



Azure Active Directory: адміністрування та захист доступу до програм



Розділ 1

Що таке керування
ідентичностями й доступом?

Що таке керування ідентичностями й доступом?

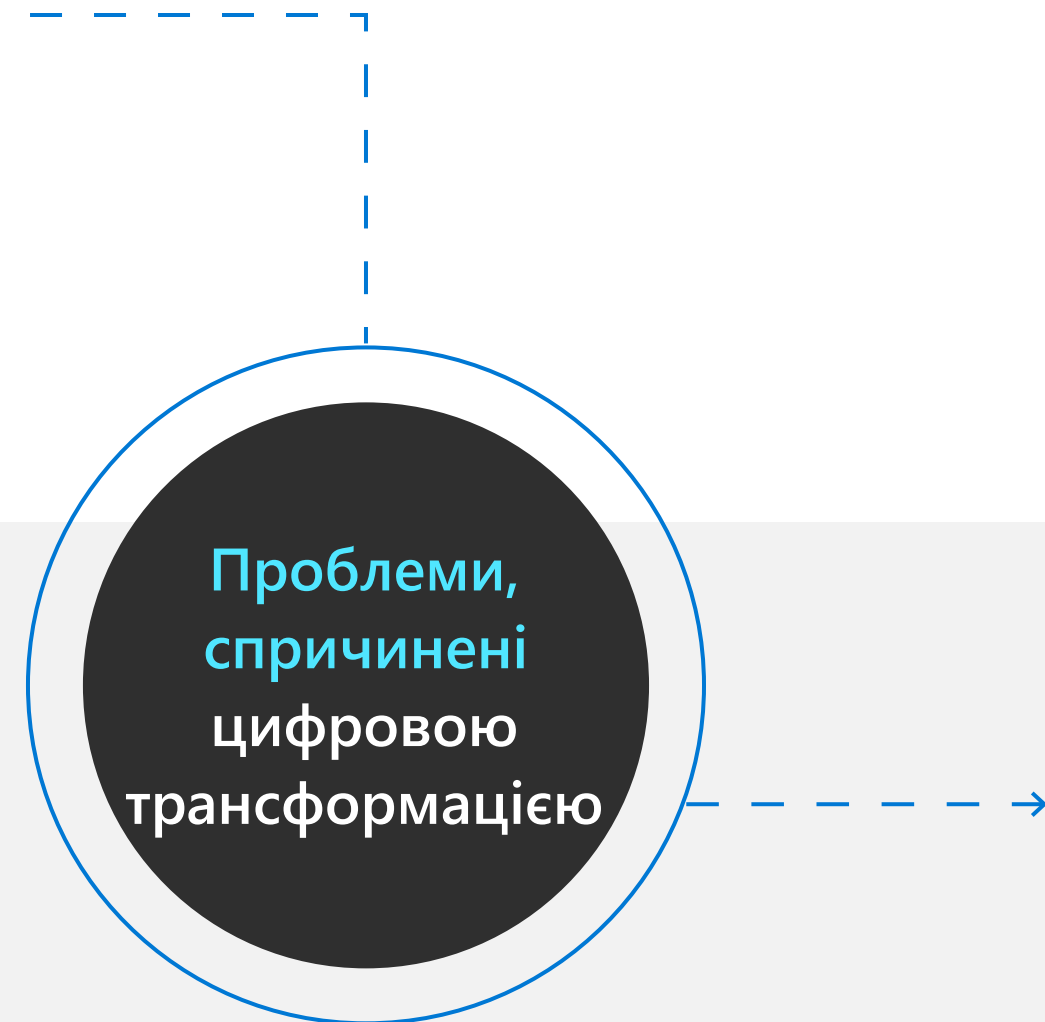
Цифрова трансформація

Хмарні обчислення та мобільні пристрої радикально змінили сучасний підхід до організації роботи. Дедалі більше людей у всьому світі отримують можливість працювати віддалено за допомогою дешевих або й зовсім безкоштовних програм, які надаються за моделлю SaaS ("програмне забезпечення як послуга") і допомагають вирішувати поширені проблеми з організацією співпраці та забезпеченням продуктивності. Великі підприємства модернізують архітектуру своїх інфраструктур, переносячи ПЗ й обчислювальні операції до хмари, а галузеві підрозділи компаній активно розробляють хмарні програми спеціально під свої специфічні потреби. Нові технології подарували великому бізнесу можливість значно підвищити продуктивність роботи за рахунок цифрової трансформації, але вони ж при цьому створили три додаткові проблеми.



Що таке керування ідентичностями й доступом?

Нові проблеми



Ризики для безпеки. До початку хмарної революції IT-відділи контролювали всі технології, що використовувались у компанії. Робота з програмами та платформами обмежувалася периметром корпоративної мережі, що забезпечувало їх повний контроль і надійний захист. Усі, хто входив у корпоративні ресурси, спершу проходили перевірку брандмауером. Але тепер ситуація змінилася. Персонал отримав більший контроль над робочими пристроями й технологіями, адже з багатьма програмами потрібно працювати через Інтернет. І кіберзлочинці навчилися використовувати цю вразливість. Навіть якщо користувач вводить правильний пароль, у наш час ніколи не можна бути певним, що це дійсно працівник компанії.

Проблеми з адмініструванням. Завдяки вибуховому зростанню кількості кінцевих точок користувачі отримали більше можливостей для віддаленої роботи, але з адміністративної точки зору ці зміни стали справжнім кошмаром. У багатьох компаніях IT-відділи навіть не знають повного списку програмних інструментів, якими користується персонал. А якщо й знають, то це означає нову проблему: через велику кількість хмарних програм часто доводиться застосовувати відразу кілька систем керування ідентичностями, а це дорого й небезпечно.

Незручності для користувачів. Навіть працівники не завжди в захваті від ситуації. Адже багато програм – це не лише багато гнучких можливостей, а й маса імен користувачів і паролів, і всіх їх доводиться тримати в голові.



Ризики для
безпеки



Проблеми з
адмініструванням



Незручності для
користувачів

Що таке керування ідентичностями й доступом?

Системи керування ідентичностями й доступом як центральний командний пункт

Системи керування ідентичностями й доступом вирішують ці проблеми

У всіх розглянутих проблем є одна спільна першопричина – слабкі системи перевірки ідентичності. Адже тепер саме ідентичність, а не мережевий периметр, стала основним засобом контролю. Сучасним компаніям потрібні рішення, які б об'єднали розрізнені корпоративні інструменти, архітектури, пристрої й служби та дали змогу краще контролювати права доступу працівників і зовнішніх партнерів. Без цього в наш час неможливо забезпечити надійний захист організації. Такі рішення називаються системами керування ідентичностями й доступом і забезпечують єдиний доступ до всіх компонентів корпоративної інфраструктури. Він допомагає вбезпечити корпоративні ресурси та налагодити максимально ефективну співпрацю в межах усієї компанії. Якісна система керування ідентичностями й доступом працює так. Користувачі входять в усі локальні та хмарні робочі програми за допомогою одного набору облікових даних. Кожен користувач має доступ лише до тих корпоративних ресурсів, які потрібні йому по роботі. Несанкціонований доступ до даних блокується. Адміністратори централізовано керують правами доступу та дозволами користувачів на спеціальному порталі, який допомагає автоматизувати більшість ручних завдань із підготовки й деініціалізації облікових записів користувачів. На цьому ж порталі можна керувати політиками безпеки для всіх корпоративних програм та ідентичностей. Найкращі системи керування ідентичностями й доступом не лише ефективно захищають ідентичності користувачів, а й забезпечують працівникам комфортну роботу та допомагають IT-спеціалістам краще керувати інфраструктурою.



Захист ідентичностей



Комфортна робота працівників



Ефективніше керування IT-інфраструктурою

Розділ 2

Огляд Azure AD

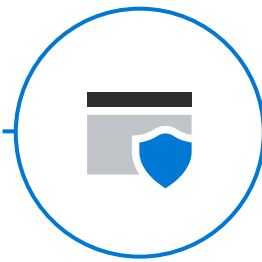
Комплексне рішення

Microsoft Azure Active Directory (Azure AD) – це комплексна хмарна система керування ідентичностями й доступом. Azure AD є лідером ринку у сфері передового захисту ідентичностей і керування каталогами та доступом до програм. Це корпоративне рішення дає змогу адмініструвати й убезпечувати ідентичності робітників, партнерів і клієнтів, щоб ті могли комфортно працювати з потрібними програмами та службами. Azure AD вже користуються мільйони організацій із понад мільярдом ідентичностей.



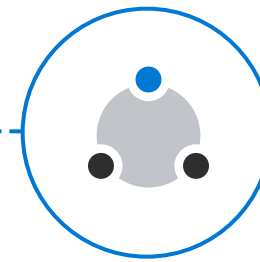
Модернізація системи доступу

Це рішення забезпечує захищений доступ до локальних і хмарних корпоративних даних та ресурсів, а також дає контроль над ним. Перевівши всіх користувачів, програми та пристрої до хмари, ви отримуєте гарантію безпроблемного доступу й можливість відстежувати всі операції в інфраструктурі. А функції самообслуговування й автоматизація робочих циклів допомагають заощаджувати кошти та підвищують продуктивність користувачів.



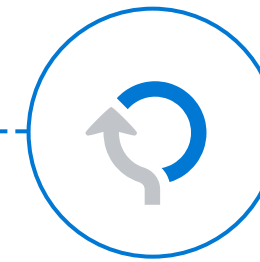
Керування й захист

Щодня реєструється велика кількість атак на облікові дані користувачів. Щоб уберегти корпоративну інфраструктуру від зламу, важливо, щоб система постійно відстежувала поведінку користувачів за допомогою максимально широкого набору сигналів, аналізувала їх засобами штучного інтелекту, виявляла підозрілі дії й автоматично реагувала на них. Наше рішення забезпечує своєчасний доступ до потрібних ресурсів, регулярні перевірки доступу та примусове застосування політик, завдяки чому досягається оптимальний баланс безпеки й продуктивності.



Спілкування та співпраця

Якщо ви плануєте розвиватись і розширюватися, вам потрібна надійна, максимально гнучка хмарна служба з передовою системою безпеки, яка може підтримувати мільйони користувачів. Вона забезпечить захищений зв'язок із зовнішніми користувачами та допоможе їм продуктивно працювати на благо вашої компанії. Можливості самообслуговування гарантують комфорт користувачів, а вбудовані засоби керування безпекою підвищують надійність інфраструктури.



Розробка й інтеграція

Створюйте програми, у які можна зручно входити за допомогою облікового запису Microsoft (особистого, робочого, навчального) або облікових записів у соціальних мережах. Підключайте ці програми до Microsoft Graph – інструмента, який допомагає отримувати й аналізувати дані з Microsoft 365. Налаштовуйте єдиний вхід і автоматичну підготовку користувачів, як у найбільших корпораціях світу.

Розділ 3

Azure AD для ваших програм

Azure AD для ваших програм

Універсальна платформа

Azure AD дає кожному користувачу змогу використовувати для всіх компонентів гібридної корпоративної інфраструктури єдину ідентичність під вашим контролем. Ця ідентичність забезпечує доступ до всіх програм – хмарних і локальних, універсальних і спеціалізованих. З єдиною платформою Azure AD ви зможете зручно й ефективно керувати ідентичностями всіх своїх користувачів, а також запроваджувати для кожної корпоративної програми детальні політики безпеки.



Azure AD для ваших програм

Економія часу та грошей

Azure AD вже інтегровано в тисячі програм – зокрема й у такі популярні рішення, як Workday, ServiceNow, SuccessFactors, Adobe і Concur. Завдяки цьому ви зможете легко запроваджувати використання таких програм на своєму підприємстві. На єдиній консолі Azure AD зручно розгортати узгоджені політики та стежити за правами доступу. Автоматизуйте робочі цикли підготовки користувачів і керування їхнім життєвим циклом, а функції самообслуговування допоможуть вам заощадити ресурси та робочий час працівників IT-відділу. Інформацію про користувачів можна буде завантажувати просто з інструментів управління персоналом, без написання спеціальних сценаріїв і без ручних операцій з атрибутами користувачів.

У програмах із Azure AD можна використовувати єдиний вхід – це набагато зручніше, ніж тримати в голові окремі облікові дані для кожної програми або, ще гірше, використовувати для різних облікових записів ті самі прості паролі, ризикуючи порушенням безпеки даних. Облікові записи з автоматичною підготовкою забезпечують користувачам майже миттєвий доступ до нових ресурсів, а новим співробітникам – можливість із першого дня працювати з усіма потрібними матеріалами.



Економія часу
та грошей



Інтеграція в
SaaS-програми



Єдиний вхід



Миттєвий доступ
користувачів до
потрібних ресурсів

Безпечніший доступ до всіх програм

Azure AD забезпечує комплексний захист ідентичностей у всіх корпоративних програмах – як локальних спеціалізованих, так і SaaS. Коли користувач намагається увійти в програму (наприклад, Microsoft Word або Box), Azure AD спершу перевіряє його ідентичність і тільки після цього надає доступ. А якщо запровадити політики керування доступом, то користувачі матимуть доступ лише до ресурсів, потрібних їм для роботи саме в цей час. За потреби навіть можна зробити так, щоб користувачі повинні були спершу надсилати запит на доступ, або встановити часове обмеження на доступ до певної програми й регулярно перевіряти дотримання вимог під час доступу.

З Azure AD ви також зможете використовувати можливості Microsoft Intelligent Security Graph і машинного навчання. Це аналіз трильйонів сигналів з усіх наших продуктів і служб, виявлення нетипових дій і оцінювання відносного ризику входу для кожного сеансу. Оцінка обчислюється на основі даних про пристрій, місцезнаходження й іншої контекстуальної інформації. А якщо налаштувати в Azure AD політики умовного доступу, служба автоматично вживатиме необхідних заходів безпеки – наприклад, блокуватиме запити на доступ або вимагатиме скидання пароля, якщо виконано певну умову або оцінка ризику входу зависока.



Заходи безпеки програм



Захист ідентичностей



Керування доступом



Політики умовного доступу

Розділ 4

Як адмініструвати й захищати програми за допомогою Azure AD

Можливості автоматизації, самообслуговування й застосування політик в Azure AD допомагають контролювати інфраструктуру та заощаджувати гроші.

Як адмініструвати й захищати програми за допомогою Azure AD



Інтеграція Azure AD з програмами

У колекції програм Azure AD легко налаштовувати та підключати до корпоративного клієнта будь-які з тисяч програм, попередньо інтегрованих із нашою службою. Усі ці програми підтримують єдиний вхід, і для них легко задати політики умовного доступу Azure AD – хоч загальнокорпоративні, хоч для окремих програм. Щойно ви додасте й налаштуєте програму, користувачі з необхідними правами доступу зможуть легко знайти та запустити її на централізованому порталі Azure AD "Мої програми".

Якщо ж у вашій компанії використовуються програми без попередньої інтеграції з Azure AD чи власні розробки, ви можете подати запит на їх внесення до нашої колекції програм.

[Перейти до колекції з тисячами попередньо інтегрованих програм >](#)



Безпечний гібридний доступ

Проксі-програма Azure AD гарантує захищений віддалений доступ без VPN до локальних веб-програм на основі тверджень. Щоб застосовувати проксі-програму, потрібно інстальовати спрощений з'єднувач. Вона забезпечує користувачам і працівникам IT-відділу ті самі можливості, що й SaaS-програми, підключені за допомогою колекції Azure AD.

Якщо ж ви не плануєте відмовлятися від уже придбаних рішень (від F5 ZScaler, SAP, Oracle, Ping Identity тощо) і хочете підключити інші типи програм – наприклад, з автентифікацією на основі заголовків або протоколом Kerberos, – то це теж можливо зробити, паралельно користуючись перевагами Azure AD, зокрема централізацією та підвищеною безпекою.

[Як додати локальну програму за допомогою проксі-програми >](#)

[Підключити сторонні хмари чи мережі програм >](#)

Як адмініструвати й захищати програми за допомогою Azure AD



Автоматична підготовка

В Azure AD можна автоматизувати створення, обслуговування та видалення ідентичностей користувачів у популярних SaaS-програмах – наприклад, щоб автоматично створювати для нових користувачів облікові записи в потрібних системах. Це корисно, коли в компанію чи відділ приходять нові люди. А коли вони йдуть, спеціальні політики можуть автоматично деактивувати їхні облікові записи. Завдяки цьому ідентичності у ваших програмах і системах автоматично підтримуватимуться в актуальному стані з урахуванням усіх змін у каталозі та системі управління персоналом. Це допоможе заощадити час і зменшити кількість помилок.

[Як налаштувати автоматичну підготовку й деініціалізацію для SaaS-програм >](#)



Керування групами

В Azure AD можна надавати доступ до корпоративних ресурсів як окремим користувачам, так і групам в Azure AD. Завдяки цьому відповідальним за ресурси не доведеться налаштовувати права доступу для кожного працівника окремо, адже це можна буде швидко й зручно робити на рівні групи. Такий спосіб керування ще й безпечніший, адже так менший ризик випадково надати певному користувачу зайві права доступу. Крім того, керування групами можна динамічно масштабувати, автоматизувавши реєстрацію за допомогою політик на основі атрибутів ідентичностей.

[Як створити групу на порталі Azure >](#)

Як адмініструвати й захищати програми за допомогою Azure AD



Самообслуговування користувачів

У деяких справах втручання IT-спеціаліста не обов'язкове. Такі завдання в Azure AD можна делегувати іншим працівникам – наприклад, дозволити користувачам створювати й адмініструвати власні групи безпеки в Azure AD. Власники таких груп зможуть схвалювати й відхиляти запити на вступ, а також делегувати керування членством у групі.

[Створити групи із самокеруванням >](#)

Користувачі теж зможуть самостійно вирішувати проблеми, щодо яких раніше зверталися в IT-відділ. Наприклад, користувачі з перевіреною адресою електронної пошти зможуть реєструвати облікові записи на порталі самообслуговування. На тому самому порталі можна буде скинути пароль. Це дуже відчутно розвантажить IT-відділ і забезпечить помітну економію коштів.

[Налаштувати самостійне скидання паролів >](#)



Сучасні методи автентифікації

Якщо зараз ви користуєтесь засобами локальної автентифікації, наприклад службами об'єднання Active Directory (AD FS), ваші програми варто перенести до Azure AD. Ви зможете користуватись усіма перевагами старого рішення (єдиним входом тощо) і отримаєте нові хмарні можливості: надійний захист, масштабування тощо. Зокрема, в Azure AD можна буде налаштовувати детальні політики умовного доступу до окремих програм і надавати партнерам доступ до корпоративних ресурсів завдяки засобу співпраці B2B. Перенесення можливе для всіх програм на основі стандартів федеративного входу SAML 2.0, WS-Federation, OAuth і OpenID Connect.

[Захистити програми за допомогою політик умовного доступу в Azure AD >](#)

[Налаштувати роботу із зовнішніми партнерами за допомогою засобу співпраці B2B в Azure AD >](#)

Безпечно підключайте до Azure AD будь-яку програму з будь-якої хмарної служби чи сервера.

Уже підключено **мільйон** активних унікальних програм.

Спробуйте зараз

Випробуйте місячну безкоштовну ознайомлювальну версію Azure AD та самі переконайтеся, як це просто – керувати доступом користувачів до всіх програм і захищати корпоративні дані.

