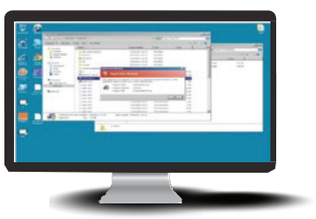
CYBERARK®

On-Demand Privileges Manager™ для Windows

Проблематика

Компьютеры с операционной системой Windows используются наиболее часто, но бизнес-среда, в которой они работают, неоднородна. Нужды бизнес-пользователей разнятся, некоторым необходим запуск приложений, требующих установки ActiveX, в то время как другим просто требуется установить принтер. Многие из подобных действий требуют прав администратора, однако дать такие мощные и неограниченные права всем пользователям в организации значило бы значительно осложнить ее деятельность:

Значительное снижение затрат засчет применения политик “минимальных привилегий” для десктопов и серверов.



Административные привилегии пользователя незаметно повышаются без необходимости вводить привилегированные логин и пароль. Если у пользователя отсутствуют привилегии на установку или запуск приложения, появится предупреждение.

- **Проблемы безопасности.** Управление с правами администратора создает прямой и непрямой риск нарушения безопасности системы. Чем больше уровень привилегий, тем выше шанс неправильного обращения с системой и, как следствие, ее повреждения. Более того, большая часть вредоносных программ пользуется правами администратора, косвенно повреждая систему и подвергая организацию риску внешних и внутренних угроз.

- **Угрозы производительности.** При наличии неограниченных прав велик шанс нарушения работоспособности ПК конечным пользователем, что создает излишнюю нагрузку на службу ИТ, которая вынуждена будет устранять неисправности. В средах Windows Server администраторы могут внести несанкционированные или нежелательные изменения, которые также наносят ущерб и снижают производительность.

- **Проблемы соответствия нормативным требованиям.** Когда пользователи нормативным требованиям. по умолчанию наделены правами администратора, это не только противоречит ряду директив соответствия, без “минимальных привилегий” становится невозможным отследить и зарегистрировать действия пользователей, что необходимо для прохождения аудиторских проверок. С другой стороны, если организация решает лишить всех пользователей прав администратора, это также негативно скажется на продуктивности работы. Пользователям придется полностью полагаться на IT-команду при выполнении задач, входящих в их должностные обязанности. Это создает большую нагрузку на подразделение ИТ и делает его “бутылочным горлышком” компании, замедляющим ведение бизнеса. В результате расходы значительно возрастут. При отсутствии решения, позволяющего управлять политикой “привилегий”, организации придется жертвовать либо безопасностью, либо производительностью; в обоих случаях это будет означать большие эксплуатационные расходы

Решение

On-Demand Privileges Manager™ (OPM) для Windows значительно сокращает использование привилегированных прав и позволяет внедрять политику “минимальных привилегий”. Известно, что практически 90% уязвимостей Windows нейтрализуются при работе с “минимальными привилегиями”. За счет возможности работы пользователей в стандартном режиме и увеличения прав отдельных приложений под четким управлением и в заданных пределах организации могут снизить затраты и повысить уровень безопасности.

С OPM для Windows Вы сможете:

Вести бизнес эффективнее. Позвольте пользователям выполнять административные задачи, требуемые их должностными инструкциями, что снизит зависимость от IT-отдела и повысит удовлетворенность конечного пользователя.

Уверенно выполняйте требования соответствия. Повысьте качество ежедневно выполняемых операций, лишив стандартных пользователей доступа к неограниченным правам локальных администраторов, что удовлетворяет требованиям соответствия FDCC, Government Connect, PCI DSS, HIPAA, SOX и др.

Устранить угрозы. Большая часть вредоносного ПО не может быть запущена с правами стандартного пользователя, что снижает риск внутренних и внешних угроз.

OPM для Windows предлагает Вам уникальные возможности:

- Снижение общих эксплуатационных расходов и нагрузки на службу ИТ, сокращение числа обращений в службы поддержки, вызванных некорректным использованием привилегий
- Соблюдение корпоративной политики и полная прозрачность деятельности привилегированных пользователей для лучшего обеспечения безопасности
- Снижение риска заражения ПК вредоносным ПО, которое может привести к ущербу и крупным убыткам для организации

Почему именно CyberArk?

CyberArk - признанный эксперт в остановке кибератак до того, как они нанесут вред бизнесу.

Преимущества

OPM для Windows обеспечит Вам лучший контроль за пользователями или группами, имеющими выделенные права администратора для конкретных приложений, скриптов или задач. За счет централизованного установления политик,
внедряемых во всей организации, Вы можете дать пользователям права, необходимые для выполнения ежедневных задач, при этом снизив нагрузку и расходы ИТ. OPM для Windows обеспечивает ряд полезных возможностей, таких как:

- **Централизованное управление.**
  Приложение плотно интегрировано с Групповой политикой Windows для установки и конфигурации, применяет инфраструктуру службы каталогов Active Directory для моментального распространения в организации без необходимости создания дополнительной внутренней инфраструктуры. Решение также плотно интегрировано с McAfee ePolicy Orchestrator (ePO) для централизованного управления в рамках консоли McAfee ePO.

- **Простая конфигурация политик.**
  Идентифицируйте приложения, разрешенные к запуску с расширенными правами, и задайте опции их идентификации, например, по имени файла, хэшу, сертификату, командной строке и т.д. Затем соотнесите приложение с пользователями, требующими расширенных привилегий.

- **Задание гибкой политики.**
  Пользователям можно ограничивать возможность запуска приложений, команд или задач без необходимости ввода имени пользователя или пароля. Также могут устанавливаться дополнительные опции, такие как: отправка сообщений конечному пользователю, подсказки с указанием причин запрета конкретных действий или дополнительных требований аутентификации, проведение аудита и мониторинг привилегий.

- **Прозрачность для пользователя.**
  Полная интеграция с системой управления пользовательскими аккаунтами Windows' User Account Control (UAC) устраняет или заменяет неподходящие запросы UAC на доступ к приложениям, требующим расширенных привилегий, что обеспечивает простоту работы для конечного пользователя.

- **Непрерывная защита ПК и серверов.**
  Сразу после установки OPM политики сохраняются в кэше машины, что обеспечивает выполнение политик даже при отсутствии сетевого подключения. Поддержка фонового обновления обеспечивает обновление политик даже без необходимости выхода пользователя из системы.

- **Управление приложениями.**
  Заранее определите белый список приложений, также включив в него приложения, не требующие прав администратора, что позволит запускать и устанавливать только разрешенных приложений. Любые несанкционированные приложения будут блокированы, а попытки их пуска запротоколированы. Конечные пользователи получают полностью настраиваемые уведомления, включающие возможность отправить по электронной почте сообщение с запросом на разрешение доступа к заблокированному приложению.

- **Увеличение полномочий по запросу.**
  Для более опытных пользователей, таких как администраторы и разработчики, которым требуется больше гибкости, OPM интегрируется с Windows таким образом, чтобы после входа под стандартным пользовательским аккаунтом позволить увеличение полномочий для доступа к приложениям из контекстного меню. Во избежание затруднений для конечного пользователя, стандартное меню Windows "Run as" (Запустить от имени другого пользователя) также возможно скрыть.

- **Централизованный аудит и отчеты.**
  Вся деятельность пользователей, выполняющих привилегированные операции, регистрируется в защищенном и недоступном для злоумышленников Digital Vault (цифровом хранилище). Оно обеспечивает единый центр хранения данных обо всех действиях привилегированных пользователей. Основанное на проверенных, легкомасштабируемых технологиях, решение OPM для Windows обеспечивает единое пространство наблюдения, позволяющее аудитору получать доступ к таким данным, как время использования и замены привилегированных паролей, а также их применение для выполнения привилегированных операций.

- **Готовность к внедрению.**
  Данное решение легко масштабируется, позволяет управлять сотнями тысяч компьютеров и даже интегрируется в корпоративные приложения для применения политики "минимальных привилегий" в данных средах.

- **Удаленная поддержка пользователей и поддержка пользователей без доступа к сети.**
  Механизм запросов/ответов может давать временный или постоянный доступ к установке приложений и ПО для дистанционной поддержки конечных пользователей. Система авторизации ответственных пользователей позволяет администраторам, находящимся в офисе, принимать решения на основе "вида от первого лица". Это обеспечивает гибкую, легко контролируемую политиками альтернативу традиционной функции Windows 'Run As'.

Мощь On-Demand Privileges Manager™

Привилегированных пользователей, использующих 'root' в средах Unix/Linux, также можно контролировать при помощи On-Demand Privileges Manager (OPM) для Unix/Linux от компании CyberArk. За счет детализированного управления правами доступа Вы можете устанавливать для привилегированных пользователей разрешенные к запуску команды с возможностью расширения прав по запросу, что позволяет разрешить'root'-доступ к конкретным задачам, также производится регистрация всех входных/выходных данных для полной отслеживаемости.
OPM обеспечивает унифицированный обзор и контроль взаимосвязи привилегированных пользователей и привилегированных аккаунтов, обеспечивая полную прозрачность и контроль во всей организации.

Характеристики

Поддерживаемые платформы:
- Windows 2012
- Windows 8
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Для всех платформ доступны 32-битные и 64-битные версии

Расширенная поддержка приложений:
- Исполняемые файлы
- Приложения панели управления
- Интегрируемые модули консоли управления
- Пакеты Windows installer
- Скрипты Windows Scripting Hosts
- Командные файлы
- Настройки реестра
- Скрипты PowerShell
- Средства управления ActiveX

Гибкие и безопасные правила для приложений:
- Проверка пути исполняемого файла
- Проверка командной строки
- Надежный издатель
- Технология Trusted ownership
- Информация о продукте и файлах
- Использование инфраструктуры службы каталогов Active Directory без необходимости создания дополнительной внутренней инфраструктуры