Универсальность и самодостаточность продуктовой линейки ViPNet Endpoint Security

Кадыков Иван
Руководитель продуктового направления

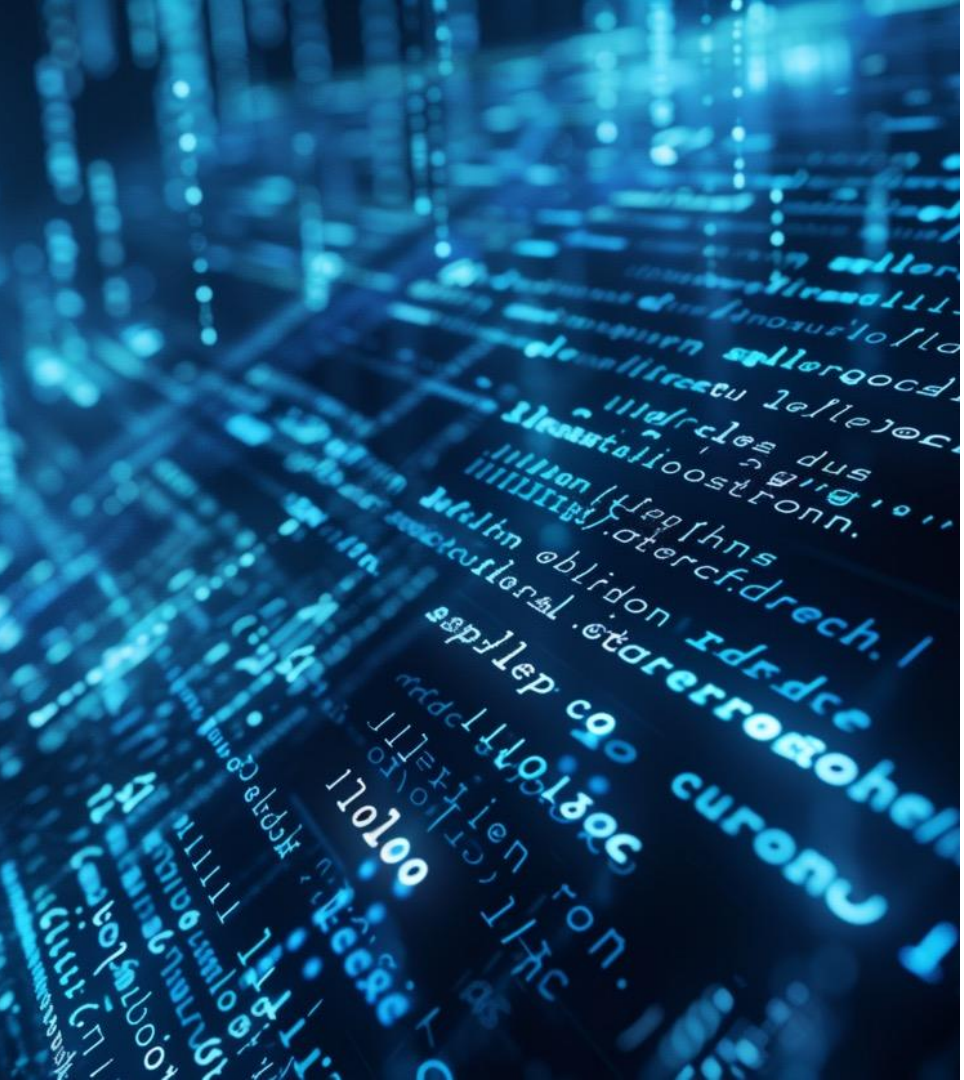
Чтобы защищаться, надо понимать от чего!

Растущее количество атак и не доверенных аппаратных компонент

Пользователь – внутренний нарушитель, низкий уровень осведомленности

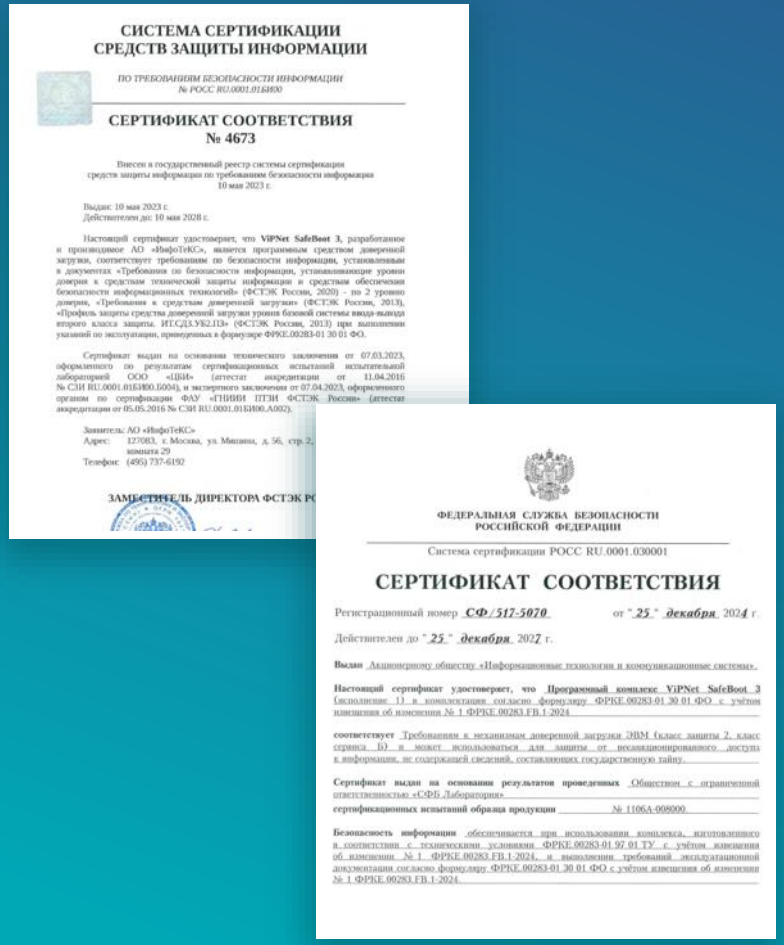
Удаленная работа, проведение приватных разговоров

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



ViPNet SafeBoot 3

Новое поколение высокотехнологичного программного модуля доверенной загрузки (ПМДЗ). Предназначен для создания точки доверия к платформе и ее компонентам, а также к загружаемой операционной системе. Ключевыми задачами продукта являются разграничение доступа к платформе, защита UEFI BIOS, контроль неизменности и защита компонентов ПК, а также организация доверенной загрузки штатной операционной системы



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4673

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
10 мая 2023 г.

Выдан: 10 мая 2023 г.
Действителен до: 10 мая 2028 г.

Настоящий сертификат удостоверяет, что **ViPNet SafeBoot 3**, разработанное и производимое 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.00283-01 30 01 ФО.

Сертификат выдан на основании технического заключения от 07.03.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 07.04.2023, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

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

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РО

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/517-5070* от "*25*" *декабря* 2024 г.

Действителен до "*25*" *декабря* 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс ViPNet SafeBoot 3 (исполнение 1) в комплектации согласно формуляру ФРКЕ.00283-01 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00283.FB.1-2024

соответствует Требованиям к механизмам доверенной загрузки ЭВМ 6класс защиты 2, класс сервиса Б) и может использоваться для защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»
сертификационных испытаний образца продукции № 1106А-008000.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.00283-01 97 01 ТУ с учётом извещения об изменении № 1 ФРКЕ.00283.FB.1-2024, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.00283-01 30 01 ФО с учётом извещения об изменении № 1 ФРКЕ.00283.FB.1-2024.

ТЕХНО infotecs ФЕСТ

ViPNet SafeBoot 3

Первые! кто получил
(второй раз подряд)
два сертификата на одну версию!

- ФСТЭК России № 4673
- ФСБ России № СФ/517-5070

Расширяя границы доверенной загрузки

ТехноФест infotecs

ViPNet SafeBoot уже давно не просто модуль доверенной загрузки, а ключевой элемент доверия к платформе

Доверенная загрузка это:

Идентификация и Аутентификация пользователей

Контроль целостность программной среды и аппаратной

Передача управления доверенному загрузчику ОС

Доверие и защита платформы

Защита UEFI BIOS

- Защита BIOS от перезаписи, чтения и от изменений EFI-переменных
- Защита после S3 – защита при выходе из спящего режима
- Блокировка обновлений UEFI BIOS
- Фильтрация и контроль программных SMI

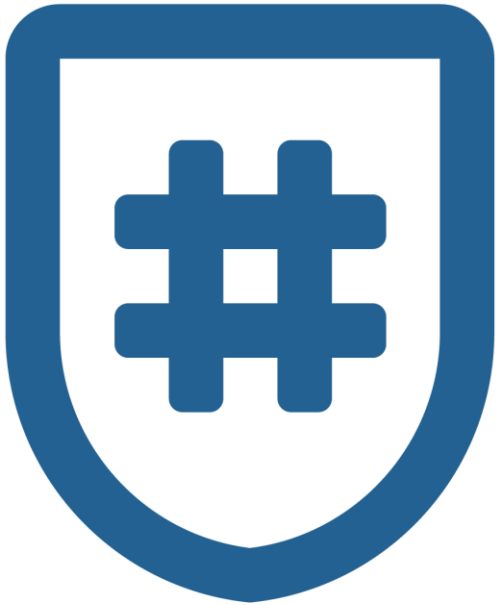
Защита от malware

- Блокировка ACPI WPBT, защита системных таблиц
- Защита дисков от записи
- Блокировка UEFI Option Rom

Эмуляция NVRAM

Что нового и интересного появилось в ViPNet SafeBoot 3?

- Поддержка syslog – отправка CEF сообщений
- Поддержка ALD PRO (Astra Linux)
- Поддержка работы на бездисковых станциях
- Профили загрузки ОС
- Поддержка LUKS
- Защита системных таблиц UEFI
- Поддержка токена Guardant ID версии 2
- Поддержка JaCarta-2 SE и JaCarta PRO
- Расписание доступа пользователей
- Регистрация всех подключенных устройств аутентификации



ViPNet SafePoint
Продолжение развития, наращиваем функциональность

ТЕХНО infotecs ФЕСТ

ViPNet SafePoint

ViPNet SafePoint – сертифицированный программный комплекс защиты информации от несанкционированного доступа уровня ядра операционной системы (ОС)

ViPNet SafePoint устанавливается на рабочие станции и серверы в целях обеспечения мандатного и дискреционного разграничения доступа пользователей к критически важной информации и подключаемым устройствам

Идентификация
и аутентификация
пользователей

Дискреционная модель
доступа

Замкнутая
программная среда

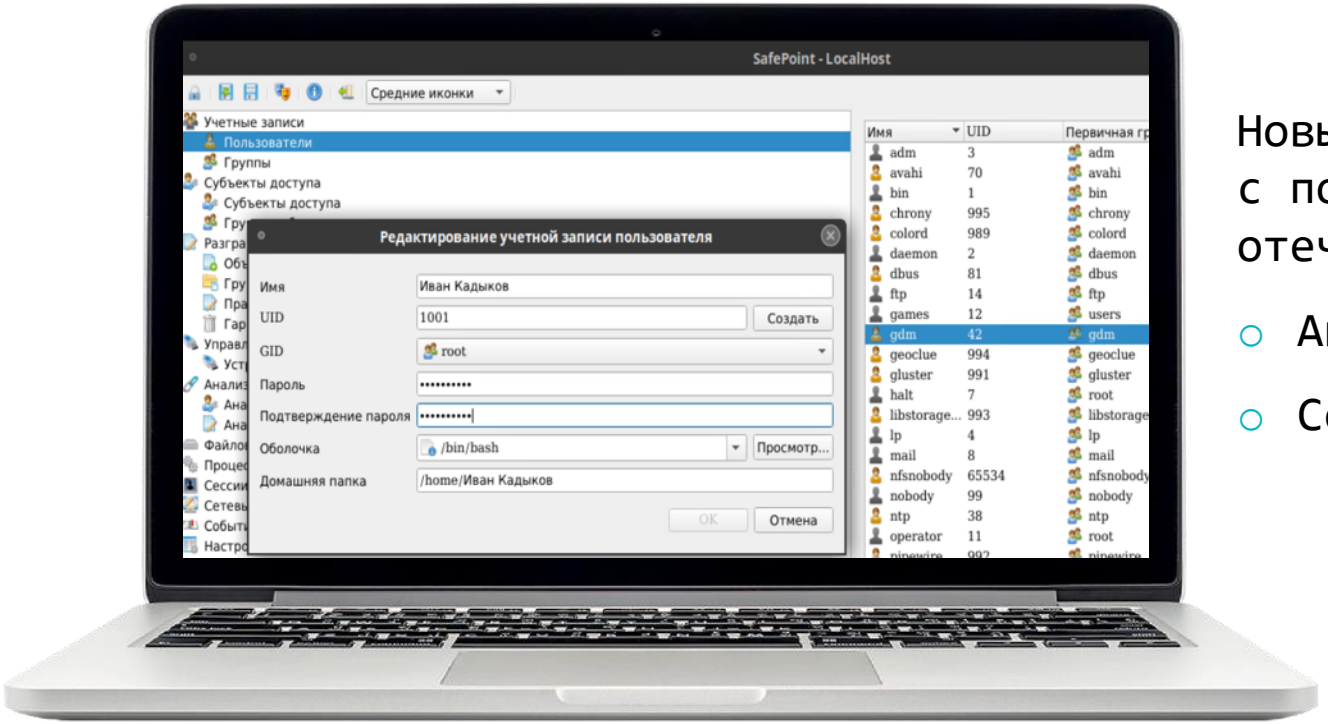
Контроль устройств

Контроль
целостности файлов

Дополнительные защитные механизмы

- 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

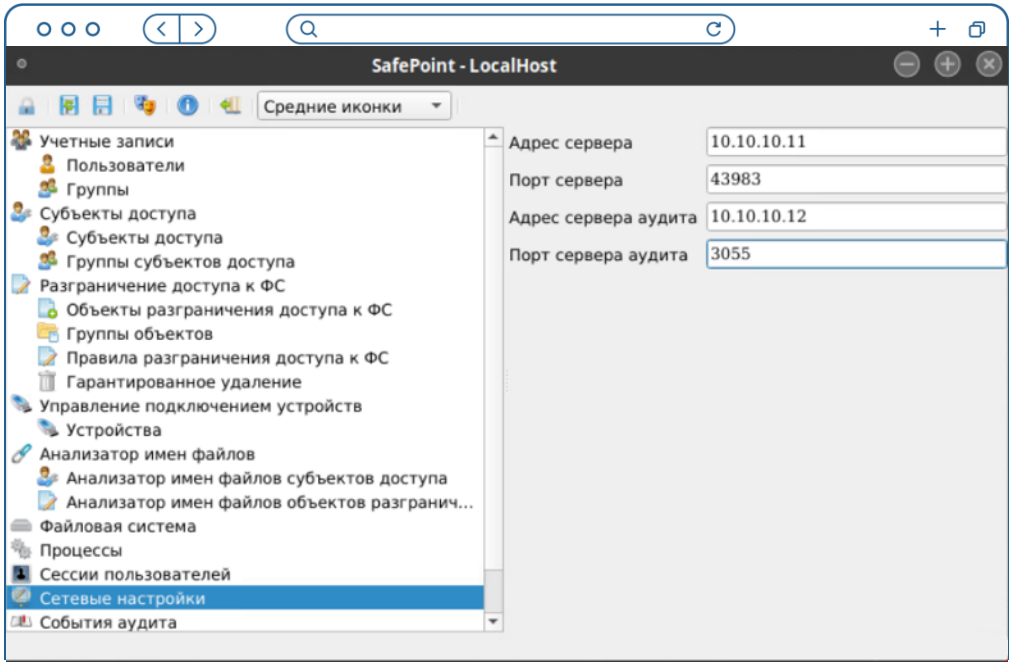
Что нового было в 2024 году



Новый Linux агент с поддержкой отечественных ОС Linux

- Автономная версия
- Сетевая версия

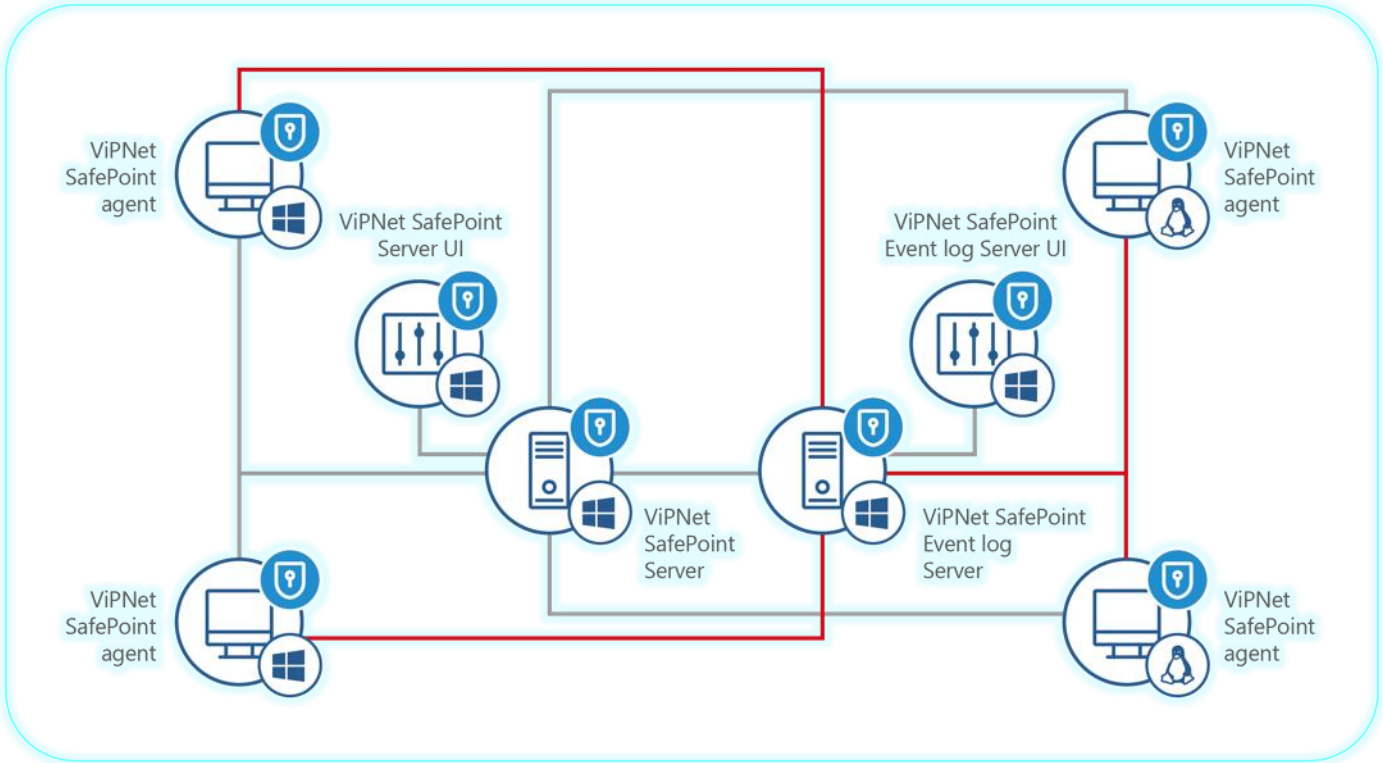
Легко внедряется в имеющуюся инфраструктуру

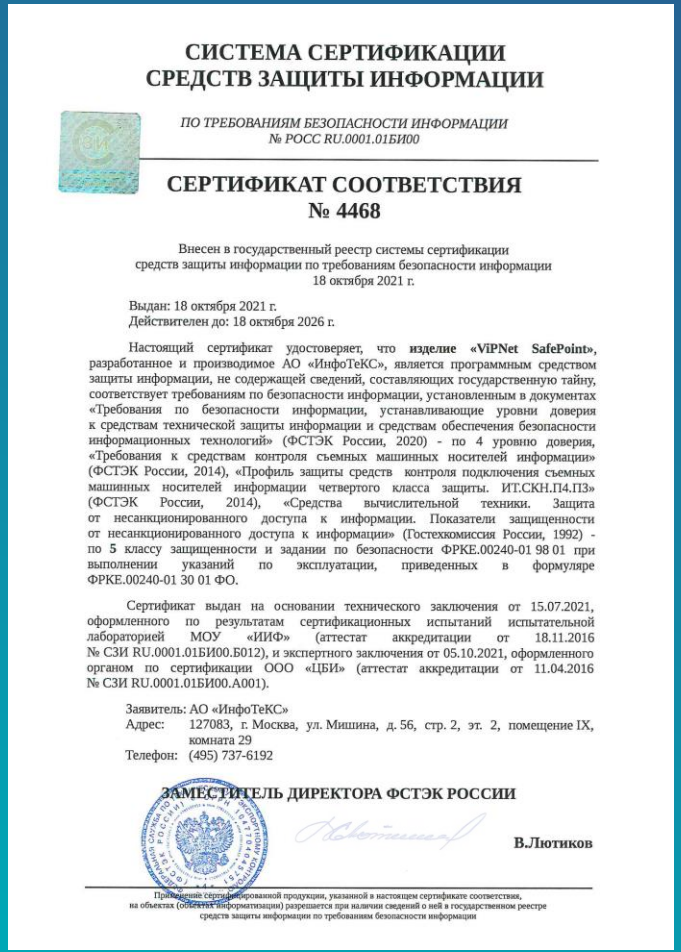


Подключение к существующему серверу безопасности и серверу аудита не займет много времени

Можно задать параметры при установке или после установки «вручную»

Архитектура





СИСТЕМА СЕРТИФИКАЦИИ
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

Сертифицировано

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

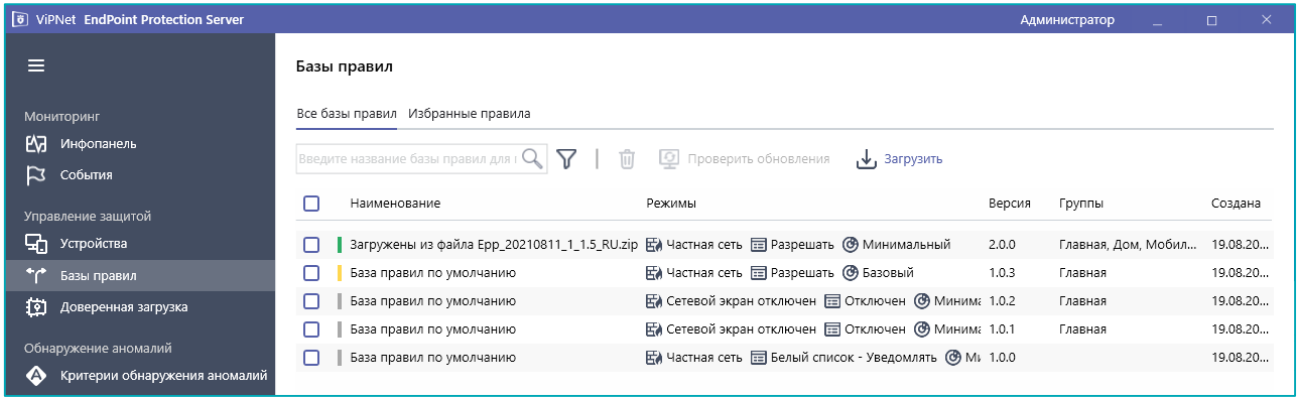
ViPNet EndPoint Protection
Новые версии!
Новая функциональность!

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

Работаем по правилам!



ViPNet EndPoint Protection работает по 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

Еще больше защитных механизмов

SSL – инспекция – возможность расшифровывания всего трафика, проходящего через модули ViPNet EndPoint Protection

SafeBrowsing – безопасный серфинг в интернете (веб-фильтрация)

Интеграционные функции

- Интеграция с ViPNet Client 4U/5

  Добавление/Редактирование/Удаление фильтров защищенной сети из локальной консоли ViPNet EndPoint Protection (агент)

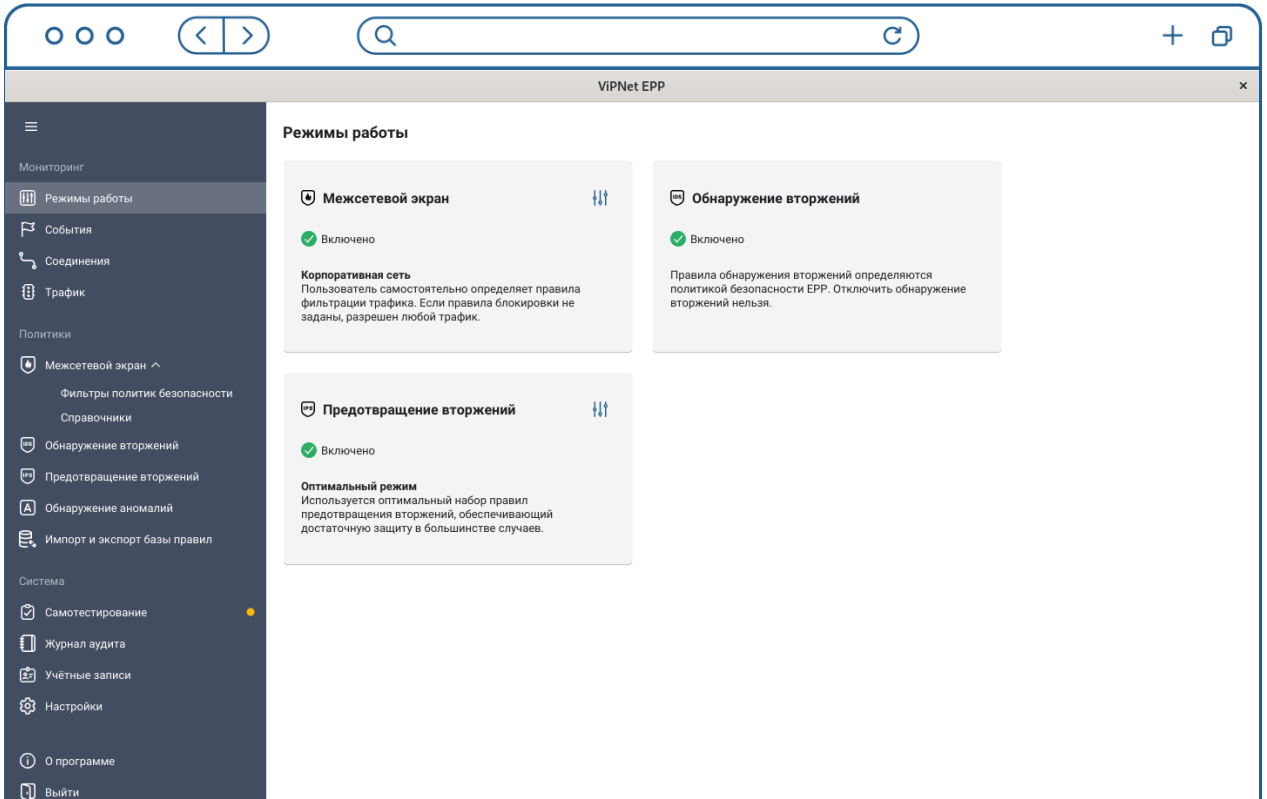
- Получение фильтров от PMM через 4U/5

ZTNA

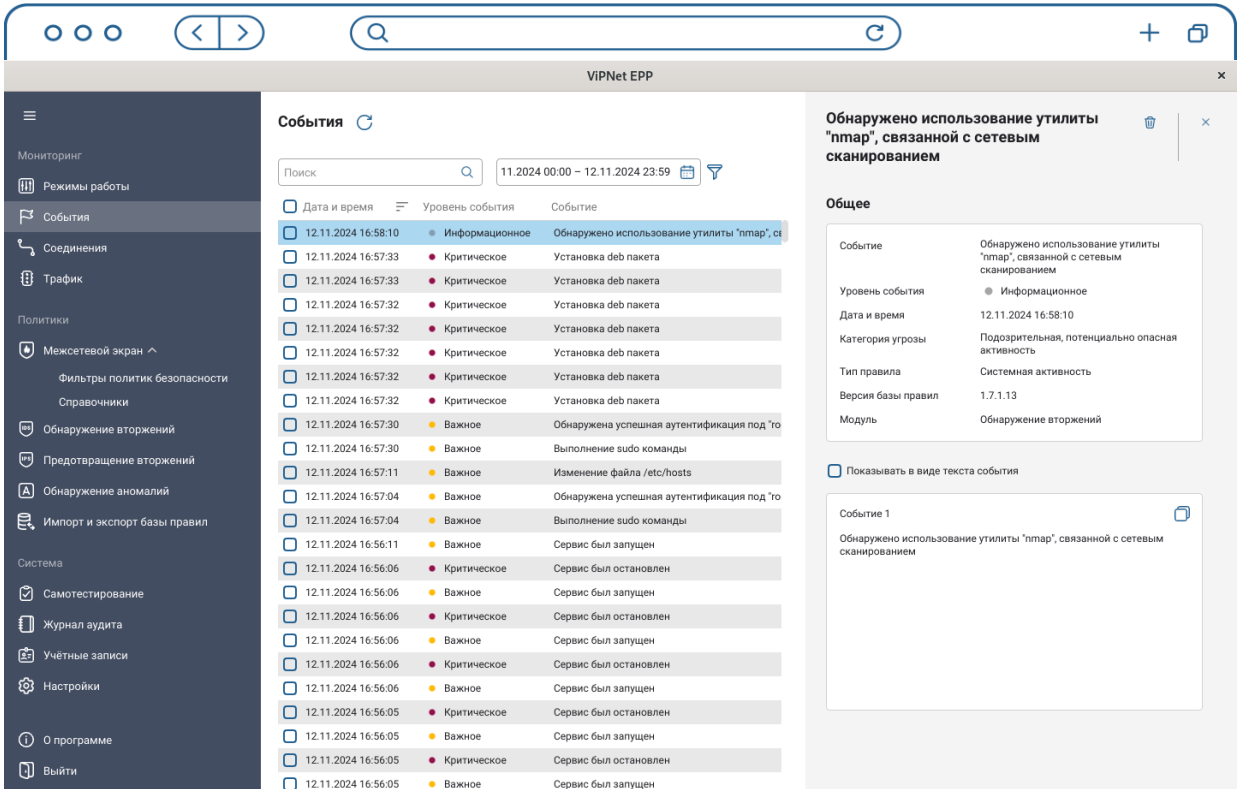
Добавление набора функций из стека технологий ZTNA и интеграция с ViPNet Client 4U/5:

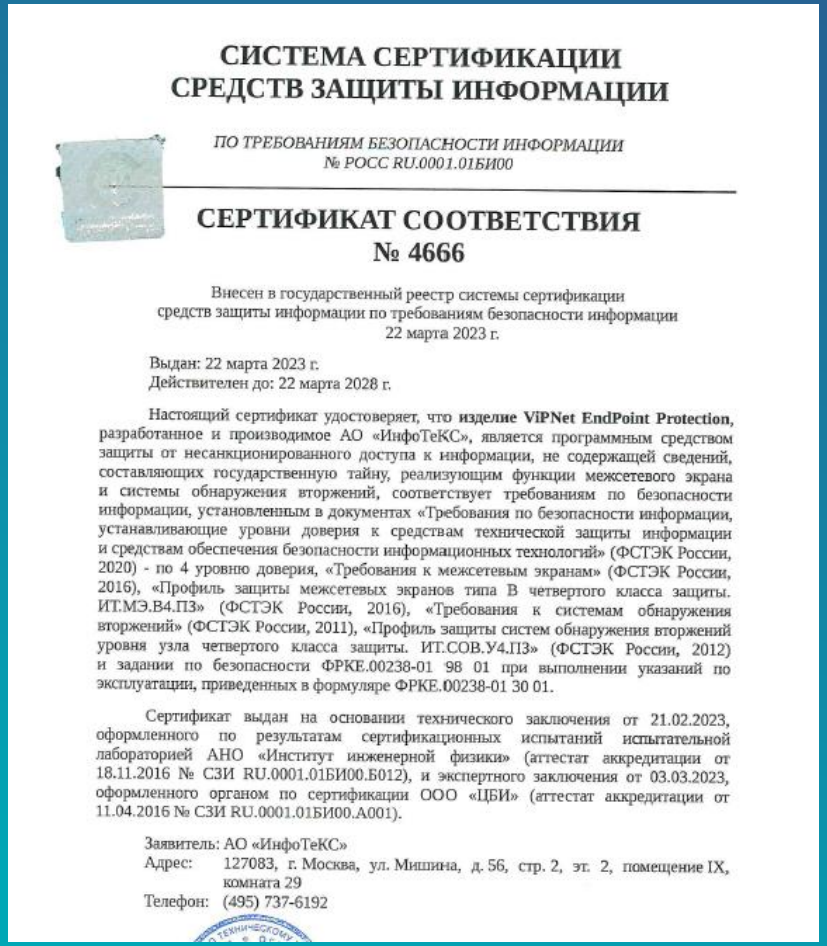
- Проверка соответствия хоста на наличие требуемого ПО, обновлений ПО, запущенных процессов, обновление антивирусных баз и т.д.
- Блокировка защищенной сети на устройстве при несоответствии устройства политикам ZTNA, информирование пользователя об этом

Новый агент под linux



Агент EPP под Linux – Журнал событий





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

Сертифицировано

- МЭ тип В класс 4
- СОВ У4
- 4 класс ТДБ

Endpoint Security

ТЕХНО infotecs ФЕСТ

ViPNet SafeBoot

ViPNet Client

ViPNet SafePoint

ViPNet EndPoint Protection

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного