Microsoft

Upravljajte in zavarujte dostop do aplikacij s storitvijo Azure Active Directory



Razdelek 1

Kaj je upravljanje identitete in dostopa?

Kaj je upravljanje identitete in dostopa?

Digitalna preobrazba

Računalništvo v oblaku in mobilne naprave so spremenile sodobno delovno mesto. Vse več delovne sile po vsem svetu lahko svoje delo opravlja kjer koli z brezplačno in nizkocenovno programsko opremo, kot so storitvene aplikacije (SaaS), s katerimi se loteva izzivov produktivnosti in sodelovanja. Velika podjetja selijo aplikacije in računalništvo v oblak. S tem želijo posodobiti svojo arhitekturo. Vse ve podjetij pa izkorišča prednosti novih storitev v oblaku za ustvarjanje aplikacij po meri za svoje specifične potrebe. Velika podjetja so izkoristila prednosti nove tehnologije, ki omogoča večjo produktivnost, vendar pa je digitalna preobrazba s seboj prinesla tudi tri nove izzive.



Kaj je upravljanje identitete in dostopa?

Novi izzivi

Varnostno tveganje: Pred revolucijo v oblaku je bila tehnologija IT varuh tehnologije. Aplikacije in platforme, ki ste jih upravljali in varovali, so bili znotraj okviru omrežja. Vse, ki so dostopali do virov vašega podjetja, pa je najprej preveril požarni zid. Teh dni je konec. Vaša delovna sila ima večji nadzor nad tehnologijo, ki jo uporablja, do večine pa dostopa prek interneta. Kibernetski napadalci so se naučili izkoristiti te ranljivosti. Tudi če uporabnik pozna pravo geslo za račun, ne morete biti vedno prepričani, da je, za kogar se izdaja.

Izzivi za skrbnike: Zaradi velikega števila končnih točk imajo uporabniki na voljo več načinov za vzpostavljanje povezave, vendar pa je lahko to prava nočna mora za skrbnike. Veliko velikih podjetij ne ve, katera orodja zaposleni uporabljajo. In tudi takrat, ko imajo dober pregled, bi morali zaradi ogromnega števila aplikacij v oblaku upravljati več sistemov za identitete, s tem pa bi se povečali stroški in varnostna tveganja.

slaba uporabniška izkušnja: Tudi uporabniki čutijo stisko. Všeč jim je prilagodljivost, vendar so nejevoljni zaradi velikega števila poverilnic, ki si morajo zapomniti.





Varnostno tveganje



Izzivi za skrbnike



Slaba uporabniška izkušnja

Kaj je upravljanje identitete in dostopa?

Upravljanje identitete in dostopa kot glavna naloga nadzora

Skupni imenovalec vseh teh težavnih točk so pomanjkljivi sistemi za preverjanje identitete. Identiteta je zamenjala omrežje kot nova raven nadzora. Potrebujete rešitve, ki povezujejo ločena orodja, arhitekture, naprave in storitve v podjetju za boljšo zaščito organizacije in upravljanje dostopa tako za zaposlene kot tudi identitete zunanjih partnerjev. Sistemi za upravljanje dostopa (IAM) združujejo dostop znotraj enega sistema, s tem pa vam dajejo večji nadzor. Omogočajo nemoteno sodelovanje prek meja organizacije, hkrati pa izboljšujejo varnost virov podjetja. Z dobro rešitvijo IAM lahko z enim naborom poverilnic uporabnike povežete z vsemi njihovimi službenimi aplikacijami, ne glede na to, ali so v oblaku ali na mestu uporabe. Rešitve IAM so zasnovane tako, da nudijo uporabnikom dostop le do virov, ki jih potrebujejo, nepooblaščenim uporabnikom pa preprečujejo dostop do podatkov, do katerih ne bi smeli dostopati. Pravice in dovoljenja za dostop uporabnikov upravljate v osrednjem portalu, s tem pa zmanjšate količino ročnih opravil, ki sodijo k omogočanju in onemogočanju uporabniških računov. Rešitve IAM nudijo tudi orodja za upravljanje varnostnih pravilnikov v identitetah in aplikacijah. Najboljše rešitve IAM bolje varujejo identitete, izboljšujejo uporabniško izkušnjo ter povečajo učinkovitost skrbnikov.

Z rešitvami IAM je mogoče premagati te izzive



Boljše varovanje identitet



Boljša uporabniška izkušnja



Večja učinkovitost skrbnikov

Razdelek 2

Pregled storitve Azure AD

Obsežna rešitev

Microsoft Azure Active Directory (Azure AD) je obsežna rešitev IAM v oblaku in vodilna rešitev na trgu za upravljanje imenikov, dostopa do aplikacij in napredno zaščito identitete. Organizacije dobijo s storitvijo Azure AD rešitev za upravljanje in zaščito identitet za zaposlene, partnerje in stranke za dostop do aplikacij in storitev, ki jih potrebujejo. Več milijonov organizacij s storitvijo Azure AD upravlja in varuje več kot milijardo identitet.



Sodoben dostop

Upravljajte in zaščitite dostop do podatkov organizacije ter virov na mestu uporabe in v oblaku. Povežite vse svoje uporabnike, aplikacije in naprave v oblaku za nemoten in varen dostop ter večjo vidljivost in nadzor. Avtomatizirajte poteke dela ter omogočite samopostrežne možnosti, s katerimi lahko znižate stroške in izboljšate produktivnost za uporabnike.

Varovanje in upravljanje

Vsak dan se zgodi ogromno napadov na poverilnice uporabnikov. Napade je mogoče preprečiti z neprekinjenim spremljanjem običajnega in neobičajnega delovanja z najrazličnejšimi signali, umetno inteligenco in avtomatizacijo odzivov. Poiščite ravnovesje med produktivnostjo in varnostjo s pravočasnim dostopom do pravih virov ter rednimi pregledi dostopov in uveljavljanjem pravilnika.

Povezovanje in sodelovanje

Razširite svoje podjetje z zanesljivo storitvijo v oblaku, ki jo je mogoče prilagoditi milijonom uporabnikov z najboljši varnostjo in prilagodljivostjo v panogi. Vzpostavite povezavo z zunanjimi uporabniki in spodbudite njihovo produktivnost z uporabniku prijaznimi samopostrežnimi izkušnjami in vgrajenimi varnostnimi kontrolniki.

Razvoj in integracija

Ustvarite aplikacije, s katerimi dobijo uporabniki preprost način za vpis z Microsoftovim osebnim, službenim ali šolskim računom ali s svojimi računi družabnih omrežij. Začnite vzpostavljati povezavo s storitvijo Microsoft Graph, prehodom do podatkov in inteligence v ogrodju Microsoft 365, ter ustvarite obogatene aplikacije. Omogočite enotno prijavo in avtomatizirajte omogočanje uporabnikov za uporabnikov ter se povzpnite med vodilne svetovne organizacije.

Razdelek 3

Azure AD za vaše aplikacije

Azure AD za vaše aplikacije

Univerzalna platforma

S storitvijo Azure AD lahko upravljate običajne identitete za vsakega uporabnika v hibridni infrastrukturi za dostop do vseh aplikacij, ki jih potrebuje, vključno s poslovnim aplikacijami v oblaku in na mestu uporabe. Upravljajte vse svoje identitete v univerzalni platformi. S tem boste izboljšali skrbniško učinkovitost, imeli pa boste tudi večji nadzor. Uporabite zrnate varnostne pravilnike za vsako aplikacijo, ki jo uporabljate v organizaciji.



Azure AD za vaše aplikacije

Prihranite čas in denar.

Storitev Azure AD je vnaprej integrirana v več tisoč aplikacij, vključno s priljubljenimi možnostmi, kot so Workday, ServiceNow, SuccessFactors, Adobe in Concur. S tem lahko te aplikacije lažje ponudite svojim uporabnikom. Z eno konzolo lahko uvedete dosledne pravilnike in nadzorujete pravice za dostop. Avtomatizirate lahko poteke dela za omogočanje uporabnikov in upravljanje življenjskega cikla ter prihranite čas in vire s samopostrežnim upravljanjem računa. Uvozite lahko tudi informacije o uporabnikih iz zaupanja vrednih orodij kadrovanja. S tem odpravite potrebo po skriptih po meri ali ročni obdelavi atributov uporabnikov.

Aplikacije, konfigurirane s storitvijo Azure AD, omogočajo enotno prijavo (SSO) za nemoten dostop. Uporabnikom si tako ni treba zapomniti poverilnic za vsak račun aplikacije ali znova uporabiti šibkih gesel, s tem pa tvegati nepooblaščen dostop do podatkov. Računi, ki so bili konfigurirani za samodejno omogočanje, dajejo uporabnikom hiter dostop do novih virov. Z omogočanjem uporabe, ki jo nudi storitev Azrure AD, imajo novi zaposleni že od prvega dne dostop do vseh pomembnih virov.



Prihranek pri času in denarju



Vgrajene integracije aplikacij SaaS



Enotna prijava



Uporabniški dostop od prvega dne

Azure AD za vaše aplikacije

Omogočite varnejši dostop do vseh vaših aplikacij

Storitev Azure AD nudi obsežno zaščito identitete v vseh vaših aplikacijah, tako v aplikacijah SaaS kot tudi v poslovnih aplikacijah na mestu uporabe. Ne glede na to, ali uporabnik zahteva dostop do aplikacij Microsoft Word ali Box, storitev Azure AD zagotavlja, da je njegova identiteta potrjena, preden ima oseba odobren dostop. Ustvarite lahko tudi pravilnike za upravljanje dostopa, s katerimi poskrite, da imajo uporabniki le dostop do vsebine, ki jo potrebujejo, ko jo potrebujejo. Od uporabnikov lahko zahtevate dovoljenje za dostop, nastavite pa lahko tudi časovno omejitev dostopa do aplikacije ter izvajate redne preglede skladnosti dostopa s predpisi.

Storitev Azure AD uporablja tudi zmogljivost storitve Microsoft Intelligent Security Graph in strojnega učenja za analiziranje na trilijone signalov v vseh naših izdelkih in storitvah, na podlagi katerih odkrije neobičajno delovanje ter dodeli vsaki seji relativno tveganje. Storitev Azure AD si ogleda napravo, lokacijo in druge kontekstne informacije ter nato na podlagi teh oceni raven tveganja vpisa. Ustvarite lahko pravilnike o pogojnem dostopu storitve Azure AD, ki samodejno uporabijo varnostne ukrepe, kot so blokiranje zahteve za dostop ali zahteve za ponastavitev gesla, ko je določeno, da gre pri vpisu za tvegan dogodek ali ko so izpolnjeni določeni pogoji pravilnika.



Varnostni ukrepi za aplikacijo



Zaščita identitete



Upravljanje dostopa



Pravilniki o pogojnem dostopu

Razdelek 4

Kako upravljati in varovati aplikacije s storitvijo Azure AD

S storitvijo Azure AD lahko lažje obdržite nadzor ter znižate stroške z avtomatizacijo, samopostrežnimi storitvami in uveljavljanjem pravilnika.

Kako upravljati in varovati aplikacije s storitvijo Azure AD



Integracije aplikacij storitve Azure AD

Z galerijo aplikacij storitve Azure AD lahko preprosto konfigurirate in z najemnikom povežete katero koli od več tisoč vnaprej integriranih aplikacij. Vse te aplikacije podpirajo izkušnjo SSO. Aplikacije lahko preprosto konfigurirate za pogojni dostop storitve Azure AD za posamezno aplikacijo ali s pravilniki, ki veljajo za celotno organizacijo. Ko dodate aplikacijo in jo konfigurirate za svoje potrebe, jo lahko uporabniki s pooblaščenim dostopom preprosto najdejo v portalu »Moje aplikacije« storitve Azure AD, ki je osrednji portal za odkrivanje in zagon aplikacij za končne uporabnike.

Če ste ustvarili aplikacijo ali pa jo želite imeti integrirano za svojo organizacijo, lahko tudi zahtevate, da je navedena v galeriji aplikacij storitve Azure AD.

Raziščite več tisoč vnaprej integriranih aplikacij >



Varen hibridni dostop

S strežnikom proxy aplikacije storitve Azure AD lahko omogočite varen oddaljen dostop do spletnih aplikacij na mestu uporabe ba podlagi zahteve brez omrežja VPN. Strežnik proxy aplikacije zahteva namestitev osnovnega povezovalnika in ponuja enako izkušnjo za osebje IT in končne uporabnike kot aplikacije SaaS, povezane prek galerije aplikacij storitve Azure AD.

Če pa želite izkoristiti vložke v obstoječo infrastrukturo, na primer s partnerji, ko so F5 ZScaler, SAP, Oracle ali Ping Identity, za povezavo drugih vrst aplikacij, kot so na tiste, ki uporabljajo protokole preverjanja pristnosti na osnovi glave ali storitve Kerberos, lahko naredite tudi to in še vedno dobite prednosti centralizacije in varnosti storitve Azure AD.

Preberite, kako dodate aplikacijo na mestu uporabe s strežnikom proxy aplikacije >

Povežite druga partnerska omrežja in oblake z aplikacijami >

Kako upravljati in varovati aplikacije s storitvijo Azure AD



Avtomatizirano omogočanje uporabe

S storitvijo Azure AD lahko avtomatizirate ustvarjanje, vzdrževanje in odstranjevanje uporabniških identitet in priljubljenih aplikacij SaaS. Samodejno lahko ustvarite nove račune v ustreznih sistemih za nove ljudi, ko se pridružijo ekipi ali organizaciji. Ko ljudje zapustijo ekipo ali organizacijo, lahko nastavite pravilnike, ki bodo samodejno dezaktivirali njihove račune v ustreznih sistemih. Z avtomatizacijo teh opravil lahko poskrbite, da so identitete v aplikacijah in sistemih posodobljene glede na spremembe v imeniku ali sistemu človeških virov, s tem znižate število napak in prihranite čas.

Več informacij o nastavitvi avtomatiziranega omogočanja in onemogočanje uporabe za aplikacije SaaS >



Upravljanje ekipe

S storitvijo Azure AD lahko dodate dostop do virov organizacije tako, da ponudite pravice za dostop enemu uporabniku ali celotni skupini v storitvi Azure AD. Lastnik vira lahko s skupinami nastavi dovoljenja za dostop za vse člane skupine. Tako mu ni treba dajati pravic posamezno. To je bolj varen način, saj je manj verjetnosti, da boste dali posamezniku nepravilen dostop, hkrati pa lahko prihranite pri času. Obseg upravljanja skupine lahko dinamično prilagodite tako, da postopek avtomatizirate s pravilniki, ki temeljijo na atributih identitete.

Več informacij o ustvarjanju skupine v portalu Azure >

Kako upravljati in varovati aplikacije s storitvijo Azure AD



Samopostrežne storitve za uporabnike

Za dokončanje nekaterih opravil ne potrebujete pomoč strokovnjaka za IT. S storitvijo Azure AD lahko ta opravila dodelite drugim v organizaciji. Uporabnikom lahko omogočite ustvarjanje in upravljanje lastnih varnostnih skupin v storitvi Azure AD. Lastniki skupine lahko odobrijo ali zavrnejo zahteve za članstvo, lahko pa tudi pooblastijo drugega za nadzor članstva v skupini.

Nastavitev samoupravljanih skupin >

Samopostrežne storitve so razširjene tudi na uporabnike. Uporabniki se lahko registrirajo za račun prek samopostrežnega portala, če imajo preverjen e-poštni naslov, s portalom pa lahko ponastavijo svoje geslo. Center za pomoč uporabnikom lahko s tem prihrani ogromno časa in denarja.

Konfiguracija samopostrežne ponastavitve gesla >



Sodobno preverjanje pristnosti

Če trenutno uporabljate preverjanje pristnosti na mestu uporabe, kot je Active Directory Federation Services (AD FS), lahko svoje aplikacije preselite v Azure AD. S tem ohranite enake ugodnosti za uporabnike, kot je SSO, dobite pa možnost prilagoditve in varnostne prednosti, ki so na voljo v oblaku, kot je na primer uporaba zrnatega nadzora dostopa do aplikacije s pogojnim dostopom storitve Azure AD, ali pa ponudite partnerjem dostop do virov s sodelovanje B2B v storitvi Azure AD. Preseliti je mogoče vse aplikacije, ki za zunanji vpis uporabljajo standarde SAML 2.0, WS-Federation, OAuth ali OpenID Connect.

Zavarujte dostop do aplikacij tako, da ustvarite pravilnike o pogojnem dostopu storitve Azure AD >

Uporabite storitev Azure AD B2B za nemoteno sodelovanje z zunanjimi partnerji >

Varno povežite poljubno aplikacijo v poljubnem oblaku ali strežniku s storitvijo Azure AD.

1 milijon povezanih aktivnih enoličnih aplikacij.

Microsoft

Začnite že danes.

Začnite brezplačen, enomesečni preizkus storitve Azure AD, da se prepričate, kako preprosto lahko upravljate dostop uporabnikov do vseh vaših aplikacij in zavarujete svoje podjetje.

