CYBERARK® PRIVILEGE ON PREMISES

ПРОБЛЕМАТИКА

Привилегированные учётные записи и доступ по ним представляют собой самую большую уязвимость системы безопасности, с которой сегодня сталкивается любая организация. В ИТ-средах такие учётные записи существуют как в аппаратном, так и программном обеспечении. При правильном использовании привилегированные учётные записи используются для обслуживания систем, упрощения автоматизированных процессов, защиты конфиденциальной информации и обеспечения непрерывности бизнеса. Но в руках злоумышленников они могут быть использованы для кражи конфиденциальных данных и нанесения непоправимого ущерба бизнесу.

Привилегированные учётные записи используются практически во всех кибератаках. Злоумышленники исользуют их, чтобы отключать системы безопасности, брать под контроль критически важную ИТ-инфраструктуру и получать доступ к конфиденциальным бизнес-данным и личной информации. Всё больше организаций сталкиваются с проблемами защиты, контроля и мониторинга привилегированного доступа, включая:

- **Управление учётными данными.** Многие ИТ-организации полагаются на ручные и подверженные ошибкам административные процессы для ротации и обновления привилегированных учётных данных. Это - неэффективный, рискованный и дорогостоящий подход.
- **Отслеживание привилегированной активности.** Многие предприятия не могут централизованно отслеживать и контролировать привилегированные сеансы, подвергая бизнес угрозам безопасности и нарушениям нормативных требований.
- **Мониторинг и анализ угроз.** Во многих организациях отсутствуют комплексные инструменты анализа угроз, и они не в состоянии превентивно выявлять подозрительные действия и устранять инциденты безопасности.
- **Контроль доступа привилегированных пользователей.** Практика показывает, что организациям сложно эффективно контролировать доступ привилегированных пользователей к облачным платформам (IaaS и PaaS), приложениям SaaS, социальным сетям и многому другому. Это создаёт риск нарушений требований нормативного регулирования и сложности в операционной деятельности.
- **Защита удалённых поставщиков.** Большинство организаций не имеют практической возможности контролировать удалённый доступ к привилегированным корпоративным ИТ-системам и инфраструктуре.

РЕШЕНИЕ

Решение Privilege On Premises является частью CyberArk Identity Security Platform. Оно включает основные средства управления для защиты, контроля и мониторинга привилегированного доступа в локальной, облачной и гибридной инфраструктурах. Решение помогает эффективно управлять привилегированными учётными данными с помощью надежных методов аутентификации, превентивно отслеживать и контролировать действия привилегированных учётных записей, интеллектуально определять подозрительную активность и быстро реагировать на угрозы.

- **Организуйте привилегированный доступ с помощью современной системы единого входа (SSO) и адаптивной многофакторной аутентификации (MFA),** а доступ к привилегированным (или корпоративным) ресурсам с помощью единого набора учётных данных, что обеспечит более строгое соблюдение политик паролей и снижение риска

Эффективная защита и контроль привилегированного доступа в локальной, облачной и гибридной инфраструктуре.

СПЕЦИФИКАЦИЯ

Алгоритмы шифрования:

- AES-256, RSA-2048
- Интеграция с HSM
- Криптография FIPS 140-2

Высокая доступность

- Поддержка кластеризации
- Несколько сайтов аварийного восстановления
- Интеграция с системами резервного копирования

Управление доступом и рабочим процессом:

- LDAP-каталоги
- Identity and Access Management
- Системы заявок и организации рабочего процесса

Многоязычный портал:

- Английский, французский, немецкий, испанский, русский, японский, китайский (упрощенный и традиционный), бразильский португальский, корейский

Методы аутентификации:

- Имя пользователя и пароль, LDAP, аутентификация Windows, RSA SecurID, Web SSO, RADIUS, PKI, SAML, смарт-карты

Мониторинг:

- Интеграция с SIEM, SNMP-ловушки, email-уведомления

СПЕЦИФИКАЦИЯ

Пример поддерживаемых устройств:

- Операционные системы, виртуализация и контейнеры: Windows, *NIX, IBM iSeries, Z/OS, OVMS, ESX/ ESXi, XenServers, HP Tandem*, MAC OSX*, Docker
- Приложения Windows: сервисные аккаунты, включая SQL-сервер в кластере, Scheduled Tasks, IIS Application Pools, COM+, IIS Anonymous Access, Cluster Service
- Базы данных: Oracle, MSSQL, DB2, Informix, Sybase, MySQL and any ODBC compliant database
- Усройства безопасности: CheckPoint,Cisco, IBM, RSA Authentication Manager, Juniper, Blue Coat*, TippingPoint*, SourceFire*, Fortinet*, WatchGuard*, Industrial Defender*, Acme Packet*, Critical Path*, Symantec*, Palo Alto*
- Сетевые устройства: Cisco, Juniper*, Nortel*, HP*, 3com*, F5*, Nokia*, Alcatel*, Quintum*, Brocade*, Voltaire*, RuggedCom*, Avaya*, BlueCoat*, Radware*, Yamaha* McAfee NSM*
- Приложения: CyberArk, SAP, WebSphere, WebLogic, JBOSS, Tomcat, Cisco, Oracle ERP*, Peoplesoft*, TIBCO*
- Каталоги: Microsoft, Oracle Sun, Novell, UNIX vendors, CA
- Удалённый контроль и мониторинг: IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fijitsu* and ESX
- Файлы конфигурации: (flat, INI, XML)
- Публичные облака Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

* Для этого подключаемого модуля может потребоваться настройка или испытания на месте. Проконсультируйтесь с отделом продаж CyberArk для получения более подробной информации.

неправильного использования паролей и получения информации о правилах доступа в масштабах всего предприятия. Обеспечьте дополнительный уровень защиты с помощью адаптивной MFA, которая использует контекстные атрибуты пользователя, такие как местоположение, устройство и сетевая информация. Это позволяет исключить риск проникновения при каждой попытке входа пользователя в систему и создать политики динамического доступа

- **Централизованно защищайте и управляйте доступом к привилегированным учётным данным на основе политик безопасности, определенных администратором.** Автоматическая ротация учётных данных привилегированной учетной записи (пароль и ключ SSH) исключает необходимость ресурсоёмкого ручного управления, обеспечивая защиту учётных данных, используемых в локальных, гибридных и облачных средах. Убедитесь, что учётные данные Windows и MacOS, которые не подключены к сети, защищены и постоянно меняются.
- **Изолируйте и защищайте сеансы привилегированных пользователей.** Мониторинг и запись позволяют службам безопасности просматривать привилегированные сеансы в режиме реального времени, автоматически приостанавливать и удаленно завершать подозрительные сеансы, а также вести полный, с функцией поиска контрольный журнал активности привилегированных пользователей. Физическое разграничение конечных точек пользователей от критически важных целевых систем при помощи безопасного, усиленного jump-сервера гарантирует, что вредоносные программы на зараженном пользовательском устройстве не смогут попасть на критически важные объекты.
- **Обнаруживайте, предупреждайте и реагируйте на аномальные действия.** Это решение собирает данные из нескольких источников и применяет сложную комбинацию статистических и детерминированных алгоритмов для выявления злонамеренных действий с привилегированным доступом. Двунаправленный поток данных позволяет обмениваться информацией о привилегированном доступе с высоким риском с помощью общих инструментов SIEM.
- **Безопасный удаленный доступ к поставщику.** С помощью биометрической многофакторной аутентификации без использования VPN, агента и пароля вы легко и безопасно сможете аутентифицировать внешних поставщиков, получающих доступ к CyberArk. Просто предоставьте авторизованным пользователям своевременный доступ к критически важным внутренним ресурсам и включите автоматическую изоляцию сеансов, мониторинг и запись.

ПРЕИМУЩЕСТВА

- **Защита от атак.** Повышение безопасности привилегированного доступа. Защита доступ к паролям привилегированных учётных записей и SSH-ключам. Защита системы от вредоносных программ и атак. Эффективный контроль подозрительных активностей и вредоносных действий. Защита от несанкционированного доступа к привилегированным учётным записям, подделки, мошенничества и кражи.
- **Высокая операционная эффективность.** Исключение ресурсоёмких административных процессов и подверженных ошибкам. Упощрение операций и повышение эффективности групп ИБ. Концентрация усилий ценных ИТ-специалистов на стратегических задачах для поддержки основной деятельности.
- **Соответствие нормам аудита и нормативного регулирования.** Внедрение средств управления привилегированным доступом на основе политик обеспечивает соответствие государственным и отраслевым нормам. Простая демонстрация политик и процессов аудиторам. Подробные контрольные журналы и истории доступа.
- **Развитие цифрового бизнеса.** Баланс между безопасностью и удобством работы с пользователями. Беспрепятственный доступ для привилегированных пользователей, подключающихся к активам уровня Tier0, с централизованной видимостью и элементами контроля для управления привилегированным доступом..