Ivanti Device Control

Утечка данных, вызванная случайным или иногда злонамеренным использованием съемных устройств и / или съемных носителей, достигла тревожных показателей. Ivanti® Device Control применяет политики безопасности при использовании съемных устройств и шифровании данных. Решение централизует управление устройствами и данными с использованием подхода «белый список» или «по умолчанию», а также обеспечивает дополнительный уровень защиты от вредоносного ПО, вводимого с помощью физических средств.

Защитите свои данные

С большим количеством сотрудников, работающих удаленно, требуется доступ из-за пределов сети. Но потенциальное влияние потери данных, будь то случайное или злонамеренное, вызывает серьезную озабоченность. Сегодня съемные носители / устройства являются наиболее распространенными маршрутами утечки данных: нет ограничений на копирование файлов, отсутствие шифрования, отсутствие контрольных маршрутов и отсутствие управления. Ivanti Device Control позволяет безопасно использовать такие инструменты, не снижая производительность, но ограничивая возможности утечки данных.

Ключевые характеристики

Белый список разрешенных устройств

Создание разрешений для авторизованных съемных носителей для отдельных пользователей, либо групп пользователей. На первом этапе в «режиме аудита» для проверки корректности политик, затем переход в «режим защиты».

Принудительное шифрование

Централизованно шифрует съемные устройства (например, USB) и носители (такие как DVD-диски), а также применяет политики шифрования при копировании на устройство.

Ограничение копирования данных

Ограничивает ежедневный объем данных, копируемых на съемные устройства и носители для каждого пользователя

Фильтрация по типу файла

Контролирует типы файлов, которые могут перемещаться на и со съемных устройств для каждого пользователя

Централизованное управление

Консоль определяет и управляет пользователями, группами пользователей, компьютерами и группами компьютеров доступ к авторизованным съемным устройствам / медиа в сети. По умолчанию этим устройствам и пользователям, явно неразрешенным, запрещается доступ.

Доступ по расписанию

Предоставляет пользователям временный / запланированный доступ к съемным, чтобы предоставлять доступ «в будущем» на ограниченный период времени.

Контекстные ограничения

Политики доступа / использования остаются в силе вне зависимости от состояния соединения и могут быть адаптированы, связана ли конечная точка с сетью или нет.

Ролевой контроль доступа

Назначает разрешения отдельным пользователям или группам пользователей на основе их идентификатора Windows Active Directory или Novell eDirectory, оба из которых полностью поддерживаются.

Агент защиты от несанкционированного доступа

Устанавливает агенты на каждой конечной точке в сети. Агенты защищены от несанкционированного удаления - даже пользователями с административными правами. Администраторы устройств могут отключать эту защиту.

Гибкая, масштабируемая архитектура

Обеспечивает общесистемный контроль и обеспечение соблюдения с использованием масштабируемой архитектуры клиент-сервер с центральной базой данных, оптимизированной для производительности. Поддержка виртуализированных конфигураций сервера.

Как работает Ivanti Device Control

1. **Обнаружение:** все съемные устройства, которые в настоящее время подключены или когда-либо были подключены к вам.
2. **Определение:** все устройства “plug and play” по классу, группе, модели и / или конкретному идентификатору и определяя политику с помощью белого списка.
3. **Внедрение:** ограничения на копирование файлов, фильтрацию типов файлов и политики принудительного шифрования для данных, перемещаемых на съемные устройства.
4. **Мониторинг:** все изменения политики, действия администратора и передачи файлов для обеспечения непрерывного применения политики.
5. **Отчетность:** на устройстве и использовании данных для документирования соответствия корпоративной и / или регулирующей политике.

«Одним из основных преимуществ при развертывании Ivanti Device Control является его функция «белый список», которая гарантирует, что никакое устройство, если оно не разрешено, никогда не будет использоваться, независимо от того, как оно подключается. USB-устройства представляют значительный риск с возможностью украсть данные компании или ввести «вредоносное ПО», что может сделать компьютер непригодным для использования и быстро заразить другие ПК в одной сети. Именно поэтому Barclays выбрал это решение»

Пол Дуглас
ADIR Desktop Build Team Manager
Barclays

Узнайте о преимуществах Ivanti Device Control

- Защищает данные от потери / кражи
- Обеспечивает безопасное использование инструментов повышения производительности
- Повышает эффективность политики безопасности
- Обеспечивает точное управление с ограничениями доступа
- Предотвращает проникновение вредоносного ПО через физические средства / отображение централизованных и децентрализованных структур управления
- Позволяет осуществлять мониторинг всех передач файлов на принтеры и физические носители

www.ivanti.ru

7.495.737.4814

contact@ivanti.ru