

Acesso à rede Zero Trust

O Cloudflare Access verifica o contexto (como identidade e postura do dispositivo) para proteger o acesso em todo o seu ambiente, sem necessidade de VPN.

Acesso simples e seguro para o trabalho híbrido

Acesso à rede Zero Trust (ZTNA) rápido e confiável

O ambiente de trabalho distribuído atual exige uma abordagem distribuída para a segurança. O “perímetro” não existe mais e as soluções tradicionais de acesso remoto, como VPNs, não conseguem atender às expectativas modernas de segurança ou desempenho.

O ZTNA fornece acesso simples e seguro entre qualquer usuário e aplicativo, em qualquer dispositivo, em qualquer local, verificando continuamente o contexto granular, como identidade e postura do dispositivo, recurso por recurso. Com uma abordagem totalmente nova, não existe mais um “ato de equilíbrio” entre segurança e experiência do usuário. O ZTNA capacita sua empresa melhorando ambos.

Ele também torna as organizações mais ágeis e mais capazes de navegar pelas mudanças, sejam migração para a nuvem, atividades de fusões e aquisições ou inovação e expansão rápida. A Cloudflare é o centro de uma estratégia Zero Trust ou de modernização da segurança, fornecendo ZTNA em nossa nuvem de conectividade global e programável.

80%

Redução média do tempo gasto na resolução de tickets de suporte de acesso remoto relacionados ao uso de VPN¹

72%

Tempo contínuo economizado para configuração mensal de políticas em comparação com o fornecedor anterior¹

68%

Observaram um impacto significativo na simplificação das experiências de autenticação para funcionários e prestadores de serviços¹

Capacite sua empresa com acesso modernizado



Fortalecer a experiência do usuário

Melhore a produtividade da equipe com segurança modernizada que faz com que os aplicativos locais pareçam aplicativos SaaS. Chega de VPNs lentas e desajeitadas ou reclamações de funcionários.



Eliminar o movimento lateral

Reduza o risco cibernético e sua superfície de ataque concedendo acesso baseado em contexto com menos privilégios por recurso, em vez de acesso em nível de rede.



Escalar o Zero Trust sem esforço

Melhore a eficiência tecnológica protegendo aplicativos críticos ou grupos de usuários de alto risco e, em seguida, expanda o ZTNA nativo da internet para proteger toda a sua empresa.

Principais casos de uso do Access

Adotar Zero Trust e proteger o trabalho híbrido

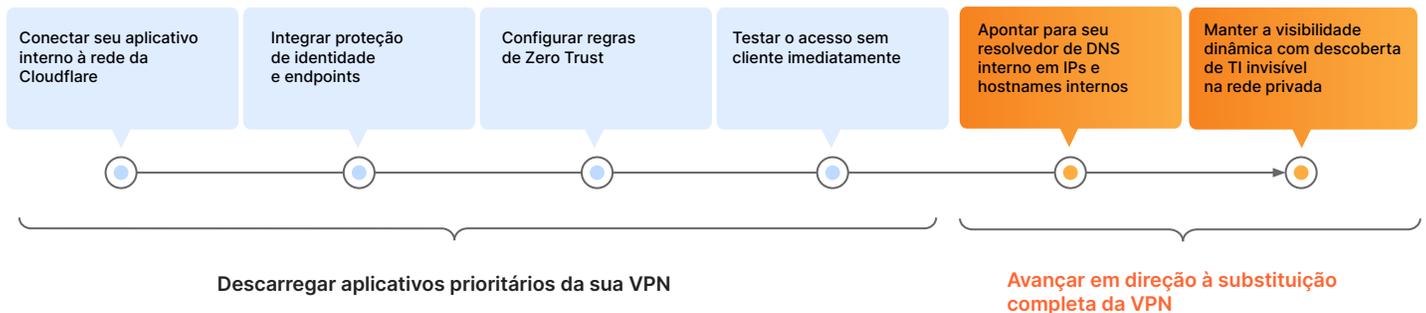
- ★ **Aumento e substituição de VPN** — O Access é mais rápido e seguro do que as VPNs tradicionais. Comece a descarregar aplicativos essenciais para melhorar a segurança e a experiência do usuário final.
- ★ **Acesso de prestadores de serviços** — Autentique usuários terceirizados, como prestadores de serviços, com opções sem cliente, IdPs sociais e muito mais.
- **Acesso de desenvolvedores** — Forneça acesso seguro aos usuários técnicos privilegiados para a infraestrutura crítica sem comprometer o desempenho.

Habilite a modernização digital

- **Acelere fusões e aquisições** — Evite uma fusão de rede tradicional completamente. Faça a integração com vários IdPs e forneça acesso interno por aplicativo durante fusões e aquisições.
- **MFA resistente a phishing** — Implemente autenticação forte, como chaves de segurança compatíveis com FIDO2, em qualquer lugar.
- **Proteger fluxos de trabalho de DevOps** — Proteja fluxos de trabalho entre serviços com conectividade mesh/peer-to-peer, compatível com tráfego bidirecional.

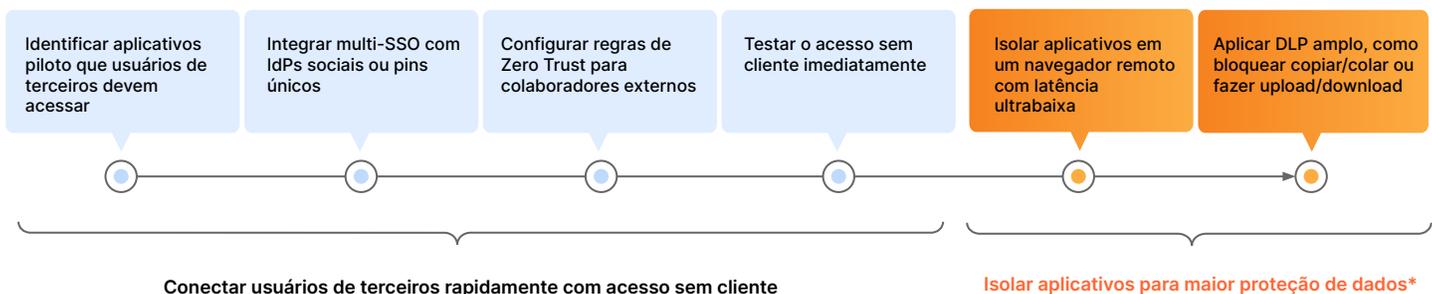
Inicie o aumento e a substituição da VPN

Priorize aplicativos críticos ou usuários de risco para um piloto de ZTNA para aumentar sua VPN. Use acesso sem cliente para aplicativos web ou SSH no navegador para agilizar os testes. Adote recursos avançados ao longo do tempo para avançar em direção à substituição completa da VPN e manter a visibilidade dinâmica à medida que sua rede muda.



Inicie o acesso de prestadores de serviços (terceiros)

Forneça experiências do usuário tranquilas e, ao mesmo tempo, mitigue os riscos de dispositivos não gerenciados. Configure opções simples de autenticação para prestadores de serviços, não é necessário software para o usuário final. Adote recursos avançados ao longo do tempo para aplicar maior proteção de dados.



*usando recursos em outras partes da plataforma Zero Trust

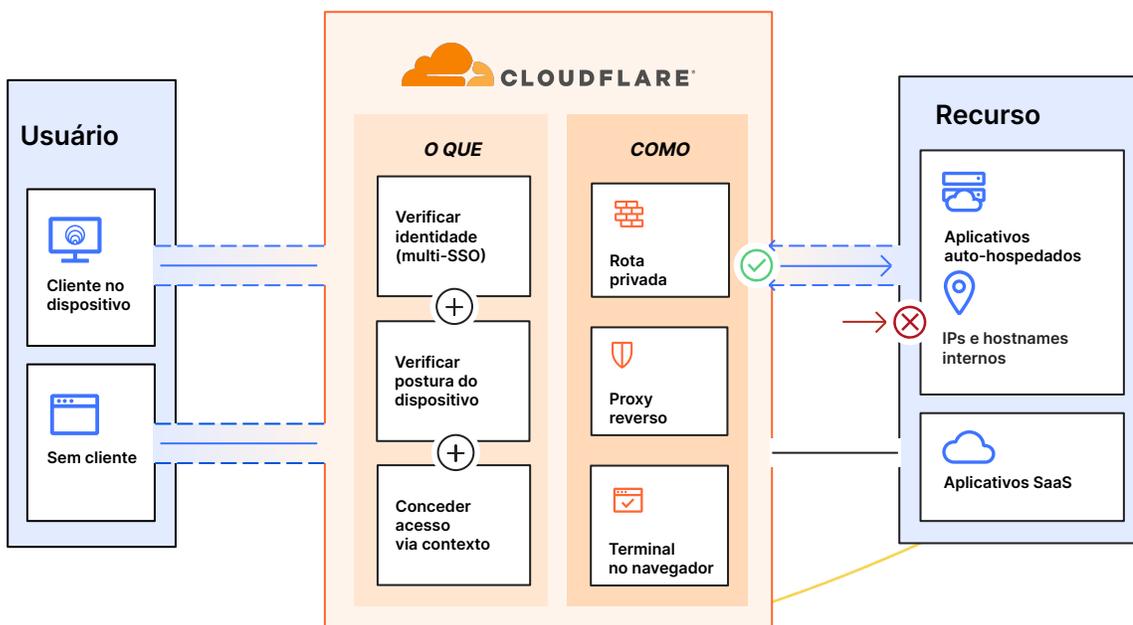
Como o Access funciona

O Cloudflare Access é uma camada de agregação flexível que verifica continuamente o contexto granular, como identidade e postura do dispositivo, para fornecer acesso simples e seguro a todos os recursos de uma organização individualmente, criando um perímetro definido por software. Quando um usuário se autentica e atende a todos os critérios da política de acesso, o Access emite um JSON Web Token assinado, válido por uma duração de sessão especificada. Realizamos a inspeção de passagem única em todas as solicitações de usuários por meio de nossa plataforma combinável, e nossa experiência centralizada de administração de políticas avalia as alterações de políticas globalmente em segundos devido à nossa arquitetura de rede Anycast exclusiva.

A operação unificada sem cliente e baseada em cliente lida com todos os tipos de dispositivos. Usamos um cliente de dispositivo para todos os serviços Zero Trust que criptografa o tráfego de nossa rede para manter a privacidade dos dados de nossos clientes. Também fornecemos acesso simples e seguro a dispositivos fora da empresa por meio de nossa configuração sem cliente. Nossos serviços ZTNA, DNS e os líderes de mercado WAF e proteção contra DDoS, trabalham juntos para criar e proteger hostnames públicos acessíveis a usuários de terceiros e a força de trabalho híbrida em qualquer dispositivo. Nossas opções de autenticação sem usuário (tokens ou certificados mTLS) também atendem a casos de uso de serviços automatizados e dispositivos de IoT.

Para controles Zero Trust, os recursos usam hostnames públicos para proxy reverso para aplicativos auto-hospedados (nuvem/no local) ou SSH/VNC no navegador, proxy de identidade para aplicativos SaaS ou roteamento privado baseado em cliente/túnel via camadas 4 e 7, encaminha proxy para qualquer recurso da web ou não (por exemplo, TCP/UDP arbitrário) dentro de uma sub-rede privada. Nosso software de rede global e conector de aplicativos oferece suporte a qualquer ambiente de computação (nuvem pública, incluindo Kubernetes e contêineres ou recursos legados de rede no local), sem exigir infraestrutura de VM e sem limitações de taxa de transferência, ao contrário de outros fornecedores de Zero Trust.

Ferramentas de identidade de terceiros, endpoints, vias de acesso à rede, registro/análise de dados e SIEM são integradas ao nosso painel junto com opções nativas para nosso cliente de dispositivo e análise de dados, permitindo que os administradores permaneçam ágeis e criem com as ferramentas que já usam.



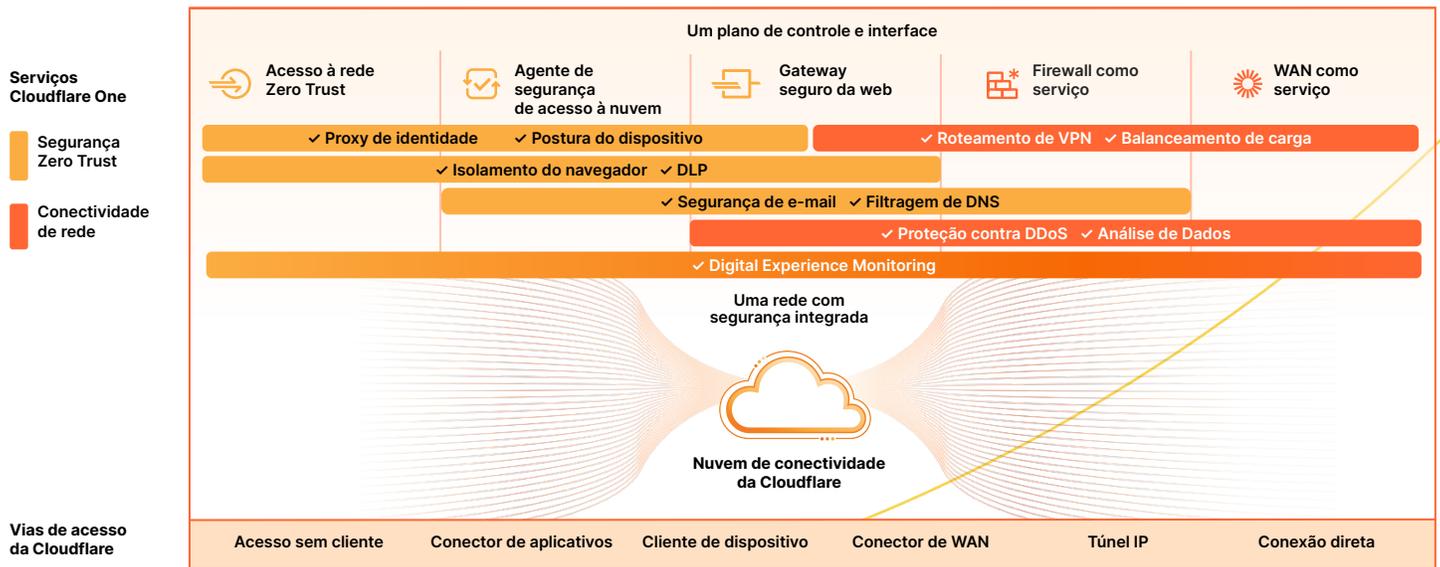
Access como parte da plataforma SSE e SASE da Cloudflare

Embora o SSE e o SASE geralmente envolvam uma jornada estratégica de vários anos, a Cloudflare frequentemente vê as organizações começando com ZTNA porque envolve etapas práticas e acessíveis para as equipes de TI, ao mesmo tempo que demonstra um valor comercial significativo no curto prazo. Os líderes de TI buscam proteger o trabalho híbrido, defender-se contra ameaças e proteger seus dados no caminho para a consolidação, e estão cada vez mais escolhendo a Cloudflare como seu parceiro de confiança.

A flexibilidade de implantação e a arquitetura combinável da Cloudflare permitem que qualquer organização proteja e acelere o desempenho de dispositivos, aplicativos e redes inteiras para manter o trabalho híbrido seguro e produtivo. Para isso, oferecemos suporte à integração sem agente para usuários finais, isolamento da web sem cliente para conter tráfego inseguro e um painel de gerenciamento unificado que permite visibilidade de todos os serviços de segurança e de rede, independentemente de onde os administradores ou usuários estão se conectando. A amplitude da rede global da Cloudflare permite que a segurança seja aplicada mais perto dos usuários finais, minimizando a latência e proporcionando uma experiência inteligente aos funcionários. Nossa arquitetura Anycast ajuda a contornar interrupções na internet, mantendo as equipes on-line e ajudando a garantir a continuidade dos negócios.

Com nossa plataforma unificada SSE e SASE, o contexto compartilhado entre nossas políticas ZTNA, CASB, DLP e SWG ajuda a reforçar a postura de segurança e ao mesmo tempo simplifica a implementação por meio de um fluxo de trabalho administrativo consistente. Os mesmos atributos de identidade e postura do dispositivo podem informar as políticas de acesso para ZTNA e CASB, bem como as políticas de SWG, simplificando o gerenciamento de políticas nas organizações.

ZTNA, isolamento do navegador remoto e segurança de e-mail também podem ser usados juntos para fornecer acesso condicional a recursos e, ao mesmo tempo, isolar os usuários de conteúdo malicioso (links, anexos) aos quais eles estão expostos através de e-mails e ferramentas de colaboração. Prestadores de serviços e usuários em dispositivos não gerenciados podem ter acesso limitado a recursos corporativos com interações de usuário (por exemplo, fazer upload/download, copiar/colar, entrada de teclado) desativadas para evitar comprometimento de dados, e outras políticas de DLP na camada de aplicação podem ser aplicadas para detectar dados confidenciais.



O que os clientes dizem



A Cloudflare foi eleita a Customers' Choice no [Gartner® Peer Insights™](#) Voice of the Customer: Zero Trust Network Access de 2024²

"O Cloudflare Access é uma alternativa incrível às VPNs tradicionais. Os usuários simplesmente abrem seus navegadores e entram, sem necessidade de baixar nem configurar softwares adicionais."

— **Platzi**, Head of Cloud Engineering

"O Cloudflare Access foi disponibilizado bem a tempo de evitar que tivéssemos que passar pelo trabalho de implantar uma VPN. Foi uma escolha fácil para nós e surpreendentemente simples de implantar."

— **ezCater**, Head of Security

"O Access é muito mais simples e seguro do que uma VPN para limitar o acesso a ativos internos. Apenas o ativamos e adicionamos os usuários. Simplesmente funciona."

— **Bitpanda**, CTO e Co-fundador

"Antes da implementação do Cloudflare Access, a preparação de um aplicativo para implantação segura era um projeto de duas a quatro semanas. Com o Cloudflare Zero Trust, economizamos 90% desse tempo."

— **Creditas**, Network Engineering Team Lead

O que os analistas dizem



A Cloudflare é indicada como Líder no IDC MarketScape for Zero Trust Network Access (ZTNA) de 2023

O IDC cita a "estratégia de produto agressiva para atender às necessidades de segurança corporativa" da Cloudflare. Acreditamos que nosso reconhecimento valida nossa abordagem para ajudar empresas de qualquer tamanho a começar com o Zero Trust e acesso seguro para qualquer usuário a qualquer recurso, sem VPNs.



A Cloudflare é indicada como Líder no KuppingerCole Leadership Compass for ZTNA de 2024

Por meio de sua análise de mercado ZTNA de 2024, a KuppingerCole Analysts AG citou vários pontos fortes da Cloudflare, como nossa plataforma de segurança desenvolvida organicamente, totalmente integrada, grande infraestrutura em nuvem e presença massiva global no mercado.

Recursos do Access

Criação/edição de políticas Zero Trust para acesso seguro	
Políticas de acesso granulares e personalizadas	Experiência centralizada em administração de políticas . Os aplicativos na camada de aplicação são protegidos em nível de subdomínio e caminho com suporte a caracteres curinga e vários hostnames e oferecem suporte a solicitações CORS . As mudanças nas políticas proliferam globalmente em segundos. Inclui testador de política .
Amplitude de recursos: o que podemos proteger e como	Os recursos usam hostnames públicos para proxy reverso para aplicativos auto-hospedados (nuvem/no local) ou SSH/VNC no navegador , proxy de identidade para aplicativos SaaS ou roteamento privado baseado em cliente/túnel via proxy de encaminhamento nas camadas 4 e 7* para qualquer recurso web/não web (TCP/UDP arbitrário) dentro de uma sub-rede privada . Também oferecem suporte a recursos/fluxos de trabalho com tráfego bidirecional (por exemplo, pipeline VoIP/SIP ou CI/CD).
Identidade	Autenticar por meio de todos os principais provedores de identidade empresarial e social (IdPs), incluindo vários IdPs simultaneamente. Também pode usar conectores SAML e OIDC genéricos. Suporta (e pode aplicar) qualquer método AuthN fornecido pelo IdP, AuthN temporário , justificativa de finalidade , intervalos de re-AuthN em base global ou por sessão de política/aplicativo e opção de revogação imediata de sessão por aplicativo ou por usuário. Pode usar o dispositivo cliente (WARP) como método AuthN (identidade armazenada em cache por sessão WARP).
Postura do dispositivo	Verifica a postura do dispositivo usando integrações de cliente de dispositivo e provedor de proteção de endpoints (EPP) de terceiros. Usa integrações entre serviços para incluir pontuações de risco de EPP em políticas de Zero Trust.
Sinais contextuais para políticas	Configura sinais como grupo de e-mail, intervalos de IP, geolocalização, método de login (por exemplo, tipo de MFA, tipo de IdP), certificado mTLS ou SSH válido, token de serviço, lista de números de série, atributos de postura do dispositivo, cliente do dispositivo instalado, duração da sessão, aplicação de regras SWG ou sinais de chamadas de APIs externas . Também pode fazer referência direta aos contextos de autenticação de acesso condicional do Microsoft Entra ID (Azure AD).
Outras compatibilidades relacionadas	<ul style="list-style-type: none"> • SCIM: provisiona/desprovisiona automaticamente usuários para aplicativos auto-hospedados e SaaS (exemplos para Okta e Azure AD) • DNS interno: configura o substituto do domínio local e resolve solicitações de rede privada • Túneis divididos: inclui/exclui IPs para redes privadas ou em execução junto com uma VPN • Autenticação mTLS: autenticação baseada em certificado para IoT e outros casos de uso de mTLS • Isolamento de aplicativos: com uma única caixa de seleção, isola aplicativos em nosso navegador remoto ultrarrápido*
Acessos de entrada e saída	
Conector de aplicativos	A orquestração simples de nosso conector de aplicativo leve (Cloudflare Tunnel) agiliza a conexão de recursos à Cloudflare, sem exigir infraestrutura de VM e sem limitações de rendimento. Inclui monitoramento , redes virtuais (para sobreposições de IP) e recursos de redundância e failover .
Cliente de dispositivo: quando usar	<ul style="list-style-type: none"> • Sem cliente: estende as políticas Zero Trust a usuários de terceiros em dispositivos não gerenciados, também combina bem com políticas de isolamento do navegador remoto sem cliente e DLP na camada de aplicação*. Oferece suporte a aplicativos web e SSH/VNC no navegador. • Baseado no cliente: nosso cliente de dispositivo (Cloudflare WARP) estende o acesso seguro a redes privadas, permite integrações de postura do dispositivo entre serviços e reconhece a localização para aplicar políticas personalizadas para usuários locais. Também pode conectar dois ou mais dispositivos executando o WARP para criar redes privadas. Os usuários podem se inscrever automaticamente ou implantar via MDM.
Extensibilidade e visibilidade	
Personalização de página	Faz upload de HTML personalizado para telas de bloqueio e inicializadores de aplicativos de acordo com sua marca ou transmite instruções de acesso específicas para agilizar a experiência do usuário final.
Registro	Registro abrangente para todas as solicitações, usuários e dispositivos. Pode usar logpush ou API para integração com ferramentas existentes de SIEM, orquestração e análise. Para ativos desconhecidos, nossa TI invisível na infraestrutura interna cataloga passivamente o tráfego exclusivo que surge em todas as origens.
Automação	APIs intuitivas e provedor Terraform disponíveis para gerenciar programaticamente todos os aspectos de uma implementação Zero Trust. Também oferece suporte a token de serviço sem usuário para serviços automatizados.

*usando recursos em outras partes da plataforma Zero Trust

Por que a Cloudflare?



Facilidade de configuração e gerenciamento

Simplifica radicalmente a configuração e a operação do tráfego de vias de acesso para recursos privados com software conector de aplicativos e orquestração de túneis.



Experiência perfeita e sempre ativada

Alcança desempenho máximo do usuário final e resiliência a interrupções de rede com a tecnologia Anycast global da Cloudflare, garantindo confiabilidade.



Inovação rápida para os primeiros usuários

Acompanhe a evolução da própria internet com um provedor que constantemente supera seus pares em inovação para tornar o acesso a aplicativos mais rápido e seguro.

Vamos conversar sobre acesso simples e seguro para sua organização

Solicite um workshop



Ainda não está pronto para uma conversa ao vivo?

Continue aprendendo mais sobre nossa [arquitetura de referência SASE](#), ou veja como ela funciona em um [tour interativo de nossa plataforma Zero Trust](#).



1. 2023 survey: techvalidate.com/product-research/cloudflare/charts
2. Gartner, Voice of the Customer for Zero Trust Network Access, 30 de janeiro de 2024, colaboradores parceiros. GARTNER, PEER INSIGHTS e o selo Gartner Peer Insights Customers' Choice são marcas registradas da Gartner, Inc. e/ou de suas afiliadas e são usados aqui com permissão. Todos os direitos reservados. O conteúdo do Gartner Peer Insights é constituído das opiniões de usuários finais individuais com base nas experiências deles com os fornecedores listados na plataforma. Ele não deve ser interpretado como declarações de fato e não representa as opiniões da Gartner ou de suas afiliadas. A Gartner não endossa nenhum fornecedor, produto ou serviço representado nesse conteúdo e não oferece garantias, expressas ou implícitas, com relação ao conteúdo e sobre a exatidão ou completude dele, incluindo garantias de comercialização ou adequação a um propósito específico.