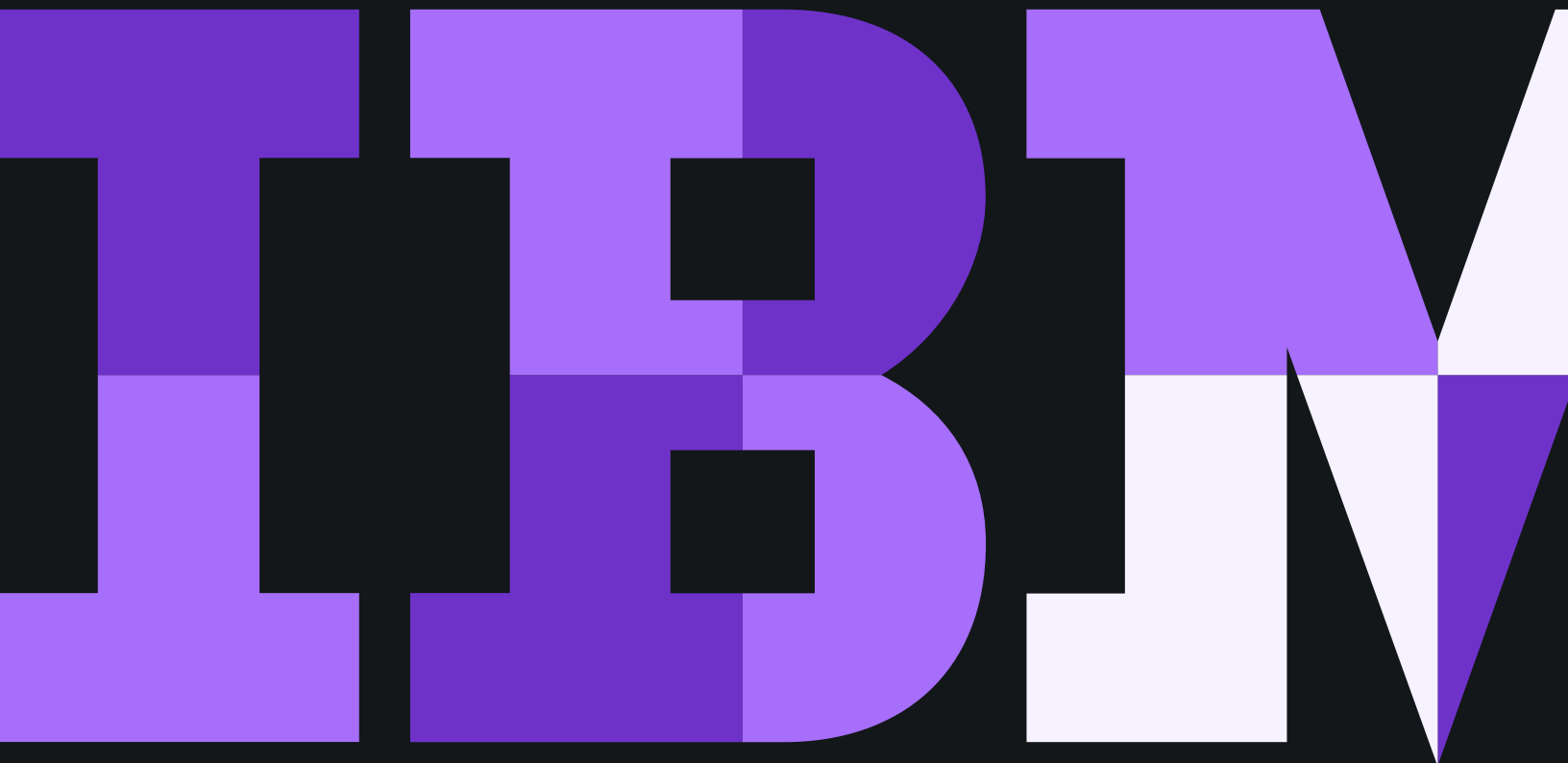


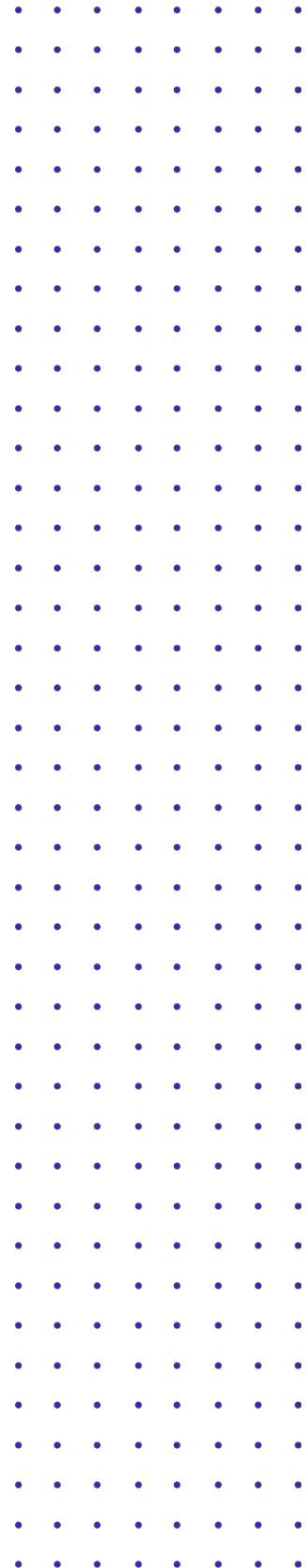
# Crie confiança digital com melhores experiências

Tenha acesso a novas oportunidades de receita por meio de uma confiança digital segura e integrada



## Sumário

- 3 Cultive a confiança em um mundo digital
- 3 Tenha acesso ao contexto para estabelecer confiança
- 4 Alinhe a segurança corporativa à confiança
- 5 Mantenha sua empresa segura
- 6 Impulsione a transformação digital estabelecendo uma base de confiança
- 7 A segurança pode abrir novas oportunidades



## Cultive a confiança em um mundo digital

Como seres humanos, confiamos em nossos sentidos, memória e inteligência para estabelecer confiança. Mas o que acontece quando essas ferramentas são removidas? No mundo digital, é necessário um conjunto complexo de ferramentas de informações, identificação e segurança para estabelecer confiança.

A confiança digital é o alinhamento de controles e privilégios de privacidade que ocorre quando o usuário certo tem o acesso certo aos dados certos pelo motivo certo e pelo objetivo certo. Os benefícios da confiança digital vão além da segurança. Quando implementada de maneira cuidadosa, integrada e pensando na experiência do usuário, a confiança digital pode proporcionar um melhor engajamento que leva ao aumento da produtividade e a mais oportunidades de crescimento de receita.



## Tenha acesso ao contexto para estabelecer confiança

Os clientes exigem que você proteja as informações pessoais deles. Além disso, como profissional de segurança, você foi encarregado de proteger seus negócios. Existem requisitos de privacidade e compliance a serem considerados, mudanças nos negócios a administrar e, no meio de tudo isso, ataques virtuais cada vez mais sofisticados provenientes de uma comunidade global de fraudadores. Mesmo assim, os usuários esperam mecanismos de segurança simples e integrados.

No passado, sua empresa poderia ter procurado principalmente as soluções de gerenciamento de identidade e acesso (IAM) para criar confiança. **Mas a confiança digital é mais do que estabelecer a identidade. É uma combinação de análise e entendimento que coloca as informações contextuais acima da identidade,** considerando:

- O usuário e os atributos exclusivos dele
- O dispositivo e a autenticação específica do endpoint, como biometria
- A atividade relacionada aos dados, ao aplicativo e ao usuário
- O ambiente do usuário e o ambiente de rede
- O comportamento do usuário, conforme determinado pela análise de uso

## Alinhe a segurança corporativa à confiança


Como qualquer relação, as relações digitais são compostas por várias pequenas interações ao longo do tempo. Juntas, essas interações fornecem uma visão cumulativa sobre quem somos: nossos comportamentos, interesses, responsabilidades e papéis. No mundo digital, no entanto, as empresas precisam testar e validar continuamente essas relações à medida que as pessoas trocam de dispositivos, redes, aplicativos e canais. Isso pode criar atritos quando os usuários devem inserir senhas várias vezes, precisam passar por outras etapas de autenticação e, às vezes, têm o acesso legítimo negado aos aplicativos.

### O objetivo da confiança digital deve ser criar uma experiência segura e sem atritos para os usuários.

Para conseguir isso, as organizações precisam combinar as tecnologias e os processos de segurança certos para automatizar os mecanismos de confiança, em vez de confiar nos controles manuais. Por exemplo, substituir uma senha para cada aplicativo pelo logon único ou usar análises avançadas para iniciar a autenticação por etapas são maneiras eficazes de ativar os controles de segurança sem desativar os usuários.

#### Obtenha segurança sigilosa com o IBM Security Identity & Access Management

Como empresa, você precisa garantir que as pessoas certas tenham o acesso certo aos dados no momento certo. Faça a coisa certa para os seus funcionários com o IBM Identity & Access Management.

[Assistir ao vídeo](#) 

A estrutura de confiança digital certa usa tecnologia avançada, como detecção de fraudes com infusão de IA, gerenciamento de acesso e identidade forte e contínuo, segurança de dados com um conjunto integrado de recursos e segurança móvel com gerenciamento unificado de vários dispositivos. Quando combinadas, essas tecnologias podem ajudar sua empresa:

- Amplie a segurança e a identidade facilmente entre sistemas locais e baseados na nuvem
- Faça a ponte entre antigas e novas tecnologias para criar uma base compartilhada de confiança
- Reduza os custos e simplifique os processos de segurança em toda a organização
- Forneça visibilidade multifuncional às equipes de segurança para que elas possam realmente trabalhar em equipe

As soluções e os serviços da IBM Security ajudam as empresas a criar uma plataforma de confiança digital de nível internacional. Oferecemos o IBM Security Guardium para proteger os dados e garantir o compliance, o IBM Security Identity & Access Management para gerenciar com eficiência as identidades e validar o comportamento do usuário e o IBM Security MaaS360 para gerenciar a segurança móvel na empresa e fora dela.

## Mantenha sua empresa segura

Você passou anos cultivando a confiança dos seus clientes e deseja manter essa confiança. O cumprimento dos requisitos de compliance e a prevenção de fraudes podem fazer mais do que proteger sua reputação, podem melhorar seus resultados. Você pode reforçar a segurança e simplificar os processos de login e autenticação, enquanto transita dentro dos limites de privacidade, consentimento e compliance. Aproveitando tecnologias avançadas, como inteligência artificial e análise comportamental, você pode usar mecanismos silenciosos para estabelecer a confiança digital.


Como as identidades mudam constantemente de locais, dispositivos e aplicativos, os controles de segurança precisam ser ágeis e invisíveis. Essa segurança invisível e ágil pode assumir várias formas:

- Controles de autenticação simples e multifatoriais de fácil implementação com suporte para experiências contínuas
- Sólidos mecanismos de autenticação por etapas que são ativados apenas para usuários em risco
- Telas de login único e launchpads de aplicativos unificados que simplificam o acesso entre dispositivos e entre aplicativos

A IBM Security pode proteger seus negócios, preservando excelentes experiências do usuário. Os serviços da IBM Security ajudam você a identificar, classificar e proteger dados críticos. IBM Security Guardium — monitora a atividade do usuário e alerta as equipes de segurança sobre um acesso não autorizado, enquanto protege seus dados por meio de controles de segurança, como criptografia, mascaramento e tokenização. IBM Security Identity & Access Management — serve de base para o compliance regulatório (FFIEC, 2FA, PSD2 etc.), gerencia centralmente as certificações de acesso, simplifica a integração e o desligamento de funcionários e prepara sua empresa para se adaptar aos novos requisitos regulatórios à medida que surgem. IBM Security Trusteer — oferece proteção avançada contra fraudes usando consórcios de IA e dados para rastrear tendências no cenário de fraudes em diferentes organizações, depois compartilha esses dados para proteger e configurar linhas de defesa.

### Obtenha proteção de dados mais inteligente com o IBM Security Guardium

A proteção inteligente de dados lê os insights, automatiza com uma finalidade e dimensiona à medida que você inova. Saiba como o IBM Security Guardium pode proteger seu mundo.

[Assistir ao vídeo](#) 

O IBM Security Guardium monitora a atividade do usuário e alerta as equipes de segurança sobre um acesso não autorizado



## Impulsione a transformação digital estabelecendo uma base de confiança


A transformação digital é motivada pela promessa de inovação, eficiência e experiências mais ricas. Implícita nessa promessa está a existência de segurança e confiança. **As empresas que oferecerem experiências digitais seguras e descomplicadas vencerão no mercado digital, seja na forma de maior produtividade dos funcionários ou maior lealdade dos clientes.** Da mesma forma, as empresas que não alinharem os mecanismos de segurança às expectativas dos usuários descobrirão que essa transformação será cada vez mais dolorosa.

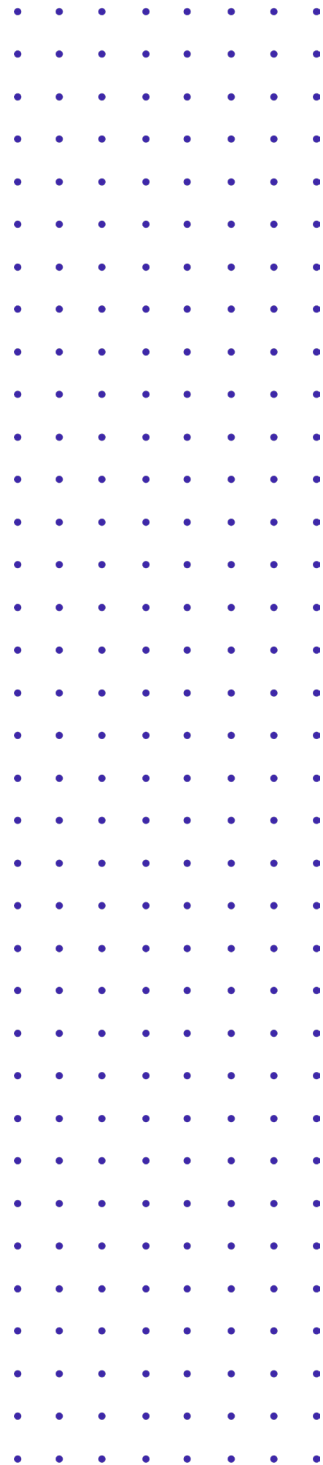
O que os usuários digitais esperam? Cibersegurança com simplicidade. Eles querem a proteção da autenticação multifator sem o trabalho manual de se autenticar várias vezes. Eles querem ferramentas de autoatendimento simples de usar, se perderem uma carteira ou simplesmente perderem uma senha. E eles querem que a identidade deles mude de dispositivos e aplicativos sem problemas.

A IBM Security pode ajudar a construir essa base digital de confiança. O IBM Security Identity & Access Management oferece logon único seguro para que os usuários possam fazer login uma vez nos aplicativos sem precisar reinserir a senha várias vezes. O IBM Security MaaS360 oferece aos usuários a liberdade de acessar aplicativos de qualquer lugar sem sacrificar a segurança. O IBM Security Trusteer protege contra fraudes, oferecendo integração e login integrados, que ativam inteligentemente a autenticação por etapas apenas quando fatores de risco estão presentes.

### Crie confiança de identidade digital com o IBM Security Trusteer

Com o IBM Security Trusteer, seus clientes podem levar as identidades e as relações confiáveis com eles na jornada digital com a sua empresa.

Assistir ao vídeo 



## A segurança pode abrir novas oportunidades

A abordagem correta da confiança digital vai além da segurança para ver a oportunidade que existe na oferta de melhores experiências do usuário. No passado, a segurança na forma de registros longos e várias solicitações de senha era vista pelos usuários como um obstáculo a melhores experiências. O que os usuários realmente querem são mecanismos de segurança que ocorram nos bastidores, seja uma identidade digital que os siga pelos dispositivos ou análises comportamentais discretas que examinam anomalias sutis, como a forma como um usuário está segurando o dispositivo.

Pense em como a confiança digital é estabelecida hoje. Em muitos casos, o ônus da prova é do usuário. **Eles inserem uma senha, digitam um código, respondem a um prompt etc. Mas imagine uma experiência diferente, em que as senhas são substituídas por autenticação silenciosa que acontece automaticamente como parte de uma estrutura mais ampla de confiança contextual**, uma que o usuário nunca toca e nunca vê. Em vez de apresentar os mesmos desafios de confiança para todos os usuários, apenas a pequena porcentagem de usuários que apresentam riscos seria contestada. Os dados ainda seriam protegidos,



O que os usuários realmente querem são mecanismos de segurança que acontecem nos bastidores

as contas protegidas e a confiança estabelecida, mas sem a experiência negativa de tratar cada usuário como uma ameaça em potencial.

As empresas que acertam na confiança digital têm o potencial de criar relações mais fortes, longas e lucrativas com os usuários.

As soluções de confiança digital da IBM Security ajudam a criar essas relações confiáveis e estendê-las perfeitamente entre dispositivos e aplicativos. A IBM Security oferece uma solução completa de confiança digital que combina detecção de dados, proteção de dados, gerenciamento de identidade e acesso, autenticação, gerenciamento de riscos, detecção de fraudes e inteligência global contra ameaças, apresentando:

**IBM Security Trusteer** — inteligência em nuvem, IA e aprendizado de máquina se combinam para ajudar a oferecer garantia de identidade digital contínua com autenticação contínua e poderosa detecção de fraude

**IBM Security MaaS360** — uma solução baseada em IA para gerenciamento unificado de endpoints, entregue na nuvem e projetada para proteger dados, dar suporte à privacidade e compliance e oferecer experiências móveis seguras e contínuas

**IBM Security Guardium** — uma plataforma de proteção completa que analisa os riscos de privacidade e conformidade, protege seus dados e monitora continuamente as vulnerabilidades

**IBM Security Identity & Access Management** — oferece segurança sigilosa com recursos de gerenciamento de acesso e identidade nos bastidores, que incluem logon único, autenticação multifator e controle de acesso



© Copyright IBM Corporation 2020

IBM Global Services  
Route 100  
Somers, NY 10589  
U.S.A.

Produzido nos Estados Unidos da América  
Janeiro de 2020  
Todos os direitos reservados

IBM, a logomarca da IBM e [ibm.com](http://ibm.com) são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos, outros países, ou ambos. Se estes e outros termos de marca comercial da IBM forem mostrados na primeira ocorrência dessas informações com um símbolo de marca comercial (® ou ™), esses símbolos indicarão marcas comerciais comuns ou registradas nos EUA pertencentes à IBM no momento da publicação destas informações. Essas marcas comerciais também podem ser marcas comerciais de lei comum ou registradas em outros países. Há uma lista atualizada de todas as marcas comerciais da IBM disponível na Internet em "Copyright and trademark information" em [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml) Outros nomes de empresas, produtos e serviços podem ser marcas comerciais ou marcas de serviço de terceiros.

Referências nesta publicação a produtos e serviços da IBM não implicam que a IBM pretenda disponibilizá-los em todos os países nos quais opera.



Por favor, recicle