



Gerencie e proteja o acesso a todos os seus aplicativos com o **Azure Active Directory**



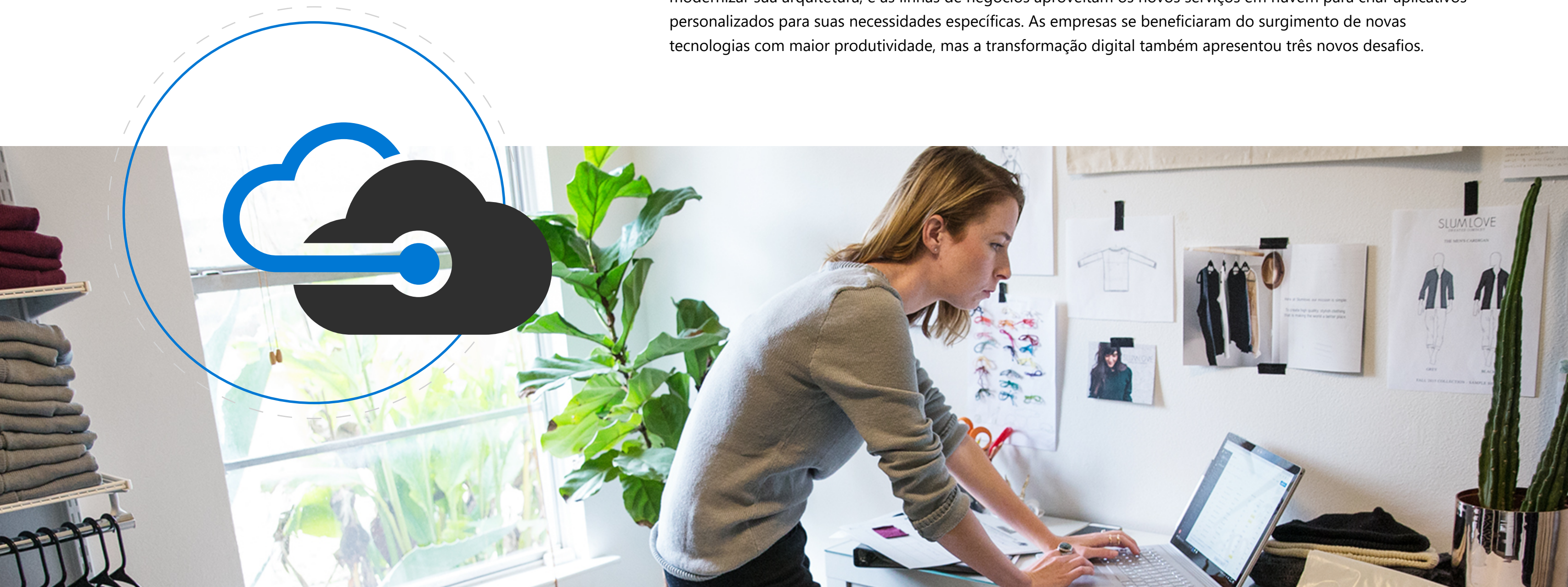
Seção 1

O que é gerenciamento
de identidade e acesso?

O que é gerenciamento de identidade e acesso?

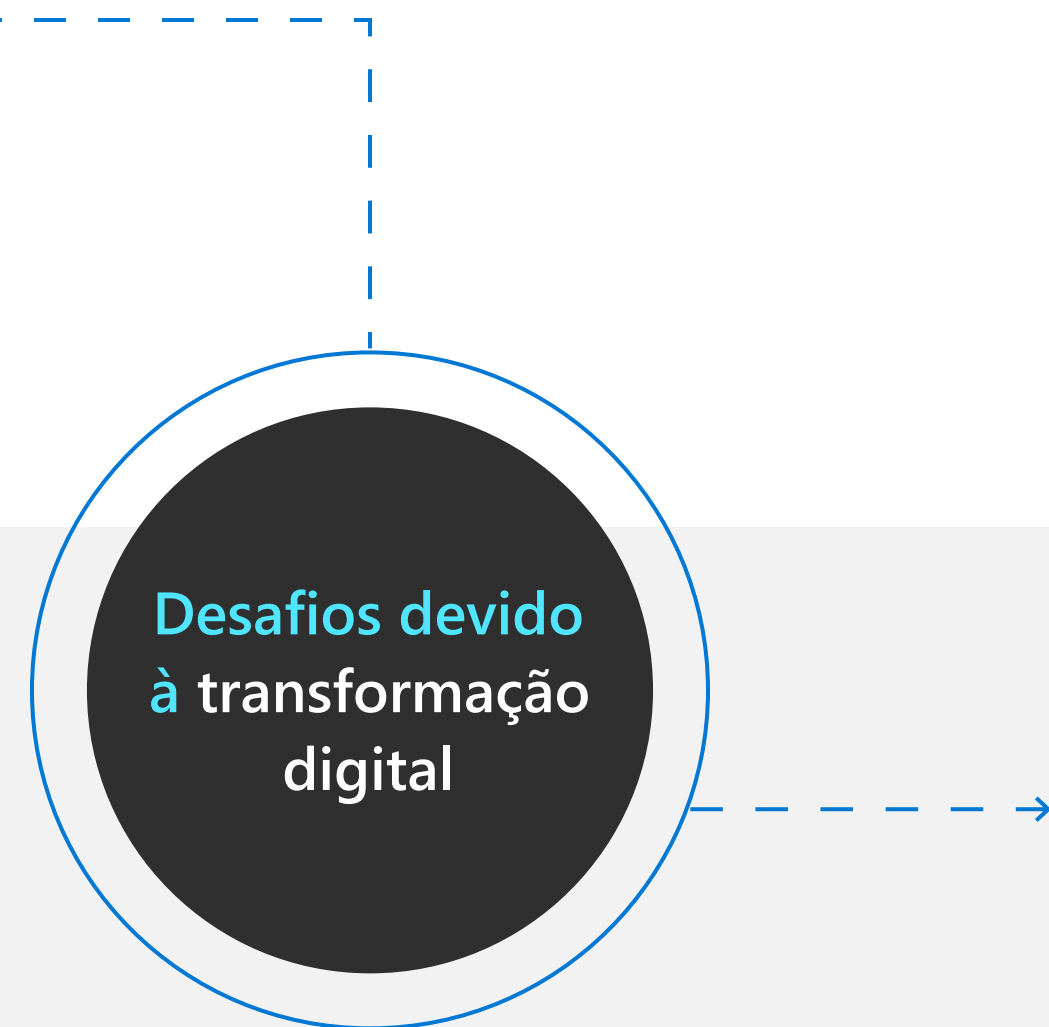
Transformação digital

A computação em nuvem e os dispositivos móveis transformaram o local de trabalho moderno. Uma força de trabalho cada vez mais global tem a flexibilidade de trabalhar em praticamente qualquer lugar, usando aplicativos SaaS (software como serviço) gratuitos e de baixo custo para solucionar os desafios de produtividade e colaboração. Grandes empresas estão migrando os aplicativos e a computação para a nuvem a fim de modernizar sua arquitetura, e as linhas de negócios aproveitam os novos serviços em nuvem para criar aplicativos personalizados para suas necessidades específicas. As empresas se beneficiaram do surgimento de novas tecnologias com maior produtividade, mas a transformação digital também apresentou três novos desafios.



O que é gerenciamento de identidade e acesso?

Novos desafios



Riscos de segurança: antes da revolução da nuvem, a TI atuava como guardiã de tecnologia. Os aplicativos e plataformas que você gerenciava e protegia estavam contidos no perímetro da rede, e todos os que acessavam seus recursos corporativos eram primeiro validados pelo firewall. Esses dias acabaram. A força de trabalho tem mais controle sobre a tecnologia usada, que é acessada, em grande parte, via Internet. Os invasores cibernéticos aprenderam a explorar essas vulnerabilidades. Mesmo quando um usuário sabe a senha correta da conta, você não pode ter sempre a certeza de que ele é quem diz ser.

Carga administrativa: a explosão de pontos de extremidade fornece aos usuários diversas maneiras de se conectar, mas isso também cria um pesadelo administrativo. Muitas empresas não estão cientes de todas as ferramentas que os funcionários usam e, mesmo quando possuem um bom inventário, o grande número de aplicativos em nuvem implica na necessidade de gerenciamento de vários sistemas de identidade, aumentando os custos e os riscos de segurança existentes.

Experiência de usuário ruim: os usuários também sofrem. Eles amam a flexibilidade, mas ficam frustrados com o número de credenciais de que precisam se lembrar.



Riscos de segurança



Carga administrativa



Experiência de usuário ruim

O que é gerenciamento de identidade e acesso?

Gerenciamento de acesso e identidade como plano de controle central

O denominador comum entre esses pontos problemáticos são os sistemas ineficientes para verificação da identidade. A identidade substituiu o perímetro da rede como o novo plano de controle. Você precisa de soluções que conectem as diferentes ferramentas, arquiteturas, dispositivos e serviços em toda a empresa para proteger melhor a organização e gerenciar o acesso de funcionários e parceiros externos, enquanto os sistemas de IAM (gerenciamento de identidade e acesso) concentram o acesso em um sistema, proporcionando mais controle. Eles fornecem uma colaboração perfeita entre os limites da sua organização e melhoram a segurança dos seus recursos corporativos. Uma boa solução de IAM permite conectar seus usuários a todos os aplicativos de trabalho, estejam eles na nuvem ou no local, por meio de um conjunto de credenciais. As soluções de IAM foram projetadas para fornecer aos usuários acesso apenas aos recursos necessários e impedir que usuários não autorizados acessem dados fora de seus limites. Você gerencia direitos e permissões de acesso de usuário em um portal centralizado, reduzindo grande parte dos processos manuais envolvidos no provisionamento e desprovisionamento de contas de usuários. As soluções de IAM também fornecem ferramentas para gerenciar políticas de segurança em suas identidades e aplicativos. As melhores soluções de IAM proporcionam mais proteção para as identidades, aprimoram a experiência do usuário e aumentam a eficiência administrativa.

As soluções de IAM **resolvem** estes desafios



Melhorar a proteção de identidades



Aprimorar a experiência do usuário



Aumentar a eficiência administrativa

Seção 2

Visão geral do Azure AD

Visão geral do Azure AD

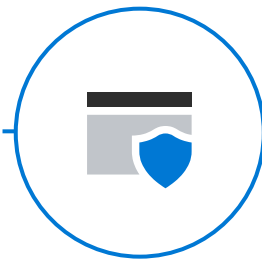
Uma solução abrangente

O Microsoft Azure AD (Azure Active Directory) é uma solução abrangente de IAM na nuvem e líder do mercado para gerenciar diretórios, acesso a aplicativos e proteção avançada de identidade. O Azure AD capacita as organizações a gerenciar e proteger identidades de funcionários, parceiros e clientes ao acessarem os aplicativos e serviços necessários. O Azure AD ajuda milhões de organizações a gerenciar e proteger mais de um bilhão de identidades.



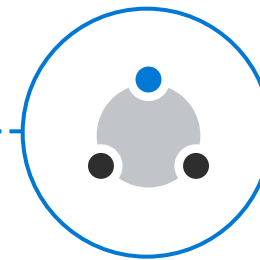
Modernizar o acesso

Gerencie e proteja o acesso aos dados e recursos da sua organização no local e na nuvem. Conecte todos os usuários, aplicativos e dispositivos à nuvem para acesso contínuo e seguro e maior visibilidade e controle. Automatize os fluxos de trabalho e habilite as opções de autoatendimento para ajudar a manter os custos baixos e a melhorar a produtividade dos usuários.



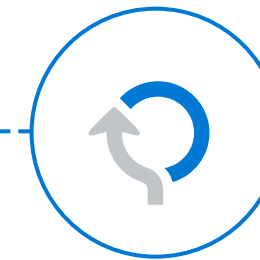
Proteger e governar

Com o alto volume de ataques a credenciais de usuário todos os dias, a maneira de evitar comprometimentos é rastrear continuamente o comportamento normal e anormal no conjunto mais amplo de sinais possível, aplicar inteligência artificial e automatizar as respostas. Equilibre a produtividade e a segurança com acesso oportuno aos recursos corretos, revisões regulares de acesso e aplicação de políticas.



Conectar e colaborar

Expanda seus negócios com um serviço de nuvem confiável que pode ser dimensionado para milhões de usuários com segurança e flexibilidade líderes no setor. Conecte-se com seus usuários externos e capacite-os a serem produtivos com experiências de autoatendimento fáceis de usar e controles de segurança integrados.



Desenvolver e integrar

Crie aplicativos que ofereçam aos usuários uma maneira fácil de entrar em suas contas pessoais, corporativas ou de estudante da Microsoft ou com suas contas sociais. Comece se conectando ao Microsoft Graph, o gateway para dados e inteligência no Microsoft 365, e crie aplicativos avançados. Ative o logon único, automatize o provisionamento de usuários e alcance as maiores organizações do mundo.

Seção 3

Azure AD para
aplicativos

Azure AD para aplicativos

Uma plataforma universal

Com o Azure AD, você pode gerenciar uma identidade comum para cada usuário de sua infraestrutura híbrida a fim de acessar todos os aplicativos de que eles precisam, incluindo aplicativos de linha de negócios no local e na nuvem. Gerencie todas as suas identidades a partir de uma plataforma universal, aumentando a eficiência administrativa e possibilitando mais controle. Aplique políticas de segurança granulares a cada um dos aplicativos usados em sua organização.



Economize tempo e dinheiro

O Azure AD está pré-integrado a milhares de aplicativos, incluindo opções populares como Workday, ServiceNow, SuccessFactors, Adobe e Concur, facilitando a disponibilização desses aplicativos para seus usuários. Com um console, implante políticas consistentes e monitore os direitos de acesso. Você pode automatizar fluxos de trabalho para provisionamento de usuários e gerenciamento do ciclo de vida, além de economizar tempo e recursos com o gerenciamento de contas de autoatendimento. Também é possível receber informações do usuário das ferramentas de RH como uma fonte de verdade, eliminando a necessidade de scripts personalizados ou processos manuais para gerenciar os atributos do usuário.

Os aplicativos configurados pelo Azure AD habilitam o SSO (logon único) para acesso contínuo, o que significa que os usuários não precisam se lembrar de credenciais para cada conta de aplicativo nem reutilizar senhas fracas, que envolvem o risco de uma violação de dados. As contas configuradas para provisionamento automático fornecem aos usuários o acesso a novos recursos o mais rápido possível. Para provisionamento de entrada, o Azure AD garante que as novas contratações tenham acesso a todos os recursos relevantes desde o primeiro dia.



**Economia de
tempo e dinheiro**



**Integrações
internas a SaaS**



Logon único



**Acesso de usuários
no primeiro dia**

Azure AD para aplicativos

Forneça acesso mais seguro a todos os seus aplicativos

O Azure AD oferece proteção abrangente de identidade em todos os seus aplicativos: aplicativos SaaS e aplicativos de linha de negócios no local. Esteja o usuário solicitando acesso ao Microsoft Word ou ao Box, o Azure AD garante a confirmação da identidade antes de conceder acesso. Você também pode instituir políticas de governança de acesso para garantir que os usuários tenham acesso apenas ao que precisam, quando precisarem. Você pode exigir que os usuários solicitem permissão de acesso, definir um prazo no qual eles podem acessar o aplicativo e realizar revisões regulares da conformidade do acesso.

O Azure AD também aproveita a capacidade do Gráfico de Segurança Inteligente da Microsoft e do aprendizado de máquina para analisar trilhões de sinais em todos os nossos produtos e serviços a fim de descobrir comportamentos atípicos e atribuir riscos relativos a cada sessão. O Azure AD examina o dispositivo, o local e outras informações contextuais para avaliar o risco de entrada. Você pode estabelecer políticas de Acesso Condicional do Azure AD que aplicam medidas de segurança automaticamente, como bloquear uma solicitação de acesso ou exigir uma redefinição de senha quando uma entrada for considerada arriscada ou as condições específicas da política forem atendidas.



**Medidas de segurança
do aplicativo**



**Proteção de
identidade**



**Governança de
acesso**



**Políticas de acesso
condicional**

Seção 4

Como gerenciar e proteger aplicativos com o Azure AD

O Azure AD simplifica o controle e reduz os custos usando automação, autoatendimento e imposição de políticas.

Como gerenciar e proteger aplicativos com o Azure AD



Integração de aplicativos do Azure AD

A galeria de aplicativos do Azure AD facilita a configuração e a conexão de qualquer um dos milhares de aplicativos pré-integrados ao seu locatário. Todos esses aplicativos oferecem suporte a uma experiência de SSO, e é simples configurar os aplicativos para o Acesso Condicional do Azure AD com base no aplicativo ou nas políticas corporativas. Depois que você adicionar e configurar o aplicativo às suas necessidades, os usuários com acesso autorizado poderão encontrá-lo facilmente no portal Meus Aplicativos do Azure AD, um portal centralizado para descoberta e inicialização de aplicativos do usuário final.

Se você criou um aplicativo ou precisa integrar um na sua organização, também pode solicitar que ele seja listado na galeria de aplicativos do Azure AD.

[Explore os milhares de aplicativos pré-integrados >](#)



Acesso híbrido seguro

Use o Proxy de Aplicativo do Azure AD para fornecer acesso remoto seguro ao aplicativo Web local com base em declarações sem a necessidade de VPN. O Proxy de Aplicativo requer uma instalação leve do conector e concede a mesma experiência de TI e de usuário final dos aplicativos SaaS conectados por meio da galeria de aplicativos do Azure AD.

Ou, se você quiser, também é possível aproveitar os investimentos em infraestrutura existentes, como parceiros no F5 ZScaler, SAP, Oracle ou Ping Identity, para conectar outros tipos de aplicativos, como os que usam protocolos de autenticação baseados em cabeçalho ou Kerberos, e ainda obter os benefícios de centralização e segurança do Azure AD.

[Leia como adicionar um aplicativo local por meio do Proxy de Aplicativo >](#)

[Conecte outras nuvens e redes de aplicativos parceiros >](#)

Como gerenciar e proteger aplicativos com o Azure AD



Provisionamento automatizado

O Azure AD permite automatizar a criação, manutenção e remoção de identidades de usuário em aplicativos SaaS populares. Você pode criar automaticamente novas contas nos sistemas certos para novas pessoas que ingressarem na sua equipe ou organização. Quando as pessoas saírem de uma equipe ou da organização, você pode definir políticas que desativarão automaticamente as contas delas nos sistemas certos. Ao automatizar essas tarefas, você pode garantir que as identidades nos aplicativos e sistemas serão mantidas atualizadas com base nas alterações no diretório ou no sistema de recursos humanos, reduzindo erros e tempo.

[Saiba mais sobre a configuração de fornecimento e desprovisionamento automatizados para aplicativos SaaS >](#)



Gerenciamento de grupos

O Azure AD ajuda a conceder acesso aos recursos da sua organização, fornecendo direitos de acesso a um único usuário ou a um grupo inteiro do Azure AD. O uso de grupos permite que o proprietário do recurso defina permissões de acesso para todos os membros do grupo, em vez de precisar fornecer os direitos um por um. Esse é um método mais seguro, pois é menos provável que você forneça acidentalmente um acesso inadequado a um indivíduo, além de economizar tempo. Você também pode escalar dinamicamente o gerenciamento de grupos, automatizando a inscrição por meio de políticas baseadas em atributos de identidade.

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

Como gerenciar e proteger aplicativos com o Azure AD



Autoatendimento de usuário

Algumas tarefas não exigem um profissional de TI para sua conclusão, e o Azure AD permite delegá-las a outras pessoas na organização. Você pode capacitar os usuários para criar e gerenciar seus próprios grupos de segurança no Azure AD. Os proprietários do grupo podem aprovar ou negar solicitações de associação ou podem delegar o controle da associação ao grupo.

[Configurar grupos autogerenciados >](#)

O autoatendimento também se estende aos usuários. Os usuários poderão se registrar para criar uma conta por meio do portal de autoatendimento se tiverem um email verificado e poderão usar o portal para redefinir a senha. Isso pode economizar tempo e dinheiro no suporte técnico.

[Configure a redefinição de senha de autoatendimento >](#)



Autenticação moderna

Se você usa uma autenticação local atualmente, como AD FS (Serviços de Federação do Active Directory), considere migrar seus aplicativos para o Azure AD. Você mantém os mesmos benefícios de usuário, como o SSO, mas obtém benefícios de escalabilidade e segurança disponíveis na nuvem, como a aplicação de controles de acesso granulares por aplicativo usando o Acesso Condicional do Azure AD ou concedendo aos parceiros acesso a recursos com a colaboração B2B do Azure AD. Aplicativos que usam os padrões SAML 2.0, WS-Federation, OAuth ou OpenID Connect para logon federado podem ser migrados.

[Crie políticas de Acesso Condicional do Azure AD para proteger o acesso aos seus aplicativos >](#)

[Use o Azure AD B2B para colaborar de forma fácil com seus parceiros externos >](#)

Conecte qualquer aplicativo ao Azure AD com segurança, em qualquer nuvem ou servidor.

1 milhão de aplicativos ativos e exclusivos conectados.



Comece hoje mesmo.

[Inicie uma avaliação gratuita de um mês do Azure AD](#) para ver como é simples gerenciar o acesso dos usuários a todos os seus aplicativos e proteger sua empresa.

