CYBERARK®

Privileged Session Manager

Интегрированный мониторинг привилегированной активности в БД
Уникальный подход предоставляет возможность оперативного развертывания с нулевым воздействием на БД.

Постоянный мониторинг защищает критические серверы БД и виртуальные структуры
Контролируйте и отслеживайте привилегированные сессии в реальном времени, накапливая необходимые сведения о привилегированных пользователях и их активности

Упростите аудит и соответствие
Вы знаете обо всем, что было сделано в Ваших системах, и легко найдите или используйте через единый интерфейс важные события безопасности.

Почему CyberArk?

CyberArk – доверенный эксперт в предотвращении атак до того, как они смогут остановить бизнес.

Изолирует, контролирует и обеспечивает мониторинг всех привилегированных сессий к БД, виртуальным платформам, сетевым устройствам и серверам для защиты от внутренних угроз и внешних кибер-атак, обеспечивая аудиторов сведениями о привилегированной активности.

Проблематика

Привилегированные аккаунты, такие как sysadmin, root, Oracle system, Administrator в гипервизорах и Windows, и другие доминируют над всей инфраструктурой ЦОДов. Эти привилегированные аккаунты предоставляют широкий доступ и позволяют манипулировать чувствительными данными, уничтожить их и даже привести к нарушению доступности сервисов. Поскольку привилегированные аккаунты - столь мощное средство, они постоянно являются целью и внешних, и внутренних атак. Как часто Вы спрашиваете себя: кто их использует, и что с их помощью делает? Вам понадобится узнать: что вызвало остановку продуктивной системы; или увидеть в реальном времени: что происходит в рамках привилегированной сессии. Возможно, Вам нужно контролировать тех, кто пытается получить доступ, или убедиться, что третьи лица, подключающиеся к Вашим системам, смогут это сделать, но не должны знать административные пароли? Знания о том, что происходит в сессии администратора, означают, что Вы можете:

- **Соответствовать требованиям аудита**
  Требования аудита становятся все шире и специфичнее, и Вам необходимо доказать аудитору, что Вы знаете что конкретно было сделано в данной привилегированной сессии. Множественные регулятивные документы требуют “отслеживать любой доступ к сетевым ресурсам”. Другие устанавливают принцип двойного контроля, когда для подтверждения привилегированной сессии или наблюдения за ней требуется дополнительное лицо.

- **Снижать риски инсайда и кибер-атак, способных причинить урон Вашему бизнесу**
  В 2011 году Ponemon Institute опубликовалл исследование Insecurity of Privileged Users Survey, что в более, чем 60% случаев доступ к чувствительным или конфиденциальным данным осуществляется по не связанным с рабочими функциями причинам. Слишком много лиц в компаниях имеют неконтролируемый привилегированный доступ. В то же время, кибер-атаки стали обычным явлением, и становятся более четко спланированными, изощренными, нацеленными.

  Эти атаки могут включать инфицирование вирусами бизнес-критичных систем, перехват трафика или доступ к коду, злоупотребление клиентскими данными и остановку критичных, в том числе национальных, инфраструктур. Такие атаки используют уязвимости, предоставляющие привилегированный доступ или пароли приложений, которые могут стать роковыми для компании или репутации.
  Угрозы внешнего вторжения также имеют целью получение привилегированных аккаунтов для нанесения существенного ущерба. Такие атак становятся все более сложными и лучше организованными, а поэтому требуется превентивный подход с самого начала.

- **Сократить время восстановления и минимизировать потери**
  Минимизируйте время расследования за счет отслеживания того, что происходит в привилегированных сессиях, и возможности поиска событий, которые могли вызвать нарушение работоспособности систем

Решение

Privileged Session Manager (PSM) от компании CyberArk – это центральная точка контроля целевых систем, доступ к которым возможен через привилегированные аккаунты. Это единое решение для изоляции, контроля и мониторинга всей привилегированной активности в ЦОДах.

Privileged Session Manager – часть решения CyberArk Privileged Account Security, предоставляет изоляцию, контроль и мониторинг доступа привилегированных пользователей и их активности в UNIX и Windows системах, БД и виртуальных средах.

Privileged Session Manager® позволяет:
Изолировать, контролировать и отслеживать привилегированный доступ к чувствительным серверам Windows, Unix/Linux, zOS, iSeries и сетевым устройствам. Производить видеозапись и просмотр привилегированных сессий, а также просмотр защищенного подключения в По сравнению с другими средствами мониторинга БД оперативное развертывание без риска для продуктивных бизнес-приложений или необходимости их остановки. Контролировать и отслеживать любое подключение к гипервизору или использование его привилегированных аккаунтов, видеозапись всего происходящего реальном времени.

Предоставлять удаленный доступ к чувствительным системами, используя привилегированный режим «одного окна» без необходимости передавать учетные данные пользователям, например внешним поставщикам.

Выступать jump-сервером, с дополнительными возможностями контроля и мониторинга сессий.

Система защиты БД с нулевым воздействием на них: не влияя на производительность, но фиксируя все операции администратора БД. В отличии от других средств мониторинга БД, обеспечивает оперативное развертывание без риска для продуктивных бизнес-приложений или необходимости их остановки Контролировать и отслеживать любое подключение к гипервизору или использование его привилегированных аккаунтов, видеозапись всего происходящего без установки агентов.

Выгоды

Изоляция привилегированных сессий для лучшей защиты от кибер-атак

PSM обеспечивает полную изоляцию между стацией пользователя и целевой системой отделяя потенциально вредоносный код на станции от чувствительной целевой системы, устраняя риск проникновения вредоносного кода на критические системы. Защищая и изолируя такие критические активы, при этом зная, что происходит в привилегированных сессиях, Вы избегаете ошибок персонала, минимизируете угрозы инсайда и предотвращаете внешние атаки

Одна из лучших особенностей CyberArk – это то, что решение действует как посредник для ИТ-подразделения – устраняет длительный и трудоемкий процесс, заменяя его простой, безопасной и эффективной системой

Джетро Корнолиссен,

Глава глобального операционного центра безопасности, Rabobank International

Победитель в категории «Лучшее IAM решение»

Рекомендовано как «Лучший продукт года для безопасности

Гарантия постоянного мониторинга для защиты и соответствия без влияния на бизнес

Для соответствия требованиям PCI DSS, SOX, HIPAA, Basel III и многим другим Вам необходимо доказать аудиторам, что вы контролируете привилегированный доступ к чувствительным системам и обеспечиваете сбор доказательств о том, что было сделано в целевых системах, виртуальных системах, БД и веб-приложениях, как в реальном времени, так и при расследовании инцидентов.

Повышение эффективности за счет централизованного контроля и управления

Все привилегированные сессии к любым целевым системам контролируются и управляются централизованно, на основе предопределенных политик и процессов. И при определении средств контроля сессий, и при просмотре видеозаписей или событий безопасности применяется единый веб-интерфейс.

Сокращение времени на анализ и минимизацию финансовых последствий

Легкость поиска, определения и оповещения о событиях дает элементарный анализ первопричин, минимизирующий потенциальный ущерб компании вследствие нарушений безопасности или ошибок персонала. Видеозаписи помогают видеть целостную картину происходящего в сессии в более удобной форме, нежели отбор и фильтрование исчерпывающего набора логов.

Возможности

Будьте всегда готовы к аудиту и защищены с богатым набором возможностей продукта.

Безопасность и аудит

- Высокозащищенное хранилище для хранения логов и видеозаписей
- Прокси-архитектура создает защищенное и изолированное окружение, устраняющее уязвимости конечных точек, вредоносный код на которых может влиять на административные или привилегированные сессии

Централизованный аудит и управление соответствием последствий

- Легкость поиска, определения и оповещения о событиях дает элементарный анализ первопричин, минимизирующий потенциальный ущерб компании вследствие нарушений безопасности или ошибок персонала. Видеозаписи помогают видеть целостную картину происходящего в сессии в более удобной форме, нежели отбор и фильтрование исчерпывающего набора логов.

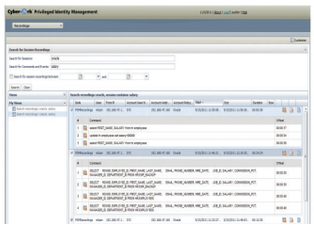
Реагирование на рискованные операции

- Отслеживая сессию в реальном времени, Вы можете вмешаться или прервать привилегированную сессию при подозрительной активности. Вы также можете наблюдать за действиями привилегированных пользователей без необходимости физически присутствовать рядом с ними.

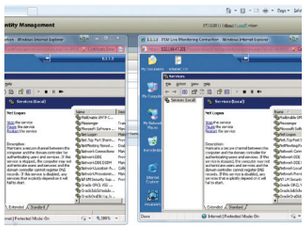
Простота внедрения

- Большинство средств мониторинга БД и гипервизоров требуют изменения сетевой топологии и перемаршрутизации сетевых потоков/приложений и бизнес-транзакций через систему защиты.

  Это удлиняет процесс развертывания, так как требуется проверить каждое бизнес-приложение для исключения нежелательных воздействий на продуктивные системы. Поскольку PSM сосредоточен только на управлении привилегированными пользователями и аккаунтами, и не требует инсталляции на продуктивных серверах, то нет необходимости в длительных тестах или анализе воздействий, что существенно сокращает время внедрения.



Поиск по привилегированным командам и воспроизведение с необходимого момента времени



Просмотр привилегированной сессии в реальном времени с возможностью взаимодействовать или прервать ее

- Запись и просмотр сессий в соответствии с политиками и ролями пользователей для всех типов привилегированных аккаунтов. Персональные и неуправляемые привилегированные аккаунты также можно отслеживать с помощью PSM
- Привилегированный Single Sign On для инициации сессий без необходимости раскрывать учетные данные

Поддерживается широкий спектр протоколов и клиентов, включая Unix, SSH, Telnet, Windows RDP, RAdmin, Remotely Anywhere, AS400, Mainframes, веб-приложения, БД и инструменты виртуализации

Запись привилегированных сессий

- Просмотр видеозаписей для анализа событий или расследования инцидентов
- Логирование команд в сессиях SSH и аудит SQL-команд в сессиях Oracle
- Поиск событий по времени их совершения
- Один PSM сервер позволяет записывать 100 одновременных сессий в формате высокой компрессии, с балансировкой нагрузки и высокой доступностью
- Поддерживается возможность вывода на экран контролируемому пользователю сообщений о записи сессии

Решение корпоративного класса

- Интеграция с CyberArk Shared Technology Platform обеспечивает масштабируемость, высокую доступность, централизованное управление и отчетность
- Готовая интеграция с продуктами Privileged Account Security обеспечивает управляемость, мониторинг, запись и защищенный SSO для привилегированных аккаунтов
- Распределенная архитектура с централизованным управлением и хранением является идеальной для множества сетей и сайтов, сохраняя единый интерфейс администрирования, аудита и мониторинга
- Интеграция с корпоративными инфраструктурами, включая строгую аутентификацию (Alladin, SecurID, Radius, PKI, LDAP и многие другие), мониторинг и интеграцию с SIEM, SNMP, Syslog и SMTP, встроенные возможности HA/и многое другое

Цифры и факты:

CyberArk защищает 8 из 10 крупнейших банков мира.

Треть компаний Fortune 50 эксплуатируют CyberArk.