CYBERARK ALERO

Сегодня при управлении компонентами своей ИТ-инфраструктуры многие компании полагаются на удалённых поставщиков. Для успешного выполнения своих задач этим организациям изначально необходим привилегированный доступ к корпоративным ИТ-системам. Однако при использовании общепринятых подходов к аутентификации и авторизации пользователей распространение корпоративных решений и методов обеспечения безопасности привилегированного доступа на удалённых поставщиков может вызывать затруднения.

Традиционные корпоративные системы управления идентификационными данными и решения по контролю доступа, предназначенные для аутентификации сотрудников компании и корпоративных устройств в современном мире, не вполне подходят для обеспечения безопасности персонала сторонних поставщиков и внешних устройств. Для большинства компаний характерны слабая прозрачность и контроль удалённого доступа к корпоративной сети либо их полное отсутствие. Стратегия предоставления доступа к корпоративным рабочим станциям каждому поставщику не реализуема по целому ряду причин, а управление развертыванием сетей VPN или агентов на ноутбуках или настольных ПК другой компании часто слишком затратно для ИТ-подразделений. С другой стороны, требования к персоналу и доступу сторонних поставщиков могут ежедневно или еженедельно меняться, делая традиционные схемы управления идентификационными данными на основе имен пользователей и паролей непрактичными.

В условиях прозрачности периметра и растущей зависимости от внешних подрядчиков корпоративные ИТ-подразделения и службы безопасности должны находить инновационные способы для предоставления удалённым поставщикам безопасного доступа к привилегированным аккаунтам без прерывания операций.

Безопасное и быстрое подключение удалённых поставщиков, управляющих ИТ-ресурсами, без использования VPN, агентов и паролей

ХАРАКТЕРИСТИКИ

- Компоненты CyberArk® Alero™
  - Мобильное приложение Alero™
  - Средство подключения Alero™
  - Облако Alero™
  - iOS 10 или более поздней версии
  - Android 6 или более поздней версии
- Компоненты CyberArk
  - Core PAS v10.3 или более поздней версии
  - Шлюз HTML5

РЕШЕНИЕ

Решение CyberArk® Alero™ призвано обеспечить быстрый, удобный и безопасный привилегированный доступ для удалённых поставщиков, которым необходимо работать с критически важными внутренними системами под управлением CyberArk. Облачная многофакторная аутентификация, предлагаемая Alero, использует биометрические возможности смартфонов, которые, в свою очередь, позволяют авторизованным удалённым поставщикам своевременно получать защищенный привилегированный доступ при помощи функции распознавания лица или касания пальца.

Alero устраняет необходимость в VPN-клиентах, агентах безопасности или паролях, которые могут не устраивать пользователей, повышать риски и создавать административные проблемы. Вместо этого удалённые поставщики подтверждают свою личность с использованием встроенных в смартфон функций распознавания лица или отпечатка пальца, а также проходят инициализацию и аутентификацию для безопасного доступа к решению CyberArk Core Privileged Access Security посредством Alero. Alero как единое решение SaaS объединяет в себе доступ Zero Trust, биометрическую многофакторную аутентификацию, своевременную инициализацию и полную интеграцию с решением CyberArk Core Privileged Access Security для обеспечения максимальной прозрачности и возможностей аудита для администраторов.

РЕГИСТРАЦИЯ НОВЫХ ПОЛЬЗОВАТЕЛЕЙ

Мобильное приложение Alero работает на телефонах под управлением iOS и Android. После загрузки приложения удаленный поставщик получает от организации электронное письмо для доступа к веб-сайту Alero™. Он подтверждает свою личность по электронной почте и зарегистрированному номеру телефона.

Достаточно ввести полученный по SMS пароль.

Биометрическая авторизация также применяется для проверки и подтверждения подлинности имени пользователя и может потребоваться в процессе регистрации для успешного первичного входа в систему. Биометрические данные в исходном формате надежно хранятся на мобильном устройстве пользователя. Клиентское устройство использует установленную консоль Alero™ для управления аккаунтами внешних поставщиков и аудита.

ПРЕИМУЩЕСТВА РЕШЕНИЙ CYBERARK

CyberArk — мировой лидер в области обеспечения безопасности привилегированного доступа, критически важного уровня ИТ-безопасности для защиты данных, инфраструктуры и активов на предприятии, в облаке и на всех стадиях интегрированной разработки и эксплуатации.

CyberArk предоставляет наиболее полное в отрасли решение для снижения рисков, связанных с привилегированными учетными данными и секретной информацией.

Ведущие мировые организации, включая более 50% участников списка Fortune 500, доверяют компании и используют ее решения для защиты от внешних атак и внутренних злоумышленников.

ПРИНЦИП РАБОТЫ

При попытке входа удалённого поставщика на веб-портал CyberArk приложение Alero отображает на его рабочей станции одноразовый краткосрочный QR-код. Используя мобильное приложение Alero, пользователь сканирует его и одновременно подтверждает свою личность с помощью распознавания лица или отпечатка пальца. В случае одобрения QR-кода и биометрических данных удалённый пользователь получает безопасный доступ к веб-порталу CyberArk и разрешение на использование привилегированных аккаунтов со своей рабочей станции. Сеанс веб-браузера изолирован, и учётные данные никогда не передаются на рабочую станцию конечного пользователя при входе в критически важные ИТ-системы для обычной работы, обслуживания или иных операций. Кроме того, сеанс подвергается полному шифрованию.

Решение CyberArk Core Privileged Access Security снижает риски, помогая предприятиям эффективно управлять правами доступа к привилегированным аккаунтам, проводить упреждающий мониторинг и контроль активности на привилегированных аккаунтах, интеллектуально выявлять подозрительные действия, а также оперативно реагировать на угрозы в автоматическом режиме. Alero эффективно интегрируется с решением CyberArk Core Privileged Access Security. Это обеспечивает своевременную инициализацию пользователей и доступ для удалённых поставщиков с возможностью использования критически важных ресурсов только в случае необходимости. Подобная интеграция также обеспечивает корпоративным службам эксплуатации и безопасности полную прозрачность и возможность контроля действий удалённых поставщиков с привилегированным доступом.

ПРЕИМУЩЕСТВА

- **Снижение рисков безопасности.** Реализация доступа Zero Trust для удалённых поставщиков, подключенных к CyberArk Core PAS. Повышение эффективности мер безопасности за счет своевременной инициализации привилегированных аккаунтов без использования паролей, физических ключей и сетевых средств контроля доступа, которые могут провоцировать уязвимости и расширять поверхность атак.
- **Снижение эксплуатационных расходов и сложности.** Решение SaaS упрощает операции за счет исключения сетей VPN, агентов и учётных данных, необходимых для доступа удалённых поставщиков. Возможность временной авторизации удалённых пользователей в режиме реального времени без вмешательства администратора и удаление пользователей на основе политик, когда необходимость в доступе уже отсутствует.
- **Упрощение удалённого доступа для сторонних поставщиков.** Безопасная проверка личности авторизованных пользователей для доступа к привилегированным корпоративным аккаунтам при помощи функции распознавания лица или отпечатка пальца. Хранение биометрических данных на мобильном устройстве отдельно от внутренних систем для обеспечения максимальной конфиденциальности и безопасности.
- **Улучшение прозрачности и соответствия нормативным требованиям.** Полная интеграция с решением CyberArk Core Privileged Access Security обеспечивает возможность мониторинга активности с привилегированным доступом в режиме реального времени посредством изолированных сеансов браузера. Обнаружение текущих и потенциальных атак до того, как нарушители получат доступ к критически важным системам и нанесут непоправимый ущерб. Подготовка отчетов за прошлые периоды для проверки соответствия нормативным требованиям.