Microsoft

Az alkalmazásokhoz való hozzáférés kezelése és biztonságossá tétele az Azure Active Directory szolgáltatással

1. szakasz

Mi az identitás- és hozzáférés-kezelés?

Mi az identitás- és hozzáférés-kezelés?

Digitális átalakulás

A felhőalapú számítás és a mobileszközök átalakították a modern munkahelyet. Az ingyenes és alacsony költségű, szolgáltatott szoftverként működő (SaaS-) alkalmazásokkal a globális munkaerő egyre növekvő számban dolgozhat rugalmasan szinte bárhonnan, és tehet eleget a produktivitással és együttműködéssel összefüggő kihívásoknak. A nagyvállalatok az alkalmazásokat és a számítási feladatokat a felhőbe áttelepítve modernizálhatják architektúrájukat, az üzletágak pedig az új felhőszolgáltatások előnyeit kihasználva egyéni appokat tudnak fejleszteni a specifikus igényeik kielégítésére. A nagyvállalatok az új technológiáknak köszönhetően nagyobb produktivitást érhetnek el, a digitális átalakulással azonban három új kihívással is szembe kell nézniük.

Mi az identitás- és hozzáférés-kezelés?

Új kihívások

Biztonsági kockázat: A forradalmian új felhőszolgáltatások megjelenése előtt az informatika a technológiai kapuőr szerepét látta el. A felügyelt és védett appok és platformok a hálózati szegélyen belül helyezkedtek el, és mindenkinek, aki bejelentkezett a vállalati erőforrásokba, először át kellett esnie a tűzfal ellenőrzésén. Mindez már a múlté. A munkaerő több szabályozási lehetőséget vehet igénybe az általa használt technológiákat illetően, és ezek legtöbbjéhez az interneten keresztül férhet hozzá. A kibertámadók megtanulták, hogy hogyan használhatják ki ezeket a biztonsági réseket. Még ha egy felhasználó ismeri is egy fiók helyes jelszavát, nem lehet biztos abban, hogy az illető az, akinek mondja magát.

Felügyeleti teher: A végpontok robbanásszerű növekedésének köszönhetően a felhasználók többféle módszerrel csatlakozhatnak, de ez egyben rendkívüli terhelést ró a felügyeletre. Sok nagyvállalat nem tud az alkalmazottak által használt összes eszközről, és még ha megfelelő nyilvántartással is rendelkeznek, a felhőappok nagy száma azt jelenti, hogy több identitásrendszert kell kezelniük, növekednek a költségek, és fokozódnak a meglévő biztonsági kockázatok.

Szegényes felhasználói élmény: A kedvezőtlen hatások a felhasználóknál is megjelennek. Miközben oda vannak a rugalmasságért, frusztrációt okoz számukra, hogy milyen sok hitelesítő adatot kell megjegyezniük.

Biztonsági kockázat

Felügyeleti teher

Szegényes felhasználói élmény

Az identitás- és hozzáférés-kezelés mint központi vezérlőfelület

Ezeknek a fájó pontoknak a közös nevezője a nem kellően hatékony rendszerek használata az identitás-ellenőrzéshez. A hálózati szegély helyét az identitás váltotta fel új vezérlőfelületként. Olyan megoldásokra van szükség, amelyek a nagyvállalatban megtalálható különféle eszközöket, architektúrákat, készülékeket és szolgáltatásokat összekötve hatékonyabb védelmet nyújtanak a szervezetnek, és az alkalmazottak és a külső partnerek identitás- és hozzáférés-kezelési (IAM-) rendszereit egyetlen rendszerbe egyesítve kezelik, így Ön több szabályozási lehetőséget vehet igénybe. Zökkenőmentes együttműködést biztosít a szervezet határain belül, miközben javítja a vállalati erőforrások biztonságát. A jó IAM-megoldással felhasználóit az összes munkahelyi – felhőbeli vagy helyszíni – alkalmazásukhoz egyetlen hitelesítőadat-készlettel csatlakoztathatja. Az IAM-megoldások úgy lettek kialakítva, hogy a felhasználóknak csak a szükséges erőforrásokhoz adjanak hozzáférést, és blokkolják a hozzáférést azon jogosulatlan felhasználók számára, akik olyan adatokat szeretnének elérni, amelyekre nincs felhatalmazásuk. A felhasználók hozzáférési jogait és engedélyeit egy központi portálon kezelheti, így sokkal kevesebb manuális folyamatra van szükség a felhasználói fiókok kiépítése és leépítése során. Az IAM-megoldások ezenkívül olyan eszközöket is biztosítanak, amelyekkel kezelhetők a különböző identitások és appok biztonsági szabályzatai. A legjobb IAM-megoldások hatékonyabb védelmet nyújtanak az identitásoknak, javítják a felhasználói élményt, és fokozzák a felügyelet hatékonyságát.

Az IAM-megoldások megoldást jelentenek e kihívásokra

Az identitások hatékonyabb védelme

A felhasználói élmény javítása

A felügyeleti hatékonyság fokozása

2. szakasz

Az Azure AD áttekintése

Egy átfogó megoldás

A Microsoft Azure Active Directory (Azure AD) egy felhőben működő átfogó IAM-megoldás, amely vezető szerepet lát el a piacon a címtárkezelés, az alkalmazás-hozzáférés és a fejlett identitásvédelem területén. Az Azure AD segítségével a szervezetek kezelhetik és megvédhetik az alkalmazottak, partnerek és ügyfelek identitásait, hogy mindenki hozzáférhessen a szükséges appokhoz és szolgáltatásokhoz. Az Azure AD szervezetek milliói számára nyújt segítséget a több mint egy milliárd identitás kezelésében és védelmében.

A hozzáférés modernizálása

Kezelheti és biztonságossá teheti a hozzáférést a szervezet adataihoz és erőforrásaihoz, ahogy a helyszínen, úgy a felhőben is. Az összes felhasználót, alkalmazást és eszközt a felhőbe csatlakoztatva zökkenőmentes, biztonságos hozzáférést és nagyobb átláthatóságot és szabályozhatóságot biztosíthat. A munkafolyamatok automatizálásával és önkiszolgáló lehetőségek bevezetésével hozzájárulhat a költségek csökkentéséhez és a felhasználók produktivitásának növeléséhez.

Biztonság és szabályozás

A felhasználók hitelesítő adatait nap mint nap érintő támadások nagy száma miatt a feltörések megelőzéséhez a jelek lehető legszélesebb körén folyamatosan nyomon kell követni a normál és a szokatlan viselkedéseket, mesterséges intelligenciát kell alkalmazni, és automatizálni kell a válaszokat. Egyensúlyt kell teremteni a produktivitás és a biztonság között úgy, hogy közben biztosítani kell az időben történő hozzáférést a megfelelő erőforrásokhoz, rendszeres hozzáférési felülvizsgálatokat kell tartani, és ki kell kényszeríteni a megfelelő szabályzatokat.

Kapcsolódás és együttműködés

Vállalkozását egy olyan megbízható felhőszolgáltatással bővítheti ki, amely akár több millió felhasználóval is használható, iparágvezető biztonság és rugalmasság mellett. Külső felhasználóihoz csatlakozva, számukra felhasználóbarát, önkiszolgáló felületeket és beépített biztonsági vezérlőket biztosítva lehetővé teheti nekik a produktív munkát.

Fejlesztés és integrálás

Olyan alkalmazásokat fejlesszen, amelyek egyszerű módot biztosítanak a felhasználóknak a személyes, munkahelyi vagy iskolai Microsoft-fiókjukkal vagy közösségi hálózati fiókjukkal való bejelentkezésre. Első lépésként csatlakozzon a Microsoft Graph-hoz, a Microsoft 365-ben az adatokhoz és ismeretekhez vezető átjáróhoz, ahol sokoldalú alkalmazásokat fejleszthet. Engedélyezze az egyszeri bejelentkezést, automatizálja a felhasználók kiépítését, és máris elérheti a világ legnagyobb szervezeteit.

3. szakasz

Azure AD az alkalmazásokhoz

Azure AD az alkalmazásokhoz

Egy univerzális platform

Az Azure AD segítségével minden egyes felhasználóhoz egy közös identitást kezelhet a hibrid infrastruktúrában, így a felhasználók az összes szükséges alkalmazáshoz hozzáférhetnek, a felhőbeli és a helyszíni üzletági alkalmazásokat is beleértve. Minden identitást egy univerzális platformról kezelhet, amivel fokozott felügyeleti hatékonyságot érhet el, és több szabályozási lehetőséget vehet igénybe. A szervezetben használt minden egyes alkalmazásra részletes biztonsági szabályzatokat alkalmazhat.

Idő és pénz megtakarítása

Az Azure AD több ezer alkalmazással lett integrálva, így például a Workday, a ServiceNow, a SuccessFactors, az Adobe és a Concur népszerű megoldásaival, így Ön egyszerűbben teheti elérhetővé ezeket az appokat a felhasználóinak. Egyetlen konzolt használva konzisztens szabályzatokat vezethet be, és figyelheti a hozzáférési jogokat. Automatizálhatja a felhasználók kiépítésével és az életciklus-kezeléssel kapcsolatos munkafolyamatokat, az önkiszolgáló fiókkezeléssel pedig időt és erőforrásokat takaríthat meg. A HR-eszközökből származó felhasználói információkat adatforrásként használhatja, így nem kell egyéni szkripteket vagy manuális folyamatokat alkalmaznia a felhasználói attribútumok kezeléséhez.

Az Azure AD-n keresztül konfigurált appokba történő egyszeri bejelentkezési lehetőség zökkenőmentes hozzáférést biztosít: a felhasználóknak nem kell minden egyes appfiókhoz külön hitelesítő adatokat megjegyezniük, illetve a gyenge jelszavak ismételt felhasználásával kitenni magukat az adatokkal való visszaélés kockázatának. Azok a fiókok, amelyekhez konfigurálták az automatikus kiépítést, a lehető leghamarabb hozzáférést adnak a felhasználóknak az új erőforrásokhoz. Az új kiépítések esetében az Azure AD gondoskodik arról, hogy az új alkalmazottak már az első napon hozzáférjenek minden releváns erőforrásukhoz.

Idő és pénz megtakarítása

Beépített SaaS-integrációk

Egyszeri bejelentkezés

Azonnali felhasználói hozzáférés

Azure AD az alkalmazásokhoz

Biztonságosabb hozzáférés minden apphoz

Az Azure AD minden egyes appban átfogó identitásvédelmet biztosít – a SaaS-appokban és a helyszíni üzletági appokban egyaránt. Ha a felhasználó hozzáférést kér a Microsoft Wordhöz vagy a Boxhoz, az Azure AD a hozzáférés megadása előtt gondoskodik a felhasználó identitásának megerősítéséről. Hozzáférés-gazdálkodási szabályzatokat is bevezethet, ezzel biztosítva, hogy a felhasználók csak a szükséges dolgokhoz férhessenek hozzá, a szükséges időben. Megkövetelheti a felhasználóktól, hogy engedélyt kelljen kérniük a hozzáféréshez, beállíthat egy időkorlátot arra vonatkozóan, hogy mennyi ideig érhessék el az alkalmazást, és rendszeres időközönként megfelelőségi vizsgálatokat végezhet a hozzáférésen.

Az Azure AD ezenkívül a Microsoft Intelligens biztonsági gráf és a gépi tanulás erejét hasznosítva több trilliónyi, termékeinkből és szolgáltatásainkból származó jelet elemez, amivel fel tudja fedni a szokatlan viselkedéseket, és hozzá tudja rendelni a relatív kockázatokat az egyes munkamenetekhez. Az Azure AD az eszközt, a tartózkodási helyet és más környezeti információkat vizsgálva értékeli a bejelentkezés kockázatát. Az Azure AD-ben olyan feltételes hozzáférési házrendeket hozhat létre, amelyek automatikusan alkalmazzák a biztonsági előírásokat, például blokkolnak egy hozzáférési kérelmet, illetve megkövetelik a jelszó alaphelyzetbe állítását, ha egy bejelentkezést kockázatosnak ítélnek, vagy ha teljesülnek bizonyos szabályzati feltételek.

Alkalmazásbiztonsági előírások

Identitásvédelem

Hozzáférés-gazdálkodás

Feltételes hozzáférési szabályzatok

4. szakasz

Appok kezelése és védelme az Azure AD segítségével

Az Azure AD segítségével egyszerűen kihasználhatja a szabályozási lehetőségeket, és automatizálással, önkiszolgáló lehetőségekkel és szabályzatkényszerítéssel csökkentheti a költségeket.

Appok kezelése és védelme az Azure AD segítségével

Azure AD-appok integrációja

Az Azure AD alkalmazásgyűjteményével egyszerűbben konfigurálhatja és csatlakoztathatja bérlői fiókjához a több ezer előre integrált app egyikét. Az appok mindegyike támogatja az egyszeri bejelentkezést, és egyszerűen, egyenként konfigurálható az Azure AD-beli feltételes hozzáférési vagy a nagyvállalati szintű szabályzatokhoz. Miután felvette és az igényeinek megfelelően konfigurálta az appokat, az arra feljogosító hozzáféréssel rendelkező felhasználók egyszerűen megtalálhatják őket a saját Azure AD-appok portálján, ahol egy helyen találhatók meg és indíthatók el a végfelhasználói appok.

Ha fejlesztett egy appot, vagy szervezetének szüksége van egy integrált appra, kérheti, hogy az felkerüljön az Azure AD alkalmazásgyűjteményébe.

A több ezer előre integrált app felfedezése >

Hibrid hozzáférés védelme

Az Azure AD-alkalmazásproxy biztonságos távoli hozzáférést nyújt az igényeken alapuló helyszíni webalkalmazásokhoz anélkül, hogy VPN-re lenne szükség. Az alkalmazásproxy egy egyszerű összekötő-telepítést igényel, és ugyanazokat az informatikai és végfelhasználói élményt nyújtja, mint az Azure AD alkalmazásgyűjteményén keresztül összegyűjtött SaaS-appok.

Vagy ha meglévő infrastrukturális befektetéseit (például F5 ZScaler, SAP, Oracle vagy Ping Identity) szeretné hasznosítani más típusú appok, például a fejlécalapú vagy Kerberos-hitelesítési protokollokat használó appok csatlakoztatásához, azt is megteheti, és ebben az esetben is kihasználhatja az Azure AD központosítási és biztonsági előnyeit.

Olvassa el, hogy hogyan vehet fel helyszíni alkalmazásokat az alkalmazásproxyn keresztül >

Más partneri apphálózatok és felhők csatlakoztatása >

Appok kezelése és védelme az Azure AD segítségével

Automatizált kiépítés

Az Azure AD segítségével automatizálhatja a felhasználói identitások létrehozását, karbantartását és eltávolítását a népszerű SaaS-alkalmazásokban. Automatikusan létrehozhatja az új fiókokat a megfelelő rendszerekben az új felhasználóknak, amikor azok csatlakoznak a csapatához vagy a szervezetéhez. Amikor valaki kilép egy csapatból vagy szervezetből, beállíthat olyan szabályzatokat, amelyek automatikusan inaktiválják az illető fiókját a megfelelő rendszerekben. E feladatok automatizálásával gondoskodhat arról, hogy az appokban és rendszerekben megtalálható identitások naprakészek maradjanak a címtárban vagy a HR-rendszerben történt változásokkal, ezzel pedig csökkentheti a hibák számát, és időt takaríthat meg.

További információ az SaaS-appokban történő kiépítésről és leépítésről >

Csoportkezelés

Az Azure AD segít abban, hogy hozzáférést adjon a szervezet erőforrásaihoz: használatával hozzáférési jogokat adhat egyetlen felhasználónak vagy egy teljes Azure AD-csoportnak. Csoportok használata esetén az erőforrás tulajdonosa a csoport összes tagjának beállíthatja a szükséges hozzáférési engedélyeket ahelyett, hogy egyenként kellene megadnia a jogosultságokat. Ez egy biztonságosabb módszer, mivel kisebb a valószínűsége annak, hogy véletlenül nem megfelelő hozzáférést ad egy felhasználónak, továbbá időt is megtakaríthat vele. Ezenkívül a csoportkezelés dinamikus méretezésére is van lehetősége, ha a regisztrációt identitásattribútum-alapú szabályzatokon keresztül automatizálja.

Információk arról, hogy hogyan hozhat létre csoportot az Azure portálon >

Appok kezelése és védelme az Azure AD segítségével

Felhasználói önkiszolgáló lehetőségek

Egyes feladatok elvégzése nem igényel IT-szakértelmet, az Azure AD segítségével pedig delegálhatók a feladatok másoknak a szervezetben. Lehetővé teheti a felhasználóknak, hogy saját biztonsági csoportokat hozzanak létre és kezeljenek az Azure AD-ben. A csoporttulajdonosok jóváhagyhatják vagy elutasíthatják a tagsági kérelmeket, vagy delegálhatják a csoporttagság szabályozását.

Saját kezelésű csoportok beállítása >

Az önkiszolgáló lehetőségek a felhasználókra is kiterjeszthetők. Az ellenőrzött e-mail-címmel rendelkező felhasználók az önkiszolgáló portálon keresztül regisztrálhatnak fiókért, a portálon pedig alaphelyzetbe állíthatják a jelszavukat. Ezzel rengeteg időt és pénzt lehet megtakarítani a technikai támogatási részlegnek.

A jelszó önkiszolgáló alaphelyzetbe állításának konfigurálása >

A hitelesítés modernizálása

Ha jelenleg helyszíni hitelesítést (például Active Directory összevonási szolgáltatások) használ, érdemes megfontolnia az appok Azure AD szolgáltatásba való áttelepítését. Ugyanazokat a felhasználói előnyöket veheti igénybe (például egyszeri bejelentkezés), de a felhő nyújtotta méretezhetőségi és biztonsági előnyöket is kihasználhatja, például részletes alkalmazásonkénti hozzáférés-vezérlőket alkalmazhat, illetve az Azure AD B2B-együttműködéssel hozzáférést adhat a partnereknek az erőforrásokhoz. Az összevont bejelentkezéshez az SAML 2.0, WS-Federation, OAuth vagy OpenID Connect szabványt használó appok mind áttelepíthetők.

Azure AD-beli feltételes hozzáférési szabályzatok létrehozása az appokhoz való hozzáférés védelméhez >

Zökkenőmentes együttműködés a külső partnerekkel az Azure AD B2B használatával >

Bármilyen appot, bármilyen felhőben vagy kiszolgálón biztonságosan csatlakoztathat az Azure AD-hez.

1 millió aktív, egyedi app csatlakoztatva.

Microsoft

Kezdje el használni még ma!

Az Azure AD egyhónapos ingyenes próbaverziójával megtapasztalhatja, hogy az összes apphoz milyen könnyen kezelhető a felhasználók hozzáférése, és milyen egyszerűen biztosítható a nagyvállalat védelme.