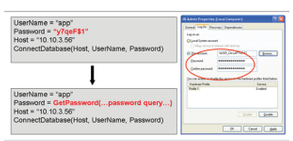
CYBERARK®

Application Identity Manager™

Готовое решение проблем с безопасностью в вашем центре обработки данных и всей инфраструктуре приложений за счет устранения встроенных скриптов верификационных данных



С модулем *Application Identity Manager* Вы сможете устранить встроенные пароли скриптов, служб и приложений. Более того, вы сможете применять обновляемые профили безопасности к файлам конфигурации, базам данных и сторонним приложениям, не допускающим изменений своего кода.

Суть проблемы

В современных сложных IT-средах множественные скрипты, процессы и приложения запрашивают доступ к мультиплатформенным ресурсам для получения и хранения конфиденциальной информации. Подобным приложениям предоставляется доступ к технологическим учетным записям, как правило, обеспечивающим неограниченный доступ к конфиденциальной информации, хранящейся в базах данных корпораций. Верификационные данные обычно встраиваются внутрь кода приложений, скриптов, сервисов, источников данных, файлов конфигурации и пр. Такие аккаунты зачастую позволяют получить доступ к важной конфиденциальной информации компании, из-за этого они зачастую становятся целью атак хакеров. Многие из зафиксированных в последнее время комплексных атак делали ставку на проникновение в систему через компрометацию встроенных в код приложения верификационных данных.

Защита, администрирование и автоматическая замена встроенных верификационных данных представляет сложную задачу и ведет к серьезным ИТ-затратам. В результате до 42% компаний сообщают, что никогда не изменяли встроенные пароли приложений, скриптов и пакетных заданий.

Неправильное администрирование App2App паролей создает серьезные риски, такие как:

- **Отрицательный результат аудиторских проверок.** Встроенные пароли создают серьезные проблемы для компании при прохождении аудиторских проверок. Стандарт безопасности данных PCI DSS, к примеру, предписывает предприятиям проводить разработку и администрирование систем и приложений безопасности, удалять из приложений любые частные имена пользователей и пароли, а также принудительно устанавливать мощные механизмы ограничения доступа и аутентификации пользователей в системах, доступ к которым осуществляется на основе данных держателей карт.

- **Отсутствие возможностей учета.** Пароли приложений могут требоваться IT-персоналу или разработчикам для устранения неисправностей и в случаях экстренных ситуаций. Существующие решения практически не обеспечивают возможностей аудита и контроля для этих сценариев.

- **Риски безопасности.** Пароли App2app практически никогда не меняются и зачастую хранятся в виде открытого текста, они известны широкому кругу IT-персонала, разработчикам и конечным пользователям, а также бывшим сотрудникам компании или внешним подрядчикам. Любые попытки изменить встроенные в код пароли обычно требуют внесения изменений в код, что, в свою очередь, может негативно повлиять на работу систем, приводя к постоянным простоям в работе критических бизнес-приложений.

- **Повышенная опасность причинения ущерба.** Аккаунты приложений имеют широкие права и практически неограниченный доступ к системам со стороны сервера. Если злоумышленники завладеют подобным аккаунтом,они получат неконтролируемый доступ к важной конфиденциальной бизнес-информации и возможность причинить серьезный ущерб.

Продукт и его ключевые преимущества

Лидирующий продукт на рынке, Application Identity Manager (AIM) от компании CyberArk, решает проблемы обеспечения безопасности за счёт устранения встроенных паролей при помощи проверенной, адаптированной для центров обработки данных технологии. С AIM Вы сможете:

Уверенно выполнять требования соответствия.
Компании могут выполнять требования соответствия внутренним и внешним нормативным указаниям по регулярной замене паролей и мониторингу безопасности систем привилегированного доступа.

Устранить внутренние и внешние угрозы.
Обеспечьте надежную защиту критических для вашего бизнеса систем с наиболее конфиденциальными данными, устранив необходимость хранить App2App пароли и ключи, используемые в приложениях, скриптах или в файлах конфигурации.

Вести бизнес эффективнее.
Защитите ключевые для вашего бизнеса системы, позволив им бесперебойно работать за счёт легкости доступа и производительности в App2App процессах, вне зависимости от наличия доступа к сети.

Application Identity Manager предлагает вам уникальные возможности:

- Минимизация финансовых потерь и ущерба деловой репутации за счет устранения встроенных и визуально отображаемых паролей приложений и скриптов.

- Решение, растущее вместе с вашим бизнесом.

- Легко масштабируемая система, позволяющая защищать все приложения на множестве платформ и сайтов по мере роста бизнеса.

- Обеспечение непрерывности и безопасности бизнес-процессов, при внедрении системы управления профилями доступа к приложениям в ваших центрах обработки данных.

Характеристики

Application Identity Manager (AIM) использует запатентованную технологию компании CyberArk - Digital Vault Technology™ - сертифицированную ICSA и разработанную в соответствии с высочайшими требованиями к системам безопасности для управления привилегированными и App2App аккаунтами. Digital Vault обеспечивает множество встроенных возможностей обеспечения безопасности: аутентификация, защита от несанкционированного доступа, аудит и безопасное хранение данных.

AIM предоставляет готовую инфраструктуру с централизацией управления профилями доступа к ресурсам, а также полный спектр возможностей управления данными сервисными аккаунтами, включая:

- **Устранение встроенных паролей.**
  При помощи различных программных пакетов для работы с паролями системы AIM, можно быстро устранить пароли из всех скриптов, кодов приложений и файлов конфигурации, сделав их невидимыми для разработчиков и обслуживающего персонала, при этом автоматически заменяя данные доступа к системе согласно политике компании без ущерба производительности приложений или увеличения времени простоя.

- **Автоматическая синхронизация паролей.**
  Для удовлетворения требований проведения аудита, AIM обеспечивает возможность изменять пароли по запросу и в соответствии с политикой компании без остановки производства или необходимости разработки/тестирования и IT-поддержки. AIM также может использоваться для внедрения пролей в различные области внутри файлов конфигурации, баз данных и сторонних приложений, где невозможно изменение кода.

- **Аутентификация приложений.**
  AIM использует сложные процедуры аутентификации приложений, запрашивающих данные доступа, что обеспечивает возможность доступа к данным только для разрешенных приложений. Эти процедуры включают принудительные ограничения по адресам компьютеров, пользователям ОС, путям приложений и динамическим подписям.

- **Высокая доступность данных, сокращение сроков простоя и обеспечение непрерывности бизнес-процессов.**
  AIM разработана согласно высочайшим корпоративным стандартам в области доступност и данных и однородности систем для наиболее критичных бизнес-приложений, даже в рамках сложных и распределенных сетевых сред. Благодаря ее возможности безопасного кэширования данных, предприятия-клиенты могут быть уверены, что критичные для их функционирования приложения всегда будут иметь доступ к своим сервисным аккаунтам, вне зависимости от качества работы сети и ее доступности. Средства кэширования не требуют технического обслуживания и обеспечивают высочайший уровень отказоустойчивости и производительности.

- **Уникальное решение для приложений, использующих профили доступа к серверу с данными.**
  AIM обеспечивает уникальное решение проблемы обеспечения безопасности и автоматического управления профилями доступа критических бизнес-приложений и и хранящихся среди данных сервера приложений. Данное решение запатентовано и может применяться без изменения кода, с нулевыми простоями и без перезагрузок при смене паролей.

- **Готовое решение для сторонних приложений.**
  Многие сторонние приложения, такие как сканеры уязвимостей, продукты CRM и другие, требуют привилегированных учетных записей для работы с сопряжёнными устройствами и базами данных. Они используют верификационные данные из файлов конфигурации, баз данных и пр. для доступа к этим системам. AIM интегрируется со сторонними продуктами для безопасного предоставления верификационных данных по мере необходимости, при этом система автоматически управляет и заменяет их для обеспечения лучшей защиты Ваших IT-ресурсов.

- **Пользовательский веб-интерфейс для управления приложениями.**
  Гибкий режим просмотра позволяет предприятиям проводить аудит, отслеживать и безопасно управлять всей деятельностью App2App.

- **Готовность к внедрению.**
  Легкая интеграция в инфраструктуру включает в себя интеграцию с LDAP; использование Windows домена, RADIUS, PKI, SSO или RSA SecurID для аутентификации; мониторинг и SIEM интеграция при помощи SNMP, Syslog и SMTP; интеграция с системами заявок и системами автоматического документооборота; надежный комплект SDK, встроенное HA/DR и многое другое!

Мощь управления привилегированным доступом

Application Identity Manager - часть лидирующего на рынке решения Privileged Account Security (PAS), комплексного пакета централизованного управления привилегированными и коллективными аккаунтами доступа в организации, детального управления доступом привилегированных пользователей, а также управления встроенными паролями в приложениях и скриптах. PAS – унифицированное решение корпоративного класса на основе установленных правил, обеспечивающее безопасность, управление имониторинг всех привилегированных аккаунтов и деятельности, связанной с управлением центрами данных как у конечных пользователей, так и в облаке.

Характеристики

Защищенная платформа:

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

Управление доступом и рабочим процессом:

- LDAP директории
- Управление профилями и доступом
- Система выдачи тикетов и автоматизации документооборота

Методы аутентификации:

- Имя пользователя и пароль
- RSA SecurID
- Web SSO
- RADIUS
- PKI и смарткарты
- LDAP
- Аутентификация на основе Windows

Высокая доступность:

- Поддержка объединения в кластеры
- Постоянно действующий безопасный локальный кэш
- Множественные точки восстановления системы
- Интеграция с системой бэкапов (резервных копий) организации

Мониторинг:

- SIEM интеграция
- SNMP
- Email уведомления

Операционные системы:

- Windows
- Linux/UNIX
- AIX
- Solaris
- HP-UX

Платформы приложений:

- Java
- CLI
- COM
- C/C++
- Серверы приложений: Websphere, WebLogic, JBOSS, Tomcat