LibraSoft

DLP-системы

LibraDLP

www.librasoft.by

Почему информации нужна защита

В каждой компании есть информация, которая нуждается в особой защите, – бухгалтерская и финансовая отчетность, базы данных клиентов и сотрудников, маркетинговые документы. Когда закрытые сведения попадают в чужие руки (например, к конкурентам) или в публичный доступ, на кону – деньги и репутация.

Повсеместная цифровизация предприятий делает возможной утечку конфиденциальной информации через электронную почту, социальные сети, мессенджеры, блоги, форумы, публичные чаты, внешние носители и другие каналы передачи данных. Причем в центре инцидентов всегда стоит человек.

Защита ИТ-инфраструктуры компании от внешних и внутренних угроз – главная задача службы безопасности. Чтобы решить ее успешно, ИБ-специалистам необходимы современные инструменты.

LibraDLP – полный контроль над информацией

Контроль максимального количества каналов передачи данных.

Защита от злонамеренных и случайных утечек, мошенничества, откатов, воровства.

Сбор информации с помощью модулей перехвата.

Оперативное оповещение службы безопасности об инцидентах.

Автоматизированный анализ содержания информационных потоков.

Сбор доказательств в процессе внутренних расследований инцидентов.

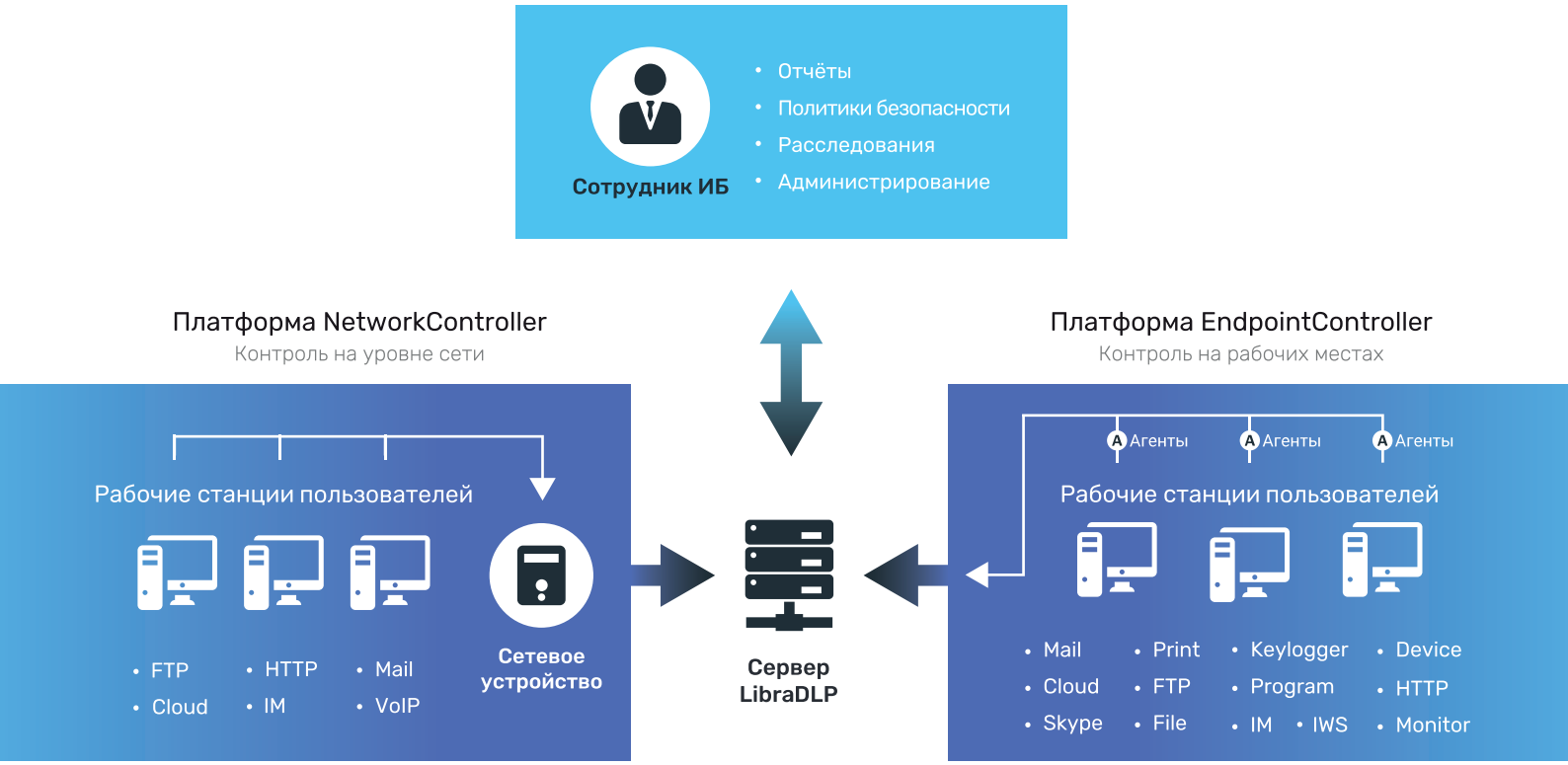
Выявление аномальных событий и нарушений внутри ИТ-инфраструктуры компании.

LibraDLP легко подстраивается под задачи конкретного бизнеса, благодаря масштабируемости, модульной архитектуре и гибкости настроек.

LibraSoft
DLP-системы

Управление LibraDLP

LibraDLP может работать на сетевой (NetworkController) или агентской (EndpointController) платформах. NetworkController осуществляет контроль на уровне сети – через подключение к сетевому оборудованию или корпоративным прокси-серверам. EndpointController собирает данные с каждой рабочей станции (компьютера) при помощи специальных агентов контроля.



В AlertCenter можно задать ключевые настройки LibraDLP. Компонент DataCenter служит для точечного управления системой.

AlertCenter

Анализирует информационные потоки, ведет журнал событий и уведомляет офицера безопасности об инцидентах в системе.

В AlertCenter задаются политики безопасности и правила, по которым ведется анализ контента. Специалист службы безопасности может использовать более 250 готовых политик, настраивая их под текущие задачи.

DataCenter

Контролирует работоспособность LibraDLP. В DataCenter можно разграничить права доступа сотрудников службы безопасности к собранной модулями перехвата информации, отчетам, настройкам системы.

Модули перехвата

LibraDLP состоит из модулей, каждый из которых защищает данные по определенному каналу передачи информации. Для лучшего контроля над информационными потоками заказчики используют модули контроля в связке.

MailController

Сканирует переписку в почтовых аккаунтах на Gmail, Outlook, Yandex.Mail, Office 365 и других веб-сервисах, которую пользователи просматривают на рабочих ПК. А также корпоративную почту. Проверяет входящие, исходящие письма и черновики на соответствие политикам безопасности.

IMController

Контролирует социальные сети и мессенджеры. Просматривает чаты, историю сообщений, звонки и контакты в Viber, WhatsApp, Telegram, Lync/Skype For Business, ICQ 10, QIP, а также переписку в Facebook, «ВКонтакте», «Одноклассники», Google+, LinkedIn.

FTPController

Следит за файлами большого объема, переданными через обычное (FTP) и шифрованное (FTPS) соединение. Предотвращает утечку баз данных, программ, отсканированных документов, проектной документации и чертежей.

Indexing workstation

Модуль для выявления конфиденциальных документов, которые хранятся с нарушением политик безопасности. Проверяет рабочие станции, серверы, папки общего доступа (Shares) и общие ресурсы на платформе SharePoint.

CloudController

Отслеживает данные, которые были приняты или отправлены в облачные сервисы и файлообменники. Контролирует платформы Google Docs, Office 365, Evernote, iCloud Drive, SharePoint, Dropbox, Яндекс.Диск, Amazon S3, DropMeFiles и другие.

KeyloggerController

Фиксирует ввод текста с клавиатуры (в том числе, перехватывает логины и пароли), а также данные, скопированные в буфер обмена. Определяет пользователей, которые вводили пароли к зашифрованным документам.

SkypeController

Наблюдает за активностью пользователей в Skype. Ведет перехват переписки, звонков, СМС и прикрепленных файлов. Видит историю сообщений, которые отправлены в Skype вне офиса.

ProgramController

Следит за действиями пользователя в приложениях на ПК (длительность сеанса и активность). Способен увидеть, что программа открыта «для вида». Собирает данные об интернет-серфинге: показывает, на каких сайтах и сколько времени провел пользователь. Сортирует посещаемые веб-ресурсы по тематическим группам (знакомства, музыка, магазины, новости, сайты поиска работы и другие).

DeviceController

Отслеживает данные, которые пользователи передают на USB-накопители, внешние диски, CD/DVD, камеры, сканеры и другие устройства. Запрещает доступ к определенным устройствам и портам, папкам и локальным дискам. Держит под контролем запуск ПО со съемных носителей. Шифрует информацию, которая была записана на съемные устройства, что делает невозможным ее прочтение на компьютерах вне офиса.

HTTPController

Отвечает за перехват и индексацию файлов и сообщений, переданных по HTTP/HTTPS-протоколам. Отслеживает запросы, заданные поисковым системам. Проверяет данные, которые отправлены в чаты, блоги, на форумы и через браузер. Не прекращает работу даже в случае использования сотрудниками сервисов-анонимайзеров.

PrintController

Собирает архив документов, отправленных на печать. Текстовые файлы – в копиях, изображения – в виде графических «отпечатков» и распознанного текста. Проверяет их содержимое, особо выделяя документы с печатью и бланки строгой отчетности.

MonitorController

Делает скриншоты и записывает видео активностей на мониторе. Регистрирует действия пользователя за компьютером с помощью веб-камеры в пределах ее обзора. Есть возможность онлайн-наблюдения за содержимым экрана (LiveView) и поведением пользователя (LiveCam).

FileController

Держит под контролем операции, которые пользователи производят с файлами на серверах и в общих сетевых папках – открытие, копирование, редактирование, удаление, изменение формата.

Анализ текста и отчеты

Для анализа больших массивов данных, собираемых в процессе перехвата, необходим удобный и понятный инструмент. В LibraDLP аналитическая функция передана компоненту AnalyticConsole.

Консоль позволяет генерировать отчеты по нужным параметрам – статистике инцидентов, активности пользователей, маршрутам перемещения документа, программам и оборудованию. Отчеты визуализируют события и связи внутри компании, что облегчает расследование инцидентов.

AnalyticConsole LibraDLP работает по различным поисковым алгоритмам:

- Поиск по словам и фразам;
- Поиск по тематическим словарям;
- Поиск по регулярным выражениям (например, серии и номеру паспорта);
- Поиск по цифровым отпечаткам;
- Поиск на основании количественных показателей (например, числу отправленных писем);
- Поиск похожих (возможность найти нужный документ, даже если в него внесли изменения);
- Поиск по комплексным запросам (простые запросы, объединенные логическими операторами И, ИЛИ, НЕ).

Анализ графики и аудио

Благодаря системе распознавания символов LibraDLP определяет документы установленных образцов – паспорта, платежные карты, водительские удостоверения и другие. Устанавливает тип изображений (скан или фотография) и категоризирует файлы.

Для быстрой оценки аудиофайлов на предмет соблюдения политики безопасности LibraDLP преобразовывает звук в текст.

Преимущества LibraDLP

Простота внедрения

Систему LibraDLP можно установить на мощностях заказчика за несколько часов. Эта задача под силу собственным IT-специалистам организации. Инсталлирование системы не влияет на работу компьютерной сети предприятия.

Контроль максимального количества каналов передачи данных

При установке всех модулей LibraDLP сможет контролировать все популярные каналы передачи информации.

Мощный аналитический инструмент для расследований

LibraDLP служит для сбора улик в случае обнаружения внутренних ИБ-угроз. В распоряжении службы безопасности компании запись переговоров, перехват содержимого мониторов, аудит файловых операций, контроль клавиатурного ввода и другие инструменты, которые позволяют восстановить преступление по шагам.

Разграниченный доступ

Доступ к перехваченным данным, отчетам и настройкам системы LibraDLP легко разграничить. За каждым специалистом службы безопасности можно закрепить особую наблюдательную роль.

Контроль человеческого фактора

Встроенный в систему модуль профайлинга позволяет оценивать потенциальные риски по каждому сотруднику, прогнозируя его поведение в нормальных, критических и стрессовых ситуациях. И в итоге предупредить ИБ-инцидент.

Гарантированная защита данных

Архив перехваченной информации хранится на внутреннем сервере заказчика. Никто более не имеет к нему доступа.

В случае установки системы в удаленных филиалах заказчика, собранные данные передаются на основной сервер в зашифрованном виде.

Информационная поддержка и обучение

Всем клиентам LibraDLP доступна консультативная помощь отдела внедрения. Специалисты компании помогут настроить политики безопасности под конкретные задачи с учетом специфики рынка, на котором работает заказчик.

На базе компании работает учебный центр, где сотрудники заказчика могут пройти обучение для актуализации знаний в информационной безопасности.

Беларусь
Минск
220040, пер. М. Богдановича, д. 1, эт. 2, каб. 3
Телефон: + 375 (17) 227-56-80
Email: official@librasoft.by