КИБЕР ПРОТЕКТ

КИБЕР Протего

Полнофункциональное решение для предотвращения утечки данных (DLP)

Не дайте информации утечь сквозь пальцы!

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 цифровизации многих бизнес-процессов, возможности удаленной работы, и главное - к упрощению доступа к корпоративным данным. В то же время, это значительно повысило риски непреднамеренной или умышленной утечки конфиденциальной информации, что может привести к серьезному финансовому и репутационному ущербу, утрате коммерческой тайны, а также к штрафам и судебным разбирательствам.

Наиболее простой и вероятный сценарий утечки данных - использование сотрудниками устройств, таких как флеш-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.

Почему Кибер Протего

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

Преимущества

Безопасность

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

Эффективность

- Полное соответствие DLP-политик корпоративному стандарту информационной безопасности
- Мониторинг событий и активности пользователей, создание точных копий передаваемых данных с хранением их в централизованном журнале системы
- Удобные инструменты интерактивного анализа действий пользователей и построения наглядных отчетов

Простота и удобство

- Единое централизованное управление DLP-агентами для Windows, macOS и Linux
- Полная интеграция с Active Directory
- Распределенный архив событий без дополнительных затрат
- Модульная архитектура и гибкое лицензирование

Ключевые функции Кибер Протего и сценарии применения

Кибер Протего — это мощный инструмент для надежной защиты корпоративной информации и исполнения нормативных требований. Продукт содержит обширный набор DLP-технологий и позволяет обеспечить предотвращение утечки данных и полномасштабный мониторинг потоков данных и активности пользователей.

Контроль устройств

Гибкий контроль доступа пользователей к локальным каналам передачи данных позволяет обеспечить реализацию любых концепций и подходов к контролю устройств, включая концепцию нулевого доверия, и предотвращение утечки данных через весь спектр периферийных устройств, портов и интерфейсов, системный буфер обмена, MTP-устройства и канал печати.

Контроль сетевых коммуникаций

Избирательный контроль сетевых коммуникаций позволяет предотвратить утечку информации по таким каналам, как электронная и веб-почта, мессенджеры, облачные сервисы обмена файлами, социальные сети, различные сетевые протоколы и другие средства коммуникаций. Благодаря использованию технологии DPI на уровне агента, распознавание сетевых протоколов, детектирование приложений и их выборочная блокировка выполняются независимо от типов сетевых приложений и веб-браузеров.

> Кибер Протего 10.0 обеспечивает контроль USB-устройств и съемных накопителей, включая избирательный контроль доступа, протоколирование, Белый список USB-устройств для ОС Альт Рабочая Станция 10

Контентный анализ данных в реальном времени

В сценариях, когда требуется своевременное выявление конфиденциальных данных, а контроль на уровне устройств или сетевых сервисов является недостаточным, Кибер Протего позволяет использовать механизмы принятия решений на основе анализа содержимого передаваемых данных. Кибер Протего обеспечивает контентный анализ и фильтрацию данных для файлов, записываемых на съемные носители, иные PnP-устройства, объектов данных, передаваемых по сетевым каналам связи, и печатаемых документов. Контентная фильтрация выполняется в режиме реального времени непосредственно на контролируемом компьютере и не зависит от наличия подключения к корпоративной инфраструктуре. Для этого применяются различные технологии анализа содержимого – поиск по ключевым словам с применением морфологического анализа, по комплексным шаблонам регулярных выражений (RegExp), проверка расширенных свойств документов и файлов, сигнатур типов файлов и др. Анализ по цифровым отпечаткам с поддержкой классификации образцов - наиболее мощная технология, позволяющая минимизировать количество ложных срабатываний и не требующая длительного предварительного обследования организации. Кроме того, встроенный модуль OCR делает возможным извлечение и анализ текста в изображениях.

Контроль передачи данных в терминальных сессиях

Виртуализация рабочих станций и серверов совместно с удаленным доступом к приложениям и данным стали ключевым трендом. Для полноценной защиты корпоративных данных от утечки при использовании терминальных сессий необходим развитый контроль каналов перемещения информации между корпоративной средой и удаленными терминалами. Технология контроля терминальных сессий Cyber Protego TS не имеет аналогов на рынке DLP-решений. Она позволяет обеспечить универсальную защиту данных от утечки для виртуализованных рабочих сред (VDI), терминальных сессий рабочих столов и приложений (Citrix XenApp / XenDesktop, Microsoft RDS и VMware Horizon View). Это становится возможным за счет эффективного сочетания возможностей контекстного контроля и уникальных механизмов фильтрации содержимого, которые работают в режиме реального времени при передаче данных на накопители, через системный буфер обмена и периферийные USB-устройства, перенаправленные в сессию с любых удаленных терминалов, от толстых клиентов до мобильных устройств. Более того, Кибер Протего позволяет контролировать сетевые коммуникации и активность пользователей внутри терминальной сессии.

Мониторинг событий, анализ журналов и оперативное реагирование на инциденты

Выделение, хранение и обработка событий, связанных с передачей данных, а также действий пользователей являются важнейшими задачами любой DLP-системы. Кибер Протего позволяет протоколировать все действия пользователей с различными типами устройств, портов и сетевых коммуникаций на контролируемых компьютерах, административные события, создавать точные копии данных, переданных по сети или через буфер обмена, записанных на флеш-накопители файлов и распечатанных документов, а также направлять тревожные уведомления для оперативного реагирования на инциденты или автоматизированной обработки в корпоративной SIEM-системе.

Для хранения и обработки событий в Кибер Протего реализован автоматический сбор журналов в централизованный архив событий и теневых копий, с поддержкой консолидации журналов для создания полного архива событий всей организации с филиальной структурой.

Наглядное графическое представление данных из архива событий в различных форматах - от статистических отчетов до интерактивных Графов связей и Досье пользователя - позволяет построить качественный процесс аудита информационной безопасности, своевременно обнаруживать риски утечки данных и расследовать произошедшие инциденты, оперативно выявлять злоумышленников и отклонения в поведении пользователей по сравнению со среднестатистическими показателями. Формируемые системой отчеты могут автоматически отправляться на заданный адрес электронной почты, в том числе и по расписанию.

Теневые копии файлов и данных создаются избирательно как для заданных пользователей, так и на основании анализа содержимого. Это позволяет выборочно сохранять в централизованном архиве DLP-системы копии только тех документов и объектов, которые значимы для задач аудита информационной безопасности, расследований нештатных ситуаций и инцидентов. В то же время, можно исключить из теневого копирования данные, которые недопустимо централизованно хранить и обрабатывать - например, частные данные сотрудников.

Мониторинг активности пользователей

Мониторинг действий пользователей (UAM) позволяет расширить доказательную базу при расследовании инцидентов ИБ, а также упростить процессы выявления подозрительного поведения пользователей. Система Кибер Протего обеспечивает возможность видеозаписи экрана и записи нажатий клавиш, а также протоколирование информации о запущенных процессах и приложениях. Запись включается по заданным событиям, причем с записью как до, так и после наступления определенного события. Так, можно получить видеозапись экрана при попытке передачи конфиденциального документа, подключении внешнего накопителя и т.д.

Контроль хранимых данных

Своевременное выявление и устранение нарушений корпоративной политики хранения данных дает возможность минимизировать риски утечки информации. Кибер Протего позволяет запускать автоматическое сканирование рабочих станций и серверов, а в случае выявления нарушений – журналировать и автоматически устранять их посредством выполнения предопределенных корректирующих действий, а также инициировать процедуры управления инцидентами.

Преимущества Кибер Протего

Белые списки и исключения

Для сценариев, когда необходим индивидуальный подход к контролю доступа, в Кибер Протего реализованы 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.

Масштабируемость централизованного управления и архива событий

Кибер Протего легко масштабируется в организациях любого размера и для любого типа ИТ-инфраструктуры. Для этого в системе реализованы разные варианты централизованного развертывания и управления, в том числе полная интеграция в групповые политики домена Active Directory. В этом сценарии Кибер Протего использует Active Directory в качестве платформы управления DLP без изменения схемы домена и использования скриптов. В средах без доменов или при невозможности использовать групповые политики роль управляющего сервера может выполнять собственный Сервер управления. Кроме того, с помощью встроенных механизмов консолидации данных Сервер управления позволяет собирать события и теневые копии в модели распределенного архива, с автоматической передачей данных с серверов филиалов в централизованный архив организации.

Работа агента вне зависимости от доступности сервера управления

В ситуациях, когда контролируемый компьютер находится вне корпоративной сети и связь между сервером и агентом невозможна, полностью защищенный от вмешательства пользователя агент Кибер Протего обеспечивает все функции защиты, заданные в DLP-политике – от контроля доступа до контентной фильтрации, и сохраняет сгенерированные события и теневые копии до восстановления связи с сервером.

Интеграция с внешними средствами шифрования

Кибер Протего поддерживает принцип открытой интеграции с внешними средствами шифрования данных на съемных носителях, что позволяет использовать широко распространенные технологии и продукты для шифрования, включая Windows BitLocker To Go, macOS FileVault, Инфотекс SafeDisk, Рутокен Диск и другие.

Почему Киберпротект

Киберпротект — российский разработчик систем резервного копирования, защиты от утечки данных (DLP) и инфраструктурного программного обеспечения. Решениями компании пользуются организации любого масштаба, которые заинтересованы в надежной киберзащите, сохранности данных и работоспособности ИТ-инфраструктуры.

ПОДДЕРЖИВАЕМЫЕ СРЕДЫ

Агенты и консоли управления

- Windows 7/8/8.1/10/11
- Windows Server 2008R2-2022 (32/64-bit)
- Альт Рабочая Станция 10 (64-bit)
- Apple macOS 10.15 - 11.2.3 (32/64-bit)

Management Server, Search Server, Discovery

- Windows Server 2008R2-2022 (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 2012 и выше
- Microsoft SQL Server 2012 и выше
- PostgreSQL 11.5 и выше

КИБЕР ПРОТЕКТ

Больше информации
www.cyberprotect.ru