CYBERARK

DATA SHEET

# CORE PRIVILEGED ACCOUNT SECURITY

Эффективная защита, мониторинг и контроль привилегированных учетных записей в локальной, облачной и гибридной инфраструктуре

## Спецификация:

**Алгоритмы шифрования:**

- AES-256, RSA-2048
- HSM integration
- FIPS 140-2 validated cryptography

**Высокая доступность:**

- Поддержка кластеризации
- Аварийное восстановление множественных сайтов
- Интеграция с корпоративной системой резервного копирования

**Управление доступом:**

- Директории LDAP
- Управление идентификацией и доступом
- Системы тикетов и управления рабочим процессом

**Языковая поддержка:**

- Английский, французский, немецкий, испанский, русский, японский, китайский, бразильский, португальский, корейский.

**Методы аутентификации:**

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

**Мониторинг:**

- интеграция с SIEM, SNMP-ловушками, уведомление по электронной почте

## Проблематика

Привилегированные учетные записи представляют сегодня самую большую угрозу для безопасности любой организации. Такие учетные записи существуют как в аппаратных средствах, так и в программном обеспечении. При правильном использовании привилегированные учетные записи обеспечивают функционирование и обслуживание рабочих систем, автоматизацию процессов, защиту конфиденциальной информации и непрерывность всех бизнес-процессов. Но в чужих руках эти учетные записи могут быть использованы для кражи конфиденциальных данных и нанести непоправимый ущерб бизнесу. Привилегированные учетные записи используются почти в каждой кибер-атаке. Нарушители могут использовать их для отключения системы безопасности, получения контроля над критической ИТ-инфраструктурой и получения доступа к конфиденциальным бизнес-данным и персональной информации.

Организации сталкиваются с большим количеством проблем, связанных с защитой, контролем и мониторингом привилегированных учётных записей, в том числе:

- Управление учётными данными. При ротации и обновлении привилегированных учётных записей многие ИТ-организации полагаются на ручные, ресурсоёмкие административные процессы с использованием человеческих ресурсов, которым свойственны частые ошибки. Это - неэффективный, рискованный и дорогостоящий подход.
- Отслеживание активности привилегированной учетной записи. Многие предприятия не могут осуществлять централизованный мониторинг и контролировать сеансы привилегированных учетных записей, подвергая бизнес постоянным угрозам и нарушая нормативные требования.
- Мониторинг и анализ угроз. Во многих организациях отсутствуют инструменты комплексного анализа угроз, из-за чего они не могут эффективно выявлять подозрительные действия и устранять связанные с нарушением инциденты безопасности.
- Контроль доступа суперпользователей. Организации много усилий тратят на проверку и контроль доступа суперпользователей к критичным для бизнеса системам, ставя под угрозу соблюдение нормативных требований и усложняя всю процедуру работы.
- Защита контроллеров домена Windows. Используя уязвимости в протоколе Kerberos, атакующие могут выдать себя за авторизованных пользователей и использовать уязвимости в протоколе аутентификации, чтобы получить доступ к критическим ИТ-ресурсам и конфиденциальным данным.

## Решение

В сфере защиты информации решение Core Privileged Account Security является наиболее эффективным средством контроля и мониторинга привилегированных учетных записей в локальной, облачной и гибридной инфраструктурах. Разработанное исключительно для обеспечения безопасности привилегированных учётных записей, решение компании CyberArk помогает эффективно управлять привилегированными учетными записями и правами доступа, активно отслеживает и контролирует активность привилегированных учетных записей, интеллектуально выявляет подозрительные действия и быстро реагируют на угрозы.

- Централизованная защита и контроль доступа к привилегированным учетным данным на основании административно определенных политик безопасности. Автоматическая ротация паролей привилегированных учётных записей и SSH-ключей полностью устраняет необходимость в ресурсоёмких и подверженных ошибкам административных процедурах, эффективно защищая таким образом учётные данные, которые используются в локальных, гибридных и облачных средах.

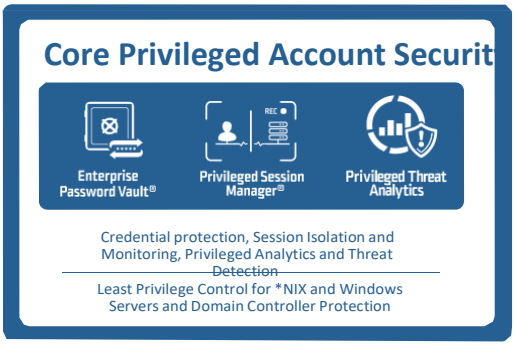
## Спецификация:

**Примеры поддерживаемых систем:**

- Операционные системы, виртуализация и контейнеры: Windows, *NIX, IBM iSeries, Z / OS, OVMS, ESX / ESXi, XenServers, HP Tandem *, MAC OSX *, Docker.
- Приложения Windows: учетные записи служб, включая учетные записи службы SQL Server в кластере, запланированные задачи, пулы приложений IIS, COM +, анонимный доступ IIS, служба кластеров.
- Базы данных: Oracle, MSSQL, DB2, Informix, Sybase, MySQL и любая ODBC-совместимая база данных
- Решения по ИБ: 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*
- Директории: Microsoft, Oracle Sun, Novell, UNIX-системы, CA
- Удалённый контроль и мониторинг: IBM, HP iLO, Sun, Dell DRAC, Digi*, Cyclades*, Fijitsu* и ESX
- Конфигурационные файлы (flat, INI, XML)
- Общедоступные облачные среды: Amazon Web Services (AWS), Microsoft Azure, Google, Cloud Platform (GCP)

* Этот плагин может потребовать настройки или проверочное тестирование на месте. Для получения дополнительной информации обратитесь к CyberArk Sales Engineering.

- Изоляция и защита сессий привилегированных пользователей, а также целевых систем от вредоносного ПО на конечных точках. Возможности мониторинга и записи сессий позволяют специалистам по безопасности просматривать привилегированные сеансы в режиме реального времени, автоматически приостанавливать и удаленно завершать подозрительные сеансы и поддерживать всеобъемлющий, контрольный журнал действий привилегированных пользователей, доступный для проверки и аудита.
- Обнаружение, предупреждение и реакция на аномальную деятельность привилегированных акканутов. Решение собирает данные из нескольких источников и применяет сложную комбинацию статистических и детерминированных алгоритмов для определения подозрительной и потенциально опасной активности привилегированных учетных записей.
- Контроль доступа с минимальными привилегиями для систем *NIX и Windows. Данное решение позволяет привилегированным пользователям запускать авторизированные административные команды непосредственно из своих сеансов Unix или Linux, не используя при этом ненужные привилегии "root". Также существует возможность блокировать и отражать атаки на серверах и рабочих станциях Windows, снижая риск кражи или шифрования информации с целью дальнейшего выкупа.
- Защита контроллеров домена Windows. Данное решение обеспечивает контроль минимальных привилегий и приложений на доменных контроллерах, а также обнаружение незавершённых атак. Оно защищает от заимствования прав, получения несанкционированного доступа и разнообразных типов Kerberos-атак, включая манипуляции с золотым билетом, использованием хеша и сертификатом атрибута привилегий (Golden Ticket, Overpass-the-Hash и Privilege Attribute Certificate (PAC)).




## Преимущества:

- Устранение угроз безопасности. Усиление безопасности привилегированных учетных записей. Защита доступа к паролям привилегированных учетных записей и SSH-ключам. Защита системы от вредоносных программ и атак. Эффективное обнаружение и реагирование на подозрительную деятельность и вредоносные действия. Защита от несанкционированного доступа к привилегированным учетным записям, имперсонификации, мошенничества и кражи.
- Сокращение операционных расходов и сложности управления. Устранение рутинных, трудоёмких и подверженных ошибкам административных процессов. Упрощение рабочего процесса и повышение эффективности работы специалистов ИТ и ИБ. Высвобождение ценного времени ИТ-профессионалов для решения стратегических задач и поддержки основных видов деятельности.
- Соответствие нормативным требованиям. Институциональный контроль доступа к привилегированным учетным записям на основе политики для обеспечения соответствия государственным и отраслевым нормам. Простой и понятный процесс предоставления аудиторам отчётов о политиках и процессах. Подробные контрольные журналы и истории доступа для демонстрации полного соответствия нормативным требованиям.
- Увеличение эффективности временных затрат. Защита и продление предыдущих инвестиций. Использование возможностей интеграции решений с широким спектром ИТ-систем и систем безопасности, включая системы аутентификации, решения по обработке сервисных запросов, платформы по идентификации и управлению доступом, а также SIEM-решения.
- Эффективный системный контроль. Понимание какие привилегированные записи существуют и кто имеет к ним доступ. Полноценные политики безопасности для привилегированных учетных записей. Мониторинг активности привилегированных учетных записей в режиме реального времени и логирование активности пользователей.