CryptoDetector

Руководство по установке

Версии компонентов: CryptoDetector Platform — 0.3.0.0; агент CryptoDetector — 0.0.5.6

Правообладатель: ООО «Безопасные программные решения» (ИНН 5836687096)

Содержание

1. Общие сведения 3
2. Комплект поставки 4
3. Требования к аппаратному и программному обеспечению 4
3.1. Операционные системы 4
3.2. Аппаратные требования 5
3.3. Необходимое программное обеспечение и зависимости 5
4. Требования к сетевой инфраструктуре 5
5. Подготовка к установке 6
6. Установка 7
6.1. Установка серверной платформы (Windows) 7
6.2. Установка серверной платформы (Linux) 8
6.3. Установка агента (рабочая станция Windows) 8
7. Запуск и первый вход 9
7.1. Серверная платформа 9
7.2. Агент 10
7.3. Запуск после перезагрузки 10
8. Проверка корректности установки и запуска 10
9. Остановка, перезапуск, обновление и удаление 11
10. Проверочный экземпляр для экспертной проверки 11
11. Контактная информация 13

1. Общие сведения

Наименование программного обеспечения: CryptoDetector (далее – ПО).

Версии компонентов программного обеспечения: серверная часть (CryptoDetector Platform) — 0.3.0.0; агент (CryptoDetector) — 0.0.5.6.

Назначение программного обеспечения: мониторинг состояния объектов файловой системы, анализ и выявление их изменений, производимых с целью шифрования, а также восстановление данных указанных объектов.

Тип программного обеспечения: клиент-серверное программное обеспечение.

Способ поставки: установочные пакеты (для серверной части — MSI для Windows и пакеты deb/rpm для Linux; для агента — исполняемый установочный файл Windows), документация.

Целевое окружение: сервер — Windows 10/11 или Windows Server (64-бит), либо Linux (Astra Linux SE, РЕД ОС); рабочие станции — Windows 10/11 или Windows Server (32- и 64-битные редакции).

ПО включает две части, работающие совместно:

• **CryptoDetector Platform (далее — Платформа)** — серверная часть ПО; устанавливается на сервер организации; включает серверное приложение, административную панель и программный интерфейс; обеспечивает централизованное управление рабочими станциями, хранение единых списков, событий и настроек;

• **CryptoDetector (далее — агент)** — клиентская часть ПО; устанавливается на рабочие станции под управлением операционной системы Windows; обеспечивает наблюдение за объектами файловой системы, выявление и блокирование изменений, производимых с целью шифрования, резервное копирование и восстановление данных; взаимодействует с Платформой (получение настроек и списков, передача событий и заявок).

Агент и Платформа применяются в едином комплексе: функции наблюдения и восстановления данных выполняются непосредственно на

рабочей станции, а управление парком рабочих станций, единые списки и настройки обеспечиваются централизованно через Платформу.

2. Комплект поставки

Компонент	Файл	Назначение
Платформа (Windows)	CryptoDetector.Platform-0.3.0-x64-ru.msi, CryptoDetector.Platform-0.3.0-x64-en.msi	Установочный пакет Платформы для Windows
Платформа (Linux)	cryptodetector-platform_0.3.0-1_amd64.deb / cryptodetector-platform_0.3.0-1_arm64.deb	Установочный пакет для Debian-семейства (Astra Linux SE и совместимые)
Платформа (Linux)	cryptodetector-platform-0.3.0-1.x86_64.rpm / cryptodetector-platform-0.3.0-1.aarch64.rpm	Установочный пакет для RPM-семейства (РЕД ОС и совместимые)
Агент	CryptoDetector.exe (установочный файл Windows, 32- и 64-разрядная редакции)	Установочный пакет агента для рабочих станций
Документация	Руководство по установке, краткое руководство пользователя	Описание установки и работы с ПО

В именах установочных пакетов Платформы версия указывается тремя полями (`0.3.0`) — таково требование средств упаковки (Windows Installer, nfpm); четвёртое поле версии (`0.3.0.0`) используется в сборках приложений.

Для варианта установки PostgreSQL 16 средствами установщика Платформы (Windows) дополнительно требуется установочный файл СУБД `postgresql-16.*-windows-x64.exe` (скачивается с сайта производителя СУБД заблаговременно, см. раздел 5).

3. Требования к аппаратному и программному обеспечению

3.1. Операционные системы

Серверная платформа:

• Windows 10, Windows 11 или Windows Server (64-бит);

• Linux: Astra Linux SE 1.8.x (пакет `.deb`), РЕД ОС 8.0.x (пакет `.rpm`); архитектуры x86-64 и ARM64.

Агент:

• Windows 10 или Windows 11 (32- и 64-битные редакции).

3.2. Аппаратные требования

Параметр	Сервер (Платформа)	Рабочая станция (агент)
Процессор	не менее 4 ядер (рекомендуется 4)	не менее 2 ядер
Оперативная память	не менее 6 ГБ (рекомендуется 8 ГБ)	не менее 2 ГБ (рекомендуется 4 ГБ)
Дисковое пространство	не менее 20 ГБ (рекомендуется 50 ГБ и более)	не менее 1 ГБ + место под хранилище резервных копий

3.3. Необходимое программное обеспечение и зависимости

• **PostgreSQL 16 или выше** — обязателен для Платформы; может быть установлен заранее (рекомендуется для Linux) или установлен установщиком Платформы (только Windows, 64-бит).

• **.NET Desktop Runtime 8** — для агента; устанавливается автоматически установочным файлом агента, отдельная установка не требуется.

• **браузер** — для работы с административной панелью Платформы.

• **права администратора** (Windows) или **sudo** (Linux) — для установки и настройки.

4. Требования к сетевой инфраструктуре

• **Сетевые порты.** При установке задаются два порта: для программного интерфейса Платформы и для административной панели. Значения по умолчанию — 7010 и 7291. Порты должны быть свободны на сервере; при необходимости указываются любые другие свободные порты.

• **Профили подключения клиентов.** При установке выбирается один из профилей: «настрою позже» (сервер доступен только локально), «за reverse proxy на этой же машине», «за reverse proxy на другой машине», «прямой HTTPS». Профиль определяет настройки доступа и брандмауэра.

• **Сертификат HTTPS.** Для профиля «прямой HTTPS» используется TLS-сертификат (PFX с закрытым ключом); при его отсутствии создаётся самоподписанный сертификат (применяется в тестовых контурах).

• **Доступ агентов к Платформе.** Рабочие станции с агентом обращаются к программному интерфейсу Платформы по сети; требуется сетевой доступ между рабочими станциями и сервером (при выборе прокси-профилей — через прокси-сервер).

• **СУБД.** Подключение Платформы к PostgreSQL выполняется по сети (порт по умолчанию 5432) — локально или к внешнему серверу.

5. Подготовка к установке

До начала установки необходимо:

1. Проверить соответствие сервера и рабочих станций требованиям (раздел 3);

2. Определиться с размещением базы данных: существующий сервер PostgreSQL 16+ (получить адрес, порт, имя базы, учётную запись и пароль) либо локальная установка (скачать установочный файл PostgreSQL 16 на сервер — только Windows);

3. Определить профиль подключения клиентов и подготовить сертификат (для профиля «прямой HTTPS») либо принять создание самоподписанного сертификата;

4. Задать значения портов (по умолчанию 7010 и 7291);

5. Для агентов определить адрес Платформы, к которой они будут подключаться.

6. Установка

6.1. Установка серверной платформы (Windows)

1. Запустите установочный пакет MSI (двойной щелчок); откроется мастер установки.

2. На экране «База данных» укажите параметры подключения к PostgreSQL (хост, порт, имя базы, учётная запись, пароль). Для установки PostgreSQL 16 силами установщика включите соответствующий пункт и укажите путь к установочному файлу СУБД.

3. На экране «Подключение клиентов» выберите профиль подключения и укажите адрес прокси (при необходимости), порты программного интерфейса и административной панели.

4. На экране «Сертификат HTTPS» (для профиля «прямой HTTPS») укажите PFX-файл и пароль либо оставьте поля пустыми для создания самоподписанного сертификата.

5. Нажмите «Установить». Установщик создаст каталоги данных, сгенерирует ключи, настроит подключение к базе данных, применит профиль подключения и правила брандмауэра, установит и запустит службы `CryptoDetectorApi` и `CryptoDetectorAdmin`. Установка занимает несколько минут; окно установки закрывать не следует.

6. По завершении нажмите «Готово» и выполните проверку (раздел 8).

Результат установки на сервере:

• службы Windows `CryptoDetectorApi` (отображаемое имя «CryptoDetector Platform — API») и `CryptoDetectorAdmin` (отображаемое имя «CryptoDetector Platform — Admin») — тип запуска «Автоматически», учётная запись «Локальная система»;

• файлы программы — `C:\Program Files\Secware\CryptoDetector Platform\` (подкаталоги `Api`, `Admin`, `Tools`);

• данные и конфигурация — `%ProgramData%\Secware\CryptoDetector Platform\` (подкаталоги `config`, `keys`, `ssl`, `logs`, `data`); сохраняются при обновлении, а при удалении — по умолчанию.

Массовая (автоматическая) установка выполняется командой `msiexec` без интерфейса (ключ `/qn`) с передачей параметров через свойства командной строки; пароли при этом не отражаются в журналах. Установка выполняется от имени администратора.

6.2. Установка серверной платформы (Linux)

1. Установите пакет: `sudo apt install ./cryptodetector-platform_0.3.0-1_amd64.deb` (Astra Linux SE) или `sudo dnf install ./cryptodetector-platform-0.3.0-1.x86_64.rpm` (РЕД ОС). Файлы и системный пользователь создаются автоматически, службы включаются в автозапуск (запуск — после настройки).

2. Выполните настройку: `sudo cryptodetector-setuptools configure`. Утилита последовательно запросит параметры подключения к PostgreSQL, профиль подключения, порты и (для прямого HTTPS) сертификат. Для автоматической настройки предусмотрен режим без вопросов (`configure --unattended <файл-ответов>`).

3. Настройка создаст каталоги данных, сгенерирует ключи, при необходимости создаст базу и роль, проверит версию PostgreSQL и запустит службы `cryptodetector-platform-api` и `cryptodetector-platform-admin`.

6.3. Установка агента (рабочая станция Windows)

1. Запустите установочный файл `CryptoDetector.exe` от имени администратора; откроется мастер установки.

2. Примите условия лицензионного соглашения.

3. При необходимости на этом шаге можно передать установщику адрес Платформы (для корпоративного контура — параметром запуска установщика); в дальнейшем адрес задаётся и изменяется в настройках агента («Настройки» → «Адрес сервера»).

4. Завершите установку. Установщик при необходимости установит среду .NET Desktop Runtime 8, драйверы (наблюдения и контроля целостности компонентов), службу рабочей станции, приложения администратора рабочей станции и уведомлений.

5. После завершения установки откроется приложение администратора рабочей станции; проверьте работоспособность (раздел 8).

Результат установки на рабочей станции:

• служба Windows `CDService` (описание «CryptoDetector Service») — тип запуска «Автоматически», учётная запись «Локальная система»;

• драйверы `CryptoDetector` (наблюдение за объектами файловой системы) и `CryptoDetectorSP` (контроль целостности компонентов агента);

• файлы программы — `C:\Program Files\Secware\CryptoDetector\` (подкаталоги `Driver`, `Service`, `UI`); при установке 32-разрядного пакета — `C:\Program Files (x86)\Secware\CryptoDetector\`;

• настройки агента и лицензия — файл `Configurations\MainConfig.json` в каталоге установки; базы списков — `Service\Databases\`; резервные копии изменяемых файлов — `BackupData` в каталоге установки; журналы службы и приложений — `%ProgramData%\Secware\CryptoDetector\`;

• ярлык «CryptoDetector» в меню «Пуск» (папка «Безопасные программные решения») для запуска приложения администратора рабочей станции.

7. Запуск и первый вход

7.1. Серверная платформа

1. Убедитесь, что службы запущены (Windows: `CryptoDetectorApi`, `CryptoDetectorAdmin`; Linux: `systemctl status cryptodetector-platform-api cryptodetector-platform-admin`).

2. Откройте административную панель по адресу, определяемому выбранным профилем подключения (например, `https://<сервер>:7291/` — для прямого HTTPS; `http://127.0.0.1:7291/` — при первом входе на сервере).

3. Войдите с учётной записью **Admin** и паролем **admin**; система потребует сменить пароль — задайте новый пароль и сохраните его.

4. Активируйте лицензию: «Настройки» → вкладка «Лицензия» → «Загрузить лицензию» → выберите предоставленный файл лицензии. До активации лицензии функциональность ограничена.

7.2. Агент

1. Откройте приложение администратора рабочей станции.

2. В разделе «Лицензия» активируйте лицензию: корпоративная лицензия получается с Платформы (укажите адрес Платформы в настройках), автономная — файлом лицензии.

3. В разделе «Статус» включите наблюдение.

4. Обеспечьте регистрацию рабочей станции на Платформе: новые станции появляются в разделе «Компьютеры» со статусом «Ожидает». Администратор Платформы подтверждает станцию (статус «Активен»).

7.3. Запуск после перезагрузки

Службы Платформы и служба агента запускаются автоматически после перезагрузки сервера и рабочей станции; дополнительные действия не требуются. Состояние служб в любой момент проверяется способами, указанными в разделе 8.

8. Проверка корректности установки и запуска

Серверная платформа:

• выполните самопроверку: `"%ProgramFiles%\Secware\CryptoDetector Platform\Tools\cryptodetector-setuptools.exe" verify` (Windows) или `sudo cryptodetector-setuptools verify` (Linux) — все строки отчёта должны иметь состояние `[OK]`;

• проверьте ответ программного интерфейса (`http(s)://<сервер>:<порт API>/health`);

• войдите в административную панель, убедитесь в доступности разделов.

Агент:

• служба рабочей станции `CDService` запущена (оснастка «Службы», `services.msc`); драйверы `CryptoDetector` и `CryptoDetectorSP` загружены;

• в приложении администратора рабочей станции отображаются разделы «Статус», «Журнал», «Списки», «Лицензия», «Настройки»;

• наблюдение включается и выключается, лицензия отображается со статусом «Действует»;

• рабочая станция отображается в административной панели Платформы (при корпоративном режиме).

9. Остановка, перезапуск, обновление и удаление

Остановка и перезапуск. Windows: службы останавливаются и запускаются через оснастку «Службы» либо командами `net stop` / `net start` (для служб `CryptoDetectorApi`, `CryptoDetectorAdmin`; на рабочей станции — для службы `CDService`). Linux: `sudo systemctl stop|start|restart cryptodetector-platform-api cryptodetector-platform-admin`.

Обновление. Платформа: установка пакета новой версии поверх установленной (MSI — запуск пакета новой версии; Linux — установка нового пакета). Конфигурация, ключи, лицензия и данные сохраняются; изменения схемы базы данных применяются автоматически при первом запуске. Агент: запуск установочного файла новой версии поверх установленной.

Удаление. Платформа: Windows — «Параметры → Приложения» (при удалении предлагается сохранить данные — по умолчанию данные сохраняются); Linux — `sudo apt remove cryptodetector-platform` (данные сохраняются), полная очистка — `sudo apt purge cryptodetector-platform`. PostgreSQL при удалении не затрагивается. Агент: удаление через «Параметры → Приложения»; служба и драйверы выгружаются автоматически, служебные данные удаляются.

10. Проверочный экземпляр для экспертной проверки

Для проведения экспертной проверки ПО предоставляется в виде архива с образом виртуальной машины (Oracle VirtualBox) с операционной системой Windows, на которой развёрнуты серверная платформа и агент (на одной машине).

Состав экземпляра:

• Платформа: службы Windows `CryptoDetectorApi` («CryptoDetector Platform — API») и `CryptoDetectorAdmin` («CryptoDetector Platform — Admin») — запускаются автоматически; файлы программы — в каталоге `C:\Program Files\Secware\CryptoDetector Platform\` (подкаталоги `Api`, `Admin`, `Tools`); данные и конфигурация — в каталоге `%ProgramData%\Secware\CryptoDetector Platform\` (подкаталоги `config`, `keys`, `ssl`, `logs`, `data`); административная панель открывается в браузере по адресу экземпляра;

• агент: служба Windows `CDService` — запускается автоматически; драйверы `CryptoDetector` (наблюдение за объектами файловой системы) и `CryptoDetectorSP` (контроль целостности компонентов агента); приложение администратора рабочей станции и компонент уведомлений; файлы программы — в каталоге `C:\Program Files\Secware\CryptoDetector\` (подкаталоги `Driver`, `Service`, `UI`); настройки и лицензия — в файле `Configurations\MainConfig.json` каталога установки, журналы — в каталоге `%ProgramData%\Secware\CryptoDetector\`; агент подключён к локальной Платформе;

• база данных PostgreSQL с предварительно настроенной базой данных;

• активированная лицензия, действующая на период проведения экспертной проверки.

Экземпляр функционирует автономно (все компоненты размещены на одной машине); для входа в административную панель используется предоставленная учётная запись администратора.

Параметры доступа к экземпляру:

• архив с образом виртуальной машины: пароль распаковки vmpostgresql;

• операционная система виртуальной машины: учётная запись `VM`, пароль `0000`;

• административная панель: на самой виртуальной машине — `https://localhost:7291/`; с внешнего компьютера — `https://<IP-адрес виртуальной машины>:7291/` (при подключении по IP-адресу браузер

сообщит о несовпадении имени в самоподписанном сертификате — предупреждение необходимо принять);

• учётная запись административной панели: логин `admin`, пароль `adminadmin`;

• программный интерфейс (API): `https://localhost:7010/`;

• каталоги установки: серверная платформа — `C:\Program Files\Secware\CryptoDetector Platform`, агент — `C:\Program Files\Secware\CryptoDetector`;

• установочные пакеты (дистрибутивы): `C:\Users\VM\Desktop\CD Installers`.

IP-адрес виртуальной машины в сети, где она запущена, отображается командой `ipconfig` на самой машине; он используется для открытия административной панели с внешнего компьютера.

Порядок работы с экземпляром:

1. Развернуть виртуальную машину из архива, запустить её и войти в операционную систему (учётная запись `VM`, пароль `0000`).

2. Открыть административную панель по адресу `https://localhost:7291/` и войти (логин `admin`, пароль `adminadmin`).

3. Открыть приложение администратора рабочей станции (ярлык «CryptoDetector» в меню «Пуск», запустить с правами администратора).

4. По завершении проверки выключить завершить работу операционной системы обычным способом.

Для самостоятельного развёртывания экземпляра на чистом стенде используйте разделы 6.1 (и/или 6.2) и 6.3 руководства.

11. Контактная информация

Техническая поддержка и консультирование по вопросам развёртывания, установки и настройки ПО:

• организация: Общество с ограниченной ответственностью «Безопасные Программные Решения» (ИНН 5836687096);

• телефон: +7 (841) 220-06-03;

• электронная почта: help@secware.ru;

• сайт: www.secware.ru;

• режим работы службы поддержки: в рабочие дни с 9:00 до 18:00 по московскому времени (GMT+3).

Фактический адрес размещения службы поддержки: 440000, Пензенская область, город Пенза, Московская ул., стр. 29, помещ. 1, этаж 7.