КИБЕРПРОТЕКТ

Кибер Протего (Cyber Protego)

Краткий обзор

Что умеет Кибер Протего?

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ (КОНТРОЛЬ ДОСТУПА)

- Контроль всех видов устройств и интерфейсов
- Контроль множества каналов сетевых коммуникаций
- Технологии контентной фильтрации – в **режиме реального времени**

ДЕТАЛЬНЫЙ МОНИТОРИНГ СОБЫТИЙ

- Детализированное протоколирование событий
- Теневые копии для большинства контролируемых каналов передачи данных
- User Activity Monitor
- Тревожные оповещения

СКАНИРОВАНИЕ ХРАНИМЫХ ДАННЫХ

- Автоматическое устранение выявленных нарушений политики безопасного хранения данных
- Различные режимы сканирования (локально, удаленно)
- Работа по заданному расписанию, автоматические отчеты

АНАЛИЗ АРХИВА СОБЫТИЙ

- Полнотекстовый поиск по теневым копиям в централизованном или распределенном архиве DLP-системы
- Автоматическое выполнение поисковых запросов по расписанию
- Статистические отчеты, графы связей
- Досье пользователя

Главные ценности Кибер Протего

Предотвращение утечки данных непосредственно на рабочих станциях, выполнение требований регуляторов, анализ в реальном времени

Просто: используются классические методы управления ПО в ИТ

- Нативная интеграция в домен Active Directory
- Централизованное управление для различных вариантов сетевой инфраструктуры предприятия
- Установка обновлений продукта и оптимизация DLP-политик без остановки деятельности сотрудников

Эффективно: высокая производительность, богатое функциональное оснащение

- User Activity Monitor в сочетании с детализированным журналированием событий
- Встроенные отчеты, включая графы связей и досье сотрудников, инструменты просмотра событий и перехваченных данных
- Модульная архитектура, позволяющая решать любые задачи

Надежно: данные не утекут, независимо от места работы пользователя

- Полноценный контроль для всех локальных каналов передачи данных
- Контроль потоков данных для множества каналов сетевых коммуникаций независимо от подключения к локальной сети предприятия
- Высокая степень детализации для всех операций и каналов

Предотвращение утечек

Через все возможные локальные каналы утечки

Порты / интерфейсы	Проводные и беспроводные
Устройства хранения	Съёмные устройства, CD/DVD/BluRay, FDD, HDD, Tape
Принтеры	Локальные, сетевые, виртуальные
Терминальные сессии, VDI	Решения/протоколы Microsoft, Citrix, VMWare, Oracle
Буфер обмена	Текст, файлы, изображения, аудио, снимки экрана
Синхронизация мобильных устройств	iPhone, MTP, BlackBerry, Palm, контроль типов данных

Через множество каналов сетевых коммуникаций

Протоколы	HTTP(S), FTP(S), Telnet, Torrent
Электронная и веб-почта	SMTP(S), MAPI, IBM Notes, более 30 сервисов веб-почты
Zoom	**Сетевые ресурсы общего доступа (SMB)**
Мессенджеры	Skype, Telegram, Zoom, Viber, WhatsApp, Jabber, IRC, Mail.ru Agent
Социальные сети	Более 15 сервисов
Облачные хранилища	Более 30 сервисов

Из разнообразных хранилищ данных

Цели сканирования

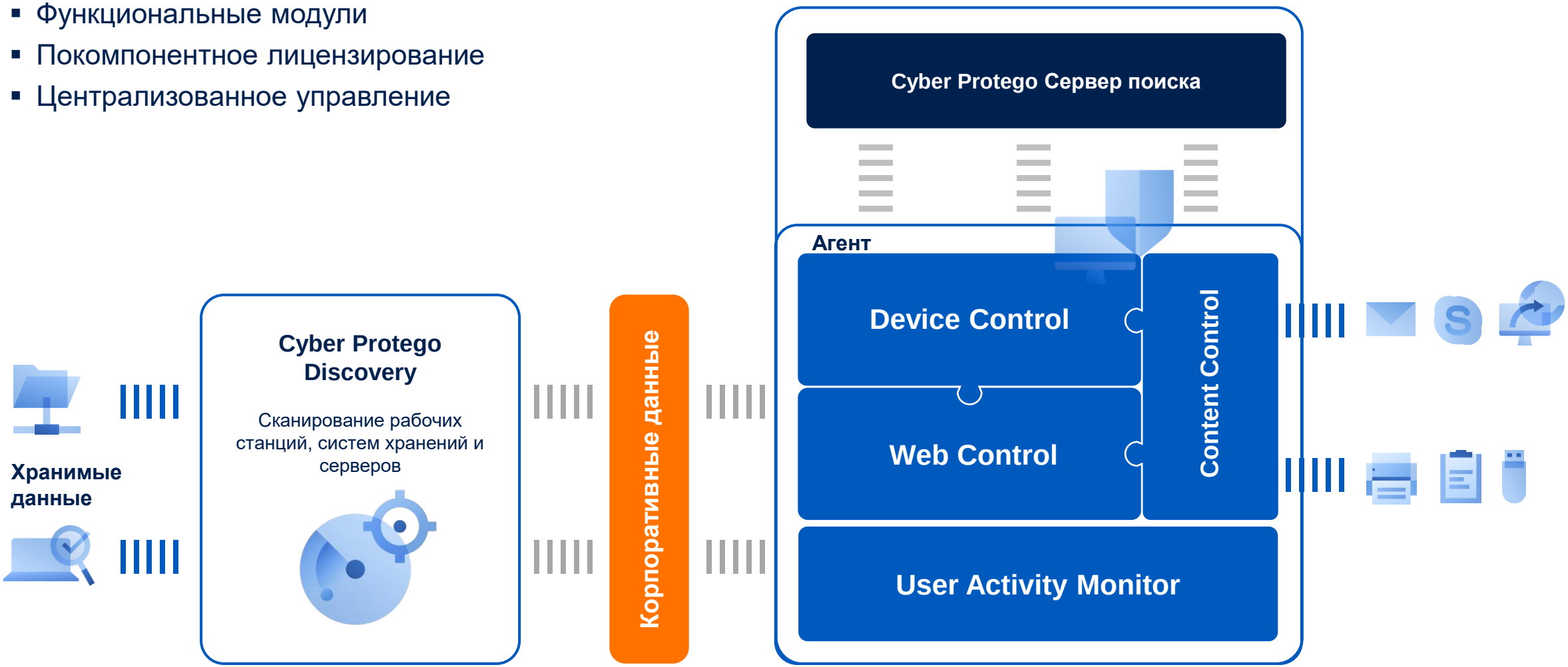
- Рабочие станции
- Общие сетевые папки SMB
- Хранилища NAS/SAN
- БД Elasticsearch

Для ОС Windows

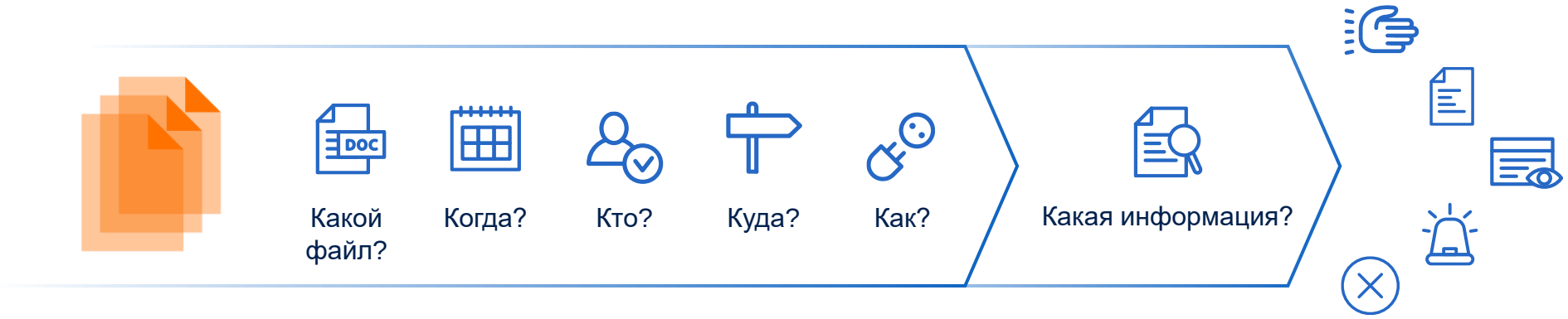
- Файловая система и подключённые устройства хранения
- Папки синхронизации облачных хранилищ
- Репозитории электронной почты (.ost, .pst)

Модульная архитектура

- Функциональные модули
- Покомпонентное лицензирование
- Централизованное управление



Агент – ключевая часть Кибер Протего



Полностью автономен

- Контроль рабочей станции вне офиса
- Контроль «закрытых» протоколов
- Анализ передаваемых данных в реальном времени (передача, сохранение, печать)
- Регулярное сканирование локальной файловой системы
- Запись экрана и клавиатуры

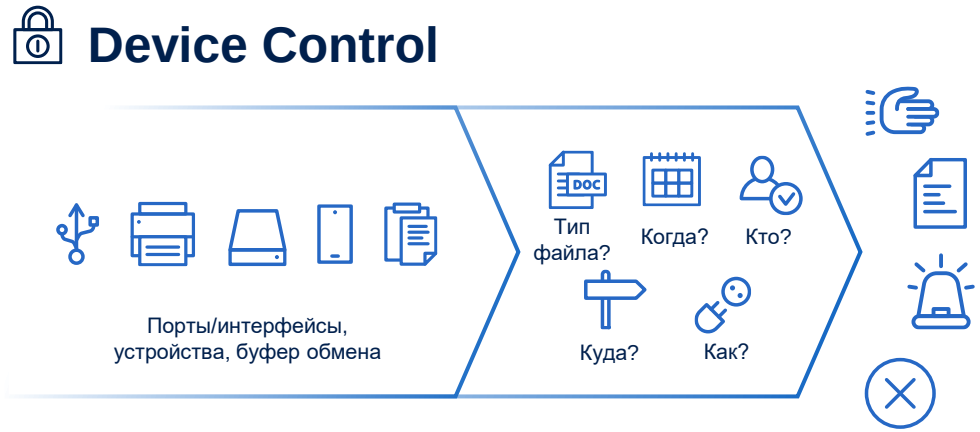
Реализует все DLP-функции

- Защита данных при операциях с устройствами
- Защита данных в сетевых коммуникациях
- Контентный анализ в режиме реального времени
- Защита данных при операциях с системными функциями
- Сканирование хранимых данных на защищаемой рабочей станции
- User Activity Monitor

Device Control

Базовый компонент комплекса, в составе агента.
Реализует **контекстный** контроль данных при их сохранении и печати

- **Контролируемые каналы (локальные):** Порты, интерфейсы, канал печати, периферийные и перенаправленные устройства (в т.ч. в терминальных сессиях), буфер обмена.
- **Возможности:**
  - Выборочный контроль операций (только чтение, запись, форматирование, извлечение)
  - Сбор журналов и оповещение
  - Определение класса устройства независимо от интерфейса подключения
  - Контроль на основе классов устройств
  - Белый список
    - USB устройств - по модели устройства вплоть до серийного номера
    - Временный белый список USB – в режиме офлайн
    - Белый список оптических носителей - доступ к только к авторизованным оптическим дискам
  - Контроль передачи данных на съемные устройства зашифрованные внешними продуктами шифрования



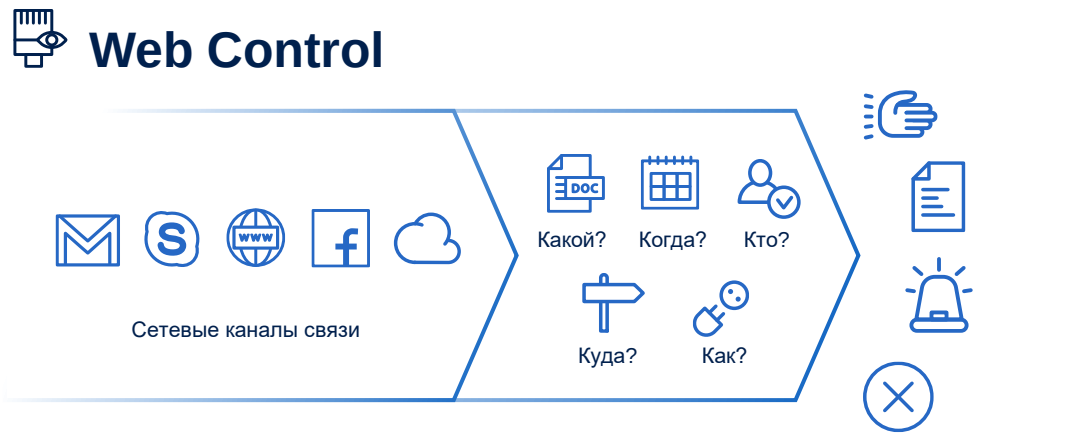
- Предотвращение утечки данных через устройства
- Оповещения о попытках несанкционированного доступа к устройствам
- Белые списки USB устройств и оптических носителей

Web Control

Опционально лицензируемый компонент комплекса, в составе агента.

Реализует **контекстный** контроль передаваемых данных

- **Контролируемые каналы (сетевые коммуникации):**
  - E-mail, http, ftp, web почта, социальные сети, мессенджеры, облачные хранилища, веб-поиск, поиск работы, SMB, другие сетевые протоколы и сервисы
- **Возможности:**
  - Высокая степень избирательности для контроля сетевых протоколов (раздельные права на отправку сообщений, вложений и т.п.)
  - Встроенный DPI: универсальный контроль трафика независимый от используемого приложения/порта
  - Белый список сетевых протоколов
  - Прозрачный для конечного пользователя контроль открытого и защищенного SSL трафика
  - Встроенный IP-фаервол с возможностью избирательной блокировки сетевых подключений (т.н. черный список), в том числе и не поддерживаемых компонентом
  - Событийное протоколирование, теневое копирование, тревожные оповещения



- Предотвращение утечки данных через каналы сетевых коммуникаций
- Оповещения о попытках несанкционированного доступа к сетевым сервисам
- Ограничение доступа до заданного перечня необходимых для рабочих процессов каналов сетевых коммуникаций, корреспондентов, …
- Контроль сетевого трафика независимо от приложения, порта или SSL-шифрования

Content Control

Опционально лицензируемый компонент комплекса, в составе агента.

Реализует анализ содержимого данных в режиме реального времени

- **Контролируемые каналы:** локальные и сетевые
- **Проверяемый тип контента:** текстовые данные, бинарные файлы, метаданные
  - Анализ расширенных свойств файлов и документов
  - Определение типа файла на основе сигнатуры
  - Анализ данных в буфере обмена, в т.ч. в терминальных сессиях
  - Поддержка классификаторов Boldon James
- **Возможности:**
  - Контентный анализ для детектирования и\или фильтрации потоков данных – для разрешения или запрета передачи определенных данных
  - Детектирование защищаемых данных:
    - По ключевым словам и регулярным выражениям
    - Цифровым отпечаткам
  - Оптическое распознавание символов (OCR) для текстовых данных в изображениях
  - Возможность создания сложносоставных правила контентного анализа с поддержкой логических операторов

- Предотвращение несанкционированной передачи, печати и сохранения защищаемых данных по результатам проверки содержимого на уровне агента
- Контроль текстового содержимого в изображениях
- Множество предустановленных словарей и шаблонов регулярных выражения, возможность их расширения и модификации

User Activity Monitor (UAM)

Зачем

Как

Гибкая настройка правил записи по комбинации двух типов триггеров

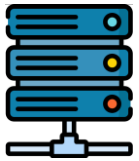
Системные

Вход в систему, работа процесса, обнаружение подключений VPN, LAN, WLAN, подключение периферийных устройств

Событийные

Правила контекстного и контентного контроля, использование устройств и носителей в белых списках, др.

Простые правила с одним условием и сложносоставные правила



Локальное хранение записей или передача их на сервер

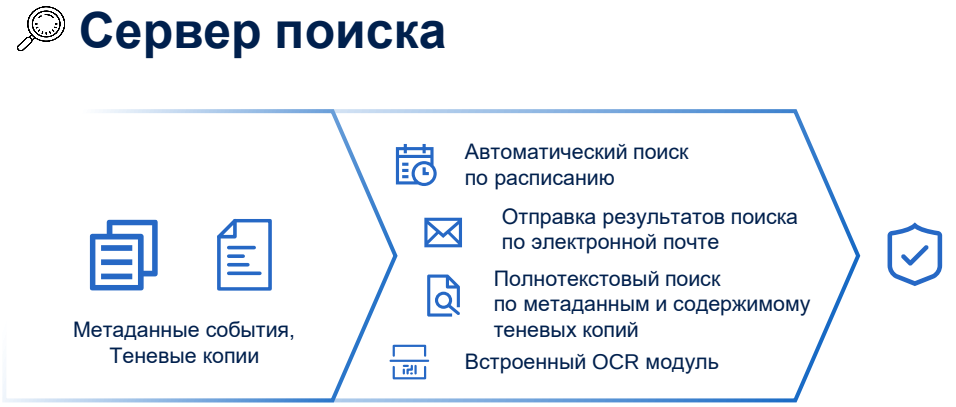
Цветная или ч/б запись с нескольких мониторов

Остановка записи при отсутствии активности

Search Server

Обеспечивает полнотекстовый поиск данных в архиве событий и теневых копий

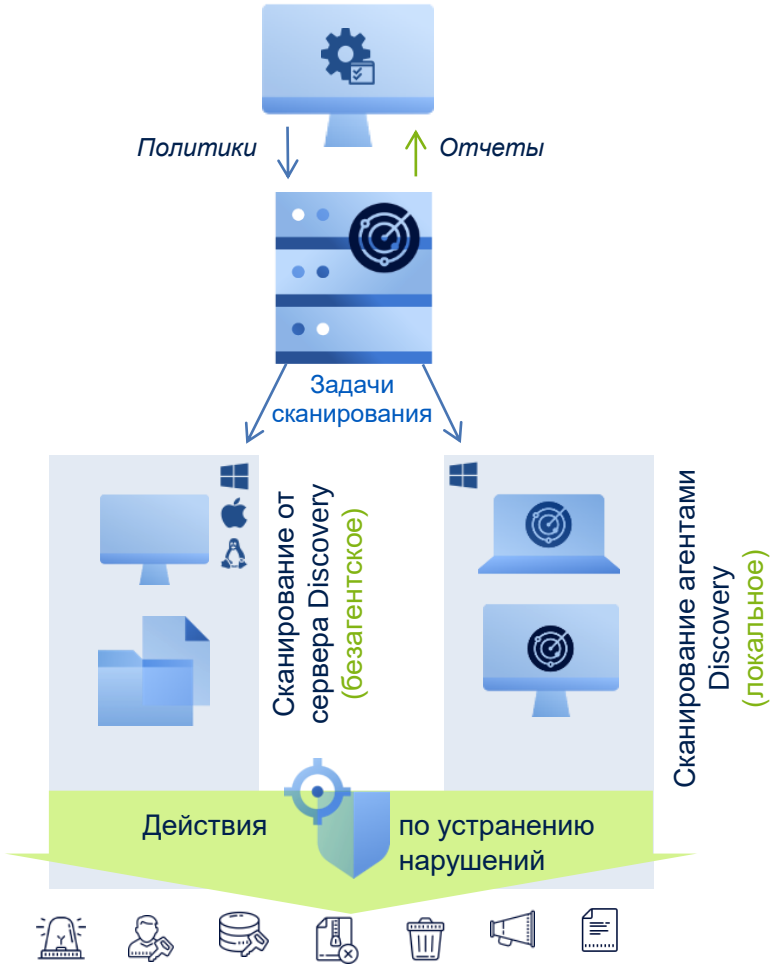
- **Для чего нужен?**
  - Для упрощения, ускорения и автоматизации поиска данных, в журналах (архиве) теневых копий и событий
- **Как это устроено**
  - Поисковый сервер автоматически распознает, индексирует, выполняет поиск внутри документов многих форматов, таких как: Adobe Acrobat (PDF), архивы (GZIP, RAR, ZIP), документы Microsoft Office и OpenOffice и многие другие.
  - Поиск может выполняться вручную или по расписанию с отправкой результатов поиска (в т.ч. инкрементальных) по электронной почте
- **Источник поиска:** журналы теневых копий и событий, хранящиеся в централизованном или распределенном архиве Сервера(ов) управления



- Облегчает аудит журналов и теневых копий, поиск и обнаружение инцидентов безопасности
- Полнотекстовый поиск в базе данных событий и теневых журналов
- Более 160 поддерживаемых форматов файлов и архивов, поддержка логических операторов в поисковом языке и многое другое
- Встроенный OCR

Discovery Server. Контроль хранимых данных

Автоматическое устранение нарушений и детализированные отчеты



Обнаружение

Текстового и бинарного содержимого, **типов данных** по форматам и свойствам файлов / документов / встроенных изображений, **меток** классификатора Boldon James Classifier

Цели	Для ОС Windows
• Рабочая станция **с агентом** Cyber Protego, Discovery **или без агентов** • Общие сетевые папки **SMB** • Хранилища **NAS/SAN** • БД **Elasticsearch**	• Файловая система и подключённые устройства хранения • Папки синхронизации облачных хранилищ • Репозитории электронной почты (.ost, .pst)

Автоматические действия по обнаружении защищаемых данных

Протоколирование; Оповещение службы ИБ, пользователя;

Устранение нарушения: шифрование, удаление, изменение прав доступа

Контролируемый удаленный доступ к данным

Cyber Protego TS

Агент функционирует “внутри” терминальной сессии

- Приложения, опубликованные на гипервизорах
- Локальные виртуальные машины
- Терминальные сессии рабочих столов, в т.ч. опубликованных на гипервизорах
- Решения для виртуализации от Microsoft (RDS/RDP), Citrix (XenApp, XenDesktop) и VMware (VMware View)
- Детектирование перенаправленных устройств в сессии независимо от используемых протоколов (Microsoft RDP/RemoteFX, Citrix ICA/HDX)
- Никаких агентов на удаленном устройстве!

Особенности реализации и преимущества

Полноценный DLP-контроль в любых условиях – в офисе или вне его с автоматическим переключением DLP-политик

Контентная фильтрация **в режиме реального времени**

Централизованное управление, включая интеграцию в MS Active Directory

User Activity Monitor (UAM), интегрированный в DLP-политики

Защита данных в средах виртуализации **Cyber Protego TS**

Наибольшая широта охвата потенциальных каналов утечки данных

Высочайший уровень **самозащиты агентов**

Автоматические действия по устранению нарушений хранения данных (Discovery)

Независимый от приложений и портов контроль сетевых протоколов, встроенный **резидентный модуль DPI** (Deep Packet Inspection)

КИБЕРПРОТЕКТ

- Выполнение требований по защите КИИ и импортозамещению
- Доступная цена не привязанная к курсу валют
- Поддержка более 45 платформ, в том числе отечественных ОС
- 100% российская компания с собственной экспертизой

Защита инфраструктуры предприятия