CYBERARK

РЕШЕНИЕ CYBERARK PRIVILEGED ACCESS SECURITY

Наиболее полное решение по снижению рисков в процессе работы с привилегированными учётными данными и секретами

Содержание

Привилегированный доступ — реальная и распространенная угроза

Злоумышленники сеют хаос по всему миру, совершая новейшие, тщательно спланированные и изощрённые кибератаки, которые нацелены непосредственно на самые ценные активы предприятия. Все больше организаций внедряют приоритетные облачные стратегии и методики интегрированной разработки и эксплуатации (DevOps). Это приводит к увеличению поверхности атаки и предоставляет злоумышленникам новые возможности для использования незащищённых корпоративных ресурсов. Проникнув в сеть, они ищут доступ к самым ценным информационным ресурсам предприятия, чтобы причинить вред репутации, обеспечить финансовые потери и украсть интеллектуальную собственность. Известны также случаи, когда сами сотрудники разглашали конфиденциальную информацию посторонним или создавали предпосылки для нанесения ущерба внутри компании. По оценкам Forrester, 80% нарушений безопасности связано с привилегированными учётными данными[1].

Привилегированные аккаунты и предоставляемый ими доступ — это крупнейшие на сегодня уязвимости в организациях. Почему внутренние и внешние злоумышленники нацелены на привилегированные аккаунты компании?

- Привилегированные аккаунты существуют повсюду: в каждом сетевом устройстве, базе данных, приложении и сервере, в локальных и облачных средах, промышленных системах управления и на всех стадиях процесса интегрированной разработки и эксплуатации.
- Привилегированные аккаунты, используемые как людьми, так и машинами, предоставляют наиболее полный доступ к конфиденциальным данным и системам.
- Привилегированные аккаунты имеют общий административный доступ, что делает их пользователей анонимными.
- Привилегированные аккаунты предоставляют слишком широкие права доступа, выходящие далеко за рамки необходимых пользователям для выполнения своих должностных обязанностей.
- Привилегированные аккаунты не подвергаются мониторингу и протоколированию, а значит, остаются незащищёнными.

Проще говоря, привилегированные аккаунты позволяют любому их владельцу контролировать ресурсы организации, отключать системы безопасности и получать доступ к огромным объёмам конфиденциальных данных. Все прогнозы свидетельствуют о том, что в настоящее время без надлежащих мер злоупотребление привилегированными аккаунтами только усилится. Передовой опыт указывает на необходимость включения привилегированных аккаунтов в основную стратегию безопасности компании. Привилегированные аккаунты создают проблему безопасности и требуют внедрения механизмов особого контроля защиты, мониторинга, обнаружения, оповещёния и реагирования на все действия с ними.

Привилегированные учётные данные — ключи к «царству информационных технологий»

Привилегированные учётные данные открывают дверь в «царство информационных технологий». Они позволяют получить доступ к привилегированным аккаунтам и требуются внешним и внутренним злоумышленникам для прямого проникновения в самое «сердце» предприятия. Как результат, защита критически важных систем и конфиденциальных данных организации напрямую зависит от уровня безопасности привилегированных учётных данных, необходимых для использования этих ресурсов.

Сегодня для подтверждения доступа пользователей и систем к привилегированным аккаунтам большинство организаций полагается на сочетание привилегированных учётных данных, таких как пароли, ключи API, сертификаты, устройства идентификации и ключи SSH. Без надлежащей защиты эти ценные конфиденциальные и учётные данные могут быть скомпрометированы злоумышленниками с целью присвоения привилегированных аккаунтов и их использования для дальнейших атак на организацию. Результаты исследования кибербезопасности свидетельствуют о том, что для успешной атаки злоумышленнику достаточно получить доступ к привилегированному аккаунту. Следует отметить, что некоторые организации начинают защищать привилегированные пароли, поэтому злоумышленники выбирают для атак SSH-ключи, которые часто упускаются из виду при обеспечении безопасности привилегированных аккаунтов.

Для предотвращения целенаправленных атак, для защиты ключей от «царства ИТ» и конфиденциальной информации от киберпреступников организации должны внедрять стратегию безопасности привилегированного доступа, которая включает в себя упреждающую защиту и мониторинг всех привилегированных конфиденциальных и учётных данных.

Учитесь у профессионалов: CyberArk Privileged Access Security

Компания CyberArk — лидер профильного рынка и авторитетный эксперт по безопасности привилегированного доступа. Мы обладаем наиболее богатым опытом среди всех поставщиков подобных решений и используем его для работы с нашими заказчиками в рамках чёткого и эффективного подхода к управлению рисками, связанными с привилегированным доступом.

Для снижения риска серьёзных утечек данных предприятиям необходимо внедрять решение по обеспечению безопасности, специально предназначенное для защиты привилегированного доступа. Решение CyberArk Privileged Access Security включает в себя возможности комплексной защиты, мониторинга, выявления, оповещёния и отчётности, позволяющие опережать злоумышленников и обеспечивать безопасность наиболее важных ресурсов организации.

[1] The Forrester Wave™: «Управление привилегированными идентификационными данными», 3-й квартал 2018 г.

Вы правильно оцениваете уровень риска?

Согласно нашему недавнему отчету о ландшафте угроз 2018 года, 89% ИТ-специалистов признают тот факт, что защита инфраструктуры и критически важной информации не может считаться полной без обеспечения безопасности привилегированных аккаунтов, учётных и конфиденциальных данных. Однако многие из них отмечают, что в их организациях до сих пор не используется решение по обеспечению безопасности привилегированного доступа, хранению привилегированных и/или административных паролей и управлению ими. Более того, в отчете 2018 года сообщается о недостаточных мерах для защиты от вредоносного ПО и сложных атак. При этом, 87% респондентов указали, что они по-прежнему позволяют пользователям работать с привилегиями локального администратора, которые, как мы знаем, необходимы большинству вредоносных программ для закрепления в организации. Сочетание учётных записей пользователей с правами локального администрирования с реальными администраторами создаёт постоянно увеличивающуюся поверхность атаки, связанную с привилегированными аккаунтами.

Кроме того, безопасность сред DevOps ещё не достигла уровня зрелости традиционных корпоративных ИТ. Половина респондентов не имеют стратегии привилегированной безопасности для облачных сред или DevOps. Почти 40% из них хранят пароли и конфиденциальную информацию привилегированных аккаунтов в простых текстовых файлах, которые, несмотря на свою ценность, остаются без управления и защиты, формируя среду с высокой степенью риска. Когда вы осознаете риск для обычного предприятия, связанный с [недостаточной] безопасностью привилегированного доступа, а затем тот факт, что более чем в 80% успешных атак за последние 8 лет были использованы привилегированные аккаунты, становится предельно ясно, на что должен быть направлен план действий ИТ-специалистов.

Соответствие нормативным требованиям — быть или не быть

Увеличивающийся риск изощрённых угроз вынуждает ужесточать требования таких стандартов, как PCI DSS, Sarbanes Oxley, NIST, NERC-CIP, HIPAA, GDPR и SWIFT CSCF, в области соответствия контроля, управления и мониторинга привилегированного доступа.

Не имея полного представления о своей привилегированной среде, организации рискуют не пройти проверку, что приведёт к последующим крупным штрафам. И что особенно важно, без стратегии защиты привилегированного доступа они продолжают оставаться уязвимыми перед серьёзными нарушениями безопасности.

Кто ваши привилегированные пользователи?

Компании часто оставляют без внимания многочисленные возможности доступа к привилегированным аккаунтам. У них практически отсутствуют определенные политики безопасности и аудита для контроля связанных с ними рисков. Анонимный неконтролируемый доступ к этим аккаунтам оставляет организации открытыми для злоупотреблений и может нанести им вред в случае компрометации.

Удалённые поставщики. Привилегированный доступ предоставляется подрядчикам для выполнения должностных обязанностей, позволяя им работать под покровом анонимности. Попадая в ИТ-среду компании, удалённые поставщики имеют неограниченные права, аналогичные правам любого «стандартного» привилегированного пользователя, и могут повышать их для доступа к конфиденциальным данным во всей организации.

Распорядители гипервизоров или облачных серверов. Бизнес-процессы, связанные с финансами, кадрами и закупками, переводятся в облачные приложения, подвергая активы предприятия высокому риску ввиду широкого доступа, предоставляемого администраторам облачных сред.

Системные администраторы. Практически каждое устройство в ИТ-инфраструктуре (каждая конечная точка или сервер) имеет коллективный аккаунт с повышенными привилегиями и беспрепятственным доступом к ОС, сетям, серверам и базам данных.

Администраторы приложений или баз данных. Администраторам приложений или баз данных предоставляется широкий доступ для управления выделенными системами. С его помощью они также могут подключаться практически к любым другим базам данных или приложениям на предприятии.

Отдельные бизнес-пользователи. Руководители высшего звена и сотрудники ИТ-подразделений часто имеют привилегированный доступ к бизнес-приложениям, содержащим конфиденциальную информацию. Попадая в руки злоумышленников, эти учётные данные открывают доступ к финансовым показателям, интеллектуальной собственности и другой конфиденциальной информации компании.

Конечные пользователи. Очень многие компании по-прежнему предоставляют конечным пользователям права локального администратора для решения таких задач, как установка ПО или настройка принтера. Попадая в чужие руки, эти привилегированные учётные данные в первую очередь дают злоумышленникам возможность получить доступ к финансовым показателям, интеллектуальной собственности и другой конфиденциальной информации компании.

[2] CyberArk, «Отчет CyberArk о глобальном ландшафте новейших угроз за 2018 г.», 2018 г.

Социальные сети. Привилегированный доступ предоставляется для администрирования внутренних и внешних социальных сетей компании. Кроме того, сотрудники и подрядчики получают привилегированный доступ для публикации своих собственных записей. Ненадлежащее использование таких учётных данных приводит к краже аккаунтов и нанесению ущерба товарному знаку организации или репутации руководства.

Приложения. Приложения используют привилегированные аккаунты для взаимодействия с другими приложениями, сценариями, базами данных, веб-службами и т. д. Эти аккаунты часто упускаются из виду и создают серьёзную угрозу из-за редкой смены паролей и статичности учётных данных. Хакер может использовать такие точки атаки для расширения привилегированного доступа на все ресурсы организации.

DevOps. Среды DevOps позволяют организациям достигать высокого уровня гибкости за счёт автоматического создания и развёртывания служб и приложений. Для доступа к информации, другим приложениям и службам им требуются секреты и учётные данные, которые должны находиться под защитой. Кроме того, типовые среды DevOps поддерживаются несколькими мощными инструментами, каждый из которых управляется через консоль администрирования. Для доступа к ней используются привилегированные учётные данные, также требующие защиты.

Политика превыше всего: согласование управления рисками с бизнес-целями

Передовой опыт свидетельствует о необходимости создания, внедрения и соблюдения политик безопасности привилегированного доступа в организациях для снижения риска серьёзных нарушений. Эффективная защита и соответствие компании нормативным требованиям начинаются с продуманной реализации бизнес-политики. В её основе должен лежать подход, гарантирующий снижение рисков внешних и внутренних угроз и злоупотреблений, а также обеспечивающий соблюдение строгих государственных и отраслевых требований.

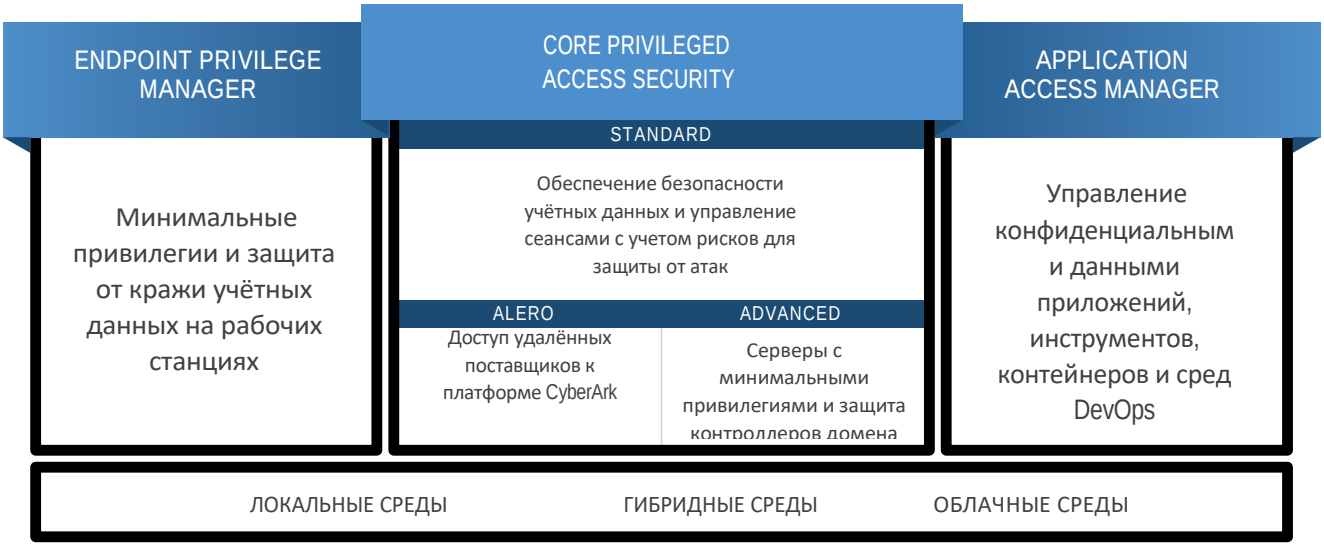
Общая технологическая платформа CyberArk

Платформа CyberArk изначально ориентирована на защиту привилегированного доступа и объединяет мощную базовую инфраструктуру с ключевыми продуктами для предоставления наиболее комплексного решения организациям любого размера.

Основа инфраструктуры – это изолированный сервер безопасного хранения данных, унифицированная подсистема обработки политик, механизм обнаружения и уровни безопасности, обеспечивающие масштабируемость, надёжность и полную защиту привилегированного доступа. Гибкая архитектура может начинаться с малых развёртываний и масштабировать до самых крупных и ресурсоемких корпоративных размеров.

Только CyberArk предоставляет решения, которые позволяют защищать, контролировать и проверять учётные данные пользователей и приложений, предоставлять доступ с минимальными привилегиями, а также управлять приложениями на конечных точках и серверах. Кроме того, эти решения обеспечивают защиту, мониторинг и анализ всей привилегированной активности с активным оповещённием об аномальном поведении. Это комплексное решение корпоративного уровня предназначено для защиты, мониторинга, обнаружения и реагирования на угрозы. Оно не допускает фальсификаций, поддерживает масштабирование и обеспечивает максимальную защиту сложных распределённых сред от внутренних и передовых атак.

РЕШЕНИЕ CYBERARK PRIVILEGED ACCESS SECURITY



Master Policy™— простое, унифицированное и непревзойденное решение для приоритетного определения политик

Master Policy предоставляет инновационный механизм обработки политик, позволяющий заказчикам определять, регулировать и контролировать политику безопасности привилегированного доступа, используя единый, простой интерфейс на естественном языке. Некогда сложный процесс преобразования бизнес-политик и процедур в технические настройки становится легким в управлении и понятным для всех участников бизнес-процессов организации, включая специалистов по безопасности, рискам и аудиту. Master Policy лежит в основе решения CyberArk Privileged Access Security Solution, обеспечивая удобное, унифицированное и максимально эффективное управление политиками.

Master Policy преобразует письменные политики безопасности в технические настройки и управляет ими на естественном языке. Благодаря данному решению механизмы контроля безопасности привилегированного доступа могут внедряться за считаные минуты, ускоряя процесс, который без Master Policy занимал бы несколько дней или даже недель. Master Policy позволяет быстро внедрять и гибко определять глобальную корпоративную политику, одновременно предусматривая контролируемые и точные исключения с учётом уникальных эксплуатационных потребностей ОС, региональных филиалов или бизнес-подразделений.

Digital Vault™

Отмеченное наградами, запатентованное решение Digital Vault™ — это изолированный защищённый сервер с шифрованием FIPS 140-2, доступ к которому возможен только через специализированные безопасные протоколы. Для обеспечения целостности все продукты CyberArk работают с защищённым хранилищем напрямую. Они обмениваются данными, позволяя всем модулям и компонентам безопасно взаимодействовать друг с другом и использовать преимущества безопасного хранения паролей, ключей SSH, параметров политик и журналов аудита в локальных, гибридных и облачных средах. При этом отсутствует единая точка отказа.

- Разделение обязанностей и жёсткий контроль доступа. Администратор безопасного хранилища не имеет доступа к содержащимся в нем учётным данным, что способствует надлежащему разделению обязанностей. Решение поддерживает несколько методов аутентификации, обеспечивая комплексную безопасность и контроль привилегированного доступа и активности.
- Уровни безопасности. Семь уровней встроенных функций безопасности для аутентификации, управления доступом, шифрования, надёжного хранения данных и защиты информации без возможности обхода защиты или доступа администратора баз данных обеспечивают исключительную конфиденциальность.
- Высокая готовность и аварийное восстановление. Инфраструктура спроектирована с учётом высокой готовности и содержит встроенные, устойчивые к отказам инструменты, позволяющие удовлетворять и превосходить требования аварийного восстановления, включая безопасное резервное копирование и быстрое восстановление работы.

Механизм обнаружения

Механизм обнаружения, предназначенный для непрерывного выявления изменений в локальных или облачных ИТ-средах, обеспечивает постоянную актуальную защиту, а также регистрацию и безопасность всей привилегированной активности. При добавлении или удалении серверов и рабочих станций все изменения в привилегированных аккаунтах выявляются в автоматическом режиме.

Надёжный аудит

Решение CyberArk Privileged Access Security обеспечивает автоматизированное применение политик в отношении привилегированных аккаунтов, позволяя непрерывно контролировать соблюдение требований аудита. Специалисты по ИТ-аудиту получают полное представление о том, «кем, когда и почему», а также «что» именно совершалось во время всех привилегированных сеансов. Решение позволяет удобно и экономически эффективно предоставлять отчеты о результатах аудита через единый централизованный репозиторий всех контрольных данных.

Интеграция корпоративного уровня

Решение Privileged Access Security легко интегрируется с существующими системами безопасности, операциями и инструментами DevOps благодаря широкой поддержке автоматизации посредством API-интерфейсов REST.

- Системы SIEM (управление информационной безопасностью и событиями безопасности). Полная двусторонняя интеграция с поставщиками решений SIEM улучшает возможности обнаружения угроз и оповещёния. CyberArk передаёт в системы SIEM информацию о событиях, связанных с привилегированным доступом и операциями, а также об активности командного уровня, зарегистрированной с помощью мониторинга привилегированных сеансов.
- Гибридное облако. Поддержка гибридных облачных сред обеспечивает безопасность аккаунтов гипервизоров и гостевого доступа для администраторов облака, а также защиту привилегированных учётных записей Amazon Web Services, Microsoft Azure и Google Cloud Platform.
- Управление уязвимостями. Полная интеграция с ведущими поставщиками систем управления уязвимостями позволяет упрощать «аутентифицированное сканирование» (также известное как «глубокое сканирование») и извлекать привилегированные аккаунты из хранилища каждый раз при необходимости авторизации на целевом сервере для проведения проверки.
- Управление идентификацией. Интеграция с ведущими системами идентификации и управления доступом (IAM) для инициализации аккаунтов в решении с учётом особенностей каталогов, групповой принадлежности или политик управления идентификацией. Подобное объединение также позволяет нашим заказчикам использовать предыдущие инвестиции в технологии строгой аутентификации, например PKI, Radius, Web-SSO, LDAP и другие.

- Служба поддержки. Интеграция с большинством корпоративных систем регистрации запросов, а также собственными решениями. Возможность проверки и создания новых заявок на обслуживание, а также интеграция с процедурами согласования, такими как одобрение руководителя (двойной контроль) и готовность ко времени.
- Среды DevOps. Интеграция с комплексом инструментальных средств DevOps обеспечивает защиту и управление конфиденциальной информацией, используемой инструментами непрерывной интеграции/разработки, такими как Ansible, Chef, Jenkins и Puppet, а также ПО для оркестровки контейнеров, например Docker.

Масштабируемая, гибкая и устойчивая архитектура

Решение CyberArk Privileged Access Security минимально подвержено внешнему воздействию и защищает ваши инвестиции в существующую ИТ-среду. Все его компоненты работают независимо, но используют преимущества совместных ресурсов и данных. Такой гибкий подход позволяет организации начинать проект на уровне отделов и со временем масштабировать его до сложного, распределенного корпоративного решения.

Продукты CyberArk

Все продукты в составе решения CyberArk Privileged Access Security самостоятельны, поддерживают независимое управление, но при этом совместно используют ресурсы и данные из общей инфраструктуры.

Каждый продукт служит для удовлетворения различных требований к безопасности привилегированного доступа. Все вместе они предоставляют комплексное, безопасное решение для ОС, конечных точек, серверов, баз данных, приложений, гипервизоров, сетевых устройств, систем безопасности и т. д. Организации могут использовать их в локальных и облачных средах, промышленных системах управления, а также на всех стадиях интегрированной разработки и эксплуатации.

Рекомендуемые меры по защите привилегированного доступа:

- Приоритетное определение политик.
- Обнаружение всех привилегированных аккаунтов и учётных данных.
- Защита учётных данных привилегированных аккаунтов пользователей и приложений и управление ими.
- Контроль, безопасность и мониторинг привилегированного доступа к серверам, базам данных, веб-сайтам, решениям SaaS и любым целевым приложениям.
- Доступ с минимальными привилегиями для бизнес-пользователей и ИТ-администраторов.
- Управление приложениями на конечных точках и серверах.
- Использование интеллектуального анализа привилегированных аккаунтов в режиме реального времени для обнаружения текущих атак и реагирования.

Core Privileged Access Security

Защита учётных данных и управление ими

Обнаружение, контроль и защита привилегированных учётных данных

Решение CyberArk предотвращает злонамеренное использование привилегированных паролей и SSH–ключей, а также обеспечивает надлежащий порядок и безопасность уязвимых аккаунтов. Оно защищает привилегированные учётные данные на основе политики безопасности привилегированного доступа и контролирует, кто и когда может получить доступ к определенным учётным данным. Этот автоматизированный процесс сокращает трудоёмкие и подверженные ошибкам задачи по отслеживанию и обновлению привилегированных учётных данных в ручном режиме, позволяя легко соблюдать стандарты аудита и соответствия.

- Защита от несанкционированного получения учётных данных привилегированных аккаунтов и предоставление авторизованным пользователям необходимого доступа для допустимых служебных целей.
- Обновление и синхронизация привилегированных паролей и SSH-ключей на регулярной основе или по требованию исходя из политик.
- Обнаружение и защита привилегированных учётных данных в локальных, гибридных и облачных средах, на всех стадиях DevOps, а также на непостоянно подключенных конечных точках за пределами сети.
- Автоматизация и упрощение задач по управлению привилегированными аккаунтами посредством API-интерфейсов REST, включая операции в аккаунтах, правила регистрации, предоставление разрешений и другие.
- Специалисты по безопасности и аудиту имеют чёткое представление о том, к каким привилегированным или коллективным аккаунтам, когда и зачем обращались отдельные пользователи.

Изоляция и мониторинг сеансов

Изоляция, контроль, а также мониторинг и протоколирование сеансов в режиме реального времени

Решение CyberArk обеспечивает защиту, изоляцию, контроль и мониторинг доступа и действий привилегированных пользователей при работе с критически важными системами Unix, Linux и Windows, базами данных, виртуальными машинами, сетевыми устройствами, мейнфреймами, веб-сайтами, решениями SaaS и т. д. Оно предлагает единую точку управления, предотвращает попадание вредоносного ПО на целевую систему за счёт изоляции конечных пользователей и регистрирует каждое нажатие клавиши и щелчок мыши для непрерывного мониторинга.

Последовательная запись даёт полное представление о сеансе с возможностями поиска, локализации и оповещёния о важных событиях без необходимости фильтрации данных в журналах. Мониторинг в режиме реального времени обеспечивает постоянную защиту привилегированного доступа, а также автоматическую приостановку и завершение привилегированных сеансов при выявлении подозрительной активности. Решение также предлагает полную интеграцию с решениями SIEM сторонних поставщиков, включая предупреждения о необычной активности.

- Изоляция привилегированных сеансов предотвращает распространение вредоносных программ из конечной точки на критически важные системы.
- Защита привилегированных паролей и ключей SSH от новейших методов злоумышленников, таких как регистрация нажатия клавиш и атаки типа Pass-the-hash.
- Защита и контроль привилегированных сеансов для предотвращения обхода системы безопасности вредоносными программами или атаками «нулевого дня».
- Создание индексированных, устойчивых к фальсификациям протоколов привилегированных сеансов и предоставление метаданных с поисковым механизмом.
- Управление из командной строки и встроенный доступ по протоколу SSH с сохранением возможности использовать пароли или ключи SSH для безопасной работы с привилегированными аккаунтами.
- Возможность создания моста Active Directory, позволяющая организациям централизованно управлять пользователями и аккаунтами Unix, связанными с Active Directory через платформу CyberArk.

Анализ активности в привилегированных аккаунтах и обнаружение угроз

Аналитика и оповещёние о вредоносной активности в привилегированных аккаунтах

CyberArk предлагает решение по интеллектуальному анализу безопасности для обнаружения, оповещёния и реагирования на аномальную активность в привилегированных аккаунтах, которая указывает на проводимую атаку. Решение собирает целевой набор данных из нескольких источников, включая CyberArk Digital Vault, SIEM и сеть. После этого оно применяет сложную комбинацию статистических и детерминированных алгоритмов, позволяя организациям выявлять признаки компрометации на начальных этапах атаки с помощью обнаружения вредоносных привилегированных действий.

- Обнаружение и оповещёние в режиме реального времени с автоматическим реагированием на зафиксированные инциденты.
- Определение аномалий и вредоносных действий, связанных с привилегированным доступом, с возможностью обнаружения текущих атак.
- Адаптация распознавания угроз к меняющемуся набору рисков с помощью алгоритмов самообучения.
- Сопоставление инцидентов и присвоение уровней угроз.
- Повышение ценности существующих решений SIEM посредством встроенной интеграции.
- Оптимизация процессов аудита благодаря информативным данным о моделях и активности пользователей.

Alero™: доступ удалённых поставщиков

Быстрое и безопасное подключение удалённых поставщиков к платформе CyberArk без VPN, агентов или паролей

CyberArk® Alero™ — это решение SaaS, сочетающее в себе доступ Zero Trust, биометрическую многофакторную аутентификацию и своевременную инициализацию. Alero предоставляет удалённым поставщикам доступ только к необходимым им ресурсам за счёт полной интеграции с решением CyberArk Core Privileged Access Security для возможностей комплексного аудита, регистрации и восстановления. Alero обеспечивает быстрый, удобный и безопасный привилегированный доступ для удалённых поставщиков, которым нужно работать с критически важными внутренними системами.

Не требуя VPN, агентов или паролей, Alero исключает эксплуатационные расходы для администраторов и повышает уровень безопасности организации.

- Интеграция с CyberArk Core PAS для предоставления дополнительного уровня защиты критически важных систем
- Внедрение более безопасного решения, чем традиционные подходы на базе устройств идентификации или VPN
- Устранение эксплуатационных издержек, связанных с управлением VPN, агентами и паролями

Управление минимальными привилегиями

Детальный контроль уровня серверов *NIX и Windows

CyberArk позволяет привилегированным пользователям использовать команды администрирования из собственных сеансов Unix/Linux, исключая ненужный доступ с правами суперпользователя или администратора. Это защищённое решение корпоративного уровня с возможностью делегирования полномочий предлагает унифицированную и согласованную регистрацию действий суперпользователей. Оно связывает их активность с личными именами, одновременно обеспечивая свободу для выполнения должностных функций. Точное управление доступом осуществляется при постоянном мониторинге всех административных команд, выполняемых суперпользователями, с учётом их ролей и задач. Решение также позволяет организациям блокировать и сдерживать атаки на серверы Windows для снижения риска кражи информации или ее шифрования с целью получения выкупа.

- Замена часто используемых систем для делегирования полномочий централизованным альтернативным решением, обеспечивающим точное управление привилегиями и безопасное хранение журналов аудита.
- Подтверждение возможностей защиты, контроля и мониторинга привилегий суперпользователей для аудиторов.
- Предоставление подробных контрольных записей о том, кем, когда и по какой причине привилегии повышались до прав суперпользователя.
- Сокращение привилегий суперпользователей до действительно необходимых с целью снижения риска злоупотреблений или ошибок.
- Доступ к полностью делегированным оболочкам суперпользователя для интуитивно понятной работы в соответствии с поставленными задачами.
- Встроенные шаблоны политик для разграничения обязанностей на серверах Windows с помощью управления привилегиями администратора исходя из роли пользователя.
- Возможность включения команд в белый/черный список отдельно для каждого пользователя и/или для каждой системы.

Обеспечение безопасности контроллеров домена

Защита контроллеров домена Windows от атак Kerberos

CyberArk предлагает агент Windows, который практически не потребляет ресурсы системы и анализирует сетевое поведение для обнаружения текущих атак Kerberos. Данное решение обеспечивает мониторинг и защиту контроллеров домена, исключая работу под чужим именем и несанкционированный доступ. Кроме того, оно помогает обезопасить организацию от множества распространенных типов атак на протокол Kerberos.

- Обнаружение различных потенциальных угроз, включая предполагаемое хищение учётных данных, перемещёние по сети и повышение привилегий.
- Оповещёние в режиме реального времени через информационную панель CyberArk, электронную почту или информационную панель SIEM.
- Применение точных средств управления для мониторинга наименьших привилегий и приложений на контроллерах домена.
- Обнаружение целого ряда текущих атак на протокол Kerberos, включая Golden Ticket, Overpass-the-Hash и манипуляции с сертификатами атрибутов привилегий (PAC).

Управление конфиденциальной информацией приложений, контейнеров и сред DevOps

Application Access Manager™

Защита, контроль и аудит учётных данных приложений в локальных, гибридных, контейнерных и мультиоблачных средах

CyberArk Application Access Manager обеспечивает комплексное управление привилегированным доступом, учётными данными и секретами для широко используемых типов приложений и машинных идентификаторов. Например, Application Access Manager защищает учётные данные готовых коммерческих приложений, традиционных приложений собственной разработки, сценариев, а также контейнерных приложений, созданных с использованием методик DevOps.

Application Access Manager предоставляет мощное решение по обеспечению безопасности, которое позволяет организациям внедрять контроль, управление и аудит в отношении любого машинного привилегированного доступа для различных типов приложений в локальных, гибридных, контейнерных и мультиоблачных средах.

- Внедрение строгой аутентификации за счёт использования собственных атрибутов приложений, контейнеров и других машинных идентификаторов для устранения проблемы загрузки первичного ключа и потенциальных уязвимостей.
- Упрощенная интеграция за счёт поддержки широкого спектра проверенных коммерческих программных платформ, приложений и инструментов, таких как бизнес-приложения, средства безопасности, платформы RPA, инструменты непрерывной интеграции/разработки и контейнерные платформы.
- Ускоренное развёртывание и использование благодаря удобному для разработчиков решению для защиты конфиденциальных данных в средах приложений и DevOps, позволяющему сосредоточиться на разработке ПО. Кроме того, решения с открытым исходным кодом помогают разработчикам и администраторам DevOps легко оценивать, развёртывать и защищать свои среды DevOps.

- Всесторонний аудит любых возможностей доступа путем их комплексного отслеживания и проверки с защитой от фальсификаций.
- Последовательное применение политик доступа: внедрение ролевой модели управления доступом для машинных идентификаторов, использование интеграции с другими решениями CyberArk и партнеров для централизованного управления политиками на всем предприятии, а также применение иных средств управления на основе политик.
- Поддержка непрерывных бизнес-процессов и других требований компании, включая масштабируемость, готовность, избыточность и отказоустойчивость, оповещёние, ротацию на основе политик и т. д.

Управление привилегиями конечных устройств и защита от кражи учётных данных

Endpoint Privilege Manager

Применение минимальных привилегий на конечных точках

Решение Endpoint Privilege Manager защищает привилегии на конечных точках (настольные ПК/ноутбуки Windows и Mac) и сдерживает атаки на самом раннем этапе. Оно позволяет аннулировать права локального администратора с минимальным влиянием на продуктивность работы пользователей, плавно повышая привилегии для разрешенных приложений или задач. Управление приложениями с автоматическим созданием политик предотвращает выполнение вредоносных приложений в организации и запускает их неизвестные экземпляры в безопасном режиме. В сочетании с защитой от кражи учётных данных это препятствует внедрению вредоносного ПО и сдерживает атаки на конечных точках.

- Возможность удаления прав администратора у повседневных бизнес-пользователей без снижения их продуктивности, а также плавное повышение привилегий на основе политик при необходимости запуска разрешенных приложений или команд.
- Защита от проникновения и распространения вредоносных приложений, в том числе программ-вымогателей, по всей среде и возможность запуска неизвестных приложений в «ограниченном режиме» для продуктивной и безопасной работы пользователей.
- Обнаружение и блокировка попыток кражи учётных данных Windows и тех, что хранятся в популярных веб-браузерах, для предотвращения распространения через среду.
- Полная интеграция со службой CyberArk Application Risk Analysis для автоматизированного анализа и своевременного определения политик в отношении неизвестных приложений.
- Плавная интеграция с системами обнаружения угроз Check Point, FireEye и Palo Alto Networks.
- Поддержка вариантов развёртывания для локальных серверов и решений SaaS.

О компании CyberArk

CyberArk — мировой лидер в области обеспечения безопасности привилегированного доступа, критически важного уровня ИТ-безопасности для защиты данных, инфраструктуры и активов на предприятии, в облаке и на всех стадиях интегрированной разработки и эксплуатации. CyberArk предоставляет наиболее полное в отрасли решение для снижения рисков, связанных с привилегированными учётными данными и секретной информацией. Ведущие мировые организации, включая более 50% участников списка Fortune 100, доверяют компании и используют ее решения для защиты от внешних атак и внутренних злоумышленников. Штаб-квартира международной компании CyberArk находится в г. Петах-Тиква, Израиль. Компания также имеет головное представительство в США (г. Ньютон, штат Массачусетс), а ее офисы работают в странах Северной и Южной Америки, регионе EMEA, Азиатско-Тихоокеанском регионе и в Японии.

Чтобы узнать больше о компании CyberArk, посетите веб-сайт www.cyberark.com.