КИБЕР ПРОТЕКТ

CYBER Protego

Полнофункциональное решение для предотвращения утечки данных (DLP)

Высочайшие темпы развития ИТ, электроники и телекоммуникаций в сочетании с активным проникновением в корпоративную информационную среду «личных» вычислительных устройств и программ для персонального использования привели к значительному упрощению бизнес-процессов, возможности удаленной работы, и главное - к упрощению доступа к корпоративным данным. В то же время предоставление сотрудникам организаций такого широкого доступа к данным значительно повышает риски непреднамеренной или умышленной утечки конфиденциальной информации.

Попадание конфиденциальных данных в руки неуполномоченных лиц может привести к серьезному финансовому и репутационному ущербу, утрате коммерческой тайны, а также к штрафам и судебным разбирательствам.

Использование сотрудниками любых устройств, таких как флэш-накопители и принтеры, или веб-сервисов, включая электронную почту, социальные сети, мессенджеры и другие ресурсы, доступные на персональном уровне и не требующие обслуживания корпоративными службами ИТ – наиболее простой и вероятный сценарий утечки данных.

Cyber Protego (Кибер Протего)

Программный комплекс Cyber Protego – это специализированное решение для предотвращения утечки данных с корпоративных компьютеров, серверов и виртуальных сред. Cyber Protego использует различные методы контроля данных – как контекстные, так и основанные на анализе содержимого в режиме реального времени, обеспечивая надежную защиту от утечек информации при минимальных затратах на приобретение и обслуживание комплекса.

Комплекс Cyber Protego построен в виде модульной архитектуры, состоящей из опциональных компонентов, лицензируемых в различных комбинациях, что позволяет клиентам выбрать оптимальную конфигурацию DLP-решения в соответствии со своими требованиями к обеспечению безопасности и бюджетом.

Преимущества

Безопасность

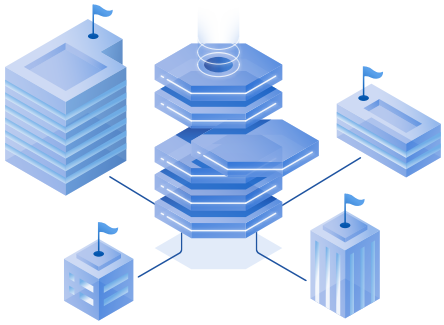
- Снижение рисков инсайдерской утечки информации
- Блокировка недопустимых попыток передачи данных
- Авторизация только необходимых для бизнес-процессов операций

Эффективность

- Полное соответствие DLP-политик корпоративной политике информационной безопасности
- Мониторинг событий, теневых копий и активности пользователей
- Мощные и наглядные инструменты анализа и построения отчетов

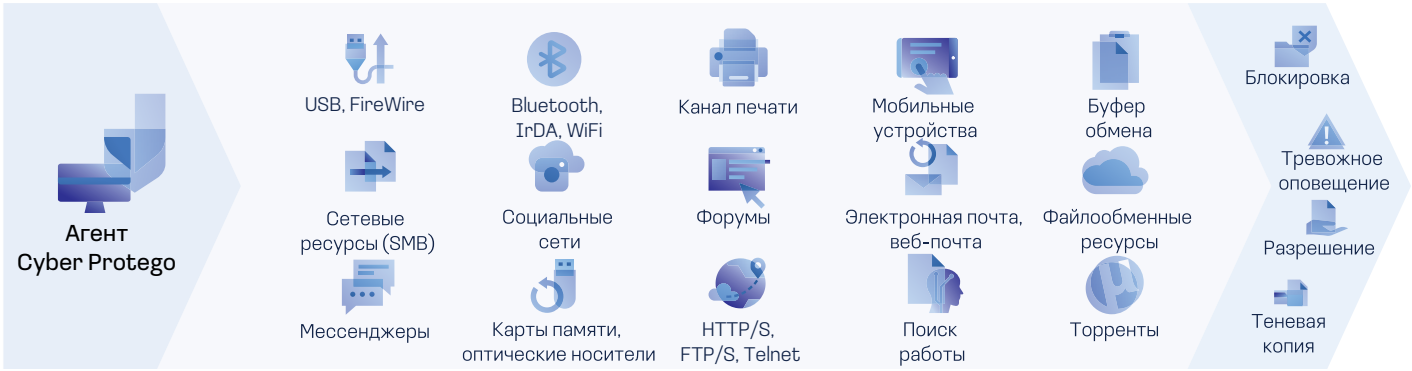
Простота и удобство

- Единое централизованное управление
- Полная интеграция с AD
- Модульная архитектура и гибкое лицензирование



© ООО “Киберпротект”, 2022.

Компоненты комплекса Cyber Protego



Базовый **Device Control**

Обеспечивает гибкий контекстный контроль доступа пользователей к локальным каналам передачи данных, а также ведение журнала событий, теневое копирование данных и тревожные оповещения. Контроль обеспечивается для всего спектра периферийных устройств, портов и интерфейсов (USB, FireWire, COM, LPT, IrDA), системного буфера обмена, подключенных мобильных устройств, MTP-устройств, канала печати, а также перенаправленных в терминальные сессии устройств.

Опциональный **Web Control**

Обеспечивает гибкий контекстный контроль сетевых коммуникаций пользователей через распространенные сетевые протоколы и сервисы, включая веб-браузинг, электронную и веб-почту, мессенджеры, облачные хранилища, социальные сети, сетевые протоколы SMB, FTP и многое другое. Также обеспечивает ведение журнала событий, теневое копирование переданных данных и тревожные оповещения. Благодаря использованию технологии DPI на уровне агента распознавание сетевых протоколов, детектирование приложений и их селективная блокировка выполняются независимо от типов сетевых приложений и веб-браузеров.

Опциональный **User Activity Monitor**

Обеспечивает мониторинг действий пользователя в целях расширения доказательной базы при расследовании инцидентов ИБ, упрощения процессов выявления подозрительного поведения пользователей. Выполняются видеозапись экрана, запись нажатий клавиш, сохранение информации о процессах и приложениях. Активация мониторинга действий возможна по заданным событиям, например, при обнаружении указанного содержимого, подключении внешнего накопителя, изменении состояния сетевого подключения и т.д.

Опциональный **Content Control**

Осуществляет контентный анализ и фильтрацию данных, перехваченных компонентами Device Control (Контроль Устройств) и Web Control (Контроль Сетевых Коммуникаций) - файлов, передаваемых на съемные носители, иные Plug-and-Play устройства, печатаемых на любых принтерах, объектов данных, передаваемых по сетевым каналам связи. Анализ содержимого выполняется в режиме реального времени непосредственно на контролируемом компьютере, не зависит от подключения к корпоративной инфраструктуре. Применяются такие технологии контентного анализа, как анализ по цифровым отпечаткам с поддержкой классификации образцов, поиск по ключевым словам с применением морфологического анализа, по встроенным комплексным шаблонам регулярных выражений (RegExp), инспекция расширенных свойств документов и файлов и др. В компонент также встроен резидентный модуль OCR.

Автономный **Cyber Protego Discovery**

Обеспечивает автоматическое сканирование рабочих станций, корпоративных сетевых ресурсов, баз данных Elasticsearch в целях выявления и устранения нарушений корпоративной политики хранения данных ограниченного доступа посредством предопределенных автоматических корректирующих действий с обнаруженными файлами, а также инициирования процедур управления инцидентами.

Опциональный **Search Server**

Обеспечивает автоматизированный полнотекстовый поиск по централизованной или распределенной базе данных теневого копирования и событийного протоколирования. Использование Сервера поиска позволяет сделать трудоемкие процессы аудита информационной безопасности, расследования инцидентов и криминалистического анализа более точными, удобными и оперативными.

© ООО “Киберпротект”, 2022.

Ключевые функции Cyber Protego

Cyber Protego предоставляет обширный набор технологий предотвращения утечки данных, позволяющий обеспечить надежную защиту корпоративной информации и соблюдение нормативных требований.

Централизованное управление

Система содержит все инструменты, необходимые для централизованного развертывания и управления DLP-системой в организациях любого размера и для любого типа ИТ-инфраструктуры. Полная интеграция централизованного управления в групповые политики домена Active Directory позволяет легко масштабировать систему в инфраструктурах любых размеров - Cyber Protego использует Active Directory в качестве собственной платформы управления DLP без изменения схемы домена, использования скриптов. В недоменных средах или при невозможности использовать групповые политики роль управляющего сервера может исполнять Cyber Protego Management Server.

Технология Cyber Protego TS

Обеспечивает предотвращение утечек данных при использовании решений для виртуализации рабочих столов и приложений, таких как Citrix XenApp / XenDesktop, Microsoft RDS и VMware Horizon View. Универсальная для любых видов терминалов защита данных от утечек для виртуализованных рабочих сред (VDI), терминальных сессий рабочих столов и приложений достигается за счет применения эффективного сочетания возможностей контекстного контроля и уникальных для DLP-отрасли механизмов контентной фильтрации, работающих в режиме реального времени, при передаче данных на накопители, через системный буфер обмена и периферийные USB-устройства, перенаправленные в сессию с удаленных терминалов. Более того, сетевые коммуникации пользователей внутри терминальной сессии также могут контролироваться DLP-механизмами Cyber Protego.

Белые списки и исключения

В ситуациях, когда требуется индивидуальный подход к контролю доступа, Cyber Protego предлагает Белые списки для USB-устройств и сетевых протоколов, а также Временный белый список для предоставления доступа к устройству при отсутствии сетевого подключения. Белый список USB-устройств позволяет идентифицировать устройства по производителю, модели или уникальному серийному номеру и назначать их для заданных пользователей и групп. Белый список сетевых протоколов позволяет гибко предоставлять доступ отдельным пользователям только к тем сервисам и узлам, которые необходимы им для работы, и может детализироваться по IP-адресам, их диапазонам и маскам подсетей, а также по сетевым портам и их диапазонам.

Аудит событий

Cyber Protego предлагает исчерпывающую, масштабируемую подсистему протоколирования событий с автоматическим сбором журналов в централизованную СУБД MS SQL, SQL Express или PostgreSQL, с поддержкой консолидации журналов для распределенных архивов событий. Также доступна опция использования стандартной подсистемы событийного протоколирования Windows.

Функция аудита событий в Cyber Protego позволяет протоколировать все действия пользователей с различными типами устройств, портов и сетевых коммуникаций на контролируемых компьютерах, а также административные события (изменения в настройках агента, время его старта и остановки). Для просмотра событий предусмотрены обширный набор встроенных и настраиваемых фильтров, а также экспорт журнала событий.

Теневое копирование

В дополнение к подсистеме событийного протоколирования Cyber Protego обладает исключительно гибкой подсистемой создания и хранения теневых копий. Функция теневого копирования в Cyber Protego позволяет для заданных пользователей или групп сохранять точную копию данных, копируемых на внешние устройства, передаваемых через последовательные и параллельные порты, печатаемых на локальных и сетевых принтерах, а также передаваемых по каналам сетевых коммуникаций. Точные копии всех файлов и данных сохраняются в централизованном или распределенном архиве на основе SQL-базы данных.

Технологии контентной фильтрации Cyber Protego позволяют выборочно сохранять копии только тех документов и объектов, которые значимы для задач аудита информационной безопасности, расследований нештатных ситуаций и инцидентов, а также исключить из теневого копирования данные, которые недопустимо централизованно хранить и обрабатывать, например, частные данные сотрудников.

© ООО “Киберпротект”, 2022.

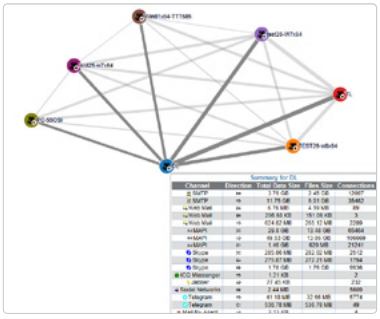
Тревожные оповещения

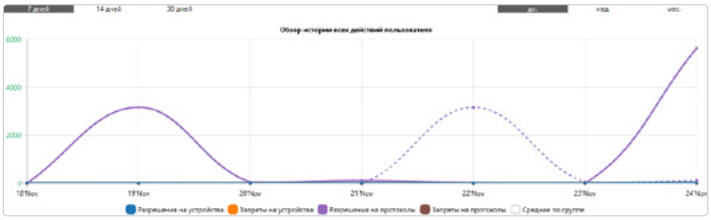
Cyber Protego предлагает возможность использования протоколов SNMP, SYSLOG и SMTP в целях оперативного уведомления служб ИБ в реальном времени о значимых действиях пользователей. Тревожные оповещения в Cyber Protego также могут рассматриваться как альтернатива встроенному аудиту событий или функционировать одновременно с ним.

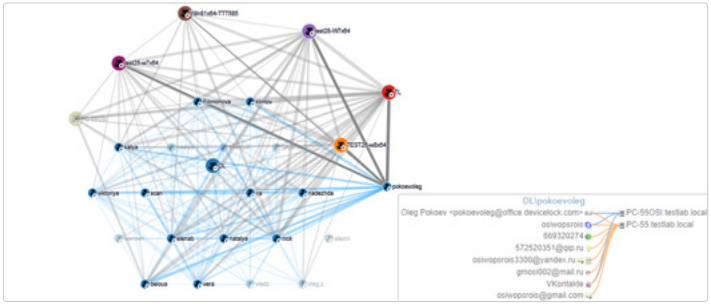
Отчеты

Cyber Protego позволяет создавать сводные статистические и графические отчеты, в том числе динамический Граф связей и Пользовательские досье, на основе централизованно хранимых журналов аудита и теневого копирования. Отчеты могут автоматически отсылаться на заданный адрес электронной почты.

Пользовательские досье позволяют существенно упростить аудит информационной безопасности и повысить прозрачность потоков данных и связанных с ними действий посредством статистического обзора действий пользователей с наглядным графическим представлением. В целях мониторинга и оценки различных аспектов поведения пользователя, этот вид отчета содержит также такие статистические показатели, как частота попыток совершения несанкционированных операций, передача больших объемов данных, изменение характера онлайн-активности и т.д.







Интеграция с внешними средствами шифрования

Cyber Protego использует принцип открытой интеграции с внешними средствами шифрования данных на съемных носителях, что позволяет нашим клиентам использовать лучшие технологии и продукты для шифрования, включая Windows BitLocker To Go, macOS FileVault, Sophos SafeGuard, Symantec Drive Encryption, SecurStar DriveCrypt, TrueCrypt, Инфотекс SafeDisk и Рутокен Диск.

Контроль по типу файлов

Cyber Protego позволяет контролировать доступ пользователей к операциям с файлами в зависимости от их типов (форматов). Определение типов файлов основано на сигнатурном методе и не зависит от расширения файла.

ПОДДЕРЖИВАЕМЫЕ СРЕДЫ

Агенты и консоли управления

- Windows 7/8/8.1/10
- Windows Server 2008-2019 (32/64-bit)
- Apple macOS 10.15 - 11.2.3 (32/64-bit)

Management Server, Search Server, Discovery

- Windows Server 2008-2019 (32/64-bit)

Среды виртуализации/VDI

- Microsoft RDS, Citrix XenDesktop/XenApp, XenServer, VMware Horizon View
- VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC

Интеграция со службами каталогов

- Microsoft Active Directory (полная интеграция)
- NetIQ (Novell) eDirectory и любые другие LDAP (импорт объектов)

Базы данных

- Microsoft SQL Server Express 2005 и выше
- Microsoft SQL Server 2005 и выше
- PostgreSQL 9.5 и выше

КИБЕР ПРОТЕКТ

Больше информации
www.cyberprotect.ru

© ООО "Киберпротект", 2022. Все права защищены. Наименование и логотип Киберпротект являются товарными знаками компании. Прочие товарные знаки и зарегистрированные товарные знаки являются собственностью соответствующих владельцев. Технические изменения и отличия от иллюстраций возможны. 2022-03