Microsoft

Gestisci e proteggi l'accesso alle tue applicazioni con Azure Active Directory

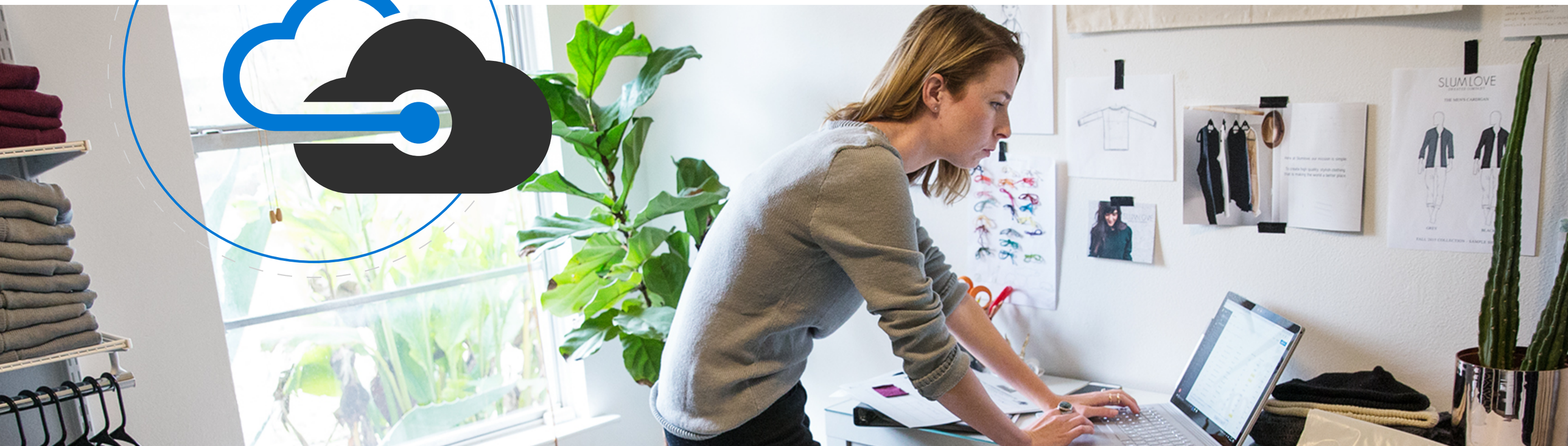
Sezione 1

Cos'è la gestione delle identità e degli accessi?

Cos'è la gestione delle identità e degli accessi?

Trasformazione digitale

Il cloud computing e i dispositivi mobili hanno trasformato l'ambiente di lavoro moderno. Una forza lavoro sempre più ampia beneficia della flessibilità di lavorare ovunque con applicazioni Software as a Service (SaaS) gratuite o a basso costo che consentono di vincere le sfide di produttività e collaborazione. Le imprese più grandi stanno eseguendo la migrazione di applicazioni e servizi informatici al cloud per modernizzarne l'architettura e le line-of-businesses sfruttano i nuovi servizi cloud per creare app personalizzate per le proprie esigenze specifiche. Grazie all'ampia offerta di nuove tecnologie, le grandi imprese hanno aumentato la produttività. Tuttavia la trasformazione digitale le ha messe davanti a tre nuove sfide.



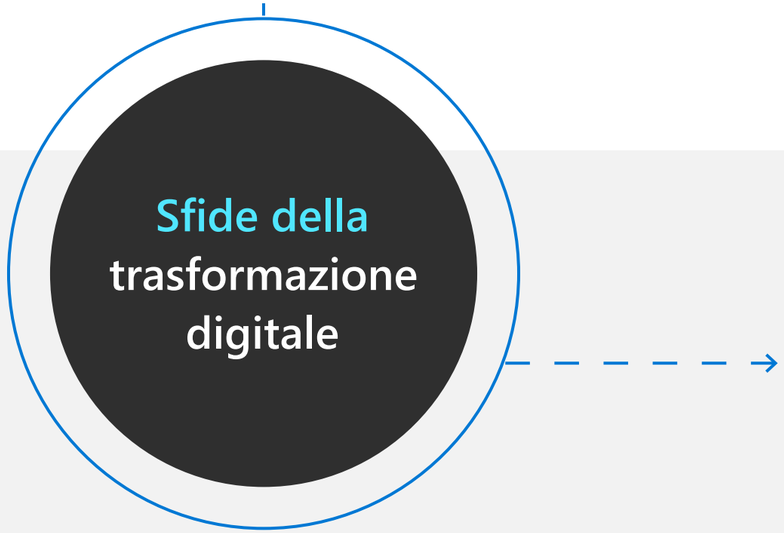
Cos'è la gestione delle identità e degli accessi?

Nuove sfide

Rischio per la sicurezza: prima della rivoluzione cloud, l'IT svolgeva il ruolo di guardiano della tecnologia. Le app e le piattaforme gestite e protette erano contenute nel perimetro di rete, e chiunque avesse voluto accedere alle risorse aziendali doveva prima superare i controlli del firewall. Ora non è più così. La forza lavoro ha maggiore controllo sulla tecnologia che usa, cui accede da Internet nella maggior parte dei casi. Gli autori di attacchi informatici hanno imparato a sfruttare le vulnerabilità presenti. Anche se un utente conosce la password di un account, non si può mai essere del tutto certi della sua reale identità.

Costi indiretti amministrativi: l'incremento di endpoint offre agli utenti altri modi per connettersi, creando però un incubo amministrativo. Le imprese non hanno idea di tutti gli strumenti usati dai propri dipendenti e anche se l'avessero, la molteplicità delle app cloud rende necessario gestire più sistemi di identità, l'aumento dei costi e la combinazione degli esistenti rischi per la sicurezza.

Esperienza utente insoddisfacente: anche se gli utenti apprezzano molto la flessibilità che deriva dall'uso di più applicazioni, non possono non avvertire la frustrazione di dover ricordare un gran numero di credenziali.



Rischio per la sicurezza

Costi indiretti amministrativi

Esperienza utente insoddisfacente

Cos'è la gestione delle identità e degli accessi?

Gestione di identità e accesso come piano di controllo centrale

Il denominatore comune tra questi punti negativi è l'inefficienza dei sistemi di verifica delle identità. L'identità ha sostituito il perimetro di rete come piano di controllo centrale. Sono necessarie soluzioni che colleghino diversi strumenti, architetture, dispositivi e servizi in tutta l'azienda, al fine di garantire all'organizzazione una maggiore protezione e la possibilità di gestire i sistemi IAM di gestione delle identità e degli accessi di dipendenti e partner esterni con un unico sistema per avere maggiore controllo. Sono necessarie soluzioni in grado di semplificare la collaborazione oltre i confini dell'organizzazione, che migliorino al contempo la sicurezza delle risorse aziendali. Una buona soluzione IAM consente la connessione degli utenti a tutte le applicazioni aziendali, nel cloud o locali, con un solo set di credenziali. Le soluzioni per la gestione delle identità e degli accessi sono ideate per consentire agli utenti di accedere solamente alle risorse necessarie e per impedire a chi è privo di autorizzazione di accedere a dati non pertinenti. Diritti e autorizzazioni di accesso vengono gestiti da un portale centralizzato, per ridurre gran parte dei processi manuali implicati nel provisioning e deprovisioning degli account utente. Le soluzioni IAM forniscono inoltre gli strumenti per gestire i criteri di sicurezza in tutte le identità e in tutte le app. Le migliori soluzioni IAM possono proteggere meglio le identità, migliorare l'esperienza utente e aumentare l'efficienza amministrativa.

Soluzioni IAM che vincono queste sfide

Migliore protezione delle identità

Migliore esperienza utente

Maggiore esperienza amministrativa

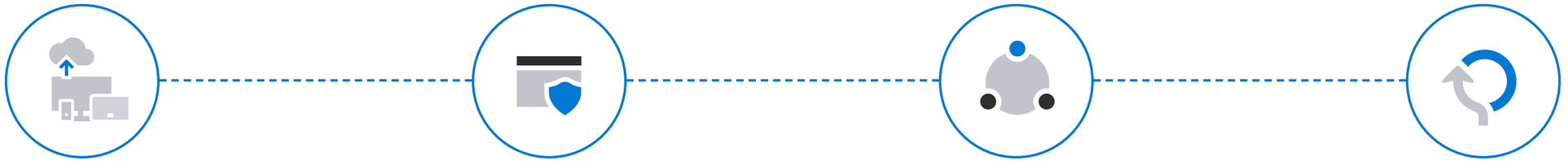
Sezione 2

Panoramica di Azure AD

Panoramica di Azure AD

Una soluzione completa

Microsoft Azure Active Directory (Azure AD) è una soluzione di gestione delle identità e degli accessi nel cloud completa, ed è leader di mercato per la gestione di directory, accesso alle applicazioni e protezione avanzata delle identità. Azure AD consente alle organizzazioni di gestire e proteggere le identità di dipendenti, partner e clienti affinché possano accedere alle app e ai servizi necessari. Azure AD aiuta milioni di organizzazioni a gestire e proteggere oltre un miliardo di identità.



Modernizza l'accesso

Gestisci e proteggi l'accesso ai dati e alle risorse dell'organizzazione locali e nel cloud. Collega tutti gli utenti, le applicazioni e i dispositivi al cloud per un accesso semplice e sicuro e per avere maggiore visibilità e controllo. Automatizza i flussi di lavoro e abilita le opzioni self-service per mantenere bassi i costi e aumentare la produttività degli utenti.

Proteggi e controlla

Dato l'alto numero quotidiano di attacchi alle credenziali utente, per prevenirne la compromissione, devi tenere continuamente traccia di comportamenti normali e anomali nel più ampio set di segnali possibile, applicare l'intelligenza artificiale e automatizzare le risposte. Bilancia produttività e sicurezza con accesso opportuno alle risorse pertinenti, normali verifiche di accesso e applicazione di criteri.

Collegati e collabora

Espandi il tuo business con un servizio cloud affidabile e scalabile a milioni di utenti con flessibilità e sicurezza leader di settore. Entra in contatto con i tuoi utenti esterni e aumenta la loro produttività con esperienze self-service e controlli di sicurezza predefiniti facili da usare.

Sviluppa e integra

Crea applicazioni che consentano agli utenti di accedere facilmente al proprio account personale Microsoft, al proprio account aziendale o dell'istituto di istruzione tramite l'account social. Avvia la connessione a Microsoft Graph, il gateway per dati e intelligence di Microsoft 365, e crea applicazioni complete. Abilita Single Sign-On, automatizza il provisioning degli utenti e raggiungi il livello delle più grandi organizzazioni del mondo.

Sezione 3

Azure AD per le tue applicazioni

Azure AD per le tue applicazioni

Una piattaforma universale

Azure AD ti permette di gestire un'identità comune per gli utenti nell'infrastruttura ibrida affinché ciascuno possa accedere a tutte le applicazioni necessarie, tra cui le applicazioni delle line of business nel cloud e locali. Gestisci tutte le identità da una piattaforma universale, aumentando l'efficienza amministrativa e assumendo maggiore controllo. Applica criteri di sicurezza granulari a ciascuna delle applicazioni dell'organizzazione.

Azure AD per le tue applicazioni

Risparmia tempo e denaro

Azure AD è una soluzione pre-integrata in migliaia di applicazioni, incluse le più comuni come Workday, ServiceNow, SuccessFactors, Adobe e Concur, il che facilita maggiormente la distribuzione delle applicazioni stesse. Con una sola console, puoi distribuire criteri coerenti e monitorare i diritti di accesso. Puoi automatizzare i flussi di lavoro per il provisioning degli utenti e la gestione del ciclo di vita e risparmiare tempo e risorse con la gestione self-service degli account. Puoi anche inserire le informazioni utente dagli strumenti delle risorse umane come origine di riferimento, eliminando la necessità di script personalizzati o processi manuali per gestire gli attributi degli utenti.

Le app configurate tramite Azure AD abilitano Single Sign-On (SSO) per un accesso più semplice, che solleva gli utenti dal dover ricordare le proprie credenziali per l'account di ogni app o dal riutilizzare password vulnerabili rischiando che i propri dati vengano violati. Gli account configurati per il provisioning automatico consentono agli utenti di accedere a nuove risorse il prima possibile. Per quanto riguarda il provisioning in ingresso, Azure AD garantisce ai nuovi assunti di accedere a tutte le risorse di pertinenza dal primo giorno.

Risparmia tempo e denaro

Integrazioni SaaS predefinite

Single Sign-On

Accesso degli utenti dal primo giorno

Azure AD per le tue applicazioni

Accesso più sicuro a tutte le tue app

Azure AD offre protezione completa alle identità in tutte le tue app, sia app SaaS sia app delle line of business locali. Se l'utente richiede accesso a Microsoft Word o a Box, Azure AD ne verifica l'identità prima di concedere l'accesso. Inoltre, puoi introdurre criteri di governance dell'accesso affinché gli utenti abbiano accesso solo quando necessario. Puoi impostare la richiesta necessaria di autorizzazioni da parte degli utenti e un limite di tempo per l'accesso all'applicazione e condurre delle regolari verifiche di conformità degli accessi.

Azure AD sfrutta inoltre la potenza di Microsoft Intelligent Security Graph e dell'apprendimento automatico per analizzare miliardi di segnali in tutti i prodotti e servizi al fine di identificare comportamenti atipici e assegnare ad ogni sessione il relativo livello di rischio. Per valutare il rischio dell'accesso, Azure AD controlla il dispositivo, la posizione e altre informazioni contestuali. Puoi stabilire criteri di accesso condizionale di Azure AD che applicano automaticamente misure di sicurezza, quali il blocco di richieste di accesso o di reimpostazione della password in caso di accesso considerato rischioso o se vengono soddisfatte le condizioni di particolari criteri.

Misure di sicurezza delle applicazioni

Protezione dell'identità

Governance dell'accesso

Criteri di accesso condizionale

Sezione 4

Come gestire e proteggere le app con Azure AD

Azure AD consente di mantenere il controllo e ridurre i costi facilmente tramite automazione, modalità self-service e applicazione dei criteri.

Come gestire e proteggere le app con Azure AD

Integrazioni di app di Azure AD

La raccolta di applicazioni di Azure AD facilita la configurazione e la connessione di ciascuna delle migliaia di app pre-integrate al tuo tenant. Tutte queste app supportano un'esperienza SSO, ed è facile configurarle per l'accesso condizionale di Azure AD in base all'app o ai criteri per l'organizzazione. Una volta aggiunta e configurata l'app in base alle tue esigenze, gli utenti con autorizzazioni di accesso possono trovarla facilmente nel portale App personali di Azure AD, un portale centralizzato che consente all'utente finale di individuare e avviare l'app.

Se hai creato un'app o hai bisogno di un'app integrata per la tua organizzazione, puoi anche richiedere che venga elencata nella raccolta di applicazioni di Azure AD.

Esplora le migliaia di app pre-integrate >

Accesso ibrido sicuro

Il proxy di applicazione di Azure AD offre accesso remoto sicuro alle applicazioni Web locali e basate sulle attestazioni, senza bisogno di VPN. Il proxy di applicazione richiede l'installazione di connettori disattivi e assicura la stessa esperienza dell'IT e dell'utente finale delle app SaaS tramite la raccolta di applicazioni di Azure AD.

Se lo desideri, puoi anche sfruttare gli investimenti dell'infrastruttura esistente, ad esempio con partner quali F5 ZScaler, SAP, Oracle o Ping Identity, per connettere altri tipi di app come quelle che utilizzano protocolli di autenticazione Kerberos o basati su intestazione, e comunque usufruire dei benefici di sicurezza e centralizzazione di Azure AD.

Scopri come aggiungere un'applicazione locale tramite il proxy di applicazione >

Collega cloud e reti di app di altri partner >

Come gestire e proteggere le app con Azure AD

Provisioning automatizzato

Con Azure AD puoi automatizzare la creazione, la manutenzione e la rimozione delle identità utente nelle comuni applicazioni SaaS. Puoi creare automaticamente nuovi account per nuovi utenti che entrano a far parte del team o dell'organizzazione nei sistemi pertinenti. Se un utente lascia un team o un'organizzazione, puoi impostare criteri che ne disattiveranno automaticamente l'account dai sistemi pertinenti. L'automatizzazione di queste attività consente di tenere aggiornate le identità nelle tue app in base alle modifiche della directory o del sistema delle risorse umane, riducendo errori e risparmiando tempo.

Scopri di più su come impostare il provisioning e il deprovisioning automatizzato per le app SaaS >

Gestione dei gruppi

Con Azure AD puoi fornire l'accesso alle risorse dell'organizzazione concedendone i diritti a un utente singolo o a un intero gruppo Azure AD. Il proprietario della risorsa imposta le autorizzazioni di accesso per tutti i membri del gruppo, anziché fornirle singolarmente. Si tratta di un metodo più sicuro perché riduce gli errori di concessione di accesso inappropriato e consente di risparmiare tempo. Puoi anche scalare la gestione del gruppo in modo dinamico automatizzando l'iscrizione tramite criteri basati su attributi dell'identità.

Scopri come creare un gruppo nel portale di Azure >

Come gestire e proteggere le app con Azure AD

Modalità self-service per l'utente

Poiché per alcune attività non è necessario il completamento da parte di un professionista dell'IT, con Azure AD puoi delegarle ad altri utenti dell'organizzazione. Gli utenti possono creare e gestire i propri gruppi di sicurezza in Azure AD. I proprietari dei gruppi possono approvare o rifiutare le richieste di appartenenza, oppure possono delegare il controllo di appartenenza a gruppi.

Imposta gruppi auto-gestiti >

Modalità self-service estesa agli utenti. Gli utenti possono registrarsi a un account tramite il portale self-service se dispongono di posta elettronica verificata. Inoltre, possono usare il portale per reimpostare la password. Ciò consente all'helpdesk di risparmiare molto tempo e denaro.

Configura la reimpostazione self-service della password >

Modernizza l'autenticazione

Se attualmente usi servizi di autenticazione locale come Active Directory Federation Services (AD FS), puoi prendere in considerazione l'idea di migrare le tue app ad Azure AD. Manterrai gli stessi vantaggi dell'accesso SSO, e in più potrai beneficiare anche della scalabilità e della sicurezza del cloud ad esempio applicando controlli di accesso per applicazione granulari tramite l'accesso condizionale di Azure AD o concedendo ai partner l'accesso alle risorse con la collaborazione B2B di Azure. Possono essere migrate tutte le app che usano standard SAML 2.0, WS-Federation, OAuth o OpenID Connect per accesso federato.

Crea criteri di accesso condizionale di Azure AD per proteggere l'accesso alle tue app >

Usa B2B di Azure AD per collaborare in modo facile con i partner esterni >

Collega qualsiasi app a Azure AD su
qualsiasi cloud o server in modo sicuro.

1 milione di app attive e uniche collegate.

Microsoft

Inizia a usarlo oggi stesso.

Prova per un mese la versione di valutazione gratuita di Azure AD e scopri quanto sia semplice gestire l'accesso degli utenti a tutte le app e proteggere la tua azienda.