Enterprise Password Vault®

Это решение обеспечивает реализацию корпоративной политики, гарантирующей защиту наиболее важных систем, управление всем жизненным циклом общих и привилегированных учетных записей в центрах обработки данных.

Возможность получения данных привилегированных учетных записей и утверждения доступа непосредственно с мобильного устройства. Это обеспечивает безопасность обращения к привилегированным учетным записям в любое время и с любого устройства.

EPV содержит единую централизованную панель для управления всеми типами привилегированных учетных записей.

В чем преимущества решений CyberArk?

CyberArk предлагает решения в области информационной безопасности, которые позволяют защититься от целевых кибератак, направленных на ключевые объекты информационной среды предприятия.

Задача

Одной из ключевых проблем в области управления рисками и обеспечения соответствия ИТ-среды нормативным требованиям является некорректное управление привилегированными учетными записями и их паролями. Привилегированные учетные записи имеются практически в каждом устройстве и приложении предприятия: пользователь 'root' в серверах UNIX/ESX, Администратор на рабочих станциях Windows, технологические учетные записи, общие учетные записи SAP, Cisco Enable, Oracle system/sys, MSSQL SA и многие другие. Этим учетным записям доступна самая ценная корпоративная информация, поэтому управлять ими необходимо особенно тщательно. Однако им не всегда уделяется должное внимание. Ситуацию осложняет редкая смена паролей, а также невозможность отслеживания пользователей и времени использования этих паролей. Некорректно управляемые привилегированные учетные записи представляют значительную угрозу для организации. В числе рисков:

- Несоответствие требованиям регуляторов. Нормативные положения (например, SOX, PCI, Basel III и другие) требуют от организации предоставлять отчетность о лицах, обращавшихся к привилегированным учетным записям, времени обращения и соответствии запроса политикам организации.
- Внутренние и внешние угрозы. Внутренние угрозы по-прежнему остаются серьезной проблемой для крупных организаций. В 86% случаев несанкционированный доступ совершается лицами с правами системного администратора; в половине случаев срок полномочий этих лиц уже истек (совместное исследование CERT и служб безопасности). Внешние целевые атаки, в ходе которых злоумышленник стремится получить привилегированный доступ для обращения к критически важным системам и данным организации, также остаются серьезной угрозой.
- Простой информационных систем. Если срочно вызванному внештатному администратору не предоставить необходимый пароль, восстановление системы после сбоя может затянуться на несколько часов, которые могут дорого обойтись предприятию.
- Административные накладные расходы. Если к сети подключены сотни устройств, ручное управление привилегированными учетными записями и создание отчетов об их деятельности может занимать очень много времени; при этом велика вероятность возникновения ошибок, связанных с человеческим фактором.

Решение

Enterprise Password Vault (EPV) — комплексное решение для управления привилегированными учетными записями уровня предприятия. В число поддерживаемых функций входит обеспечение безопасности, управление, автоматизация и регистрация действий от имени таких учетных записей. Возможности Enterprise Password Vault:

Минимизация угроз. Уникальное решение CyberArk Digital Vault обеспечивает безопасность привилегированных учетных записей и соответствие операций с такими учетными записями набору предварительно созданных политик. Поддерживается интеграция с системами регистрации ошибок, смена паролей по графику, получение разрешений от уполномоченных сотрудников и другие функции.

Обеспечение соответствия нормативным требованиям. Функции создания аудиторских отчетов в соответствии с SOX, PCI и т. д. позволяют повысить эффективность повседневных операций и обеспечить соответствие нормативным требованиям.

Оптимизация бизнеса. Решение поддерживает автоматическую подготовку, обеспечивает защиту и управление доступом к сотням тысяч привилегированных учетных записей через центральное хранилище.

CyberArk Enterprise Password Vault — решение с уникальными возможностями:

Минимизация потерь бизнеса и дорогостоящих простоев инфраструктуры благодаря применению корпоративной политики для защиты Ваших критически важных систем Обеспечение подотчетности всех операций доступа к самым ценным корпоративным данным благодаря использованию готовых эффективных инструментов мониторинга и создания отчетов.

Повышение производительности труда персонала благодаря применению удобного интерфейса управления привилегированными

автоматического обнаружения новых и отключенных от сети компьютеров. Защита ценных активов при работе со сторонними организациями. Решение обеспечивает возможность прямого подключения к целевому устройству без предоставления привилегированной учетной записи, а также автоматическое подключение к локальным и удаленным системам

Автоматизация управления привилегированными учетными записями в частном облаке; повышение эффективности работы администратора VMware, связанной с обнаружением гипервизоров ESX и гостевых компьютеров и управлением ими.

Преимущества

Решение Enterprise Password Vault (EPV) использует удостоенную наград технологию CyberArk Digital Vault для хранения, защиты и регистрации доступа к привилегированным учетным записям. Это обеспечивает высочайший уровень безопасности. Технология Digital Vault поддерживает множество функций обеспечения безопасности: проверку подлинности, защищенный аудит и защиту данных. Решение Enterprise Password Vault обладает широкими функциональными возможностями:

- Широкий спектр поддерживаемых целевых систем. Решение Enterprise Password Vault поддерживает широкий спектр представленных на рынке платформ и может быть с легкостью расширено для подключения новых устройств и удовлетворения уникальных требований предприятия. Это обеспечивает возможность полномасштабного внедрения решения в ИТ-инфраструктуру. Вы также можете расширить функции управления привилегированным доступом, используя для операций с конфиденциальными веб-приложениями (например, Salesforce) корпоративную учетную запись Facebook или любые веб-приложения ERP и CRM.
- Настраиваемые процессы обработки запросов. EPV можно легко интегрировать со службами технической поддержки и системами отслеживания ошибок; Вы можете потребовать, чтобы доступ к привилегированной учетной записи предоставлялся только пользователям, имеющим активную заявку на проведение работ в автоматической системе заявок. Решение обеспечивает надежный двухэтапный контроль процесса утверждения, а также предоставляет возможность монопольного входа в систему в течение ограниченного времени с автоматическим изменением пароля учетной записи по истечении этого периода времени. Для реализации процессов, связанных с запросами и утверждениями, можно использовать мобильные устройства.
- Веб-интерфейс и встроенные функции создания отчетов для пользователей и аудиторов. EPV поддерживает гибкий механизм контроля доступа для создания персонализированных представлений управляемых устройств. Аудиторам при необходимости можно предоставить прямой доступ к веб-приложению для создания и планирования отчетов. На уникальной информационной панели представлены важные статистические данные аудита и общие сведения о системных операциях.
- Прямое подключение к управляемым устройствам. EPV предоставляет прямой доступ к Windows, Unix/Linux и другим SSH-устройствам, используя запрошенную привилегированную учетную запись и не раскрывая учетные данные пользователям. Это позволяет повысить удобство использования и эффективность работы. Эта возможность также распространяется на веб- сайты и веб-приложения, где пароли особенно важно заменять или сохранять в тайне: в противном случае сотрудник, уволившийся из компании, по-прежнему сможет подключаться к веб-сайту.
- Функции автоматического восстановления. При выявлении рассинхронизации паролей EPV может автоматически синхронизировать их без вмешательства человека.
- Автоматическая подготовка учетных записей. С помощью каталога предприятия или среды vCenter EPV может автоматически подготавливать привилегированные учетные записи, а также отражать любые изменения, такие как добавление или удаление устройств из сети, создание новых учетных записей администраторов в локальной группе администраторов и привилегированных учетных записей гипервизора ESX. Уникальные возможности автоматического обнаружения позволяют автоматически рассылать уведомления при обнаружении служебной учетной записи, не управляемой в рамках политики. Поддерживается также создание отчетов обо всех обнаруженных неуправляемых учетных записях.
- Централизованное управление с возможностью разделения инфраструктуры на сегменты. Распределенная архитектура CyberArk позволяет создать несколько серверов централизованного управления политиками для управления учетными записями в различных сегментах сети. Все эти сервера будут обращаться к единому серверу Enterprise Password Vault. Такая структура обеспечивает уникальный уровень масштабируемости, возможность централизованного аудита, функции управления доступом и пользователями.
- Возможность внедрения на крупных предприятиях. Легкость интеграции с корпоративной инфраструктурой позволяет повысить ценность имеющихся решений.

Широкие возможности управления привилегированными учетными записями

Приложение Enterprise Password Vault является частью комплекта решений Account Security (PAS) — одного из лучших решений полного жизненного цикла, представленных на рынке. Это приложение предназначено для централизованного управления привилегированными и общими учетными записями, а также паролями, встроенными в сценарии приложений, файлы конфигурации, службы Windows и планировщик заданий. PAS — решение корпоративного класса, обеспечивающее безопасность, управляемость и подотчетность всех привилегированных учетных записей и действий, связанных с управлением центром обработки данных (локальным или облачным) на основе политик.

Характеристики

Защищенная платформа:

- Многоуровневая система защиты
- Отсутствие прямого доступа к данным
- Интеграция с HSM

Управление доступом и рабочими процессами:

- Поддержка каталогов LDAP
- Идентификация и управление доступом
- Системы отслеживания ошибок и управления рабочими процессами

Многоязычный портал:

- Поддерживаемые языки: английский, французский, немецкий, испанский, русский, японский, китайский

Методы проверки подлинности:

- Имя пользователя и пароль, RSA SecurID, веб-служба SSO, RADIUS, PKI, смарт-карты, LDAP

Мониторинг проверки подлинности в системах Windows:

- Интеграция с SIEM, ловушки SNMP, уведомления по электронной почте

Примеры поддерживаемых управляемых устройств:

- Операционные системы: Windows, *NIX, IBM iSeries, Z/OS, OVMS, HP Tandem, MAC OS, ESX/ESXi, XenServers
- Приложения Windows: служебные учетные записи, в том числе учетные записи службы SQL Server в кластере, планировщики заданий, , пулы приложений IIS, COM+, анонимный доступ к IIS, служба кластеров
- Базы данных: Oracle, MSSQL, DB2, Informix, Sybase, MySQL и любые ODBC- совместимые базы данных
- Средства обеспечения безопасности: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, IBM, TippingPoint, SourceFire, Fortinet, WatchGuard, Industrial Defender, Acme Packet, Critical Path, Symantec, Palo Alto
- Сетевые устройства: Cisco, Juniper, Nortel, HP, 3com, F5, Alactel, Quintum, Brocade, Voltaire, RuggedCom, Avaya, BlueCoat, Radware, Yamaha
- Приложения: SAP, WebSphere, WebLogic, JBOSS, Tomcat, Oracle ERP, Peoplesoft, TIBCO, Cisco
- Каталоги: Microsoft, Sun, Novell, поставщики UNIX, RSA, CA
- Средства удаленного управления и мониторинга: IBM, HP iLO, Sun, Dell DRAC, Digi, Cyclades, Fijitsu
- Виртуальные среды: VMware vCenter и ESX
- Системы хранения данных: NetApp
- Универсальные интерфейсы: любые устройства с поддержкой SSH/Telnet, реестр Windows, любые веб-приложения (например, удаленное выполнение команд WMI Facebook), пароли, хранящиеся в таблицах базы данных, файлы конфигурации (текстовые, INI, XML)