SOLUTION BRIEF

Secure Desktop

Знижуйте ризики безпеки кінцевих точок за допомогою CyberArk Endpoint Privilege Manager та адаптивної мультифакторної автентифікації.

КЛЮЧОВІ ТЕЗИ

Посилення безпеки кінцевих точок
Захистіться від витоку даних і зловмисних атак через втрачені, викрадені або скомпрометовані облікові дані. Переконайтеся, що ви захищаєте та надаєте привілейований доступ на кінцевих точках за потреби.

Оптимізація користувацького досвіду
Налаштуйте швидкий, безпечний, безперешкодний і зручний доступ до кінцевих точок. Дозвольте кінцевим користувачам швидко та легко запитувати підвищені привілеї доступу, не звертаючись до служби підтримки та не вводячи другий набір облікових даних адміністратора.

Спрощення операцій
Оптимізуйте операції з безпеки та спростіть роботу персоналу, автоматизувавши трудомісткі адміністративні завдання, що займають багато часу.

Справжня нульова довіра
Диспетчер привілеїв кінцевих точок робить можливою поетапну автентифікацію для привілейованих додатків для перевірки особи користувача.

Виклик

Сучасні кмітливі кіберзлочинці завжди шукають нові способи викрадення облікових даних, підвищення привілеїв і переміщення по периметру мережі, щоб сіяти хаос. Недбале управління паролями та ручні процеси адміністрування можуть призвести до вразливостей у системі безпеки та підвищення привілеїв, що відчиняє двері зловмисникам для проникнення в мережі, викрадення даних та підриву бізнесу.

Широкий спектр кінцевих точок, включно з фізичними та віртуальними комп'ютерами і серверами, є вразливим до атак. Атаки на кінцеві точки, такі як фішинг і програми-вимагачі, можуть зашкодити репутації компанії та призвести до дорогих судових процесів, штрафів і втрати прибутку.

Компанії повинні знайти способи захистити доступ до комп'ютерів і серверів, а також суворо контролювати доступ до привілейованих облікових записів і додатків, водночас не погіршуючи якість роботи користувачів і не перевантажуючи службу підтримки.

Рішення

Рішення Secure Desktop від CyberArk дозволяє компаніям захистити доступ до кінцевих точок і забезпечити дотримання принципу найменших привілеїв, не ускладнюючи IT-операції і не знижуючи продуктивність користувачів. Уніфіковане рішення для багатофакторної автентифікації та управління привілеями на кінцевих точках допомагає організаціям посилити безпеку доступу, оптимізувати роботу користувачів і усунути трудомісткі та схильні до помилок адміністративні процеси, які можуть призвести до надмірного резервування ресурсів і зловживання привілеями.

За допомогою рішення CyberArk Secure Desktop компанії можуть підвищити безпеку кінцевих точок, вимагаючи від користувачів проходити вторинну аутентифікацію під час першого входу на кінцеву точку. Якщо користувач намагається запустити привілейовану програму або отримати доступ до привілейованого облікового запису, рішення може перевірити особу користувача за допомогою адаптивної багатофакторної автентифікації, перш ніж тимчасово підвищити його привілеї.

ЧОМУ CYBERARK

CyberArk є світовим лідером у сфері безпеки облікових даних. Орієнтуючись на управління привілейованим доступом, CyberArk надає найбільш комплексні рішення для захисту будь-якого облікового запису — людського чи програмного — у бізнес-додатках, розподілених робочих групах, гібридних хмарних робочих навантаженнях і в конвеєрах DevOps. Провідні світові організації довіряють CyberArk захист своїх найбільш важливих активів.

Адаптивна багатофакторна та безпарольна автентифікація для кінцевих точок

Адаптивна багатофакторна автентифікація CyberArk Adaptive Multifactor Authentication (MFA) дозволяє організаціям жорстко контролювати доступ до комп'ютерів і серверів. Адаптивна MFA використовує контекстну інформацію (місцеперебування, час доби, тип пристрою, ризик користувача тощо) і бізнес-правила, щоб визначити, які фактори автентифікації необхідні під час входу конкретного користувача на кінцеву точку. Adaptive MFA забезпечує високий рівень автентифікації та захищає бізнес від підміни особи, крадіжки облікових даних, фішингового шахрайства та інших загроз, пов'язаних з кінцевими точками.

Рішення також підтримує широкий спектр механізмів автентифікації, включно з безпарольними факторами, апаратними токенами, додатками-автентифікаторами, SMS-кодами та довірою до пристроїв на основі сертифікатів. Поєднання контекстної автентифікації та широкого спектра підтримуваних факторів автентифікації посилює безпеку та навантаження, що приводить до підвищення задоволеності та продуктивності кінцевих користувачів.

Диспетчер привілеїв кінцевих точок

Погано керовані привілейовані облікові записи кінцевих точок — наприклад, адміністратора та суперкористувача Windows, macOS або Linux — є однією з найбільш серйозних вразливостей безпеки, з якими стикаються організації. Зловмисники можуть отримати несанкціонований доступ до облікових даних привілейованих облікових записів і подорожувати мережею, захоплюючи робочі станції, сервери та інші об'єкти критичної інфраструктури. Зловмисники також можуть використовувати привілейовані облікові записи кінцевих точок для вимкнення програм виявлення загроз, установлення шкідливого програмного забезпечення та запуску руйнівних кібератак.

Рішення CyberArk Secure Desktop допомагає зменшити ризики, пов'язані з привілейованим доступом, видаляючи права локального адміністратора з кінцевих точок і тимчасово підвищуючи привілеї кінцевих користувачів за допомогою вбудованого адаптивного MFA для конкретних завдань — на вимогу, в режимі реального часу — з мінімальним залученням служби підтримки. Рішення захищає від програм-вимагачів, інтелектуально блокуючи або обмежуючи підозрілі або ненадійні програми, а також запобігає крадіжці облікових даних, захищаючи паролі та інші облікові дані, які кешуються Windows, веббраузерами та іншими програмами.

Ключові функції

Своєчасне підвищення привілеїв

Видаляйте права локального адміністратора з кінцевих точок і динамічно підвищуйте привілеї на заздалегідь визначений період часу, щоб дозволити кінцевим користувачам встановлювати або запускати програми чи змінювати налаштування кінцевих точок. Кінцеві користувачі можуть запитувати підвищені дозволи на вимогу безпосередньо з робочого столу під час запуску привілейованої програми без необхідності входити в систему як адміністратор або вводити інший пароль. Запити затверджуються вручну або автоматично уповноваженими адміністраторами відповідно до політики.

Захист від програм-вимагачів

Жорстко контролюйте запуск програм. Дозвольте довіреним програмам працювати в нормальному режимі. Блокуйте шкідливе програмне забезпечення. Примусьте невідомі програми працювати в обмеженому режимі без доступу до корпоративної мережі.

ДОВІРА НА ОСНОВІ СЕРТИФІКАТІВ

Агент може керувати життєвим циклом сертифіката на кінцевому пристрої. Цей сертифікат може діяти як умовний фактор доступу для чутливих програм, які не повинні бути доступні на ненадійних пристроях.

Захист від крадіжки облікових даних

Автоматично виявляйте та блокуйте спроби крадіжки облікових даних, кешованих Windows, веббраузерами, менеджерами паролів, рішеннями для єдиного входу та іншими програмами. Покращуйте захист від підміни особи, фішингу, spear-фішингу, соціальної інженерії та інших шахрайств, вимагаючи використання двох або більше різних механізмів для підтвердження особи користувача.

Адаптивна багатофакторна автентифікація з урахуванням ризиків

Посильте безпеку доступу до кінцевих точок, вимагаючи кілька форм автентифікації. Зменште розчарування користувачів, використовуючи контекстну інформацію та політики доступу, засновані на ML та ризиках, щоб визначити, які фактори автентифікації застосовувати до конкретного користувача за певних умов. Враховуйте низку змінних, зокрема місцеперебування, час доби, день тижня, IP-адресу, мережу або тип пристрою.

Широкий вибір факторів автентифікації

Вибирайте з безлічі факторів автентифікації, таких як push-повідомлення на мобільний пристрій, токени з одноразовим паролем, SMS-повідомлення або сповіщення на електронну пошту.

Аналітика та звітність щодо поведінки користувачів

Отримуйте інформацію про інциденти з обліковими записами та автентифікацією на кінцевих точках за допомогою звітів та інформаційних панелей. Розслідуйте, вивчайте та організовуйте автоматизоване реагування на інциденти, пов'язані з доступами.

Безпечне використання браузера

Налаштуйте безпечне користування вебресурсами та захист від викрадення, підробки, зміни або маніпулювання файлами cookie. Контролюйте доступ до буфера обміну, обмежте завантаження та вивантаження файлів, а також можливість зробити скриншот, друкувати та додати розширення до браузерів.

Доступ до часто використовуваних програм, ресурсів PAM і сторонніх інструментів реалізується в один клік прямо із захищеного браузера, а захист від несанкціонованого витоку паролів реалізовано шляхом автоматичної заміни на динамічно згенеровані OTP.

Різноманітність кінцевих точок

Покращуйте безпеку комп'ютерів Windows Server, Windows Desktop і macOS за допомогою єдиного рішення зі спільною адміністративною консоллю.

bako tech®

BAKOTECH — міжнародна компанія, яка займає лідируючі позиції у сфері фокусної Value Added IT-дистрибуції та постачає рішення провідних світових IT-виробників. Позиціонуючи себе як True Value-Added IT-дистриб'ютор, BAKOTECH надає професійну до- та постпродажну, маркетингову, технічну підтримку для партнерів та кінцевих замовників. BAKOTECH є регіональним представником CyberArk в Україні, країнах Балтії, Середньої та Центральної Азії.