CYBERARK® ENDPOINT PRIVILEGE MANAGER

Обеспечьте безопасность привилегий на настольных, портативных компьютерах и серверах, беспроблемно удалив права локального администратора и снизив нагрузку на службу техподдержки.

Просматривайте все политики привилегий, приложения и их репутацию в одном месте.

Платформы и развёртывания

Windows Desktop:

- MS Windows XP 32 bit Service Pack 3
- MS Vista 32/64 bit Service Pack 1
- MS Windows 7 32/64 bit
- MS Windows 8 and 8.1 32/64 bit
- MS Windows 10

Windows Server:

- MS Windows Server 2003 32/64 bit
- MS Windows Server 2008 32/64 bit
- MS Windows Server 2008 R2
- MS Windows Server 2012
- MS Windows Server 2012 R2
- MS Windows Server 2016
- MS Windows Server 2019

Mac

- High Sierra 10.13
- Mojave 10.14
- Catalina 10.15

Опции развёртывания

- Software-as-a-Service

ПРОБЛЕМАТИКА

Когда атака обходит защиту периметра и безопасность конечных точек, остаётся полагаться только на те технологии обнаружения, которые быстро отреагируют на инцидент и предотвратят распространение атаки. Злоумышленники крадут учётные данные для повышения привилегий и, проникнув в сеть, перемещаются в ней в поисках ценной информации. Защита доступа на конечной точке сокращает поверхность атаки и является фундаментальной частью программы безопасности. Это защищает настольные и портативные компьютеры, серверы, снижая риск взлома и потенциального ущерба для бизнеса. Однако обратная сторона - это потенциальное влияние на продуктивность пользователей, увеличение нагрузок и связанных с этим расходов для ИТ-персонала.

Для уменьшения площади распространения атаки и снижения риска потери данных без снижения производительности необходимо установить инструменты, которые будут обеспечивать защиту привилегий на конечных точках, блокировать и сдерживать распространение атак. Данные инструменты должны применять гибкие политики с наименьшими привилегиями для бизнес-пользователей и администраторов, контролировать, каким приложениям разрешён запуск, и гарантировать, что они смогут обнаружить и заблокировать атаки, нацеленные на учётные записи. Без таких средств защиты организации неизбежно столкнутся со следующими проблемами:

- Снижение производительности бизнеса. При удалении всех привилегий у бизнес-пользователей, они больше не смогут выполнять задачи и использовать приложения, необходимые для их повседневной работы. Поэтому отсутствие гибких политик управления привилегиями может привести к полной остановке бизнеса.
- Расходы на службу техподдержки. Когда ИТ-политики не позволяют бизнес-пользователям выполнять необходимые повседневные задачи, они обычно обращаются за помощью в техподдержку. Это может значительно увеличить расходы на ИТ и привести к перегрузке в работе персонала службы поддержки.
- Повышенные риски безопасности из-за «расползания привилегий». Иногда, после удаления всех привилегий у бизнес-пользователей, возникает необходимость восстанавливать их для выполнения определенных задач. Однако после этого они редко отзываются от привилегий, что вновь открывает лазейку в безопасности, связанную с чрезмерными административными правами.
- Повышенный риск успешных атак с использованием вредоносных программ. Минимизировав права пользователей на устройствах Windows и macOS, организации всё ещё могут оставаться уязвимыми для вредоносных программ, которым не требуются права для запуска. Без дополнительных инструментов для контроля запуска приложений и защиты учётных записей, которые являются основной целью злоумышленников, вероятность проникновения и распространения атак внутри организации при помощи вредоносных программ будет оставаться высокой.

РЕШЕНИЕ

CyberArk Endpoint Privilege Manager помогает устранить барьеры для обеспечения минимальных привилегий и позволяет блокировать атаки в конечной точке, снижать риск кражи или шифрования информации с целью получения выкупа. Управления привилегиями, целевая защита от угроз Privilege Threat и контроль приложений предотвращают вредоносные атаки в конечной точке входа. Неизвестные приложения работают в ограниченном режиме для защиты от угроз, а Privilege Threat Protection блокирует попытки кражи учётных данных. Эти критически важные технологии защиты развертываются как единый агент для обеспечения максимальной защиты всех настольных компьютеров, ноутбуков и серверов.

CyberArk Endpoint Privilege Manager также позволяет специалистам по информационной безопасности применять для ИТ-администраторов гранулярные политики минимальных привилегий, помогая тем самым эффективно распределять нагрузку на серверах Windows. Помимо управления привилегиями данный продукт обеспечивает управление приложениями, контролируя, какие приложения разрешено запускать на конечных точках и серверах.

С помощью CyberArk Endpoint Privilege Manager организации могут:

- Автоматически создавать политики на основе бизнес-требований. Политики управления приложениями и повышения привилегий на основе надежных источников, таких как SCCM, дистрибьюторы ПО, средства обновления, URL-адреса и т. д. Шаблоны политик обеспечивают быструю реализацию для таких типов серверов, как Microsoft SQL Server, экономя время и устраняя пробелы в политиках безопасности привилегий для всех ролей пользователей.

Спецификация

Всесторонняя поддержка приложений:

- PKG
- DMG
- Поддержка REST API
- Executable
- MSI, MSU
- Административные задачи
- Оснастки консоли управления
- Скрипты
- Настройки регистра
- Элементы управления ActiveX
- COM objects
- Web-приложения

Гибкие и безопасные правила приложений:

- File path matching
- Command line matching
- File hashing (SHA-1)
- Product and file information
- Trusted publisher
- Trusted Source SCCM
- Trusted Software Distribution system
- Trusted Updater
- Trusted Network
- Trusted AD group
- Trusted product
- Trusted URL

Защита учётных записей для:

- Git, Opera Browser and DbVisualizer
- Pass The Hash Attack
- Kerberos Ticket Hash Harvesting
- PuTTy
- Okta AD Agent
- Windows Credential Manager
- Local Security Authority (LSA)
- Local Security Authority Subsystem Service (LSASS)
- Security Account Manager (SAM)
- Domain Credentials Cache (msvcachedv2)
- AD Directory Data Store (NTDS.dit)
- Virtual Secure Module (including in Safe Mode)
- Crypto RSA Machine Keys
- AWS Keys
- Internet Explorer
- Microsoft Edge
- Chrome
- Firefox
- SQL Server Management Studio (SSMS)
- Quest Toad
- Remote Desktop Connection Manager
- FileZilla
- MRemoteNG

Примечание: некоторые функции могут быть доступны не для всех вариантов развертывания и ОС.

SOC 2 Type 2 compliant

- Быстро применять минимальные привилегии предоставляя доступ или повышая права на основе подхода JIT (Just In Time). Добавлять пользователей в локальную группу привилегий на ограниченное время, вести контрольный журнал на конечной точке в течение того периода, когда у пользователя были привилегированные права, отменять и прекращать доступ в конце сеанса или раньше, если это необходимо.
- Применять детализированные политики наименьших прав для администраторов Windows. Детальный контроль команд и задач каждого ИТ-администратора на серверах Windows в зависимости от их роли.
- Безопасно управлять локальным администратором. Защищённые учётные данные из CyberArk Enterprise Password Vault управляются локально на конечных точках, в сети или за её пределами.
- Обнаруживать и блокировать попытки кражи учётных данных. Кража учётных данных играет важную роль в любой атаке. Расширенная защита помогает организации обнаруживать и блокировать попытки кражи учётных данных Windows и данных, хранящихся в популярных веб-браузерах.
- Беспроблемно повышать привилегии бизнес-пользователей. После удаления прав локального администратора у бизнес-пользователей CyberArk Endpoint Privilege Manager повышает права на основе политики в соответствии с требованиями доверенных приложений.
- Быстро выявляет и блокирует вредоносные приложения. Использование Application Risk Analysis для быстрого определения рисков, связанных с любым приложением, упрощает определение политик и помогает предотвратить запуск вредоносных приложений в среде.
- Использовать "коробочное решение" по защите от программ-вымогателей. Включает определение политики OOTB для защиты от программ-вымогателей, включая комплексные средства контроля с минимальными привилегиями, которые можно легко протестировать на сотнях тысяч образцов вредоносных программ.
- Разрешать неизвестным приложениям безопасно работать в ограниченном режиме. Неизвестные приложения, которые не считаются надёжными или вредоносными, могут работать в «ограниченном режиме», который не позволяет им получать доступ к корпоративным ресурсам, конфиденциальным данным или Интернету.
- Использовать интеграцию со средствами обнаружения угроз для анализа неизвестных приложений. CyberArk Endpoint Privilege Manager может отправлять неизвестные приложения в решения в Check Point, FireEye и Palo Alto Networks для автоматического анализа файлов на наличие угроз.

ПРЕИМУЩЕСТВА

- Обеспечение критического уровня защиты, когда атака обходит традиционные средства безопасности периметра и конечных точек.
- Уникальное сочетание технологий для защиты, блокирования и сдерживания атак на конечную точку, снижение потенциального ущерба для бизнеса.
- Усиление возможностей защиты и обнаружения существующей системы безопасности конечных точек.
- Беспроблемная реализация политики безопасности с минимальным влиянием на бизнес.
- Запрет установки несанкционированных приложений и защита стабильной работы рабочей станции, в результате чего уменьшаются количество обращений в службу поддержки и затраты на техподдержку.
- Удаление бизнес-пользователей с правами локального администратора без снижения производительности пользователей и увеличения количества обращений в службу поддержки.
- Защита и замена пароля локального администратора независимо от местоположения конечной точки.
- Простое развертывание с автоматическим созданием политик и шаблоны политик OOTB облегчают нагрузку на ИТ-команду, а отдельный агент обеспечивает поддержку в сетях с физической изоляцией.
- Соответствие конечных точек требованиям группы управления безопасностью и рисками, снижение их рабочей нагрузки.
- Ограничение распространения вредоносных программ по сети, сокращение времени и усилий на исправление.

КОМПЛЕКСНОЕ РЕШЕНИЕ

CyberArk Endpoint Privilege Manager является частью более широкой платформы CyberArk Identity Security Platform, представляющего собой комплексное решение для превентивной защиты от сложных атак, использующих административные привилегии с целью получения доступа к "сердцу" предприятия, кражи конфиденциальных данных и повреждения критически важных систем.

Данное решение помогает организациям уменьшить поверхность атаки, устраняя ненужные права локального администратора и усиливая безопасность привилегированных учётных записей. Продуктами можно управлять независимо или объединять их в единое и комплексное решение для защиты привилегированных учётных записей.