CryptoDetector

Описание функциональных характеристик программного обеспечения

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 о программном обеспечении 3
2. Область применения и назначение 3
3. Функциональные возможности 5
   3.1. Функции агента (рабочая станция) 5
   3.2. Функции серверной платформы 6
4. Описание технической архитектуры 7
   4.1. Состав серверной платформы 7
   4.2. Состав агента 8
   4.3. Взаимодействие элементов 9
   4.4. Сторонние компоненты 9
5. Взаимодействие компонентов и внешние интеграции 10

1. Общие сведения о программном обеспечении

Полное наименование программного обеспечения: «CryptoDetector» (далее — ПО).

Правообладатель: Общество с ограниченной ответственностью «Безопасные программные решения» (ИНН 5836687096).

Тип программного обеспечения: клиент-серверное программное обеспечение, включающее серверную часть — CryptoDetector Platform (далее — Платформа: серверное приложение, административная панель, программный интерфейс) — и агент CryptoDetector (далее — агент), устанавливаемый на рабочие станции под управлением операционной системы Windows; Платформа и агент работают совместно в едином комплексе.

Краткое описание: ПО предназначено для мониторинга состояния объектов файловой системы на рабочих станциях, анализа и выявления их изменений, производимых с целью шифрования, а также восстановления данных указанных объектов. Управление парком рабочих станций, едиными списками доверенных и недоверенных объектов, поступающими событиями и настройками осуществляется централизованно через административную панель серверной платформы.

2. Область применения и назначение

Назначение: ПО предназначено для мониторинга состояния объектов файловой системы, анализа и выявления их изменений, производимых с целью шифрования, а также восстановления данных указанных объектов.

Область применения: применение в организациях, эксплуатирующих парк рабочих станций под управлением операционной системы Windows; ПО развёртывается в инфраструктуре организации (on-premise) и используется в локальных вычислительных сетях организаций.

Целевые пользователи:

• администраторы и специалисты, отвечающие за эксплуатацию парка рабочих станций (ИТ-подразделения организаций);

• сотрудники организаций, работающие за рабочими станциями, на которых установлен агент ПО (получают уведомления о событиях, могут подтверждать отдельные операции).

Основные решаемые задачи:

• централизованное наблюдение за состоянием объектов файловой системы на парке рабочих станций;

• выявление изменений объектов файловой системы, производимых с целью шифрования;

• информирование о выявленных событиях и ведение журналов событий;

• восстановление данных объектов из резервных копий, формируемых ПО;

• ведение единых списков доверенных и недоверенных объектов на уровне организации;

• обработка заявок от рабочих станций на изменение списков;

• ведение журнала действий администраторов (аудит);

• формирование сводной информации о состоянии парка рабочих станций.

Затрачиваемые ресурсы. Для работы ПО требуются:

• **серверная платформа:**

• операционная система: 64-битная Windows 10/11 или Windows Server; либо Linux — Astra Linux SE 1.8.x, РЕД ОС 8.0.x (архитектуры x86-64 и ARM64);

• система управления базами данных: PostgreSQL 16 или выше (локально или на отдельном сервере);

• процессор: не менее 2 ядер (рекомендуется 4 ядра);

• оперативная память: не менее 4 ГБ (рекомендуется 8 ГБ);

• дисковое пространство: не менее 20 ГБ (рекомендуется 50 ГБ и более — с учётом роста базы данных);

• сетевые порты: два свободных порта для программного интерфейса и административной панели — задаются при установке и настройке (по умолчанию предлагаются 7010 и 7291);

• **агент (рабочая станция):**

• операционная система: Windows 10 или Windows 11, а также Windows Server (32- и 64-битные редакции);

• права локального администратора для установки;

• среда .NET Desktop Runtime 8 — устанавливается автоматически установщиком;

• процессор: не менее 2 ядер;

• оперативная память: не менее 2 ГБ (рекомендуется 4 ГБ);

• дисковое пространство: не менее 1 ГБ под компоненты ПО, дополнительно — место под хранилище резервных копий объектов файловой системы (объём зависит от интенсивности изменения данных).

3. Функциональные возможности

3.1. Функции агента (рабочая станция):

• **Наблюдение за объектами файловой системы.** Специализированный драйвер операционной системы перехватывает операции запуска процессов и записи файлов на рабочей станции и передаёт данные на анализ;

• **Выявление изменений, производимых с целью шифрования.** Анализ поведения процессов позволяет выявлять операции, вносящие изменения в объекты файловой системы с целью шифрования. Чувствительность анализа регулируется режимом работы детектора (мягкий, стандартный, жёсткий);

• **Блокирование выявленных изменений.** Операции, классифицированные как изменения с целью шифрования, блокируются; пользователю выводится уведомление с возможностью разрешить конкретную операцию;

• **Формирование резервных копий и восстановление данных.** ПО сохраняет резервные копии изменяемых объектов в отдельном каталоге; файлы резервных копий исключаются из операций шифрования. Восстановленные файлы сохраняются отдельно, под именем с добавлением служебного суффикса;

• **Списки доверенных и недоверенных объектов.** На рабочей станции ведутся белый и чёрный списки объектов по значению хеша (SHA-256): добавление файла из проводника с автоматическим расчётом хеша, ручной ввод значения хеша, контроль пересечений между списками;

• **Журнал событий рабочей станции.** Фиксируются включение и выключение наблюдения, блокирование запуска процессов, блокирование изменений и разрешение операций пользователем, изменение конфигурации, события лицензии, действия со списками, очистка журнала;

• **Уведомления пользователя.** Всплывающие уведомления о блокировании операций с возможностью подтверждения или отклонения операции;

• **Настройки.** Язык интерфейса (русский/английский), автоматическое добавление подозрительных объектов в чёрный список, режим работы детектора, отслеживание ассоциированных файлов (все или только загруженные из внешних источников), поддержка сетевых дисков и папок, адрес серверной платформы;

• **Лицензирование.** Активация и контроль лицензии (пробная, домашняя, коммерческая; корпоративная — через серверную платформу), отображение состояния и срока действия лицензии.

3.2. Функции серверной платформы:

• **Учёт рабочих станций.** Регистрация агентов по аппаратному идентификатору, статусы (ожидает подтверждения, активен, заблокирован), удаление записей;

• **Централизованные списки доверенных и недоверенных объектов.** Единые списки организации, версионирование, журнал изменений, импорт и экспорт в формате CSV;

• **Заявки от рабочих станций.** Приём заявок на добавление объектов в списки, рассмотрение (одобрение/отклонение) с комментарием; при необходимости — авто-одобрение;

• **События.** Сбор событий с рабочих станций (блокирование запуска процессов, блокирование изменений), фильтрация и просмотр детальных сведений;

• **Аудит.** Журнал действий администраторов (вход, изменение настроек, управление списками, работа с лицензией и др.);

• **Настройки.** Системные настройки, общие и индивидуальные настройки рабочих станций, сроки хранения событий и журналов;

• **Управление лицензией.** Загрузка, замена и удаление (деактивация) лицензии, контроль срока действия и лимита количества рабочих станций;

• **Уведомления по электронной почте.** Настройка почтового сервера (SMTP), выбор типов событий и получателей уведомлений.

4. Описание технической архитектуры

ПО построено по клиент-серверной архитектуре и состоит из серверной платформы и агентов рабочих станций. Применяемый архитектурный стиль — слоистая (многоуровневая) архитектура: серверная часть разделена на доменную модель, прикладную логику, инфраструктуру и интерфейсы представления; клиентские компоненты реализованы в виде отдельных служб и приложений, взаимодействующих с серверной частью через программный интерфейс. Взаимодействие агентов с серверной платформой осуществляется по программному интерфейсу (REST) по протоколу HTTPS, а также через канал уведомлений в реальном времени.

4.1. Состав серверной платформы

• **Сервер приложений (программный интерфейс)** — веб-приложение ASP.NET Core 8; предоставляет REST API (`/api/v1`), канал уведомлений в реальном времени (SignalR, `/hubs/client`), аутентификацию на основе JWT-токенов (подпись RSA); содержит фоновую службу контроля лицензии. Служба Windows — `CryptoDetectorApi`.

• **Административная панель** — веб-приложение Blazor Server (компоненты MudBlazor), взаимодействует с сервером приложений по программному интерфейсу; интерфейс локализован (русский/английский). Служба Windows — `CryptoDetectorAdmin`.

• **Подсистема доступа к данным** — слой Entity Framework Core 8 и драйвер Npgsql; используется СУБД PostgreSQL 16.

• **Доменный слой, прикладной слой, контракты** — бизнес-логика и модели данных, разделённые по слоям.

• **Клиентский SDK** — библиотека для рабочих станций (NuGet-пакет `CryptoDetector.Client`): HTTP-клиент, автоматическое обновление JWT-токенов, подписка на уведомления в реальном времени (SignalR).

4.2. Состав агента

• **Драйвер наблюдения** (`CryptoDetector`) — драйвер операционной системы, перехватывающий запуск процессов и операции записи файлов, выполняющий анализ и блокирование; передаёт службе сведения о событиях.

• **Драйвер контроля целостности компонентов** (`CryptoDetectorSP`) — обеспечивает неизменность компонентов ПО на рабочей станции; поддерживает режимы работы enforcing (штатный) и permissive (обслуживание).

• **Служба рабочей станции** (`CDService`, приложение Windows-службы C#/.NET 8) — обработка событий драйвера, ведение списков, журнала, резервных копий, взаимодействие с серверной платформой, лицензирование.

• **Приложение администратора рабочей станции** (`CDUi`, настольное приложение WPF) — статус, журнал, списки, лицензия, настройки.

• **Приложение уведомлений** (`CDNotificationUi`) — компонент вывода всплывающих уведомлений пользователю.

• **Служебные утилиты** — средства генерации лицензий и обслуживания драйвера контроля целостности компонентов.

4.3. Взаимодействие элементов

• агент → серверная платформа: регистрация и получение заданий/настроек, синхронизация списков, отправка событий и заявок, получение корпоративной лицензии — по REST API (HTTPS, JWT); уведомления в реальном времени — по каналу SignalR;

• приложение администратора рабочей станции ↔ служба рабочей станции — обмен сообщениями по локальному каналу (RPC);

• административная панель ↔ сервер приложений — по программному интерфейсу (HTTPS);

• серверная платформа ↔ СУБД — по протоколу PostgreSQL;

• межпроцессное взаимодействие на рабочей станции (служба ↔ драйверы) — через управляющие запросы операционной системы.

4.4. Сторонние компоненты

Компонент	**Назначение**	**Лицензия**
.NET 8 / ASP.NET Core	платформа выполнения и веб-фреймворк серверной части	MIT
Entity Framework Core 8 + Npgsql	доступ к данным (PostgreSQL)	MIT / PostgreSQL
Blazor Server + MudBlazor 7	административная панель	MIT / MIT
Serilog	журналирование серверных компонентов	Apache-2.0
MailKit	отправка уведомлений по электронной почте	MIT
Microsoft IdentityModel / System.IdentityModel.Tokens.Jwt	работа с JWT-токенами	MIT
Swashbuckle.AspNetCore	описание программного интерфейса (OpenAPI)	MIT
Riok.Mapperly	преобразование моделей данных	Apache-2.0
.NET 8 (WPF)	настольные приложения агента	MIT

Компонент	Назначение	Лицензия
Entity Framework Core + SQLite	локальное хранилище агента (события, списки)	MIT
Microsoft.Toolkit.Uwp.Notifications	всплывающие уведомления Windows	MIT
System.Management, System.ServiceProcess	доступ к системной информации Windows	MIT
Autofac	контейнер внедрения зависимостей (агент)	MIT
NLog	журналирование агента	BSD-3-Clause
Newtonsoft.Json, nanojson3	обработка JSON	MIT / MIT
Vanara	обёртки системных API Windows	MIT
BouncyCastle.Cryptography	криптографические операции при выпуске лицензий	MIT
PostgreSQL 16	система управления базами данных	PostgreSQL License

Все перечисленные компоненты распространяются по свободным лицензиям, допускающим их использование в составе проприетарного программного обеспечения.

5. Взаимодействие компонентов и внешние интеграции

Интеграция	Способ	Назначение
Агент → серверная платформа	REST API по HTTPS (JWT), канал уведомлений SignalR	регистрация, получение настроек и списков, отправка событий и заявок, получение корпоративной лицензии
Административная панель → серверная платформа	REST API по HTTPS	управление списками, рабочими станциями, настройками, лицензией
Серверная платформа → СУБД	протокол PostgreSQL	хранение данных о станциях, списках, событиях, аудите, настройках

Интеграция	Способ	Назначение
Серверная платформа → почтовый сервер	SMTP (опционально)	отправка уведомлений о событиях администраторам