iBatyr Monitor

Программное обеспечение поддерживает работу в сетях любой конфигурации и сложности, а также поддерживает возможность подключения агентов к серверу через сеть Интернет.

- Серверная часть программного обеспечения, реализующая функционал управления агентами, хранения собираемой информации и формирования отчетов поддерживает возможность установки всех необходимых компонентов на одном сервере.
- Для сбора информации должен устанавливается только один модуль (агент) на один ПК.
- Агент унифицирован для работы на терминальных серверах и рабочих станциях пользователя.
- Для доступа к собранной информации, управления политиками безопасности, настройки конфигурации агента используется единая консоль администратора с возможностью разграничения доступа.
- Система имеет возможность вертикального и горизонтального масштабирования.
- Серверные компоненты не требуют наличия у заказчика дополнительных платных лицензий на программное обеспечение.
- Задержка обновления отчетов составляет не более 15 минут при максимальной загрузке системы.

Архитектура программного обеспечения:

- Архитектура системы обеспечивает выполнение OLAP запросов в реальном режиме времени.
- Для исполнения аналитических запросов в реальном режиме времени система имеет возможность дополнительно использовать БД типа columnar store (Clickhouse).
- Метаданные хранятся в БД, медиа файлы в файловом хранилище.
- Хранение файлов обеспечивается в режиме «кольцевой буфер» с возможностью автоматического перемещения на долговременное хранилище.
- Протокол обмена между агентом и сервером, а также доступ в панель администратора защищен шифрованием семейства TLS (на основе клиентских сертификатов).
- Интерфейс администратора обеспечивает вывод суммарной (агрегированной) информации на основе больших массивов данных, структурированных по многомерному принципу.
- Интерфейс администратора поддерживает распределение полномочий, основанных на ролях, в том числе заданных в Active Directory

Администрирование системы:

- Установка агентов происходит централизовано с помощью групповых политик AD, с помощью инсталлятора модуля агента и локально, с помощью запуска инсталлятора на машине пользователя.
- Установка по списку ПК из AD: подключение из инсталлятора агента к контроллеру домена для выбора компьютеров для установки; назначение конфигураций мониторинга по группам AD; создание учетных записей веб-консоли через AD.
- Модуль агента умеет отправлять собранные данные на несколько ip-адресов сервера.
- Обновление агентов происходит автоматически, централизовано после подтверждения администратором системы.
- Обеспечивается возможность настройки длительности хранения информации в базе данных, в том числе возможность автоочистки файлового хранилища без удаления данных из базы данных.
- Предупреждение о заполнении дисков БД. Отправка администратору системы уведомлений по электронной почте о системных событиях (системные ошибки, предупреждения, оповещение при срабатывании политик безопасности и т.д.).
- Обеспечивается настройка максимальной скорости передачи перехваченных данных от агента на сервер.
- Журнал действий администраторов системы в консоли администратора.
- Автосмена имени агента, при смене названия компьютера.
- Обеспечиваться возможность авторизации пользователей в веб-интерфейсе консоли администратора через учётные записи AD.
- Поддержка работы агента и сервера на одном порту и IP-адресе, но с разными SNI в сертификате.

Требования к функциональным возможностям системы:

Общие требования к логируемой информации:

Фиксируются следующие типы событий действий пользователя:

- вход/выход из системы;
- активность пользователя в приложениях и на сайтах;
- подключение к удаленному рабочему столу, перехват управления;
- запись видео рабочего стола;
- снимок экрана;
- операции с файлами;
- теневые копии перехваченных файлов;
- печать документов;
- буфер обмена;

- реестр оборудования;
- реестр установленных программ;
- посещение веб-ресурсов;
- сетевые подключения;
- интернет-мессенджеры;
- почта;
- установка ПО;
- запуск и завершение приложения;
- внешние диски и устройства;
- присутствие на рабочем месте.

Фиксируются следующие атрибуты логируемой информации:

- агент:
- ip-адрес;
- дополнительная метка;
- название ПК;
- статус;
- версия OS;
- версия агента;
- учетная запись пользователя:
- комментарий;
- отдел;
- организация;
- телефон;
- полное имя;
- почта;
- должность;
- домен;
- пользователь;
- приложение:
- полный путь;
- название;
- описание;
- сайт:
- полный домен;
- протокол;
- URL;
- основной домен;
- тип контента;
- сетевая активность:
- сетевой порт;
- файл:
- хеш файла;

- операции;
- тип контента;
- имя файла;
- тип диска;
- расширение;
- путь;
- устройства:
- ID устройства;
- тип диска;
- класс устройства;
- тип устройства;
- переписка:
- домен получателя;
- отправитель;
- все получатели;
- формат сообщения;
- направление;
- домен отправителя;
- получатель;
- чаты;
- канал общения;
- дата:
- час суток;
- часовой пояс;
- день недели;
- по годам;
- по месяцам;
- по дням;
- по часам;
- по минутам;

Индексируются файлы следующих форматов:

- Adobe Acrobat (*.pdf);
- Ansi Text (*.txt);
- ASCII Text;
- ASF (метаданные) (*.asf);
- CSV (Comma-separated values) (*.csv);
- DBF (*.dbf);
- EML files (электронные письма, сохраненные Outlook Express) (*.eml);
- HTML (*.htm, *.html);
- JPEG (метаданные) (*.jpg);

- MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht);
- MSG files (электронные письма, сохраненные Outlook) (*.msg);
- Microsoft Excel (*.xls) Microsoft Excel 2003 XML (*.xml);
- Microsoft Excel 2007 и выше(*.xlsx);
- Microsoft Outlook Express 5и6:базы сообщений (*.dbx);
- Microsoft PowerPoint (*.ppt);
- Microsoft Rich Text Format (*.rtf);
- Microsoft Word for DOS (*.doc);
- Microsoft Word for Windows (*.doc);
- Microsoft Word 2003 XML (*.xml);
- Microsoft Word 2007ивыше(*.docx);
- Multimate version 4 (*.doc);
- OpenOfficeверсий1, 2и3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включаяOASIS Open Document Format для офисных приложений).

Контролируемые каналы:

Контроль отправки информации посредством электронной почты:

- Перехват почтовых сообщений по протоколам – SMTP/SMTPs, POP3/POP3s, IMAP/IMAPs, MAPI;
- Перехват и анализ файлов-вложений почтовых сообщений;
- Мониторинг почтовых сообщений и вложений с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Поиск по заданным параметрам текста и атрибутам почтовых сообщений, и тексту их вложений;
- Возможность выгрузки писем в следующих видах – Excel, HTML, CSV, в формате .png, с возможностью скачать переписку в ZIP архиве или распечатать на принтере;
- Возможность построения графа переписки, с ручной настройкой параметров отображаемой информации.

Мониторинг отправки информации посредствам IM клиентов:

- Перехват текстовых сообщений по протоколам (Skype, Telegram, ICQ\QIP, Jabber, Mail.ru Agent);
- Перехват отправляемых файлов для (Skype, Telegram);
- Мониторинг сообщений и файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за

информационную безопасность, в случае обнаружения информации по заданным критериям;
- Поиск по заданным параметрам текста и атрибута сообщений и (содержимого) файлов, переданных через IM-клиенты.

Контроль информации по HTTP/HTTPs:

- Перехват данных по протоколам HTTP/HTTPS;
- Перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
- Возможность перехвата входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Odnoklasniki, Twitter;
- Возможность перехвата исходящих сообщений VK;
- Перехват исходящих электронных писем и вложений, переданных или полученных через почтовые веб-сервисы (mail.yandex.ru, mail.google.com, mail.rambler.ru, e.mail.ru, outlook.com)
- Перехват и мониторинг поисковых запросов пользователя;
- Сохранение адресов всех страниц (URL), посещенных пользователем;
- Мониторинг сообщений и файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Возможность поиска по тексту и атрибутам сообщений и файлов, переданных и перехваченных по протоколу HTTP(S);
- Возможность блокировки посещения веб-ресурсов;
- Исключение мониторинга сайтов по чёрным и белым спискам;
- Мониторинг всех посещённых сайтов и времени, проведённого на веб-страницах;
- Возможность формирования различных отчетов по времени активности пользователя за ПК. Рейтинг посещенных сайтов за день, хронология событий за выбранный временной интервал для отдельного пользователя или для групп пользователей или всей организации в следующих видах – Excel, HTML, CSV, в формате .png, с возможностью скачать отчеты в ZIP архиве или распечатать на принтере;

Контроль информации, передаваемой по протоколу FTP:

- Перехват файлов, загруженных или переданных по FTP-протоколу, а также переданных по зашифрованному FTP-протоколу (FTPs);
- Мониторинг файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Мониторинг и перехват файлов и паролей по протоколу FTP/FTPs с последующим контекстным анализом перехваченных файлов.

Контроль информации, отправляемой на печать:

- Перехват документов, отправляемых на печать;
- Извлечение и анализ текста отправленных на печать документов;
- Мониторинг документов, отправленных на печать с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Поиск по заданным параметрам текста и атрибута отправленных на печать файлов;
- Возможность выгрузки в Excel, HTML, CSV, в формате .png, с возможностью скачать в ZIP архиве или распечатать на принтере;

Контроль внешних накопителей:

- Теневое копирование файлов, отправляемых на внешние носители (Съемные жесткие диски, карты памяти, съемные накопители, CD/DVD);
- Контроль подключений и отключений USB-устройств;
- Возможность настройки правил доступа для USB-устройств по их уникальным идентификаторам, в том числе с разрешением только для чтения;
- Возможность блокировки CD-накопителей;
- Возможность настройки правил блокировки USB-устройств по черным или белым спискам, по классам устройств и по группе;
- Перехват листинга и теневое копирование файлов при подключении внешних носителей, с возможностью настройки правила для перехвата по указанным расширениям типов файлов;
- Мониторинг случаев передачи файлов на внешние носители с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Мониторинг случаев использования внешних устройств с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Аудит событий копирования файлов на внешние накопители: фиксируется имя файла, пользователь, дата, время, приложение, полный путь и данные устройства;
- Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных на внешние носители.
- Возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

Контроль информации, передаваемой в облачные хранилища (файловый канал):

- Возможность осуществления контроля по следующим облачным хранилищам – OneDrive, Dropbox, Google Drive, Yandex Disk, O-disk;
- Теневое копирование файлов, отправляемых в облачные хранилища с рабочей станции сотрудника с установленным агентом;
- Мониторинг случаев передачи файлов в облачные хранилища с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, пользователь, дата, время и имя облачного сервиса;
- Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных в облачные хранилища;
- Возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей.

Контроль файлов и файловой активности:

- Контроль файловых операций (Запись, Копирование, Оглавление диска, Отключение, Очистка корзины, Перезапись, Переименование, Перемещение, Переименование и перемещение, Подключение, Создание, Удаление, Чтение);
- Перехват файлов со съёмных носителей при подключении по заданным шаблонам расширений файлов;
- Сохранение теневых копии файлов, отправленных за информационный периметр контролируемой рабочей станцией;
- Возможность поиска по тексту и атрибутам перехваченных файлов;
- Мониторинг случаев использования файлов с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Возможность создавать индивидуальные политики контроля за файловой активностью;
- Специальные опции для ускорения работы на сетевых дисках;
- Особый контроль путей и файлов (для создания теневых копий при любых файловых операциях).

Контроль информации, отправляемые на локальные сетевые ресурсы:

- Теневое копирование файлов, отправляемых на сетевые ресурсы с рабочей станции пользователя с установленным агентом;
- Мониторинг случаев передачи файлов на сетевые диски с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Аудит событий отправки файлов на сетевые диски: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу, приложение;
- Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных на сетевые ресурсы;
- Возможность создавать индивидуальные политики контроля информации для отдельных пользователей и рабочих станций.

Возможность мониторинга действий пользователей на ПК:

Скриншоты (снимки экрана рабочего стола сотрудника):

- Возможность снятие скриншотов с заданным интервалом;
- Возможность снятия скриншотов по переключению активного окна;
- Возможность настройки для определенных приложений и сайтов с более частым интервалом снятия скриншотов;
- Возможность настройки качества получаемых скриншотов в процентах;
- Возможный формат скриншотов JPEG;
- Возможность выгрузки в следующих форматах - Excel, HTML, CSV, в формате .png, с возможностью скачать отчеты в ZIP архиве или распечатать на принтере;

Статистика активности ПК:

- Введение статистики по времени работы и простой (отсутствия действия сотрудника) ПК с представлением собранной информации в виде различных графиков;
- Ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);
- Возможность настройки периода неактивности, после которого рабочее время сотрудника будет считаться простоем;
- Возможность настройки исключений отдельных процессов из мониторинга;
- Возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений),

контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу;
- Возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в формате HTML;
- Предустановленные наборы приложений и сайтов, для классификации активной деятельности за ПК;
- Разделение деятельности на продуктивную\непродуктивную\нейтральную;
- Удобные отчёты для различных представлений и анализа накопленных данных по накопленной активности пользователей;
- Общий и групповые отчёты по активности пользователей.

Контроль буфера обмена:

- Копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;
- Возможность поиска по тексту, помещаемому пользователями в буфер обмена.
- Мониторинг определенной информации, помещенной в буфер обмена, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;
- Копирование графической информации помещаемой в буфер обмена.

Видео мониторинг:

- Возможность подключения к монитору компьютера сотрудника и просмотра изображения в режиме реального времени;
- Мониторинг рабочих столов нескольких пользователей одновременно;
- Возможность вывода окна просмотра на отдельный экран;
- Возможность записи видео с рабочих столов сотрудников;
- Возможность настройки длительности отрывка для записи видео;
- Возможность сохранения записей нескольких пользователей одновременно;
- Возможность воспроизведения файла записи средствами системы.

Модуль анализа файла на предмет наличия меток:

- Позволяет блокировать несанкционированный доступ к файлам по заданным параметрам;
- Возможности управления доступом пользователей и приложений к файлам, согласно набору правил;
- Возможность добавления меток к офисным приложениям;
- Возможность отслеживания работы над помеченными файлами;
- Возможность настройки собственных параметров через управление в WEB-консоли со следующими возможностями – выставления правил использования \ блокировок для помеченных файлов;
- Поддержка следующих форматов - .docx, .xlsx, .pptx, .odt, .ods, .odp;
- Поддержка следующих операторов при настройке правил – not, or, and, xor, eq, matches, in;
- Поддержка следующих атрибутов при настройке правил – tag, tag_value, computer_name, user_name, user_domain, file_path, file_name, file_ext, exe_name, mine.

Функциональные возможности работы web-интерфейса:

Возможность просмотра информации по следующим критериям:

Предоставляется возможность просмотра информации по типам событиям, а именно:

- Поисковые запросы, информация выводится в следующем виде – время, компьютер, пользователь, приложение, домен, текст;
- Время активности, информация выводится в следующем виде – время, тип события, компьютер, пользователь, длительность (в формате 00 ч 00 м 00 с), приложение, сайт, заголовок;
- Снимок экрана, информация выводится в следующем виде – время, компьютер, пользователь, заголовок, снимок;
- Запись звука, информация выводится в следующем виде – время, компьютер, пользователь, устройство, контент (аудиофайл);
- Перехваченный файл, информация выводится в следующем виде – время, компьютер, пользователь, приложение, контент (файл, изображение и т.д.), связь с событием, страницы (перехват печати отображает количество страниц), получатели;
- Устройства, информация выводится в следующем виде – время, компьютер, пользователь, тип устройства, устройство, ID;
- Завершение приложений, информация выводится в следующем виде – время, компьютер, пользователь, приложение, ID процесса, ID пользовательской сессии;
- Системный лог, информация выводится в следующем виде – время, тип события, компьютер, текст, контент (сам лог с возможностью скачать из web-интерфейса);

- Беспроводное подключение, информация выводится в следующем виде – время, компьютер, SSID;
- Снимок с веб-камеры, информация выводится в следующем виде – время, компьютер, пользователь, приложение, снимок;
- Буфер обмена, информация выводится в следующем виде – время, компьютер, пользователь, приложение, текст, формат буфера обмена (текст или изображение);
- FTP, информация выводится в следующем виде – время, компьютер, пользователь, приложение, событие;
- Почта, информация выводится в следующем виде – время, компьютер, пользователь, отправитель, получатели, заголовок, контент (файлы, изображение и т.д.);
- Посещение сайтов, выводится в следующем виде – время, компьютер, пользователь, приложение, ссылка;
- Ввод с клавиатуры, информация выводится в следующем виде – время, компьютер, пользователь, приложение, заголовок окна, текст;
- Сеть, информация выводится в следующем виде - время, компьютер, пользователь, приложение, сокет;
- Алерт, информация выводится в следующем виде – время, тип, компьютер, пользователь, время, алерт, текст;
- Запуск приложения, информация выводится в следующем виде – время, компьютер, пользователь, приложение, ID процесса, ID пользовательской сессии;
- Операция с файлами, информация выводится в следующем виде – время, компьютер, пользователь, приложение, операция, имя файла, устройство, тип диска;
- Внешние диски, информация выводится следующем виде – время, компьютер, пользователь, тип, устройство, ID;
- Установка ПО, информация выводится в следующем виде – время, компьютер, операция, продукт, поставщик, версия;
- Видео рабочего стола, информация выводится в следующем виде – время, компьютер, пользователь, приложение;
- Вход/выход из системы, информация выводится в следующем виде – время, компьютер, пользователь, событие (вход в систему, выход из системы и т.д.)
- Данные формы, информация выводится в следующем виде – время, компьютер, пользователь, приложение, сайт;
- Реестр оборудования, информация выводится в следующем виде – время, компьютер, тип устройства, устройство, ID;
- Реестр софта, информация выводится в следующем виде – время, компьютер, операция, продукт поставщик, версия;
- Печать документов, выводится в следующем виде – время, компьютер, пользователь, страницы (количество распечатанных страниц), текст;
- Интернет-пейджер, информация выводится в следующем виде – время, компьютер, пользователь, отправитель, получатели, сообщение.

Предоставляется возможность просмотра информации по измерениям или их комбинированием как с другими измерениями, так и с типами события, а именно:

- Измерение Агент, выбор предоставляется по следующим параметрам – IP адрес, группа (к которому относится агент), сотрудник, компьютер, статус, версия OS, версия агента;
- Измерение пользователь, выбор предоставляется по следующим параметрам – отдел, организация, телефон, полное имя, почта, должность, домен, пользователь, комментарий, (информация задается в профили пользователя);
- Измерение приложение, выбор предоставляется по следующим параметрам – полный путь, заголовок окна, название, описание;
- Измерение сайт, выбор предоставляется по следующим параметрам – полный домен, протокол, URL, основной домен, тип контента;
- Измерение сетевая активность, выбор предоставляется по следующим параметрам – Ip адрес, сетевой порт;
- Измерение файл, выбор предоставляется по следующим параметрам – хеш файла, операция, имя файла, контент извлечен (true или false), метка, тип контента, тип диска, расширение, путь;
- Измерение устройство, выбор предоставляется по следующим параметрам – устройство, ID устройства, метка, тип диска, класс устройства, тип устройства;
- Измерение переписка, выбор предоставляется по следующим параметрам – домен получателя, отправитель, все получатели, формат сообщения, направление, домен отправителя, получатель, чаты, канал общение;
- Измерение дата, выбор предоставляется по следующим параметрам – час суток, часовой пояс, день недели, по годам, по месяцам, по дням, по часам, по минутам;
- Измерение инсталляции, выбор предоставляется по следующим параметрам – поставщик, обновление, версия, операция, продукт;
- Измерение сработавшие фильтры, выбор предоставляется по следующим параметрам – категория, название.

Возможность смены режимов предоставления отчетов с отображением данных по следующим критериям:

- Таблица, выводящая информацию определенных типов события и типов измерения, с возможностью их комбинирования;
- Список, предоставляет информацию общим списком определенных типов события и типов измерения, с возможностью их комбинирования;
- Снимки, режим отображения для удобства предоставления информации по типам события снимков с веб-камеры и снимков с экрана, с возможностью выбора типов измерения;
- Активность, выводит информацию в виде тепловой диаграммы, с возможностью выбора отображения информации по типам события и измерениям;

- Переписка, режим отображения для удобства предоставления информации по типам события почта и интернет-пейджер, с возможностью выбора дополнительных типов измерения.

Возможность анализировать и наблюдать статистику по собранным данным (строить фильтры в фильтрах), тем самым, получая дополнительный срез информации при помощи следующих способов отображения информации:

- Таблица с возможностью отображения в табличном виде события по выбранным пк и фильтру;
- Линейный график с возможностью отображения количества событий по выбранным фильтрам в виде столбцов графика, а также возможность переключения графика между – линейным, гистограммой, с накоплением и без накопления;
- Круговая диаграмма с возможностью отображения количества событий в виде круговой диаграммы с поддержкой вложенных фильтров;
- Возможность построения граф в виде mind-map карты;
- Возможность построения дерева взаимосвязей, которое возможно выгрузить на печать, и возможностью провалиться в события, кликнув на элемент дерева;
- Дополнительные возможности отображения данных в следующих видах: радар, река событий, статистика.

Наличие вкладки (фильтры) включающую в себя сгруппированные измерения, политики, дашборды и словари, созданные ранее пользователем или предустановленные заранее:

- Наличие фильтров, предустановленных или созданных, с возможностью предоставления информации в отчетах или конкретных событиях;
- Наличие подразделов эффективности, безопасности и инцидентов;
- Возможность маркировки приложений и сайтов по категориям продуктивности по следующим параметрам – продуктивная деятельность, непродуктивная деятельность, нейтральная деятельность, премиальная деятельность, инцидент; а также в любую из категорий приложений и сайтов, можно добавить\удалить любое количество имён исполняемых файлов или имён сайтов;
- Наличие системных политик, являющимся скриптами для запуска внутренних обработчиков информации и возможность их изменения;
- Возможность создание новых фильтров или удаление уже имеющихся;
- Возможность задать любое имя созданному фильтру или дашборду, с возможностью его последующего изменения.

Анализ собираемой информации:

При работе с фильтрами и политиками безопасности, пользователю доступен следующий функционал:

- Возможность настройки индивидуальных фильтров и политик безопасности, с последующим комбинированием их в дашборды, позволяющие просматривать необходимую выводимую информацию в едином месте;
- Возможность настройки уведомлений на почту ответственным лицам за информационную безопасность, с настройкой интервалов отправки (при срабатывании, ежедневно, еженедельно, ежемесячно) и возможностью настройки получаемой информации об инциденте;
- Наличие встроенных политик безопасности, а именно словарь ненормативной лексики, словарь наркоманского сленга, словарь откатной тематики, словарь поиска работы, поиск кредитных карт, шифрованных архивов и т.д.;
- Возможность просмотра информации и сработавших фильтров за любой промежуток времени;
- Возможность просмотра статистки с указанием количества сработавших инцидентов по определенному фильтру или типу события;
- Наличие встроенного отчета инвентаризации устройств рабочей станции со следующими выводимыми параметрами – статус (в наличии или нет), компьютер (имя рабочей станции), производитель, тип устройства, HWID и дата последней проверки на наличие, с возможностью выгрузки отчета в HTML формате;
- Наличие встроенного отчета по инвентаризации приложений рабочей станции со следующими выводимыми данными – статус (в наличии или нет), компьютер (имя рабочей станции), продукт, поставщик, версия и дата последней проверки на наличие, с возможностью выгрузки отчета в HTML формате;
- При просмотре информации об инциденте в web-интерфейсе доступна следующая информация:
- Пользователь, допустивший нарушение;
- Дата и время инцидента;
- Тип файла, вызывающего срабатывания фильтра или политики безопасности (электронное письмо, документ отправленный на печать и т.д.);
- Содержание файла (электронного письма, документа, отправленного на печать и т.д.);
- Другая дополнительная информация (с возможностью исключения/добавления необходимых пунктов вывода).
- Возможность изменения встроенных политик безопасности, с настройкой отправки уведомлений на почту ответственному лицу за информационную безопасность и возможности изменения категорий по следующим параметрам – инцидент, непродуктивно, нейтрально, продуктивно, премиально;

При работе с отчетами учета рабочего времени, доступен следующий функционал:

Наличие встроенных отчетов учета рабочего времени, а именно:

- Комбинированный отчет, содержащий информацию за выбранный период, по выбранным пользователям и выводимый следующую информацию – дата, компьютер, начало и окончание рабочего дня, общее время работы, активное время, время простоя, информацию по опозданию и сверхурочным, продуктивное и непродуктивное время, нейтральное время;
- Ленточный график, отчет содержащий информацию за выбранный период, по выбранным пользователям и выводимый следующую информацию – дата, компьютер;
- Таблица, отчет содержащий информацию за выбранный период, по выбранным пользователям и выводимый следующую информацию – дата, компьютер, начало и окончание рабочего дня, общее время работы, активное время, время простоя, информацию по опозданию и сверхурочным, продуктивное и непродуктивное время, нейтральное время;
- Отчет активности за период, отчет содержащий информацию за выбранный период, по выбранным пользователям и выводимый следующую информацию – компьютер, общее время работ, активное время работы, время простоя, информацию по опозданию, сверхурочные, продуктивное время и непродуктивное время; а также отчет содержит информацию по продуктивности в различных критериях (например, офисные приложения, почтовые приложения и т.д.), топ приложений и топ сайтов с выводом в виде графика и общего времени;
- Продуктивное время по отделам, отчет содержащий суммарное продуктивное\непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени от общей активности пользователя;
- Активное время по отделам, отчет содержащий суммарное активное и неактивное время пользователей на рабочих местах за выбранный период времени по отношению к плановому;
- Топ непродуктивности по отделам, отчет содержащий информацию за выбранный период и сортирующий непродуктивных сотрудников по отделу, с выводом следующей информации – временной период, компьютер, пользователь, должность, отдел, название, время активности;
- Сводный отчет, отчет содержащий информацию за выбранный период, по выбранным пользователям и выводящий следующую информацию – период времени, компьютер, общее время, активное время, время простоя, продуктивное время, непродуктивное время, количество опозданий и общее время опозданий;
- Отчёт по опозданиям, отчет содержащий информацию за выбранный период, по выбранным пользователям и выводящий следующую информацию – период времени, компьютер, количество опозданий, общее время опозданий, общее время, активное время и время простоя;
- Учет ранних уходов и приходов, отчет содержащий информацию за выбранный период, по выбранным пользователям и выводящий следующую информацию –

период времени, компьютер, информацию по опозданию, фиксации раннего ухода на обед и опоздания прихода с обеда, задержание на работе и раннего прихода на работу.

- Возможность настройки рабочего расписания сотрудников, по следующим критериям – день недели, начало рабочего дня, конец рабочего дня, начало перерыва, конец перерыва, рабочее время;
- Наличие календаря, с возможностью проставления рабочих часов, праздников, больничных, отгулов и отпусков;
- Возможность назначения расписаний по отделам\пользователям, меткам.
- Возможность отправки уведомлений ответственным лицам на почту, при превышении времени активности или разговора в определенных приложениях, сайтах и т.д.

Контентный анализ:

- Возможность поиска, по ключевым словам, и словосочетаниям, с возможностью добавления слов или словосочетаний в фильтр в перехваченных файлах или документов;
- Возможность составления собственных словарей;

Распознавание изображений и документов:

- Наличие встроенного модуля OCR Tesseract4;
- Возможность распознавания перевернутых изображений;
- Возможность выбора следующих языков - русский и английский;
- Возможность распознавания следующих форматов - .pdf, .jpeg, .png;
- Возможность подключения облачного ABBYY Cloud OCR SDK.

Возможности панели администратора в web-интерфейсе:

Панель управления, со следующими возможностями:

- Возможность просмотра активных или готовых к установке компьютеров, с возможностью выбора конкретного или нескольких рабочих мест с выполнением следующих действий – выбор всех компьютеров, освобождение лицензии, назначение лицензии, автоматическое назначение лицензии, вызов деинсталляции агента, отмена деинсталляции агента, заблокировать или

разблокировать ПК, обновить агента до последней версии, отметить текущее обновление, установить агента, проверить агента, назначить свойства (выбор конфигурации и группы);

- Возможность скачать агента версии Windows и Linux, а также утилиты удаленной установки;
- Возможность установки в локальной сети, через Active Directory;
- Возможность удаления всех неустановленных агентов;
- Просмотр конфигураций пользователей, с возможностью изменения/удаления существующих или добавлением новых;
- Наличие конфигураций пользователя, с возможностью назначения по пользователю настройки правил использования USB/CD устройств;
- Наличие глобальной конфигурации, с возможностью настройки модулей мониторинга для всех пользователей, независимо от назначенной им конфигурации;
- Наличие параметров сервера, предназначенного для изменения базовых настроек веб-консоли;
- Наличие почтовых настроек, с возможностью настройки параметров отправки почты, которая используется для отправки отчетов и уведомлений по настроенным фильтрам;
- Наличие настроек AD;
- Наличие хранилища паролей для сохранения и редактирования паролей, использующихся при установке через веб-интерфейс;
- Возможность просмотра отображения разбиения базы данных по месяцам с возможностью удаления данных за выбранный месяц;
- Наличие панели администраторов с возможностью добавления, настройки или удаления учетных записей пользователей веб-консоли, а также распределять по администраторам права доступа и роли учетных записей;
- Возможность изменения настроек ролей учетных записей, добавлением новых или удаление существующих;
- Возможность просмотра все изменения, произведенные администраторами в веб-консоли;
- Возможность просмотра количества событий в очереди на обработку сервером с указанием названия политик и парсеров;
- Возможность выгрузки логов сервера, конфигурации агентов, правил мониторинга, фильтров и политик;
- Возможность просмотра информации о лицензии, сроков её активации и истечения, количестве компьютеров, которые могут подключаться к серверу и количество подключенных компьютеров;
- Возможность запуска пересчёта всех отчетов;
- Возможность удаления всех пользовательских настроек, с возвращением сервера к первоначальным настройкам;
- Возможность перезапуска всех служб, связанных со staffcop;
- Возможность выбора базы данных (Postgresql или Clickhouse)
- Возможность выбора языка веб-интерфейса (русский или английский)

- Возможность просмотра версии сервера, версии Windows и Linux агента;
- Возможность смены пароля администратора и завершения работы.

Поддерживаемые операционные системы для агента:

- Windows в 32-х или 64-х битном варианте с поддержкой следующих операционных систем – Windows XP SP3, Windows Vista SP2, Windows 7 SP2, Windows 8, Windows 8.1 SP1, Windows 10; а также поддержка работы терминальных серверов в следующих операционных системах – Windows 2008, Windows 2008 R2, Windows 2012 R2, Windows 2016;
- Linux с поддержкой следующих операционных систем – CentOS, Ubuntu Dekstop, Debian, Gentoo linux, Astra linux, Arch linux, Rosa linux, и другие Linux-like дистрибутивы;
- MacOS с поддержкой следующей операционной системой – Mac OS X 10.13X.

Поддержка операционных систем у утилиты удаленной установки следующих видах - Windows XP SP3, Windows Vista SP2, Windows 7 SP2, Windows 8, Windows 8.1 SP1, Windows 10;

Лицензирование производится по количеству одновременно активных рабочих станций или пользователей. Возможность гибкого лицензирования, с переустановкой лицензии с одной рабочей станции или пользователя, на другую рабочую станцию или пользователя неограниченное количество раз;