



Gerir e proteger o acesso às suas aplicações com o **Azure Active Directory**



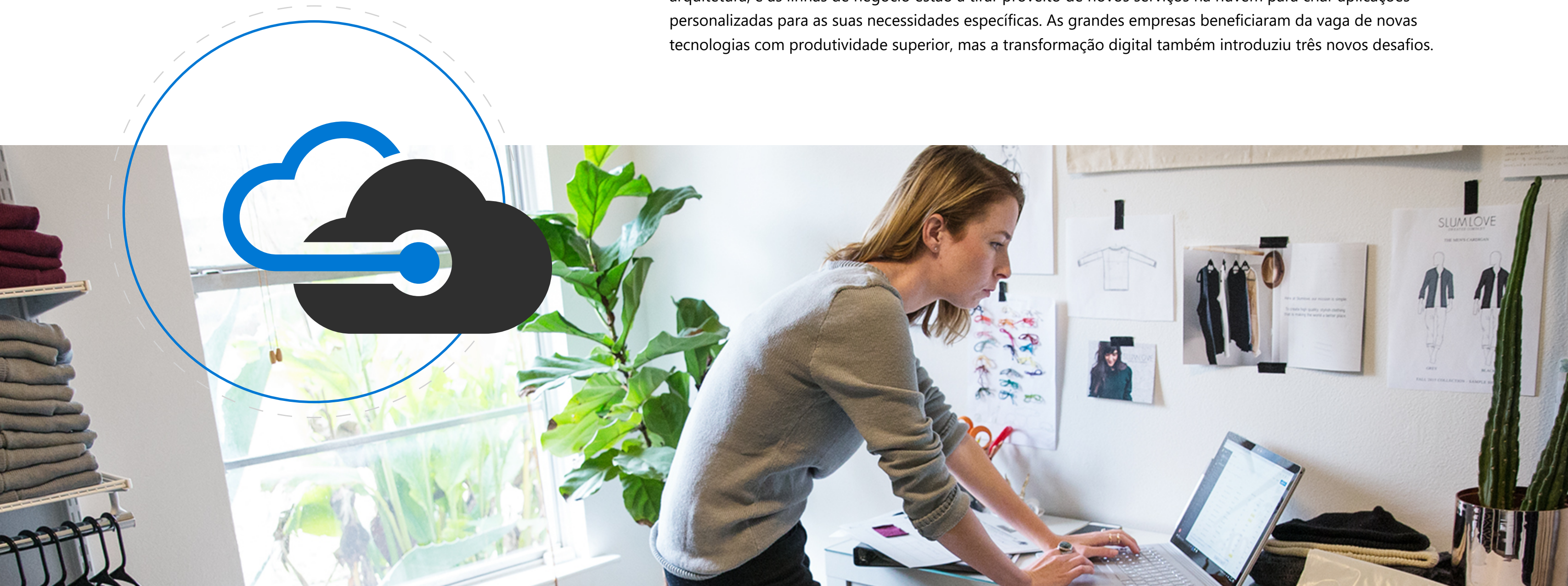
Secção 1

O que é a gestão de
identidades e acesso?

O que é a gestão de identidades e acesso?

Transformação digital

A computação na nuvem e os dispositivos móveis transformaram o local de trabalho moderno. Uma força de trabalho cada vez mais global tem a flexibilidade de trabalhar a partir de qualquer lugar com aplicações SaaS (Software como um Serviço) gratuitas e de baixo custo para resolver desafios de produtividade e colaboração. As grandes empresas estão a migrar as aplicações e a computação para a nuvem para modernizar a sua arquitetura, e as linhas de negócio estão a tirar proveito de novos serviços na nuvem para criar aplicações personalizadas para as suas necessidades específicas. As grandes empresas beneficiaram da vaga de novas tecnologias com produtividade superior, mas a transformação digital também introduziu três novos desafios.



O que é a gestão de identidades e acesso?

Novos desafios

Desafios devido
à transformação
digital

Risco de segurança: antes da revolução na nuvem, as TI serviam como protetoras da tecnologia. As aplicações e plataformas que geria e protegia eram contidas no perímetro da rede e todas as pessoas que iniciavam sessão nos seus recursos empresariais eram primeiro validadas pela firewall. Isso acabou. A sua força de trabalho tem mais controlo sobre a tecnologia que utiliza, que é maioritariamente acedida através da Internet. Os ciberatacantes aprenderam a explorar estas vulnerabilidades. Mesmo quando um utilizador sabe a palavra-passe certa de uma conta, não pode ter sempre a certeza de que essa pessoa é quem afirma ser.

Fardo administrativo: a explosão de pontos finais proporciona aos utilizadores mais formas de comunicar, mas isto também cria um pesadelo administrativo. Muitas empresas não têm conhecimento de todas as ferramentas que os colaboradores utilizam e, mesmo quando têm um bom inventário, o grande número de aplicações na nuvem significa que tem de gerir múltiplos sistemas de identidades, aumentando os custos e contribuindo para os riscos de segurança existentes.

Má experiência de utilizador: os utilizadores também sentem os efeitos. Adoram a flexibilidade, mas sentem-se frustrados pelas várias credenciais que têm de memorizar.



Risco de segurança



Fardo administrativo



Má experiência
de utilizador

O que é a gestão de identidades e acesso?

Gestão de identidades e acessos como o plano de controlo central

O denominador comum em todos estes pontos fracos é a existência de sistemas ineficazes para a verificação de identidade. A identidade substituiu o perímetro de rede como o novo plano de controlo. Precisa de soluções que ligam as diferentes ferramentas, arquiteturas, dispositivos e serviços em toda a empresa, para proteger melhor a organização e gerir o acesso dos colaboradores e dos parceiros externos. Os sistemas de gestão de identidades e acesso (IAM) reúnem os acessos num só sistema, dando-lhe mais controlo. Proporcionam uma colaboração fácil em todos os departamentos da sua organização, ao mesmo tempo que melhoram a segurança dos seus recursos empresariais. Uma boa solução de IAM permite-lhe ligar os seus utilizadores a todas as respetivas aplicações de trabalho, seja na nuvem ou no local, através de um só conjunto de credenciais. As soluções de IAM foram concebidas para conceder aos utilizadores o acesso apenas aos recursos de que necessitam e bloquear utilizadores não autorizados, impedindo o seu acesso a dados aos quais não devem aceder. Pode gerir os direitos e permissões de acesso de utilizador a partir de um portal centralizado, reduzindo muitos dos processos manuais implicados no aprovisionamento e desaprovisionamento de contas de utilizador. As soluções de IAM também fornecem ferramentas para gerir políticas de segurança em todas as identidades e aplicações. As melhores soluções de IAM salvaguardam melhor as identidades, melhoram a experiência de utilizador e aumentam a eficiência administrativa.

As soluções de IAM **resolvem estes desafios**



Salvaguardam melhor as identidades



Melhoram a experiência de utilizador



Aumentam a eficiência administrativa

Secção 2

Descrição Geral do Azure AD

Descrição Geral do Azure AD

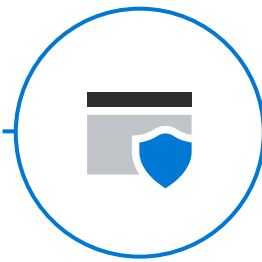
Uma solução abrangente

O Microsoft Azure Active Directory (Azure AD) é uma abrangente solução de IAM na nuvem e líder no mercado da gestão de diretórios, acesso a aplicações e proteção de identidades avançada. O Azure AD capacita as organizações para gerir e proteger as identidades para que os colaboradores, parceiros e clientes possam aceder às aplicações e serviços necessários. O Azure AD ajuda milhões de organizações a gerir e proteger mais de mil milhões de identidades.



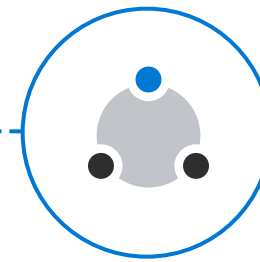
Modernize o acesso

Faça a gestão e proteja o acesso aos dados e recursos da sua organização no local ou na nuvem. Ligue todos os seus utilizadores, aplicações e dispositivos à nuvem para um acesso simples e seguro, assim como maior visibilidade e controlo. A automatização dos fluxos de trabalho e a ativação de opções de gestão personalizada ajudam a manter os custos baixos e melhorar a produtividade dos seus utilizadores.



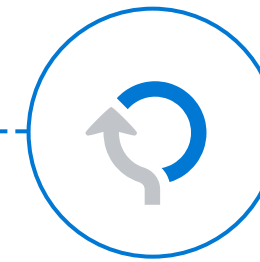
Proteja e governe

Com o elevado volume de ataques a credenciais de utilizadores todos os dias, a forma de impedir que as contas sejam comprometidas consiste em acompanhar continuamente os comportamentos normais e anormais no conjunto de sinais mais amplo possível, aplicar inteligência artificial e automatizar as respostas. Equilibre a produtividade e a segurança com o acesso atempado aos recursos adequados, assim como revisões dos acessos e implementação de políticas regulares.



Comunique e colabore

Expanda o seu negócio com um serviço na nuvem fiável que pode ser dimensionado para milhões de utilizadores com a segurança e flexibilidade líderes da indústria. Esteja em contacto com os seus utilizadores externos e dê-lhes autonomia para serem produtivos com experiências de gestão personalizada de utilização fácil e controlos de segurança integrados.



Desenvolva e integre

Crie aplicações que concedem aos utilizadores uma forma fácil de iniciar sessão com as respetivas contas pessoais, profissionais ou escolares da Microsoft, ou com as respetivas contas de redes sociais. Comece por ligar-se ao Microsoft Graph, um gateway para dados e inteligência no Microsoft 365, e crie aplicações avançadas. Ative o início de sessão único, automatize o aprovisionamento de utilizadores e alcance as maiores organizações do mundo.

Seccção 3

Azure AD para as
suas aplicações

Azure AD para as suas aplicações

Uma plataforma universal

O Azure AD permite-lhe gerir uma identidade comum para todos os utilizadores na estrutura híbrida, para que acedam a todas as aplicações necessárias, incluindo aplicações de linhas de negócio na nuvem e no local. Faça a gestão de todas as suas identidades a partir de uma plataforma universal, aumentando a eficiência administrativa e tendo mais controlo. Aplique políticas de segurança granulares a cada uma das aplicações utilizadas na sua organização.



Poupe tempo e dinheiro

O Azure AD é pré-integrado com milhares de aplicações, incluindo opções populares como o Workday, ServiceNow, SuccessFactors, Adobe e Concur, sendo mais simples para si disponibilizar estas aplicações aos seus utilizadores. Com uma consola, pode implementar políticas consistentes e monitorizar os direitos de acesso. Pode automatizar fluxos de trabalho para o aprovisionamento de utilizadores e a gestão do ciclo de vida, e poupar tempo e recursos com a gestão de contas de gestão personalizada. Também pode receber informações de utilizadores de ferramentas de RH como uma fonte fidedigna, eliminando a necessidade de scripts personalizados ou processos manuais para gerir atributos de utilizadores.

As aplicações configuradas através do Azure AD permitem o início de sessão único (SSO) para um acesso fácil, o que significa que os utilizadores não têm de memorizar as credenciais de cada conta de aplicação ou reutilizar palavras-passe fracas e arriscar uma falha de segurança de dados. As contas que foram configuradas para o aprovisionamento automático concedem aos utilizadores o acesso a novos recursos o quanto antes. Para o aprovisionamento de entrada, o Azure AD garante que as novas contratações têm acesso a todos os seus recursos relevantes no primeiro dia.



**Poupanças de
tempo e dinheiro**



Integrações de SaaS



Início de sessão único



**Acesso de utilizador
no primeiro dia**

Azure AD para as suas aplicações

Forneça um acesso mais seguro a todas as suas aplicações

O Azure AD fornece uma proteção de identidade abrangente em todas as suas aplicações (tanto em aplicações SaaS, como nas suas aplicações de linha de negócios no local). Quer o utilizador esteja a pedir o acesso ao Microsoft Word ou Box, o Azure AD garante que a sua identidade é confirmada antes de conceder acesso. Também pode instituir políticas de governação de acesso para garantir que os utilizadores só têm acesso ao que necessitam, quando o necessitam. Pode exigir que os utilizadores peçam permissão de acesso, pode definir um limite de tempo durante o qual podem aceder à aplicação e realizar revisões de conformidade regulares do acesso.

O Azure AD também tira proveito da capacidade do Grafo de Segurança Inteligente da Microsoft e da aprendizagem automática para analisar biliões de sinais em todos os nossos produtos e serviços para detetar comportamentos anormais, e atribuir um risco relativo a cada sessão. O Azure AD analisa o dispositivo, localização e outras informações contextuais para avaliar o risco do início de sessão. Pode estabelecer políticas de Acesso Condicional do Azure AD que automaticamente aplicam medidas de segurança, como bloquear um pedido de acesso ou exigir a reposição de uma palavra-passe quando um início de sessão parecer arriscado ou determinadas condições da política forem cumpridas.



Medidas de segurança de aplicações



Proteção de identidades



Governação de acessos



Políticas de Acesso Condicional

Secção 4

Como gerir e proteger aplicações com o Azure AD

O Azure AD facilita o controlo e a redução de custos com a automatização, gestão personalizada e aplicação de políticas.

Como gerir e proteger aplicações com o Azure AD



Integrações de aplicações do Azure AD

A galeria de aplicações do Azure AD facilita a configuração e ligação de qualquer uma das milhares de aplicações pré-integradas ao seu inquilino. Todas estas aplicações suportam uma experiência de SSO, sendo simples configurar as aplicações para o Acesso Condicional do Azure AD individualmente ou para políticas em toda a empresa. Depois de adicionar a aplicação e configurá-la para as suas necessidades, os utilizadores com acesso autorizado podem encontrá-la facilmente no portal As Minhas Aplicações do Azure AD, um portal centralizado para a descoberta e lançamento de aplicações dos utilizadores finais.

Se criou uma aplicação ou necessita de uma integrada para a sua organização, também pode pedir que a mesma seja incluída na galeria de aplicações do Azure AD.

[Explorar as milhares de aplicações pré-integradas >](#)



Proteger o acesso híbrido

Utilize o Proxy de Aplicações do Azure AD para conceder um acesso remoto e seguro a aplicações Web baseadas em informações no local sem a necessidade de uma VPN.

O Proxy de Aplicações exige a instalação de um conector leve e concede a mesma experiência de utilizador final e TI das aplicações SaaS ligadas através da galeria de aplicações do Azure AD.

Em alternativa, se quiser tirar proveito de investimentos em infraestruturas existentes, por exemplo com parceiros como o F5 ZScaler, SAP, Oracle ou Ping Identity, para ligar outro tipo de aplicações que utilizam protocolos de autenticação baseados em cabeçalhos ou de Kerberos, também pode fazê-lo e obter os benefícios de segurança e centralização do Azure AD.

[Saiba como adicionar uma aplicação no local através do Proxy de Aplicações >](#)

[Ligar outras nuvens e redes de aplicações de parceiros >](#)

Como gerir e proteger aplicações com o Azure AD



Aprovisionamento automático

O Azure AD permite-lhe automatizar a criação, manutenção e remoção de identidades de utilizador em aplicações SaaS populares. Pode criar automaticamente contas nos sistemas adequados para novas pessoas que entrarem na sua equipa ou organização. Quando as pessoas saírem de uma equipa ou organização, pode definir políticas que irão desativar automaticamente as respetivas contas nos sistemas adequados. Ao automatizar estas tarefas, poderá garantir que as identidades nas suas aplicações e sistemas estão atualizadas com base nas alterações no diretório ou no sistema de recursos humanos, reduzindo erros e poupando tempo.

[Saiba mais sobre como configurar o aprovisionamento e desaprovisionamento de aplicações SaaS >](#)



Gestão de grupo

O Azure AD ajuda-o a conceder acesso aos recursos da sua organização, ao fornecer os direitos de acesso a um único utilizador ou a um grupo completo do Azure AD. A utilização de grupos permite ao proprietário dos recursos definir permissões de acesso para todos os membros do grupo, em vez de ter de fornecer os direitos individualmente. Trata-se de um método mais seguro, uma vez que é menos provável que conceda acidentalmente um acesso individual inadequado e pode ajudá-lo a poupar tempo. Também pode dimensionar dinamicamente a gestão do seu grupo ao optar pela automatização das inscrições através de políticas de identidade baseadas em atributos.

[Saiba como criar um grupo no portal do Azure >](#)

Como gerir e proteger aplicações com o Azure AD



Gestão personalizada de utilizadores

Algumas tarefas não exigem um profissional de TI para a sua conclusão e o Azure AD permite-lhe delegar essas tarefas a outras pessoas na organização. Pode capacitá-los para criarem e gerirem os seus próprios grupos de segurança do Azure AD. Os proprietários dos grupos podem aprovar ou rejeitar pedidos de associação, ou podem delegar o controlo da adesão a grupos.

[Configurar grupos de gestão personalizada >](#)

A gestão personalizada também abrange os utilizadores. Os utilizadores podem registar-se para obter uma conta através do portal de gestão personalizada, se tiverem um e-mail verificado, e podem utilizar o portal para repor a palavra-passe. Isto pode ajudar o seu administrador de assistência técnica a poupar muito tempo e dinheiro.

[Configurar a reposição personalizada da palavra-passe >](#)



Modernizar a autenticação

Se atualmente utiliza a autenticação no local como os Serviços de Federação do Active Directory (AD FS), pode considerar migrar as suas aplicações para o Azure AD. Manterá os mesmos benefícios de utilizador, como o SSO, mas obterá também benefícios de escalabilidade e segurança disponíveis na nuvem, como aplicar controlos de acesso granulares por aplicação com o Acesso Condicional do Azure AD ou conceder a parceiros o acesso a recursos com a colaboração B2B do Azure AD. Todas as aplicações que utilizem as normas do SAML 2.0, WS-Federation, OAuth ou OpenID Connect para o início de sessão federado podem ser migradas.

[Criar políticas de Acesso Condicional do Azure AD para proteger o acesso às suas aplicações >](#)

[Utilizar a B2B do Azure AD para colaborar facilmente com os seus parceiros externos >](#)

Ligue com segurança qualquer aplicação,
em qualquer nuvem ou servidor, ao Azure AD.

1 milhão de aplicações
únicas e ativas ligadas.



Comece já.

[Comece uma versão de avaliação gratuita de um mês do Azure AD](#) para ver como é simples gerir o acesso de utilizadores a todas as suas aplicações e proteger a sua empresa.

