CYBERARK®

DATA SHEET

CyberArk® Endpoint Privilege Manager

Задачи

Когда атака обходит периметр и защиту конечных точек, вы полагаетесь на технологии обнаружения, чтобы быстро среагировать и предотвратить распространение угрозы. Злоумышленники похищают учетные данные или используют уязвимости для повышения привилегий и проникают в вашу сеть в поисках ценной информации.

Часто IT-специалисты предпочитают предоставлять пользователям права локального администратора, не применять минимальные привилегии или придерживаться очень мягких политик, пытаясь предотвратить негативное влияние на рабочие процессы или повышение нагрузки на техподдержку. В результате организации сталкиваются с такими проблемами:

- **Потеря производительности труда.** Когда организации лишают бизнес-пользователей всех привилегий, пользователи могут лишиться возможности выполнять определенные задачи или использовать некоторые приложения, необходимые для выполнения их повседневных функций. Негибкие политики привилегий могут привести к остановке бизнеса.
- **Высокие затраты на службу поддержки.** Если политики IT не позволяют бизнес-пользователям выполнять необходимые повседневные задачи, они вынуждены обращаться в службу поддержки для восстановления необходимых прав. Это может привести к значительному увеличению затрат на IT и перегрузке службы поддержки.
- **Повышение рисков безопасности из-за «ползучего роста привилегий».** Не имея необходимых инструментов, пользователи стремятся отвоевать права локального администратора при возникновении срочной необходимости и редко возвращают их обратно.
- **Повышенный риск успешных атак на основе вредоносного ПО.** Даже если вредоносное ПО не использует повышенные привилегии, без комплексных политик контроля приложений злоумышленники все равно могут достичь своих целей, скомпрометировать учетные данные и вывести конфиденциальную информацию.

Решение

CyberArk Endpoint Privilege Manager позволяет устранить барьеры, мешающие внедрению минимальных привилегий, а также блокировать и сдерживать атаки на конечных точках, снижая риск кражи или шифрования информации. Сочетание Endpoint Privilege Management, Privilege Threat Protection и Application Control останавливает и сдерживает разрушительные атаки в точке входа. Эти критически важные технологии защиты развертываются в виде единого агента для усиления и защиты всех настольных компьютеров, ноутбуков и серверов под управлением Windows, Windows Server, macOS или Linux.

Преимущества

С помощью CyberArk Endpoint Privilege Manager организации могут:

- **Удалить права локального администратора.** Endpoint Privilege Manager помогает удалить права локального администратора, улучшая работу пользователей и оптимизируя IT-операции. Гибкое управление на основе политик упрощает оркестровку привилегий и позволяет контролировать сеансы обслуживания Just-In-Time.

CyberArk Endpoint Privilege Manager защищает от кибератак, удаляя права локального администратора, повышая уровень приложений Just-InTime, создавая аудиторский след и защищая элементы управления безопасностью от несанкционированного вмешательства.

ПЛАТФОРМЫ И РАЗВЕРТЫВАНИЕ

Microsoft Windows

- Windows 7 x32, x64
- Windows 8/8.1 x32, x64
- Windows 10 x32, x64
- Windows 11 x32, x64

Microsoft Windows Server

- Windows Server 2008 x32, x64
- Windows Server 2008 R2 x64
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Apple macOS

- macOS Monterey 12

Linux

- Red Hat Enterprise Linux 7.x, 8.x
- SUSE Linux Enterprise 12,15
- Amazon Linux 2
- CentOS 7
- Ubuntu 18.04, 20.04

Варианты развертывания

- Software-as-a-Service

- **Обеспечить наименьшие привилегии.** Всесторонний контроль приложений на основе условных политик позволяет создавать сценарии для любой группы пользователей — от HR до DevOps. Endpoint Privilege Manager учитывает контекст приложения, параметры и атрибуты для разрешения или блокирования определенного сценария, приложения или операции.

- **Быстро внедрить принцип наименьших привилегий путем повышения прав и обеспечения доступа по технологии JIT (Just In Time).** Добавление пользователей в локальную группу привилегий на ограниченное время, обеспечение аудита на конечной точке в течение всего периода, когда пользователь имел права; отмена и прекращение доступа в конце сессии или раньше, если это необходимо.

- **Безопасно управлять локальным администратором.** Управление защищенными учетными данными из CyberArk Enterprise Password Vault осуществляется локально на конечных точках, в сети или вне ее.

- **Обнаруживать и блокировать попытки кражи учетных данных.** Кража учетных данных играет важную роль в любой атаке. Усовершенствованная защита позволяет обнаруживать и блокировать попытки кражи учетных данных Windows и учетных данных, хранящихся в популярных веб-браузерах.

- **Беспрепятственно повышать привилегии бизнес-пользователей по мере необходимости.**После удаления прав локального администратора убизнес-пользователей CyberArk Endpoint Privilege Manager повышает привилегии в соответствии с требованиями доверенных приложений и на основе политик.

- **Быстро выявлять и блокировать вредоносные приложения.** Использование анализа рисков приложений CyberArk для быстрого определения риска, связанного с любым приложением, упрощает определение политик и помогает предотвратить запуск вредоносных приложений в вашей среде.

- **Получить защиту от программ-вымогателей прямо из коробки.** OOTB-политика для защиты от программ-вымогателей, включающая комплексные средства контроля наименьших привилегий, проверенные на сотнях тысяч образцов программ-вымогателей.

- **Управлять sudo на основе политик Linux,** что позволяет устранить трудоемкие и подверженные ошибкам процессы администрирования sudo, обеспечивая менеджерам по безопасности конечных точек централизованную настройку sudo и применение минимальных привилегий в зависимости от роли в масштабе.

- **Обеспечить безопасную работу неизвестных приложений в ограниченном режиме.** Неизвестные приложения, не вызывающие доверия и не являющиеся вредоносными, могут работать в ограниченном режиме, который не позволяет им получить доступ к корпоративным ресурсам, конфиденциальным данным или Интернету.

- **Для анализа неизвестных приложений можно использовать интеграцию со средствами обнаружения угроз.** CyberArk Endpoint Privilege Manager может отправлять неизвестные приложения в решения Check Point, FireEye и Palo Alto Networks для автоматического анализа файлов.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

Гибкие и безопасные правила работы с приложениями:

- Исполняемые файлы, динамически подключаемые библиотеки (dll), приложения Windows, сценарии.
- Точное, частичное, подстановочное и regexp-совпадение.
- Атрибуты файлов, такие как имя файла, контрольная сумма, владелец, тип расположения, источник и т.д.
- Атрибуты программы, такие как название продукта, название компании и т.д.
- Контекст приложения, например, параметры запуска, родительский процесс и т.д.
- Гранулярный контроль поведения приложений и дочерних процессов

Защита учетных данных от:

- Фальсификации агента Endpoint Privilege Manager
- Компрометации хранящихся в браузере учетных данных и хранилищ учетных данных
- Кражи учетных данных из IT-приложений
- Кражи учетных данных из средств удаленного доступа
- Подозрительных действий
- Сбора учетных данных Windows

Примітка: певна функціональність доступна лише для деяких платформ

Комплексное решение

CyberArk Endpoint Privilege Manager является частью более широкой платформы CyberArk Identity Security Platform — комплексного решения, предназначенного для проактивной защиты от современных атак, использующих привилегии администратора для получения доступа к сердцу предприятия, кражи конфиденциальных данных и повреждения критически важных систем. Решение помогает организациям сократить площадь атак за счет устранения ненужных привилегий локального администратора и усиления защиты привилегированных учетных записей. Продукты, входящие в состав решения, могут управляться независимо друг от друга или комбинироваться для создания целостного комплексного решения по защите привилегированных учетных записей.
По любым вопросам относительно решений CyberArk пишите на cyberark@bakotech.com.

bako tech®

BAKOTECH — международная компания, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value-Added IT-дистрибьютор, BAKOTECH предоставляет профессиональную до- и пост-продажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков.

CYBERARK®
The Identity Security Company

CyberArk – глобальный лидер в сфере identity security. Сосредоточенный на контроле привилегированных аккаунтов, CyberArk предоставляет наиболее полное предложение безопасности для любой учетной записи – человеческой или программной – на всех бизнес-приложениях, расп ределенных рабочих нагрузках, гибридных облачных средах и на протяжении жизне нного цикла DevOps. Крупнейшие организации мира доверяют CyberArk в защиту своих важнейших активов.