Product Datasheet
Ivanti Application Manager

Достижение баланса между IT стандартами и требованиями бизнеса

Ключевые функции:

- Точечное повышение прав доступа Windows
- Запрос повышения уровня доступа по требованию
- Мониторинг на корпоративном уровне
- Гибкие возможности настройки
- Ограничение доступа в зависимости от типа устройства, местоположения и т.д.
- Контроль доступа по сети
- Контроль лицензий на ПО
- Мониторинг в фоновом режиме
- Встроенные отчеты и аудит

Ключевые преимущества:

- Внедрение в желаемом подразделении
- Соблюдение лицензирования в соответствии с требованиями
- Уменьшение количества обращений в службу поддержки
- Удовлетворенность пользователей
- Широкие возможности контроля прав
- Повышение контроля Windows 10

Об Ivanti

Ivanti является лидером в области решений UEM для защиты безопасности информации. Технологии Ivanti позволяют ИТ службе упростить и обезопасить контроль за рабочими станциями (физическими, виртуальными и облачными). Решения Ivanti соиспользуются в 3,600 компаниях по всему миру и насчитывают более 9 миллионов рабочих станций в сумме.

Больше информации на сайте

http://www.ivanti.ru/

Права доступа пользователей

Использование неавторизованного ПО может внести негативные изменения в работу компьютера и тем самым усложнит работу ИТ службы по устранению неисправностей, поэтому крайне важно ограничить возможность запуска нежелательного программного обеспечения.

Существующие методы сводятся к использованию комплексных скриптов или белых/черных списков.

Владелец файла Trusted OwnershipTM

Благодаря включению функции фильтрации на уровне ядра ОС и использования s and Microsoft NTFS security policies, Ivanti Applica- tion Manager перехватывает все запущенные запросы и блокирует запуск нежелательных приложений. Запуск приложений реализован по принципу собственника приложения или файла. Если владелец файла “Доверенный Владелец/Trusted Owner» к числу которых относятся и администраторы, то запуск разрешен. Каждое приложение имеет владельца, учетная запись администратора входит в список владельцев по умолчанию. Используя данный подход, процесс контроля доступа приложений можно реализовать с первых дней эксплуатации системы, он доступен в коробочной версии продукта и не требует создания многоступенчатого процесса ввода белых списков приложений В дополнение к исполняемым файлам, Ivanti Application Manager также поддерживает работу с другими методами исполнения, такими как: ActiveX, VB-скрипты, bat-файлы, MSI и файлы конфигурации реестра reg.

Управление привилегиями

Функция контроля доступа с высокой точностью предоставляет пользователям возможность запуска только одобренных приложений. Исключив необходимость использования аккаунта локального администратора, Ivanti управляет правами доступа, которые могут быть повышены, понижены или вообще удалены у конкретного пользователя, приложения или задания.

Контроль доступа к ресурсам

В дополнении к управлению приложениями, Ivanti Application Manager также поддерживает функцию ограничения доступа к файловым ресурсам и URL, предоставляя единое решение для контроля доступа к ресурсам.

Правила подключения, адреса ссылок и приложения могут быть настроены через пользовательский интерфейс.

Ограничения доступа по типу устройству иместоположению

Уровень доступа может отличаться в зависимости от типа устройства. Например, у пользователя, подключившегося через публичную Wi-Fi сеть, уровень доступа будет отличаться от сотрудника, находящегося в защищенной корпоративной сети. Ivanti Application Manager использует информацию, такую как местонахождение устройства, тип подключения к сети, а также время для ограничения доступа к приложениям.

Поддержка работы в режиме оффлайн

Благодаря поддержке автономной работы функционал контроля приложений доступен для пользователей, неподключенных к корпоративной сети.

Управление лицензиями

Ivanti Application Manager признан компанией Microsoft® в качестве эффективного инструмента для отслеживания и контроля используемых лицензий. Запуск агента в режиме аудита позволяет отслеживать и получать детальные отчеты об использовании продуктов. Контролируя, каким пользователям и устройствам предоставлен доступ на запуск программных продуктов, можно установить ограничения на количество запусков, тип устройства или группу пользователей, а также установить ограничения по времени.

Product Datasheet
Ivanti Application Manager

Преимущества Ivanti Application Manager:

Режим анализа прав доступа

Анализ приложений, требующих административный доступ и оперативное внесение изменений в конфигурацию агента.

Запрос повышения уровня по требованию

Пользователи смогут самостоятельно запросить доступ напрямую из контекстного меню при запуске приложения. Служба технической поддержки получит заявку и сможет предоставить доступ на постоянной или временной основе.

Пассивный мониторинг

Контроль использования приложений; эта функция может быть активирована к учетной записи пользователя, устройству или группе и предоставит полезную информацию для точного отслеживания потребностей бизнеса. Вы сможете понять, какие приложения используются и построить дальнейшее управление лицензиями.

Endpoint анализ

Определение исполняемых файлов на устройстве для дальнейшего создания и управления списками авторизованных и неавторизованных программных продуктов. Сформированные списки могут быть применены к учетной записи пользователя или устройству, как к одному, так и группе из нескольких. В течение пары минут приложение получит обновленную конфигурацию.

Сканирование используемых приложений

Просканируйте устройство и выясните, сколько раз конкретное приложение запускается одним пользователем. Выявите приложения, которые не используются, удалите нелицензированное программное обеспечение и снизьте затраты на их использование.

Белые и черные списки

В дополнение к уникальной технологии Trusted Ownership могут также использоваться стандартные «белые» списки для контроля приложений. Приложения, к которым пользователи не должны иметь доступ такие как командная строка cmd.exe или ftp.exe, запрещены по умолчанию. Вы также можете создать «белый» список для гарантии запуска приложения и создания единого доверенного источника приложений.

Цифровые подписи

Создание хэш функций SHA-1, SHA-256 или ADLER32 для приложений или файлов для того, чтобы убедиться в их совместимости. Модифицированные или поддельные приложения не будут запущены.

Расширенная поддержка файлов

В дополнение к отслеживанию файлов с расширением .exe, также контролируются скрипты, пакетные и файлы реестра. Хэш может быть применен к скриптам для предотвращения внесения изменений.

Ограничения приложений и сессий

Поддержка политик ограничения количества запущенных копий приложений и времени их использования. Политика может быть создана для различных сценариев, например, для контроля и соблюдения ограничения приложений только для одного устройства.

Контроль доступа по сети

Вы можете контролировать подключения к IP адресам, URL ссылкам, FTP серверам и любым устройствам с помощью специальных правил. Нет необходимости отслеживать доступы через сетевое оборудование, такое как роутеры, коммутаторы и межсетевые экраны.

Гибкая настройка

Ivanti Application Manager позволяет получить высокий уровень контроля инфраструктуры с использованием специальных правил. ИТ департамент может создать несколько подобных правил, которые используют такие условия и параметры как версия ОС, наличие Файла/значения реестра, а также тип устройства, что позволяет получить качественный результат и увеличить эффективность выборки.

URL- перенаправление

Если браузер остался открытым на веб-странице или веб-приложении и пользователь производит повторное подключение с другого устройства, браузер может перенаправить по заранее определенному безопасному адресу.

Самостоятельное повышение уровня доступа

Позвольте специально выбранным пользователям самостоятельно запускать необходимые сервисы. Приложения могут быть добавлены даже без присутствия в офисе и без участия IT поддержки.

Вы сможете получить отчет, где будет содержаться подробная информация: название приложения, устройство, дата и время запуска. Более того, копия приложения может быть сохранена для аудита.

Права на установку веб-приложений и плагинов

Контролируйте список доверенных сайтов, с которых пользователи могут загружать и устанавливать ПО (например, с таких известных сайтов как Adobe.com и GoToMeeting.com). Это позволит пользователям получить доступ к необходимым для работы приложениям Adobe Reader, Adobe Air, Adobe Flash Player и GoToMeeting без участия службы IT.

Фильтр условий по версии ПО

Некоторым организациям требуется усиленный контроль над приложениями, которые пользователи могут быть загружены через сайт (например, установка Adobe Reader), сохранив при этом возможность блокировки для сайта adobe.com. Вы сможете задать фильтр по версии программы, что позволит пользователям загружать только специфические версии ПО.

Мониторинг на корпоративном уровне

Детальная информация по контролю приложений и управлению доступами. В целях исключения возможностей модификации журнала событий, доступ к журналам защищен паролем.