

Acesso sem senhas: uma realidade descomplicada e segura para sua empresa

Problemas com senhas são reais.



Os administradores de TI relatam que os usuários têm, em média, **63 senhas** para acessar tarefas cotidianas.¹



Quase três quartos (73%) dos administradores de TI dizem que a organização exige uma redefinição de senha a cada três meses ou mais, e **92% exigem uma redefinição pelo menos a cada seis meses.**



Como resultado dessa alta rotatividade de credenciais, quase um terço (31%) dos tickets de suporte técnico são relacionados a senhas.

A exposição da sua empresa não é mais hipotética. A questão é quando essa exposição ocorrerá.



35% Pouco mais de um terço (35%) dos administradores de TI passaram por um vazamento de dados empresariais nos últimos 2 anos.

Pare de sofrer para encontrar o equilíbrio certo entre segurança e simplicidade quando você pode ter o melhor dos dois mundos, permitindo que os colaboradores acessem o cofre digital sem senha.



Sua empresa já tem...

todos os componentes certos. Os gerenciadores de senhas e a autenticação multifator (MFA) são a base para um futuro sem senha.

64% dos administradores de TI indicam que suas empresas usam um gerenciador de senhas, com a mesma porcentagem usando logon único (SSO). **O uso de MFA é ainda maior: 67%.**

A estratégia certa em mente. Os administradores de TI são visionários e pioneiros.

57% Para mais da metade dos administradores de TI (57%), a tecnologia sem senha está no plano de suas empresas.



POR QUE DAR ADEUS ÀS SENHAS?



A remoção de barreiras relacionadas a senhas permite que os colaboradores acessem rapidamente os aplicativos e credenciais que eles mais precisam.



O acesso descomplicado incentiva o uso e aumenta a adesão dos colaboradores, melhorando os hábitos gerais relacionados a senhas.



Defina requisitos de senha mestre ainda mais seguros, pois os usuários não precisarão dela para obter acesso ao cofre.

Como o acesso sem senha funciona?

Os usuários podem acessar o cofre do LastPass no desktop **sem usar senhas** com um dos três mecanismos de autenticação segura: o LastPass Authenticator, biometria compatível com o padrão FIDO2 ou chaves físicas compatíveis com o padrão FIDO2.

O acesso sem senha ainda inclui senhas — por enquanto. As senhas mestre serão usadas para cadastrar uma conta do LastPass e outras alterações de conta relacionadas à segurança.

É hora de imaginar um mundo sem senhas

Em geral, os administradores de TI se sentiriam mais tranquilos e seguros se pudessem adotar a tecnologia sem senha.

44%

se sentiriam mais tranquilos

33%

se sentiriam mais seguros

32%

se sentiriam menos estressados

Não comprometa a segurança em prol da simplicidade quando você pode ter o melhor dos dois mundos.

Sua empresa fica mais protegida contra riscos cibernéticos quando os colaboradores usam métodos de autenticação seguros para acessar o cofre em vez de senhas fracas ou reutilizadas.

Dê adeus às senhas com o LastPass

Fontes: 1. A pesquisa foi realizada pela Lab42 e entrevistou participantes dos Estados Unidos, Austrália, Canadá, França, Alemanha e Reino Unido.