SOLUTION BRIEF

Secure Desktop

Снижайте риски безопасности конечных точек с помощью CyberArk Endpoint Privilege Manager и адаптивной мультифакторной аутентификации.

КЛЮЧЕВЫЕ ТЕЗИСЫ

Усиление безопасности конечных точек
Защититесь от утечки данных и злонамеренных атак из-за потерянных, похищенных или скомпрометированных учетных данных. Убедитесь, что вы защищаете и предоставляете привилегированный доступ на конечных точках при необходимости.

Оптимизация пользовательского опыта
Настройте быстрый, безопасный, беспрепятственный и удобный доступ к конечным точкам. Позвольте конечным пользователям быстро и легко запрашивать повышенные привилегии доступа, не обращаясь в службу поддержки и не вводя второй набор учетных данных администратора.

Упрощение операций
Оптимизируйте операции по безопасности и освободите персонал, автоматизировав трудоемкие административные задачи, занимающие много времени.

Настоящее нулевое доверие
Диспетчер привилегий конечных точек делает возможной поэтапную аутентификацию для привилегированных приложений для проверки личности пользователя.

Вызов

Современные сообразительные киберпреступники всегда ищут новые способы похищения учетных данных, повышения привилегий и перемещения по периметру сети, чтобы сеять хаос. Небрежное управление паролями и ручные процессы администрирования могут привести к уязвимостям в системе безопасности и повышению привилегий, что открывает двери злоумышленникам для проникновения в сети, похищения данных и подрыва бизнеса.

Широкий спектр конечных точек, включая физические и виртуальные компьютеры и серверы, является уязвимым к атакам. Атаки на конечные точки, такие как фишинг и программы-вымогатели, могут навредить репутации компании и привести к дорогостоящим судебным процессам, штрафам и потере прибыли.

Компании должны найти способы защитить доступ к компьютерам и серверам, а также строго контролировать доступ к привилегированным учетным записям и приложениям, не ухудшая при этом качество работы пользователей и не перегружая службу поддержки.

Решение

Решение Secure Desktop от CyberArk позволяет компаниям защитить доступ к конечным точкам и обеспечить соблюдение принципа наименьших привилегий, не усложняя IT-операции и не снижая производительность пользователей. Унифицированное решение для многофакторной аутентификации и управления привилегиями на конечных точках помогает организациям усилить безопасность доступа, оптимизировать работу пользователей и устранить трудоемкие и подверженные ошибкам административные процессы, которые могут привести к чрезмерному резервированию ресурсов и злоупотреблению привилегиями.

С помощью решения CyberArk Secure Desktop компании могут повысить безопасность конечных точек, требуя от пользователей проходить вторичную аутентификацию при первом входе на конечную точку. Если пользователь пытается запустить привилегированное приложение или получить доступ к привилегированной учетной записи, решение может проверить личность пользователя с помощью адаптивной многофакторной аутентификации, прежде чем временно повысить его привилегии.

ПОЧЕМУ CYBERARK

CyberArk является мировым лидером в сфере безопасности учетных данных. Ориентируясь на управление привилегированным доступом, CyberArk предоставляет наиболее комплексные решения для защиты любой учетной записи — человеческой или программной — в бизнес-приложениях, распределенных рабочих группах, гибридных облачных рабочих нагрузках и в конвейерах DevOps. Ведущие мировые организации доверяют CyberArk защиту своих наиболее важных активов.

Адаптивная многофакторная и беспарольная аутентификация для конечных точек

Адаптивная многофакторная аутентификация CyberArk Adaptive Multifactor Authentication (MFA) позволяет организациям жестко контролировать доступ к компьютерам и серверам. Адаптивная MFA использует контекстную информацию (местонахождение, время суток, тип устройства, риск пользователя и т. д.) и бизнес-правила, чтобы определить, какие факторы аутентификации необходимы при входе конкретного пользователя на конечную точку. Adaptive MFA обеспечивает высокий уровень аутентификации и защищает бизнес от подмены личности, кражи учетных данных, фишингового мошенничества и других угроз, связанных с конечными точками.

Решение также поддерживает широкий спектр механизмов аутентификации, включая беспарольные факторы, аппаратные токены, приложения-аутентификаторы, SMS-коды и доверие к устройствам на основе сертификатов. Сочетание контекстной аутентификации и широкого спектра поддерживаемых факторов аутентификации усиливает безопасность и нагрузку, что приводит к повышению удовлетворенности и производительности конечных пользователей.

Диспетчер привилегий конечных точек

Плохо управляемые привилегированные учетные записи конечных точек — например, администратора и суперпользователя Windows, macOS или Linux — являются одной из наиболее серьезных уязвимостей безопасности, с которыми сталкиваются организации. Злоумышленники могут получить несанкционированный доступ к учетным данным привилегированных учетных записей и путешествовать по сети, захватывая рабочие станции, серверы и другие объекты критической инфраструктуры. Злоумышленники также могут использовать привилегированные учетные записи конечных точек для отключения программ обнаружения угроз, установки вредоносного программного обеспечения и запуска разрушительных кибератак.

Решение CyberArk Secure Desktop помогает снизить риски, связанные с привилегированным доступом, удаляя права локального администратора с конечных точек и временно повышая привилегии конечных пользователей с помощью встроенного адаптивного MFA для конкретных задач — по требованию, в режиме реального времени — с минимальным привлечением службы поддержки. Решение защищает от программ-вымогателей, интеллектуально блокируя или ограничивая подозрительные или ненадежные приложения, а также предотвращает кражу учетных данных, защищая пароли и другие учетные данные, которые кэшируются Windows, веб-браузерами и другими программами.

Ключевые функции

Своевременное повышение привилегий

Удаляйте права локального администратора с конечных точек и динамически повышайте привилегии на заранее определенный период времени, чтобы позволить конечным пользователям устанавливать или запускать приложения или изменять настройки конечных точек. Конечные пользователи могут запрашивать повышенные разрешения по требованию непосредственно с рабочего стола при запуске привилегированного приложения без необходимости входить в систему как администратор или вводить другой пароль. Запросы утверждаются вручную или автоматически уполномоченными администраторами в соответствии с политикой.

ДОВЕРИЕ НА ОСНОВЕ СЕРТИФИКАТОВ

Агент может управлять жизненным циклом сертификата на конечном устройстве. Этот сертификат может действовать как условный фактор доступа для чувствительных приложений, которые не должны быть доступны на ненадежных устройствах.

Защита от программ-вымогателей

Жестко контролируйте запуск программ. Позвольте доверенным программам работать в нормальном режиме. Блокируйте вредоносное программное обеспечение. Заставьте неизвестные программы работать в ограниченном режиме без доступа к корпоративной сети.

Защита от кражи учетных данных

Автоматически обнаруживайте и блокируйте попытки кражи учетных данных, кэшированных Windows, веб-браузерами, менеджерами паролей, решениями для единого входа и другими приложениями. Улучшайте защиту от подмены личности, фишинга, spear-фишинга, социальной инженерии и других мошенничеств, требуя использования двух или более различных механизмов для подтверждения личности пользователя.

Адаптивная многофакторная аутентификация с учетом рисков

Усильте безопасность доступа к конечным точкам, требуя несколько форм аутентификации. Уменьшите разочарование пользователей, используя контекстную информацию и политики доступа, основанные на ML и рисках, чтобы определить, какие факторы аутентификации применять к конкретному пользователю в определенных условиях. Учитывайте ряд переменных, включая местоположение, время суток, день недели, IP-адрес, сеть или тип устройства.

Широкий выбор факторов аутентификации

Выбирайте из множества факторов аутентификации, таких как push-уведомления на мобильное устройство, токены с одноразовым паролем, SMS-сообщения или оповещения на электронную почту.

Аналитика и отчетность по поведению пользователей

Получайте информацию об инцидентах с учетными записями и аутентификацией на конечных точках с помощью отчетов и информационных панелей. Расследуйте, изучайте и организуйте автоматизированное реагирование на инциденты, связанные с доступами.

Безопасное использование браузера

Настройте безопасное пользование веб-ресурсами и защиту от похищения, подделки, изменения или манипулирования файлами cookie. Контролируйте доступ к буферу обмена, ограничьте загрузку и выгрузку файлов, а также возможность сделать скриншот, напечатать и добавить расширения к браузерам.

Доступ к часто используемым программам, ресурсам PAM и сторонним инструментам реализуется в один клик прямо из защищенного браузера, а защита от несанкционированной утечки паролей реализована путем автоматической замены на динамически сгенерированные OTP.

Разнообразие конечных точек

Улучшайте безопасность компьютеров Windows Server, Windows Desktop и macOS с помощью единого решения с общей административной консолью.

bako tech®

BAKOTECH — международная компания, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value-Added IT-дистрибьютор, BAKOTECH предоставляет профессиональную до- и постпродажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков. BAKOTECH является региональным представителем CyberArk в Украине, странах Балтии, Средней и Центральной Азии.