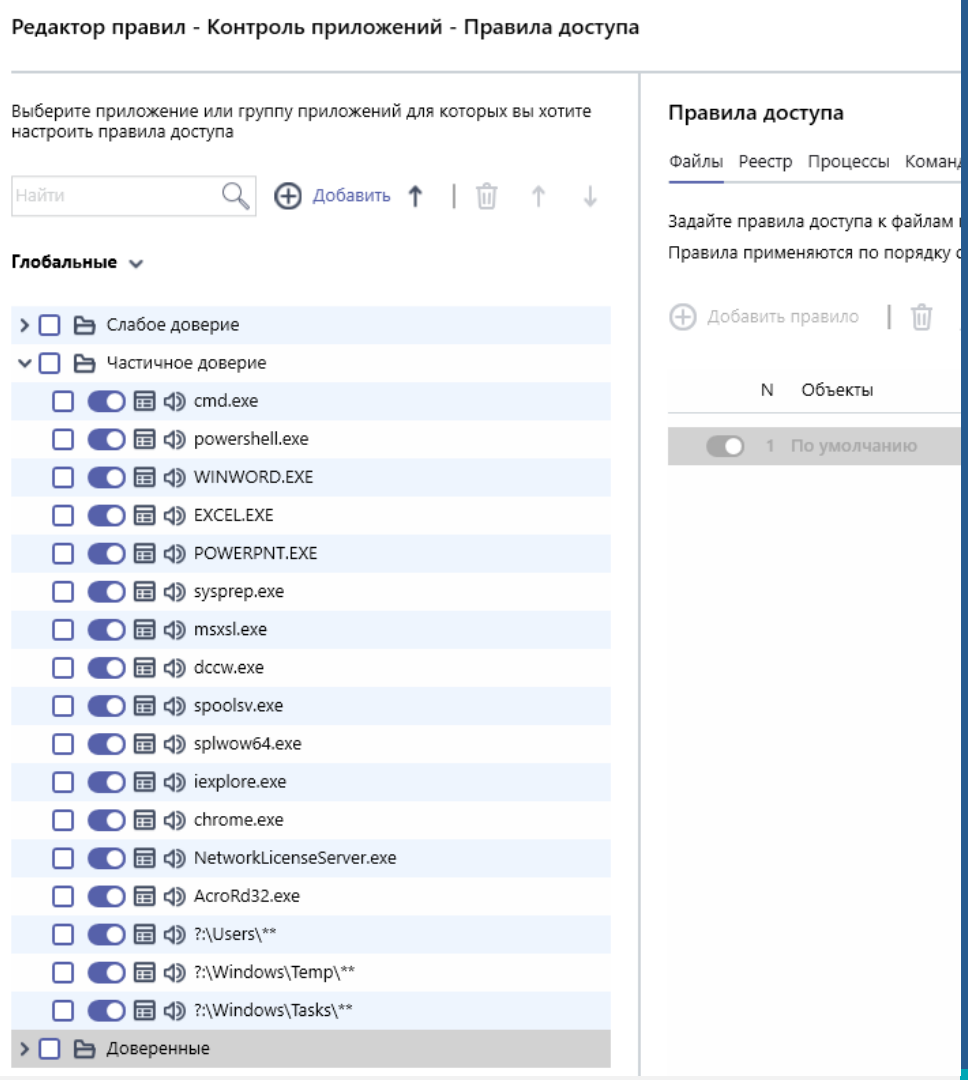
Возможность выбора режима работы Черного/Белого списка с полной блокировкой или уведомлением о запуске



ТЕХНОфест 2022 infotecs

Контроль приложений

Возможность формирования
Белых и Черных списков

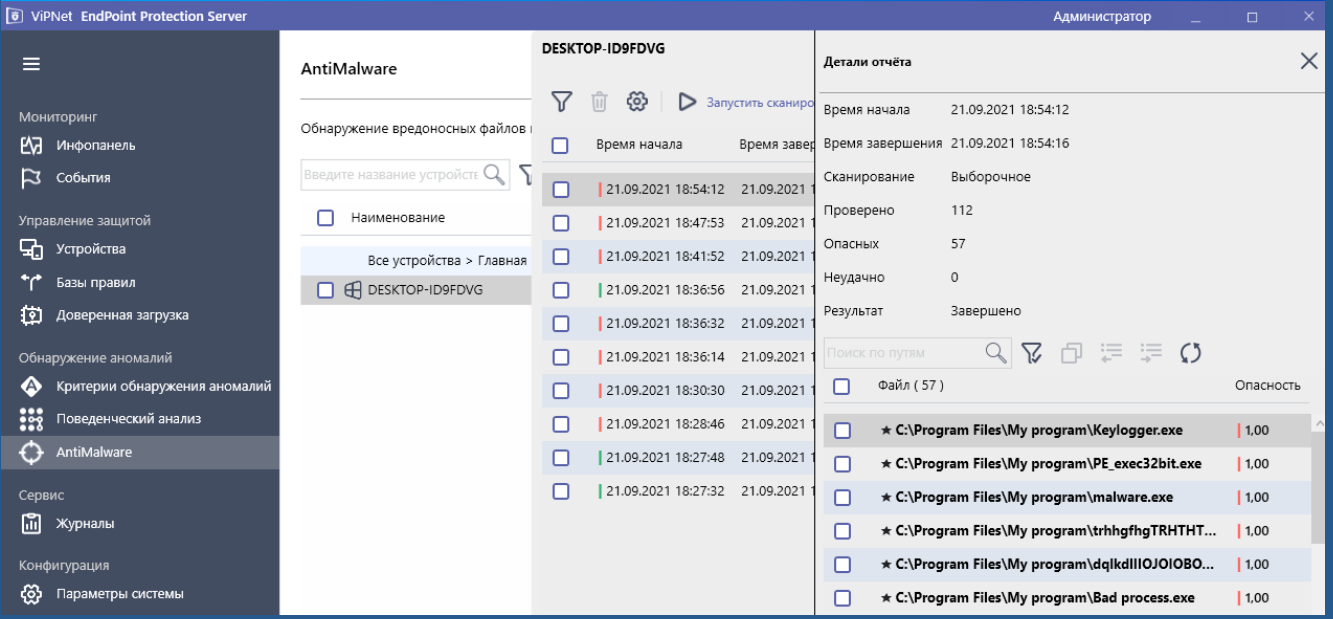


ТЕХНО infotecs 2022 ФЕСТ

Контроль приложений — правила доступа

Возможность создания правил доступа для приложений к следующим объектам:

- Файлам
- Реестру
- Процессам
- Командной строке

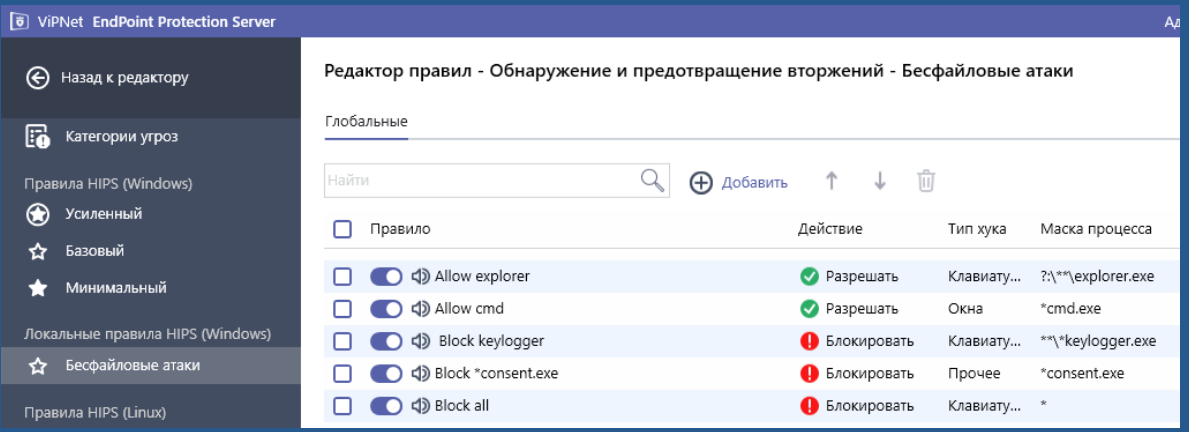


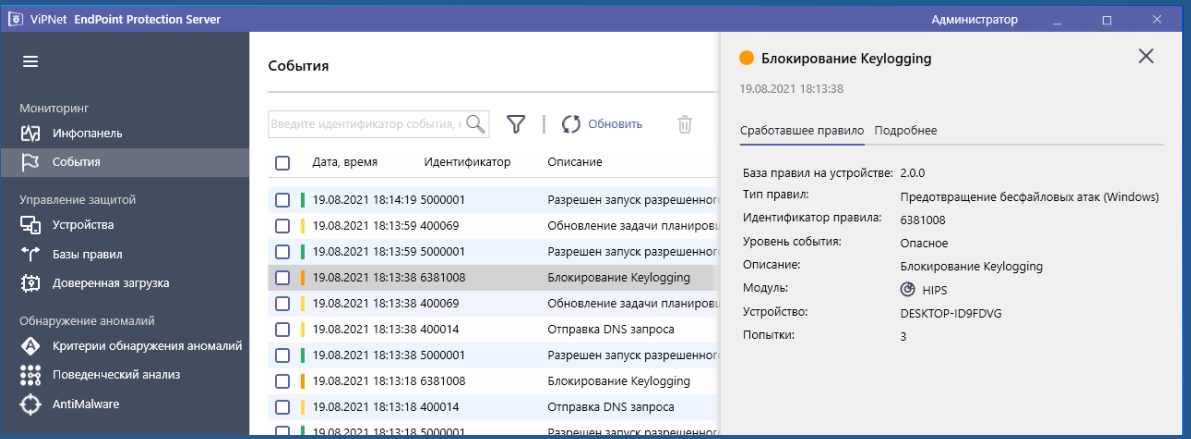
ТЕХНО infotecs 2022 ФЕСТ

Antimalware движок

Эвристический подход

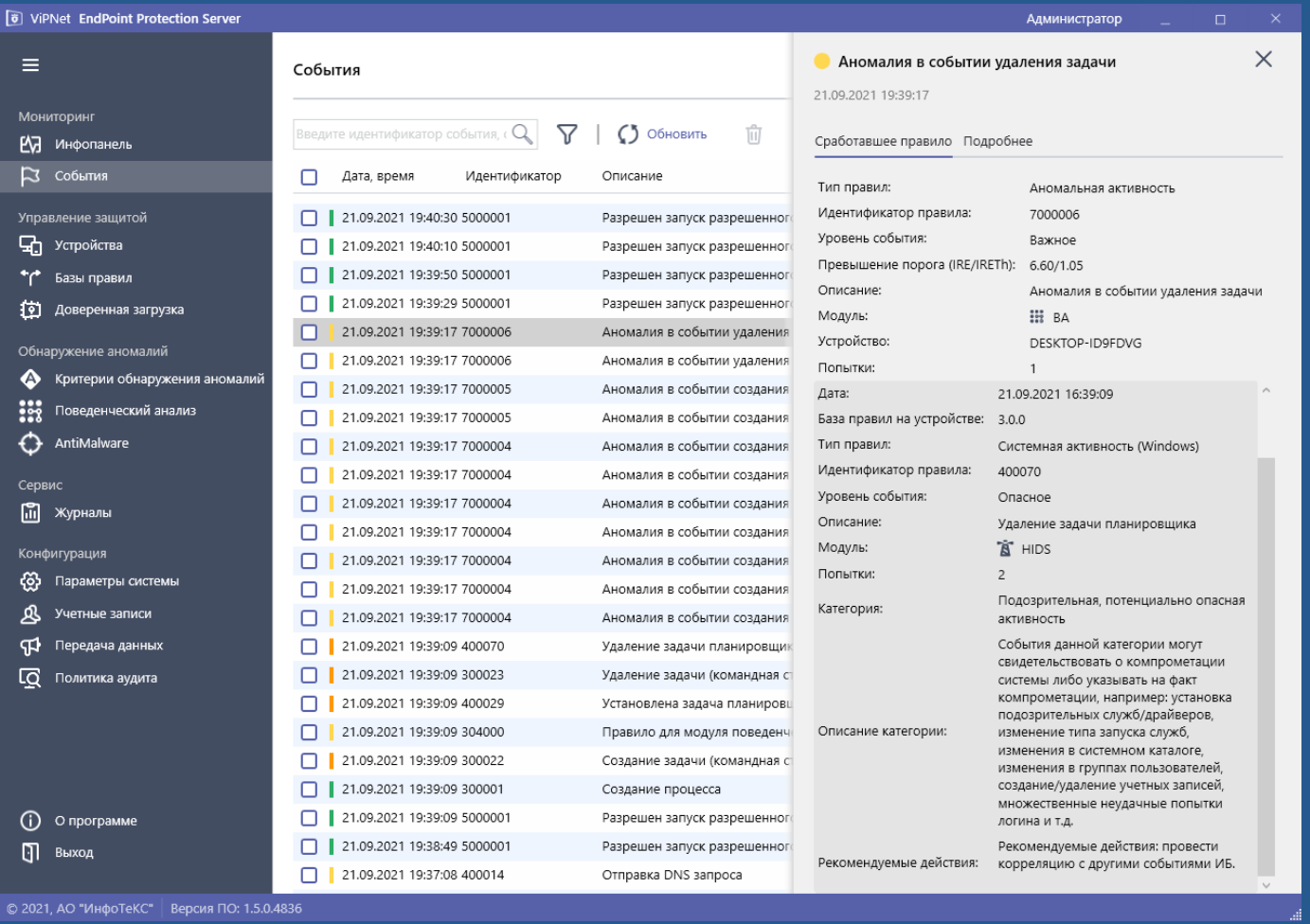
Регулярное обновление в составе БРП





Обнаружение и предотвращение бесфайловых атак

Входит в состав модуля «Обнаружения и предотвращения вторжений»



ТехноФест infotecs 2022

Выявление аномалий

Ожидание по сертификации

Продукт на сертификации по линии ФСТЭК России по требованиям к:

- Системам обнаружения вторжений уровня узла 4 класса ИТ.СОВ.У4.ПЗ
- Межсетевым экранам типа В класса 4 (ИТ.МЭ.В4.ПЗ)
- 4 классу ТДБ

Текущая концепция защиты рабочих станций

ТехноФест infotecs 2022

ViPNet SafeBoot

Доверие к платформе и обеспечение доверенной загрузки ОС

Разграничение доступа и защита данных

ViPNet SafePoint

ViPNet Client 4U

Обеспечение защищённых коммуникаций

Защита от внешних атак и угроз

ViPNet EndPoint Protection

ТЕХНО 2022 infotecs Фест

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363