ViPNet EndPoint Protection версия 1.5. Обзор новых возможностей продукта

Кадыков Иван
Руководитель направления

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

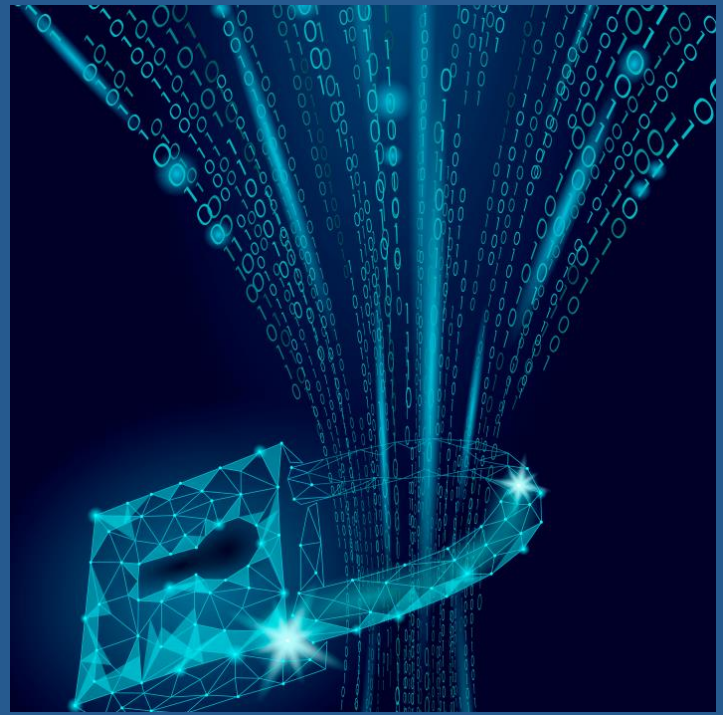
Следим за:

- 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

ViPNet EndPoint Protection версия 1.5

Новые защитные механизмы

Контроль приложений

Персональный межсетевой экран

Эвристический Anti-malware движок

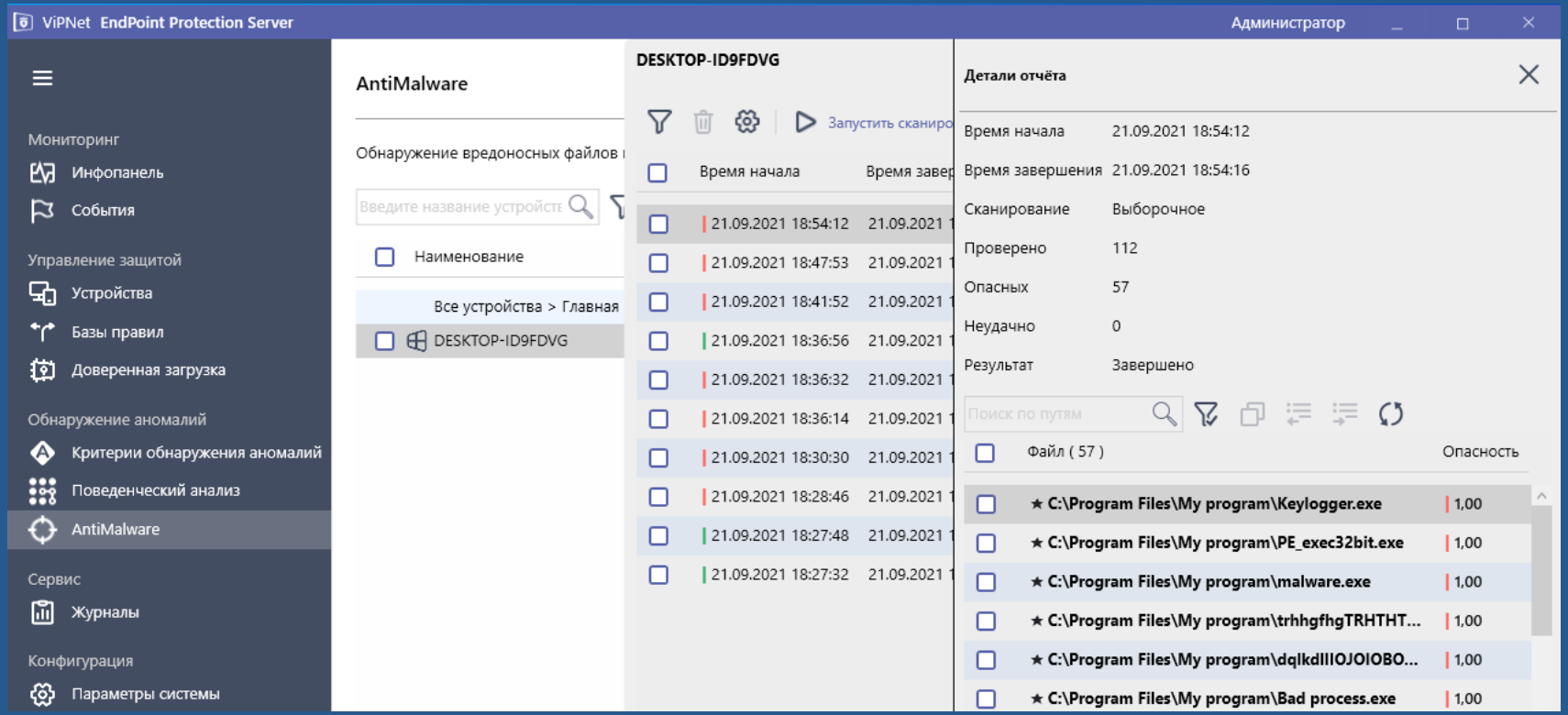
Система обнаружения и предотвращения вторжений

Модуль поведенческого анализа

Эвристический Anti-malware 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

Внешний вид Anti-malware

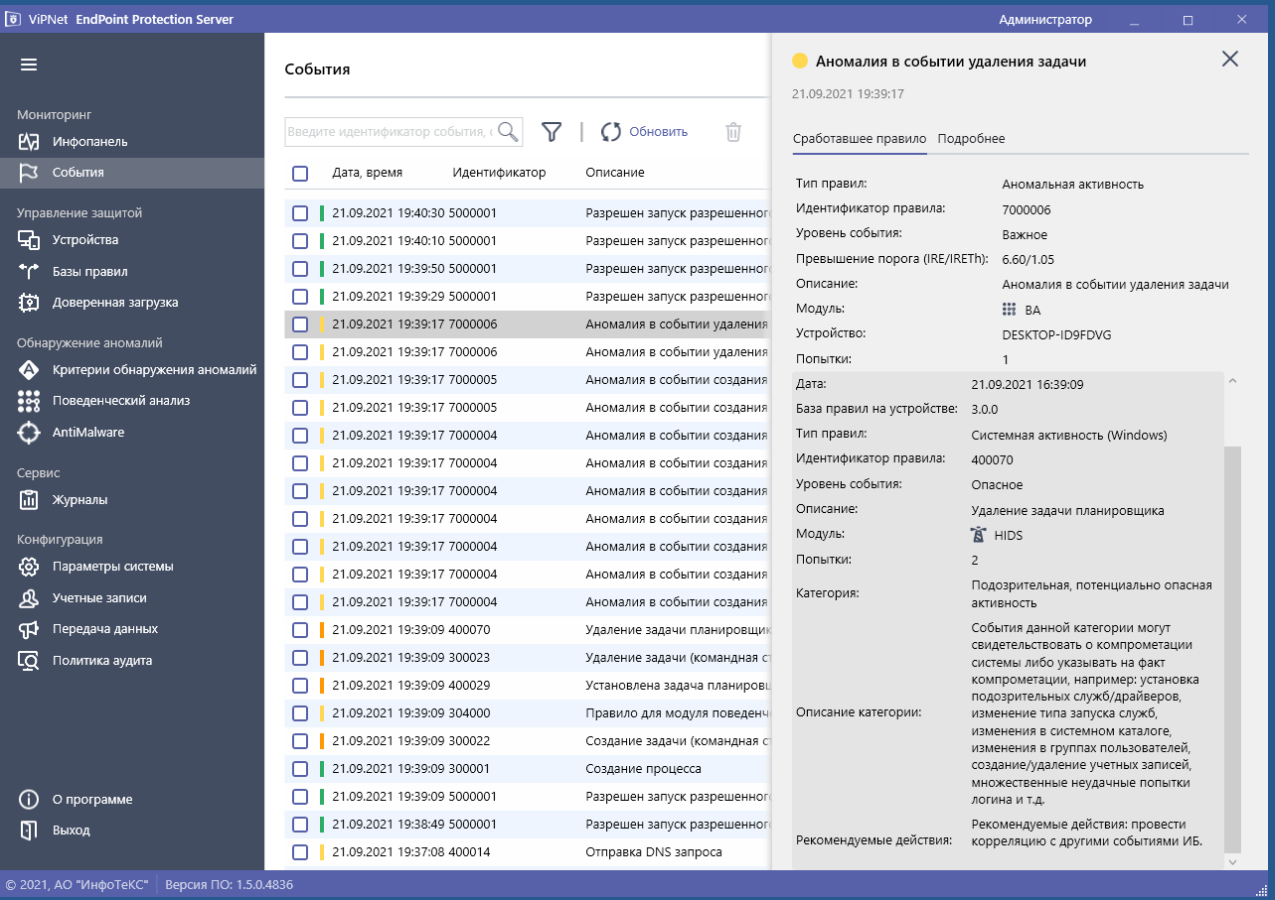


Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенную 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.



Выявление аномалий

Обнаружение и предотвращение бесфайловых атак

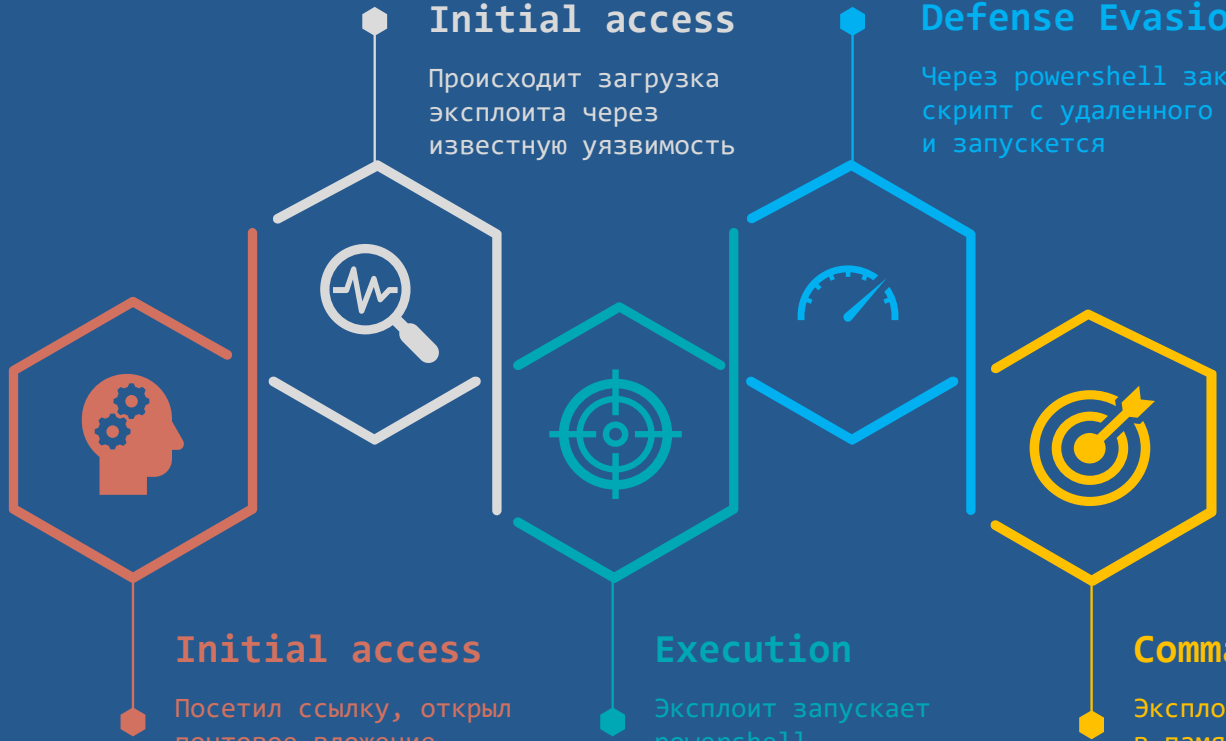
Расширение возможностей модуля обнаружения и предотвращения вторжений

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)

Как «действует» бесфайловая атака

infotecs



Initial access

Происходит загрузка эксплоита через известную уязвимость

Defense Evasion

Через powershell закачивается скрипт с удаленного сервера и запускется

Initial access

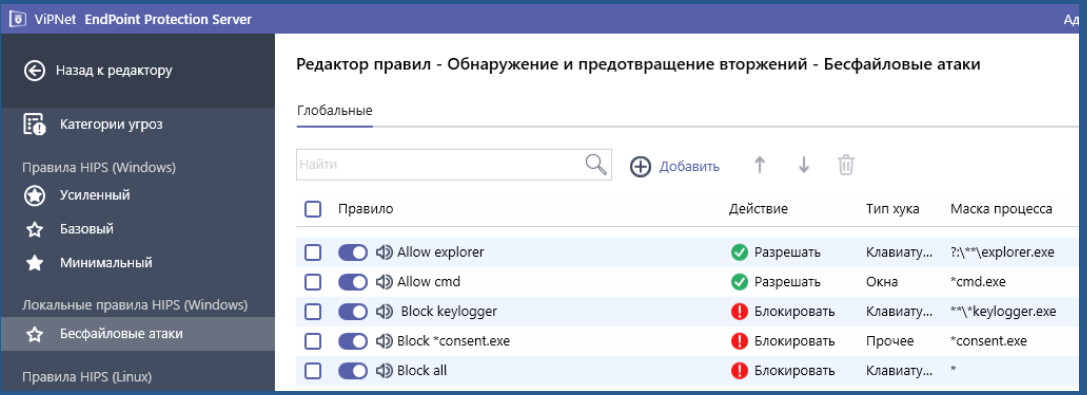
Посетил ссылку, открыл почтовое вложение

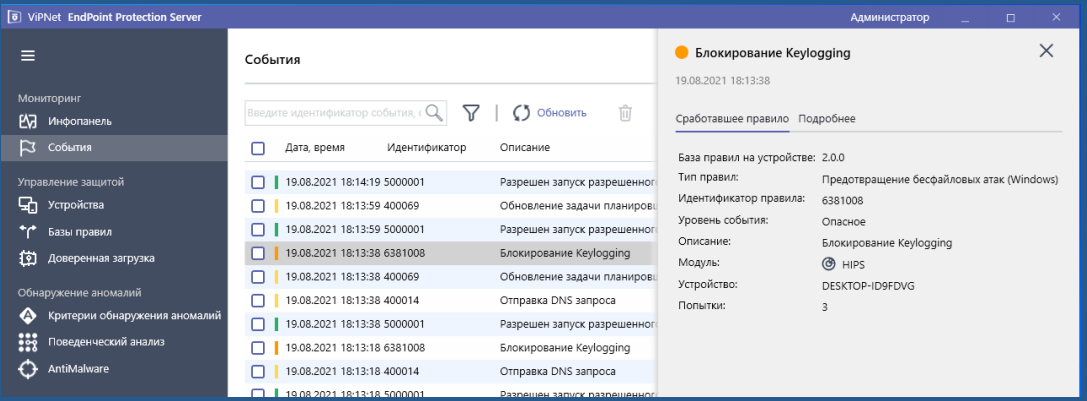
Execution

Эксплоит запускает powershell в оперативной памяти

Command and control

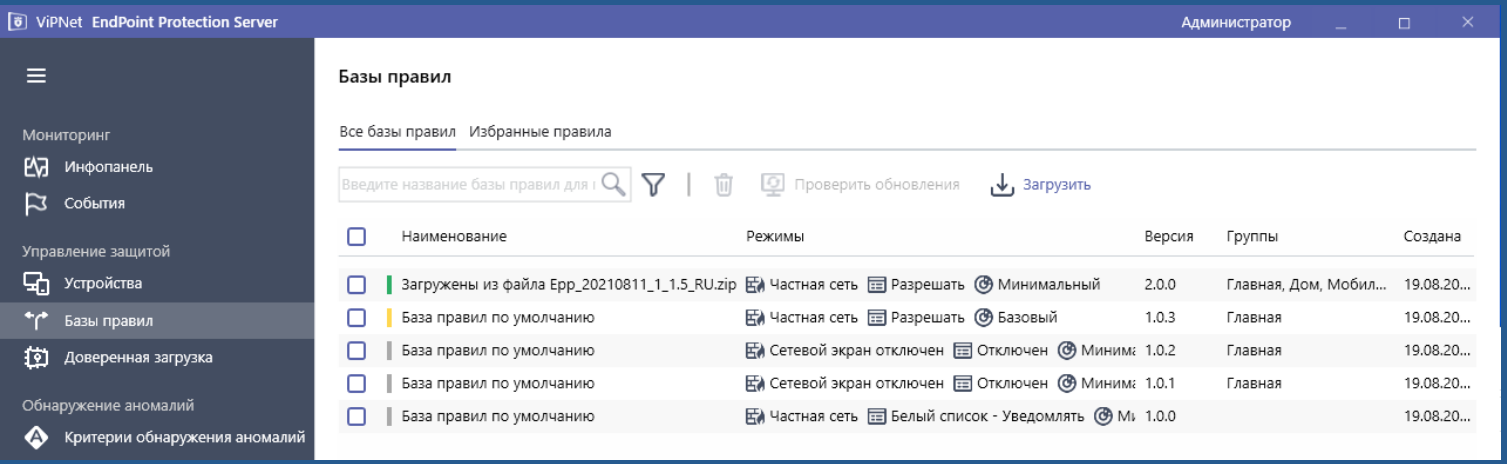
Эксплоит располагается в памяти для «плохих дел»





Обнаружение и предотвращение бесфайловых атак

Входит в состав модуля «Обнаружения и предотвращения вторжений»



Работаем по правилам!

БРП состоит из:

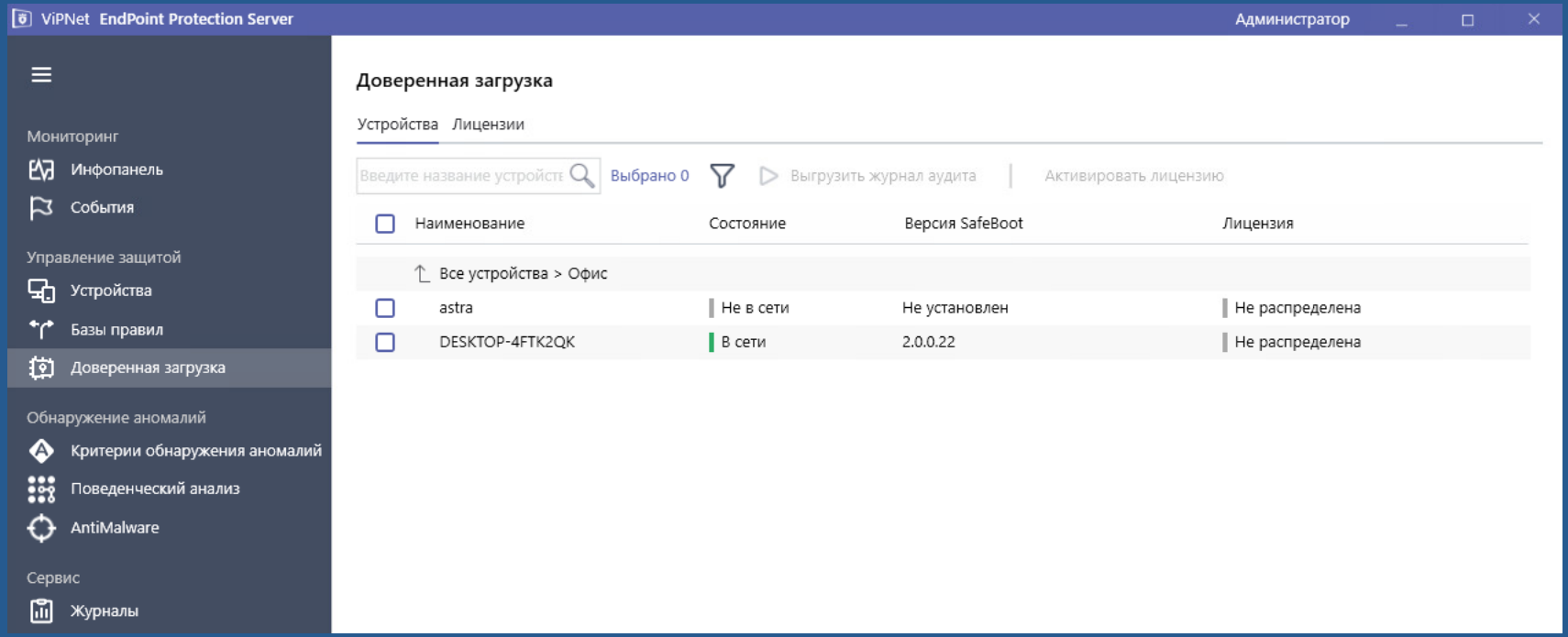
- Правил системы обнаружения и предотвращения вторжений
- Фильтров Межсетевого экрана
- Списков ПО для Черного и Белого списка
- Эвристического движка Anti-malware
- Движка обнаружения аномального поведения системных утилит

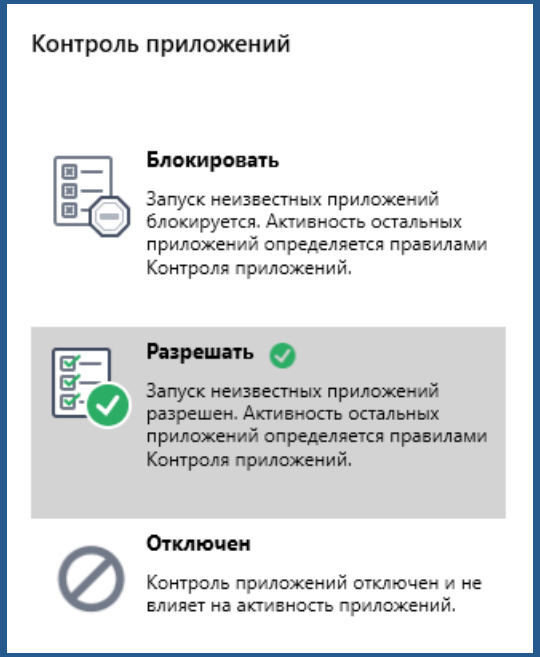
Поддержка Linux

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

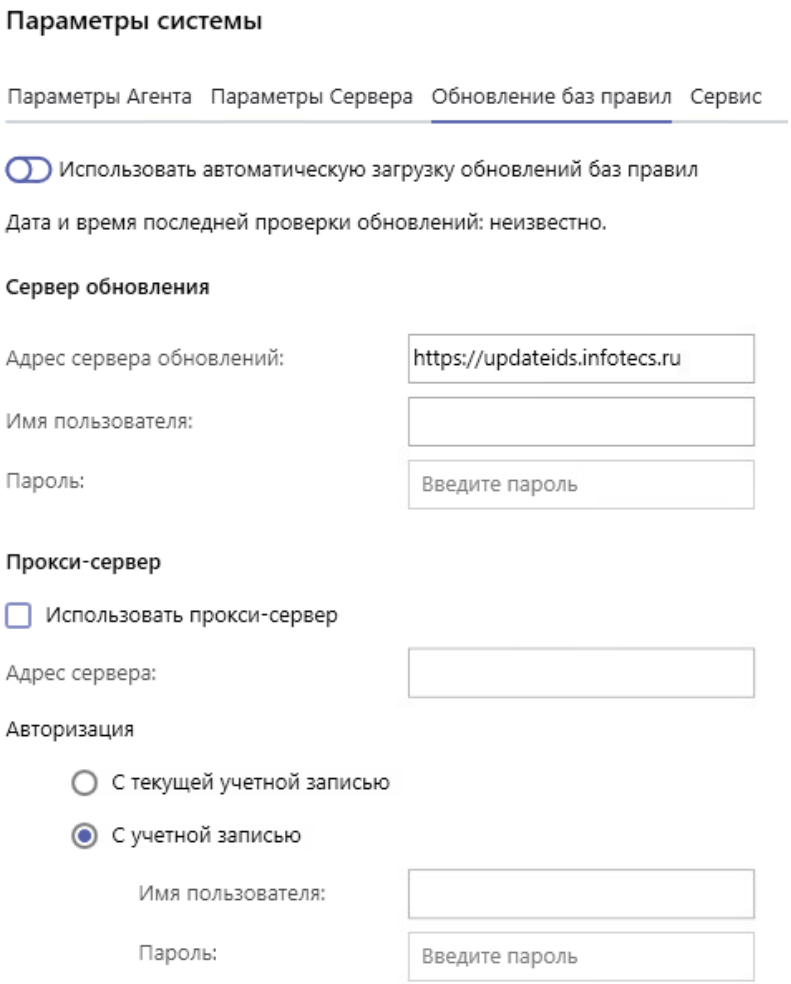
Управление ViPNet SafeBoot





Изменение в режимах работы Контроля приложений

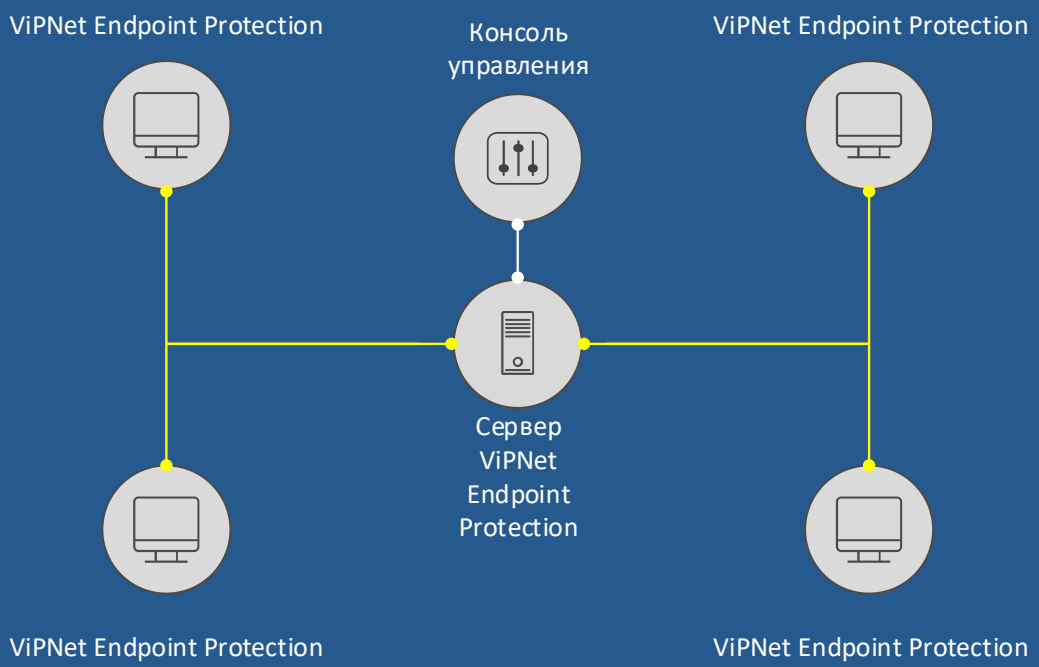
Теперь три варианта работы



Автоматическая загрузка БРП и избранные правила

Появилась возможность автоматической загрузки БРП с сохранением ранее созданных правил.

Общая информация о ViPNet EndPoint Protection



Архитектура ViPNet EndPoint Protection

- Клиент
- Сервер
- Консоль управления

Поддерживаемые ОС

Сервер и агент

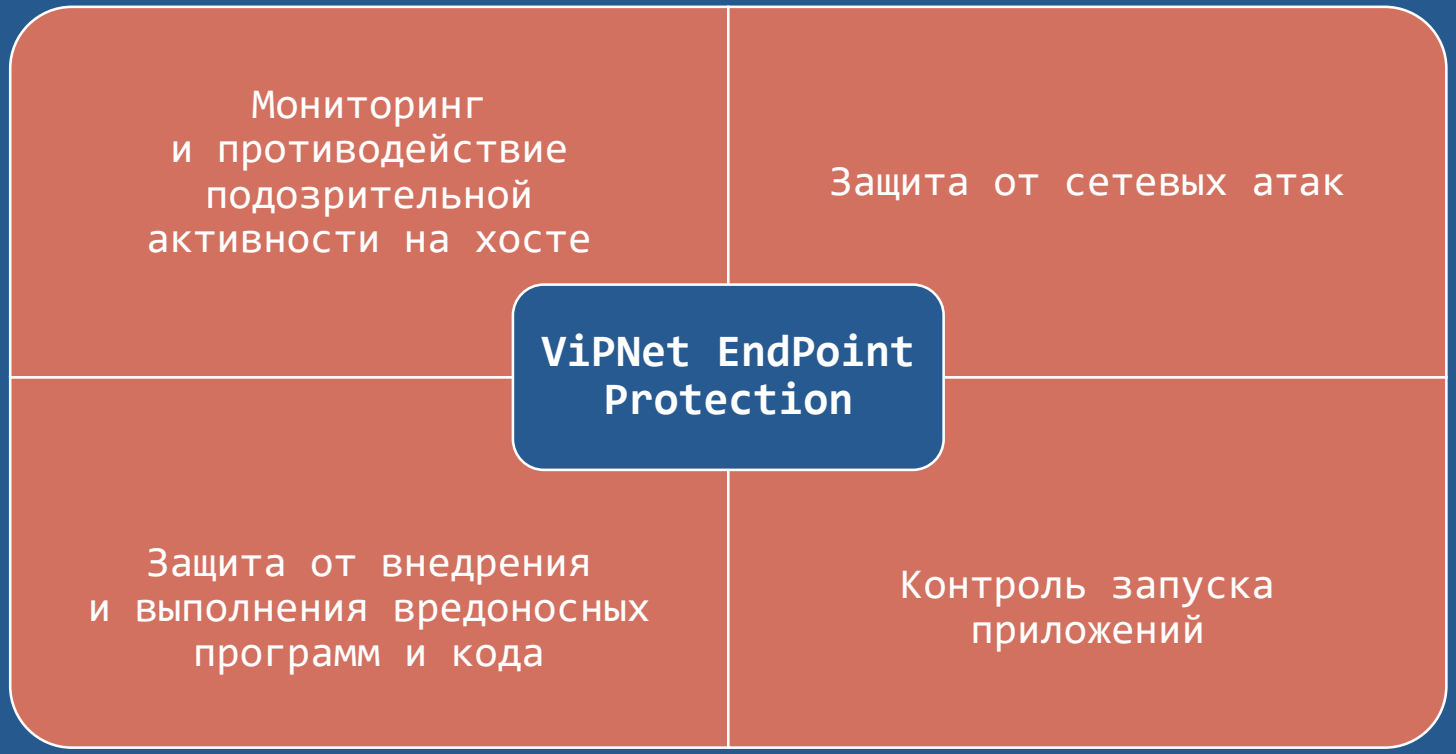
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

Только Агент

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

Полная защита

Решаемые задачи



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