ivanti

DATA SHEET

# Ivanti Security Controls

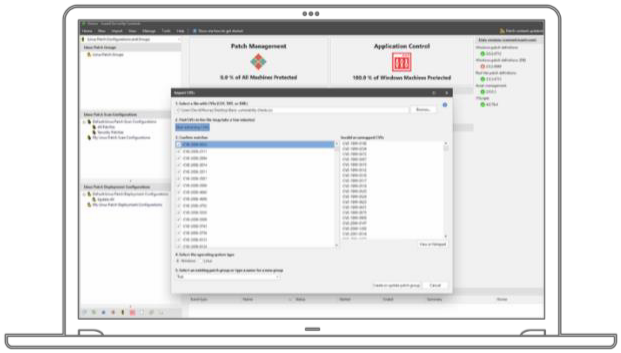
**На сегодняшний день ИТ-команды тратят слишком много времени на управление разрастающимся парком устройств, в то время как службы безопасности испытывают нехватку рабочей силы. Ivanti упрощает процесс обеспечения безопасности с помощью унифицированного решения, которое нацелено на самые крупные направления атак.**

**В Ivanti Security Controls мы объединили инструменты для безопасности, созданные мировыми экспертами, которые сформировали высокие барьеры от современных кибератак - обнаружение авторизованного и неавторизованного программного обеспечения в вашей среде, чтобы вы смогли своевременно защититься от него; управление и контроль обновлений для операционных систем и сторонних приложений; динамический белый список; детализированное управление привилегиями, а также дополнительные инструменты исправлений, которые помогают ИТ и безопасности лучше работать вместе, чтобы лучше защитить бизнес.**

## Поддержка семейства Windows и Linux ОС

Ivanti Security Controls — это единое решение для автоматического распространения обновлений, которое охватывает не только физические и виртуальные серверы Windows, но и рабочие станции. Также мы добавили поддержку Red Hat Enterprise Linux.

- **Поддержка виртуальной среды.** Найдите онлайн и офлайн рабочие станции и сервера, отсканируйте отсутствующие обновления и разверните их. Просканируйте ОС и приложения на виртуальных машинах (VMs) и даже гипервизоре ESXi, благодаря глубокой интеграции с VMware. Возможна также поддержка автономных виртуальных образов – эталонных шаблонов. Для минимизации времени на обслуживание автономных шаблонов, вы сможете подключать процесс сканирования и обновления в любое время, не беспокоясь об актуальности обновлений в самом шаблоне.




- **Установка обновлений без использования агента.** Безагентная технология позволяет сканировать и разворачивать обновления на рабочих станциях и серверах, подключенных к вашей сети, оказывая минимальную нагрузку как на работу вашей команды, так и на целевые системы. В качестве альтернативы вы можете использовать агента для создания множества различных политик, чтобы получить большую гибкость при сканировании, установке и перезагрузке устройств, которые могут быть выключены или не подключены к сети в данный момент.
- **Поддержка приложений**. Сторонние приложения, такие как Adobe, Acrobat, Flash, Reader, Google Chrome, Mozilla Firefox Oracle и Java, являются основной целью хакерских атак. Мы предоставляем самый широкий каталог обновлений в данной отрасли, и наша команда разработчиков контента тщательно проверяет все исправления, поэтому вам не нужно брать эту работу на себя. Мы поможем сэкономить вам и вашей команде больше времени, чтобы сосредоточиться на основных бизнес-задачах.

## Поддержка контроля запуска приложений и управления привилегиями

Ivanti Security Controls предлагает внедрение динамических белых списков, использующих модель проверки собственника файла, что уменьшает время на обслуживание традиционных белых списков, стоимость владения после запуска и влияние на производительность, обеспечивая при этом высокий уровень безопасности. Это также позволяет ИТ-специалистам вернуть права администратора, но при этом пользователи могут делать то, что им нужно, включая упрощение процесса добавления дополнительных разрешений, если это необходимо.

- **Упрощённый белый список.** Мы можем предоставить авторизованный доступ к приложениям, службам и компонентам, не заставляя ИТ-специалистов управлять обширными списками приложений вручную и не ограничивая пользователей. Например, Trusted Ownership ™ позволяет владельцам файлов NTFS упростить процесс создания белых списков. Использование нескольких доверенных учетных записей для определения принадлежности файлов позволяет легко внедрять белый список и непрерывно добавлять, и обновлять приложения через ваши системы управления, поскольку доверенными владельцами являются учетные записи, выполняющие действия по установке и обновлению.

- **Контроль над ключами.** Существует много уязвимостей, которые при их открытости дают злоумышленнику права, равные правам текущего пользователя. Злоумышленники могут использовать украденные учетные данные и права администратора этого пользователя для получения доступа к информации и системам, а также дальнейшего распространения в вашей сети. Предоставление полных прав администратора на сервере также сопряжено с другими рисками, такими как возможность запуска или остановка служб, установка или удаление программного обеспечения по ошибке. По-прежнему существуют компании, которые могут применять политику полной блокировки прав пользователей, но обычно пользователям требуются некоторые возможности, которые неизбежно требуют от нас предоставления им административных привилегий в системе.

Microsoft предоставляет только два уровня контроля: пользовательский и полный административный. Между ними есть некоторые различия, но их недостаточно, чтобы сделать их удобными для пользователя или администратора. Мы внедряем Just Enough Administration (JEA) и Just-in-time Administration (JIT) - позволяя вам отозвать права администратора, но при этом даем возможность пользователям делать то, что им нужно, включая упрощение процесса эскалации или добавление дополнительных разрешений, если это необходимо. Теперь вы можете выбирать. Минимизируйте уровень доступа для обычных пользователей и предоставьте расширенные привилегии, где и когда это необходимо: от доступа к установке приложений/принтера к использованию PowerShell или тому, что может потребоваться пользователю, но в установленных рамках. Вы также можете ограничить доступ администратору. Например, уберите PowerShell или доступ к определенным возможностям. Ограничьте административные привилегии определенными консолями, приложениями, службами и командами, снижая риск того, что администраторы будут внедрять вредоносные программы, останавливающие важные службы, или влиять на производительность важных служб иным способом.

## Больше инструментов для экономии времени и денег

Ivanti Security включает в себя следующие функции, которые значительно упростят задачу ИТ-подразделений по обеспечению безопасности вашей организации.

- **Интеграция и автоматизация за пределами Ivanti.** API-интерфейсы REST IPatch позволяют интегрировать элементы управления безопасностью с другими продуктами, автоматизировать общие процессы и обеспечивать удаленный доступ и управление консолью

- **Сократить разрыв между Security и IT Ops с помощью импорта базы CVE**

  Ivanti Security Controls проводит оценку уязвимости от любого поставщика, которого использует организация, найдет все исправления, относящиеся к этим распространенным уязвимостям и уязвимостям (CVE), Это поможет значительно сэкономить время, заменяя сегодняшний ручной процесс.

### Подробнее

**ivanti.ru**

**7 495 737 4814**

**contact@ivanti.ru**