



Gestionați și securizați accesul la aplicații cu **Azure Active Directory**



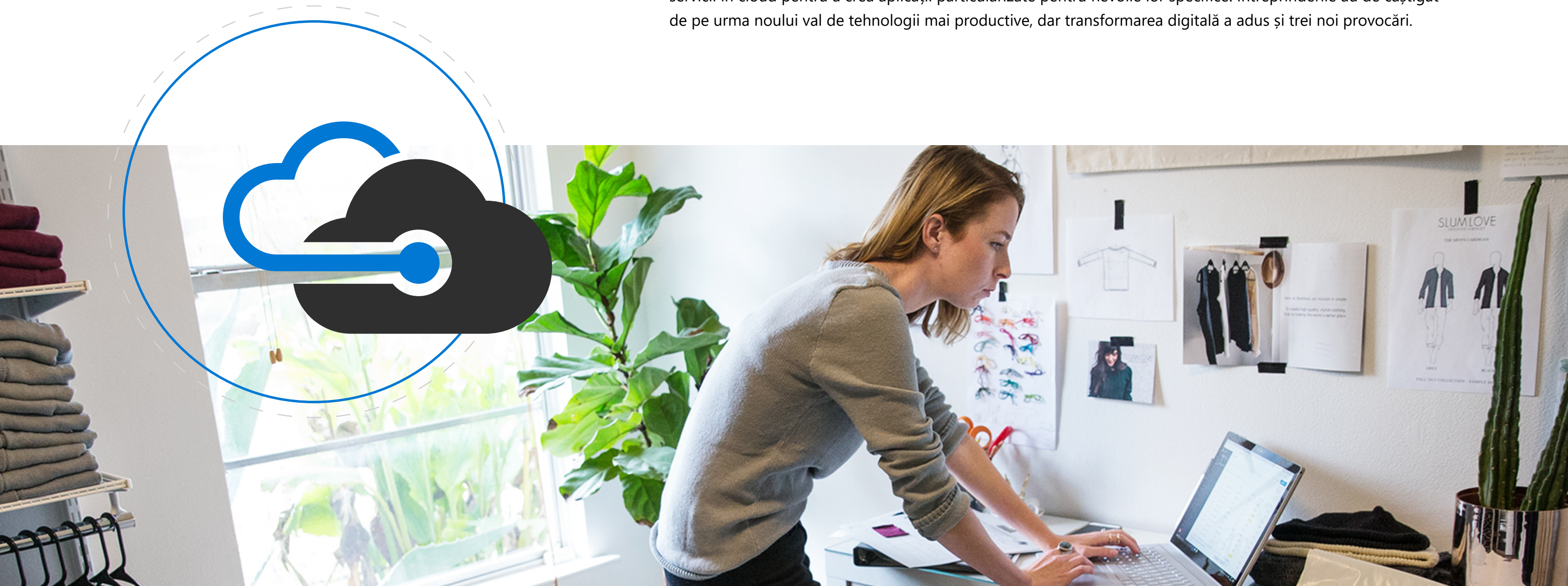
Secțiunea 1

Ce este gestionarea
identității și a accesului?

Ce este gestionarea identității și a accesului?

Transformare digitală

Informatica în cloud și dispozitivele mobile au transformat locul de muncă modern. Forța de muncă tot mai globalizată are flexibilitatea de a lucra de oriunde, utilizând aplicații software ca serviciu (SaaS) gratuite sau cu costuri reduse, pentru a rezolva problemele legate de productivitate și colaborare. Întreprinderile mari migrează aplicațiile și informatica în cloud pentru a-și moderniza arhitectura, iar domeniile de activitate profită de noile servicii în cloud pentru a crea aplicații particularizate pentru nevoile lor specifice. Întreprinderile au de câștigat de pe urma noului val de tehnologii mai productive, dar transformarea digitală a adus și trei noi provocări.



Ce este gestionarea identității și a accesului?

Provocări noi

Provocări
datorate
transformării
digitale

Riscul de securitate: Înainte de revoluția cloud, echipa IT era un fel de gardian al tehnologiei. Aplicațiile și platformele pe care le gestionați și securizați erau protejate în perimetrul de rețea și toți cei care se conectau la resursele firmei erau mai întâi validați de firewall. Acum, lucrurile s-au schimbat. Forța de muncă deține un control sporit asupra tehnologiei pe care o folosește, pe care o accesează în principal prin internet. Atacatorii cibernetici au învățat să exploateze aceste vulnerabilități. Chiar dacă un utilizator știe parola unui cont, nu puteți avea mereu certitudinea că acesta este cine spune că este.

Sarcina administrativă: Multitudinea de puncte finale le oferă utilizatorilor mai multe modalități de a se conecta, dar acestea reprezintă totodată un coșmar pentru administratori. Multe întreprinderi nu știu ce instrumente folosesc angajații și, chiar dacă au un inventar complet, numărul mare de aplicații în cloud înseamnă că trebuie să gestionați mai multe sisteme de identificare, să creșteți costurile și să calculați riscurile de securitate existente.

Experiența redusă a utilizatorilor: Și utilizatorii sunt afectați. Aceștia apreciază flexibilitatea, dar sunt frustrați de numărul de acreditări pe care trebuie să le memoreze.



Riscul de securitate



Sarcina
administrativă



Experiența neplăcută
a utilizatorilor

Ce este gestionarea identității și a accesului?

Gestionarea identității și accesului ca post central de comandă

Numitorul comun al acestor puncte slabe îl reprezintă sistemele ineficiente de confirmare a identității. Identitatea a înlocuit perimetrul de rețea, ca nou post de comandă. Aveți nevoie de soluții care să conecteze instrumentele, arhitectura, dispozitivele și serviciile disparate din întreaga întreprindere pentru a proteja mai bine organizația și a gestiona accesul atât pentru angajați, cât și pentru partenerii externi. Sistemele de identificare și gestionare a accesului (IAM) reunesc accesul într-un singur sistem, oferindu-vă un control sporit. Acestea asigură o colaborare fără probleme în perimetrul organizației, îmbunătățind securitatea resurselor firmei. Cu o soluție IAM eficientă, puteți conecta utilizatorii la toate aplicațiile lor pentru lucru, în cloud sau locale, printr-un set de acreditări. Soluțiile IAM sunt create pentru a le acorda utilizatorilor acces numai la resursele necesare și pentru a bloca accesul utilizatorilor neautorizați la date interzise. Dvs. gestionați drepturile și permisiunile pentru accesul utilizatorilor prin intermediul unui portal centralizat, reducând numărul de procese manuale necesare pentru asigurarea și retragerea accesului la conturile de utilizator. De asemenea, soluțiile IAM oferă instrumente pentru gestionarea politicilor de securitate pentru toate identitățile și aplicațiile. Cele mai bune soluții IAM protejează mai bine identitățile, îmbunătățesc experiența utilizatorului și cresc eficiența administrativă.

Soluțiile IAM
răspund acestor
provocări



Protejează mai
bine identitățile



Îmbunătățesc
experiența
utilizatorului



Cresc eficiența
administrativă

Secțiunea 2

Prezentarea generală
Azure AD

Prezentarea generală Azure AD

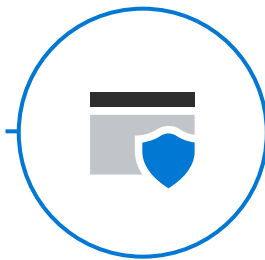
O soluție completă

Microsoft Azure Active Directory (Azure AD) este o soluție IAM completă în cloud și lider pe piață în ceea ce privește gestionarea directoarelor, accesul la aplicații și protecția avansată a identității. Azure AD ajută organizațiile să gestioneze și să securizeze identitățile angajaților, partenerilor și clienților, pentru a accesa aplicațiile și serviciile de care au nevoie. Azure AD ajută milioane de organizații să gestioneze și să securizeze peste un miliard de identități.



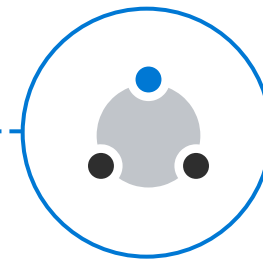
Modernizarea accesului

Gestionați și securizați accesul la datele și resursele organizației, la nivel local și în cloud. Conectați toți utilizatorii, toate aplicațiile și dispozitivele la cloud pentru acces securizat, fără întreruperi, și vizibilitate și control sporite. Automatizați fluxurile de lucru și activați opțiunile cu autoservire care vă ajută să mențineți costurile reduse și să îmbunătățiți productivitatea pentru utilizatorii dvs.



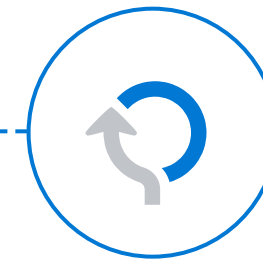
Securizare și reglementare

Din cauza numărului zilnic mare de atacuri legate de acreditările utilizatorilor, soluția împotriva compromiterii acestora este monitorizarea continuă a comportamentului normal și anormal pentru un set cât mai mare de semnale, folosirea inteligenței artificiale și automatizarea răspunsurilor. Echilibrați productivitatea și securitatea cu accesul prompt la resursele potrivite, verificările periodice ale accesului și implementarea de politici.



Conectare și colaborare

Extindeți-vă afacerea cu un serviciu în cloud fiabil care poate fi implementat pentru milioane de utilizatori, cu securitate și flexibilitate de primă clasă. Conectați-vă cu utilizatorii externi și ajutați-i să fie productivi, cu experiențe prietenoase, cu autoservire și controale de securitate încorporate.



Dezvoltare și integrare

Creați aplicații care le oferă utilizatorilor o modalitate simplă de a se conecta cu conturile Microsoft personale, de la locul de muncă sau de la școală sau cu conturile de rețele sociale. Conectați-vă la Microsoft Graph, centrul de date și informații din Microsoft 365, și dezvoltați aplicații complexe. Activați sign-on unic, automatizați asigurarea accesului utilizatorilor și luați legătura cu cele mai mari organizații din lume.

Secțiunea 3

Azure AD pentru
aplicațiile dvs.

Azure AD pentru aplicațiile dvs.

O platformă universală

Cu Azure AD, puteți să gestionați o identitate comună pentru fiecare utilizator din infrastructura hibridă, astfel încât să acceseze toate aplicațiile de care are nevoie, inclusiv aplicații de tip line-of-business în cloud și locale. Gestionati-vă toate identitățile de pe o platformă universală, crescând eficiența administrativă și sporindu-vă controlul. Aplicați politici de securitate granulare pentru fiecare aplicație utilizată de organizația dvs.



Azure AD pentru aplicațiile dvs.

Economisiți timp și bani

Serviciul Azure AD este preintegrat în mii de aplicații, inclusiv aplicații populare precum Workday, ServiceNow, SuccessFactors, Adobe și Concur, prin urmare puteți să le oferiți cu ușurință aceste aplicații utilizatorilor. Cu o singură consolă, implementați politici coerente și monitorizați drepturile de acces. Puteți să automatizați fluxurile de lucru pentru asigurarea accesului utilizatorilor și gestionarea pe durata ciclului de viață și să economisiți timp și resurse prin gestionarea cu autoservire a conturilor. De asemenea, puteți să introduceți informații despre utilizatori din instrumentele pentru resurse umane ca sursă a adevărului, eliminând necesitatea scripturilor personalizate sau a proceselor manuale pentru gestionarea atributelor utilizatorilor.

Aplicațiile configurate prin serviciul Azure AD activează sign-on unic (SSO) pentru acces fără întreruperi, ceea ce înseamnă că nu este nevoie ca utilizatorii să memoreze acreditările pentru fiecare cont de aplicație sau să refolosească parole slabe și să riște încălcarea securității datelor. Conturile care au fost configurate pentru asigurarea automată a accesului le acordă utilizatorilor acces la resurse noi cât mai curând posibil. Pentru acordarea accesului pe plan intern, Azure AD se asigură că noii angajați au acces la toate resursele relevante din prima zi.



**Economie de
timp și bani**



**Integrări SaaS
încorporate**



Sign-on unic



**Acces pentru utilizatori
din prima zi**

Azure AD pentru aplicațiile dvs.

Securizați accesul la toate aplicațiile

Azure AD vă oferă o protecție completă a identității în toate aplicațiile, atât în aplicațiile SaaS, cât și în aplicațiile line-of-business locale. Dacă utilizatorul solicită acces în Microsoft Word sau Box, Azure AD cere confirmarea identității înainte de a acorda acces. De asemenea, puteți să aplicați politici de reglementare a accesului ca să vă asigurați că utilizatorii au acces la ceea ce au nevoie, atunci când au nevoie. Puteți să le cereți utilizatorilor să solicite permisiunea pentru acces, să setați o limită de timp pentru accesul acestora la aplicație și să faceți verificări periodice ale conformității privind accesul.

În plus, Azure AD utilizează Microsoft Intelligent Security Graph și învățarea automată pentru a analiza trilioane de semnale din toate produsele și serviciile noastre, pentru a detecta eventuale comportamente atipice și a estima riscul relativ al fiecărei sesiuni. Azure AD analizează dispozitivul, locația și alte informații contextuale pentru a evalua riscul conectării. Puteți să stabiliți politici de Acces condiționat de Azure AD care aplică automat măsuri de securitate, cum ar fi blocarea unei solicitări de acces sau solicitarea resetării parolei atunci când o conectare este considerată riscantă sau sunt îndeplinite anumite condiții ale politicilor.



**Măsuri de securitate
pentru aplicații**



**Protecția
identității**



**Reglementarea
accesului**



**Politici de acces
condiționat**

Secțiunea 4

Cum să gestionați și să
securizați aplicațiile cu Azure AD

Azure AD simplifică gestionarea și reduce costurile prin automatizare, autoservire și aplicarea politicilor.

Cum să gestionați și să securizați aplicațiile cu Azure AD



Integrările cu aplicațiile Azure AD

Galeria de aplicații Azure AD facilitează configurarea și conectarea oricăreia dintre miile de aplicații preintegrate la entitatea dvs. găzduită. Toate aceste aplicații acceptă sign-on unic și sunt ușor de configurat pentru Accesul condiționat Azure AD pentru fiecare aplicație sau pentru politicile la nivel de întreprindere. După ce ați adăugat aplicația și ați configurat-o conform cerințelor dvs., utilizatorii cu acces autorizat o pot găsi cu ușurință în portalul Aplicațiile mele Azure AD, un portal centralizat pentru descoperirea și lansarea aplicațiilor pentru utilizatorii finali.

Dacă ați creat o aplicație sau aveți nevoie de o aplicație integrată pentru organizația dvs., puteți să solicitați afișarea acesteia în galeria de aplicații Azure AD.

[Explorați miile de aplicații preintegrate >](#)



Acces hibrid securizat

Utilizați proxy-ul pentru aplicații Azure AD pentru a asigura accesul securizat de la distanță la aplicații web locale bazate pe solicitări, fără a fi necesar un VPN. Proxy-ul pentru aplicații necesită instalarea unui conector ușor și oferă aceeași experiență echipei IT și utilizatorilor finali ca aplicațiile SaaS conectate prin galeria de aplicații Azure AD.

Sau, dacă doriți să folosiți investițiile în infrastructurile existente, cum ar fi cele cu parteneri precum F5 ZScaler, SAP, Oracle sau Ping Identity pentru a conecta alte tipuri de aplicații, cum ar fi cele care utilizează protocoale de autentificare bazate pe antet sau Kerberos, puteți să faceți acest lucru și să vă bucurați și de beneficiile centralizării și securității oferite de Azure AD.

[Aflați cum să adăugați o aplicație locală folosind proxy-ul pentru aplicații >](#)

[Conectați alte rețele și medii cloud cu aplicații partenere >](#)

Cum să gestionați și să securizați aplicațiile cu Azure AD



Asigurarea automată a accesului

Azure AD permite automatizarea creării, păstrării și eliminării identităților utilizatorilor din aplicațiile SaaS populare. Puteți crea automat conturi noi pe sistemele potrivite pentru persoane noi, atunci când se alătură echipei sau organizației dvs. Atunci când persoanele părăsesc o echipă sau o organizație, puteți stabili politici care să le dezactiveze automat conturile de pe sistemele respective. Prin automatizarea acestor activități, vă asigurați că identitățile din aplicațiile și sistemele dvs. sunt actualizate pe baza modificărilor din director sau de pe sistemul pentru resurse umane, cu mai puține erori și într-un timp mai scurt.

[Aflați mai multe despre configurarea asigurării accesului și a retragerii automatizate a acestuia pentru aplicațiile SaaS >](#)



Gestionarea grupurilor

Azure AD vă oferă acces la resursele organizației dvs., acordând drepturi de acces unui singur utilizator sau unui întreg grup Azure AD. Utilizarea grupurilor îi permite proprietarului resurselor să seteze permisiuni de acces pentru toți membrii grupului, în loc să acorde drepturile pe rând. Aceasta este o metodă mai sigură, deoarece există șanse mai mici să acordați din greșeală acces necorespunzător unei persoane și economisiți timp. În plus, puteți să scalați dinamic gestionarea grupurilor dacă setați automatizarea înregistrării prin politici bazate pe atributele identității.

[Aflați cum să creați un grup în portalul Azure >](#)

Cum să gestionați și să securizați aplicațiile cu Azure AD



Autoservire pentru utilizatori

În cazul anumitor activități, nu este nevoie de un profesionist IT care să le finalizeze, iar Azure AD vă dă posibilitatea să le delegați altor persoane din organizație. Puteți ajuta utilizatorii să creeze și să gestioneze propriile grupuri de securitate în Azure AD. Proprietarii grupurilor pot să aprobe sau să refuze solicitările de înscriere a membrilor sau să delege controlul asupra membrilor grupului.

[Configurați grupuri autogestionate >](#)

Autoservirea este disponibilă și pentru utilizatori. Utilizatorii își pot crea un cont în portalul cu autoservire dacă au o adresă de e-mail confirmată și pot folosi portalul pentru a-și reseta parola. Astfel, biroul de asistență poate economisi mult timp și mulți bani.

[Configurați resetarea parolei cu autoservire >](#)



Modernizarea autentificării

Dacă în prezent folosiți autentificarea locală, de exemplu, Active Directory Federation Services (AD FS), vă recomandăm să vă migrați aplicațiile la Azure AD. Veți avea aceleași avantaje ca utilizator, precum SSO, dar vă veți bucura și de beneficii de scalabilitate și securitate disponibile în cloud, cum ar fi aplicarea controalelor granulare de acces pentru fiecare aplicație utilizând Accesul condiționat de Azure AD sau acordarea accesului partenerilor la resurse prin colaborarea în Azure AD B2B. Toate aplicațiile care utilizează standardele SAML 2.0, WS-Federation, OAuth sau OpenID Connect pentru sign-on federativ pot fi migrate.

[Creați politici de Acces condiționat de Azure AD pentru a securiza accesul la aplicații >](#)

[Utilizați Azure AD B2B pentru a colabora fără probleme cu partenerii externi >](#)

Conectați în siguranță orice aplicație, din orice mediu cloud sau de pe orice server la Azure AD.

Un milion de aplicații
unice active conectate.

Începeți lucrul astăzi.

Începeți o versiune de încercare gratuită de Azure AD timp de o lună pentru a afla cât de simplu este să gestionați accesul utilizatorilor la toate aplicațiile și să securizați întreprinderea.

