CLOUDFLARE

2025

Relatório sobre sinais da Cloudflare

Resiliência em escala

PREFÁCIO DE MICHELLE ZATLYN

Estamos vivendo em tempos sem precedentes. A tecnologia está avançando em um ritmo vertiginoso.

Da ascensão explosiva da IA generativa, cheia de promessas e medo, às ameaças cibernéticas cada vez mais presentes e de um novo paradoxo de um mundo hiperconectado às implicações para as sociedades locais e uma economia global, a única constante parece ser mudança. As regras do jogo estão em constante mudança, e, se não ajustarmos continuamente nossa estratégia, ela rapidamente se tornará obsoleta.

É por isso que tenho orgulho de apresentar a edição inaugural do ***Relatório sobre sinais da Cloudflare***: um relatório anual que descreve as tendências e descobertas de segurança cibernética essenciais para desenvolver um plano estratégico sob medida para você.

A Cloudflare protege 20% dos sites do mundo e bloqueia uma média de mais de 227 bilhões de ameaças cibernéticas todos os dias. Isso nos dá um ponto de vantagem muito interessante. Vemos mais do que apenas dados, vemos padrões, comportamentos e pontos de inflexão que sinalizam para onde o mundo está indo.

O que sabemos ser verdade: as ameaças impulsionadas por IA exigem defesas com tecnologia de IA. O Zero Trust deve ser o padrão. A prontidão pós-quântica não é um problema de amanhã, precisa acontecer hoje. E tudo isso requer engajamento e endosso do alto escalão. **Resiliência não é opcional: é vital.**

O ***Relatório sobre sinais da Cloudflare*** foi projetado intencionalmente para fornecer informações sobre as forças que moldam o cenário de segurança para ajudar empresas de todos os tamanhos, governos e indivíduos em todo o mundo a tomar decisões informadas otimizadas para resiliência.

Estamos em uma missão para ajudar a construir uma internet melhor, e isso começa ajudando você a ter sucesso.

Michelle Zatlyn
Cofundadora e presidente
da Cloudflare

SUMÁRIO EXECUTIVO

Em 2025, a resiliência em escala não é mais opcional, é um teste definitivo de liderança.

À medida que as ameaças digitais se tornam mais complexas e a volatilidade geopolítica se intensifica, todos os setores da empresa: finanças, operações, conformidade e reputação, enfrentam maior exposição. Ataques com tecnologia de IA, estruturas regulatórias em mudança e ecossistemas digitais em expansão exigem uma resposta coordenada do alto escalão.

O *Relatório sobre sinais da Cloudflare de 2025* destaca cinco linhas de falhas críticas nas quais a resiliência deve estar integrada, não ser acrescentada posteriormente. Juntas, elas revelam um novo mandato para as equipes executivas: incorporar a resiliência na essência de como a empresa opera, inova e cresce, em escala.

Líderes de negócios experientes veem uma mudança clara: a resiliência não é mais responsabilidade de uma única função, é uma prioridade estratégica compartilhada por todo o alto escalão. As grandes empresas vão além das defesas reativas rumo a ambientes tecnológicos proativos, orientados por inteligência e escaláveis, integrados em toda a empresa. Aquelas que abordam a resiliência como uma responsabilidade compartilhada do alto escalão e impulsionadora do crescimento, e não apenas uma salvaguarda, estarão melhor posicionados para liderar em um mundo cada vez mais volátil.

Este relatório destaca o compromisso da Cloudflare em criar um ecossistema digital seguro, de alto desempenho e resiliente, em escala, permitindo que empresas de todos os tamanhos resistam a interrupções e operem com confiança em escala global.

Cinco linhas de falha críticas

nas quais a resiliência deve ser integrada, não acrescentada.

1

Ameaças com tecnologia de IA e riscos internos

exigem **colaboração estreita do CTO**, já que os adversários agora usam a IA para automatizar e escalar ataques mais rapidamente do que as defesas tradicionais podem responder. Ameaças impulsionadas por IA exigem defesas com tecnologia de IA, capazes de se adaptar em tempo real. A automação desses recursos não apenas aumenta a cobertura, mas permite que as organizações escalem suas defesas sem diminuir o ritmo dos negócios.

2

Zero Trust, proteção de identidade e complexidade da nuvem

exigem **liderança de CIOs**, à medida que as empresas migram de modelos baseados em perímetro para estruturas que priorizam a identidade. O Zero Trust se tornou o padrão de fato para o gerenciamento de riscos escalável e nativo de nuvem, garantindo usabilidade, visibilidade e controle em sistemas distribuídos.

3

A resiliência não é mais opcional

para **CFOs e CROs**. À medida que o risco de terceiros cresce e as estruturas regulatórias se expandem, os líderes financeiros e de risco devem garantir que os investimentos vão além da mitigação, impulsionando a continuidade operacional, a automação da conformidade e a governança escalável. A resiliência nesse nível deve ser proativa, incorporada e econômica, não um conjunto desconexo de soluções pontuais.

4

Privacidade de dados e prontidão pós-quântica

exigem envolvimento antecipado do CPO. **Com a computação quântica preparada para quebrar a criptografia tradicional**, dados preparados para o futuro exigem ação imediata. Os líderes devem acelerar a adoção da criptografia pós-quântica para proteger dados de longa duração e atender às expectativas regulatórias em evolução.

5

Risco geopolítico e operações cibernéticas visadas

exigem o **envolvimento direto do CEO e do conselho**. À medida que as campanhas patrocinadas por estados visam cada vez mais a liderança, as cadeias de fornecimento e as operações globais, a resiliência deve escalar para o topo da hierarquia, apoiada por inteligência em tempo real, prontidão executiva e coordenação transfronteiriça.

> “Ataques com tecnologia de IA, estruturas regulatórias em mudança e ecossistemas digitais em expansão exigem uma **resposta coordenada do alto escalão.**”

Conteúdo

1

Combate espelhado: defender a empresa na era da IA adversária

Combate espelhado: defender a empresa na era da IA adversária

As ameaças cibernéticas impulsionadas por IA estão evoluindo em um ritmo sem precedentes, tornando as abordagens de segurança tradicionais ineficazes. Os invasores agora usam a IA para automatizar ataques, evitar a detecção e explorar vulnerabilidades mais rapidamente do que as organizações podem responder. A mudança da defesa passiva para a segurança proativa e orientada por IA não é mais opcional, é essencial.

Ataques com tecnologia de IA já estão causando impacto real nas empresas. Setenta e quatro por cento dos profissionais de segurança de TI relatam que as ameaças impulsionadas pela IA estão afetando significativamente suas organizações.[1] Os golpes de deepfake, como videochamadas fraudulentas, resultaram em milhões em perdas, com um caso na Austrália levando a um roubo de US$ 25 milhões.[2] Os ataques de phishing gerados por IA estão se tornando mais convincentes, enquanto o malware aprimorado por IA se adapta para escapar das defesas tradicionais.

Além dos ataques diretos, a IA está alimentando campanhas de desinformação, envenenamento de dados e manipulação de modelos, possivelmente comprometendo os sistemas orientados por IA.

A produtividade aprimorada dos invasores sobrecarrega as equipes de segurança

Muitas ferramentas habilitadas por IA podem não desbloquear técnicas de ataque inovadoras, mas essas ferramentas podem ajudar os adversários a melhorar a produtividade, a eficiência e o volume de ataques. Essas ferramentas aceleram tarefas como a criação de e-mails de phishing e o uso de “dark chatbots” para ajudar na codificação de malware.

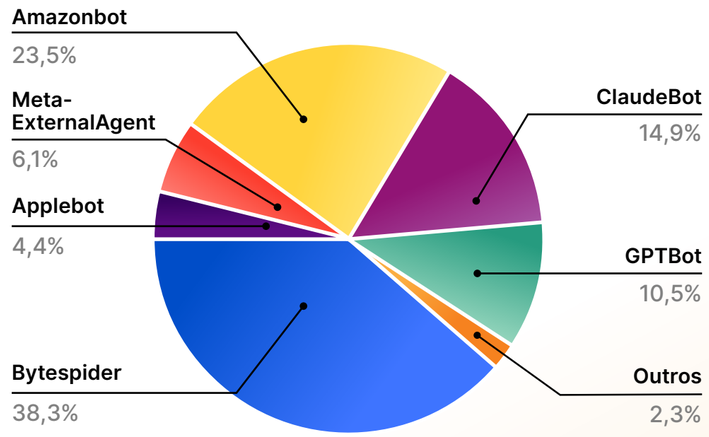
Isso significa que as organizações começarão a enfrentar volumes maiores de ataques que serão mais sofisticados, muitas vezes usando métodos de ataque modernos. Processos manuais de segurança, como triar e-mails de phishing e ajustar manualmente as detecções para impedir as ameaças mais recentes, certamente ficarão sobrecarregados à medida que o volume de ataques aumenta.

Raspagem de IA ameaçando criadores de conteúdo digital

Os modelos de IA precisam de dados para treinar, e muitas empresas de IA coletam essas informações por meio de raspagem automatizada da web. Na verdade, os crawlers de IA já representam 2% de todo o tráfego de bots que a Cloudflare processa em nossa rede.[3]

O conteúdo derivado de IA pode desviar o tráfego e as interações dos sites, prejudicando gravemente as organizações que dependem de conteúdo e publicidade on-line para obter receita. E a resistência está aumentando. Em fevereiro de 2025, a empresa de educação Chegg processou o Google por prejudicar seu tráfego com IA, e a indústria criativa do Reino Unido lançou a campanha “Make It Fair” contra o uso de conteúdo sem permissão.[4]

Principais crawlers de IA por participação no tráfego da camada de aplicação



Quase todo **(98%)** o tráfego de crawlers de IA observado pela Cloudflare em 2024 **teve origem em apenas seis empresas.**[5]

Para organizações que dependem fortemente da publicação de conteúdo digital ou publicidade digital, **os raspadores de IA são uma ameaça existencial.**

A fraude de identidade sintética que está causando disrupção em setores críticos

A IA está alimentando o aumento da fraude de identidade sintética (SIF), em que os criminosos criam identidades hiper-realistas combinando dados reais e falsos para contornar os sistemas de verificação tradicionais. Detalhes pessoais gerados por IA, deepfakes e preenchimento de credenciais tornam essas identidades mais difíceis de detectar, representando grandes riscos para setores fortemente visados, como serviços financeiros, de saúde e agências governamentais.

Ao contrário das fraude tradicional, a SIF muitas vezes passa despercebida por não ter vítimas imediatas, permitindo que os fraudadores criem histórico de crédito e executem golpes em grande escala.

A IA potencializa as ameaças internas

O trabalho remoto e a adoção da nuvem expandiram a superfície de ataque para ameaças internas, tornando-as mais difíceis de detectar. Mais da metade das organizações relatam ter enfrentado uma ameaça interna no ano passado, e 8% encontraram mais de vinte incidentes.[6]

A IA agora está ampliando esse desafio, fornecendo aos insiders ferramentas poderosas para evitar a detecção. Phishing habilitado por IA, golpes deepfake e ataques automatizados de engenharia social podem gerar mensagens convincentes e sensíveis ao contexto em segundos, tornando a fraude mais fácil e os ataques mais frequentes.[7]

Nem todas as ameaças internas são ataques intencionais. O DBIR de 2024 da Verizon constatou que 68% das violações de dados foram causadas por fatores humanos, como indivíduos sendo enganados por golpes de engenharia social ou cometendo erros.[8] O spear phishing assistido por IA explora esses erros, imitando colegas ou executivos reais com uma precisão quase perfeita para induzir os funcionários a compartilhar credenciais, aprovar transações ou expor dados confidenciais.

As organizações devem implantar análises comportamentais, monitoramento em tempo real e detecção de anomalias para identificar esses riscos antes que eles aumentem. A automação de segurança com tecnologia de IA agora é essencial para corresponder à velocidade e à escala das ameaças impulsionadas por IA.

Bots orientados por IA remodelam o cenário da segurança cibernética

Os bots orientados por IA estão aumentando a sofisticação dos ataques e a exposição ao risco. Em 2024, 28% de todo o tráfego de aplicativos observado pela Cloudflare veio de bots, um número que permaneceu estável em torno de 30% nos quatro anos anteriores. Embora os bots possam servir a propósitos legítimos, como automação de atendimento ao cliente e indexação de mecanismos de pesquisa, a grande maioria (93%) não é verificada e é potencialmente maliciosa.[9]

A mudança crítica são os bots com tecnologia de IA, que possibilitam ataques automatizados e em larga escala com eficiência sem precedentes. Os invasores agora usam bots para realizar preenchimento de credenciais, lançar ataques de negação de serviço distribuída (DDoS), raspar dados confidenciais e executar fraudes na velocidade da máquina. Os modelos de IA potencializam esses recursos gerando tentativas realistas de phishing, contornando os CAPTCHAs tradicionais e evitando a detecção com comportamento adaptativo.

A automação de segurança com tecnologia de IA agora é **essencial** para corresponder à velocidade e à escala das ameaças impulsionadas por IA.

28%

de todo o tráfego de aplicativos observado pela Cloudflare **veio de bots**

PERGUNTAS PARA O ALTO ESCALÃO

Criar uma capacidade defensiva orientada por IA

Para ficar à frente das ameaças com tecnologia de IA, as organizações precisam adotar uma abordagem proativa que previna e mitigue essas ameaças em tempo real. **Aqui estão algumas perguntas que os líderes de alto escalão podem fazer para avaliar a prontidão de sua organização.**

P1

Estamos usando a IA para impulsionar a observabilidade abrangente da segurança?

Estamos unificando logs, analytics, alertas e análise forense em uma única interface para identificar riscos e sua causa raiz?

P2

Estamos aproveitando a segurança orientada por IA para detectar e neutralizar ameaças em tempo real?

Temos detecção com tecnologia de IA para analisar vastos conjuntos de dados, identificar anomalias e automatizar respostas a ameaças emergentes?

P3

Até que ponto estamos protegidos contra phishing, deepfakes e malware com tecnologia de IA?

Estamos implantando detecção orientada por IA, autenticação resistente a phishing e controles de segurança adaptativos para combater os ataques em evolução?

P4

Estamos protegendo nossos dados proprietários contra raspadores de IA e ameaças automatizadas?

Temos gerenciamento de bots, autenticação de APIs e marcas d'água digitais implementados para evitar o roubo e a exploração de dados?

P5

Estamos aproveitando análises comportamentais orientadas por IA para detectar ameaças internas em tempo real?

Estamos analisando continuamente o comportamento do usuário, incluindo padrões de acesso, escalas de privilégios e tentativas de exfiltração de dados?

PERSPECTIVAS DE EXECUTIVOS

As novas proteções da segurança de dados da IA

Dane Knecht
CTO, Cloudflare

Proteger dados na era da IA: confiança, acesso e visibilidade

O problema mais urgente para as organizações hoje é o acesso aos dados, especificamente, como gerenciá-los e protegê-los em uma empresa cada vez mais preenchida por ferramentas de IA. À medida que a IA generativa é incorporada aos fluxos de trabalho, o desafio não é mais apenas reagir às ameaças, mas evitar o acesso arriscado ou não autorizado a dados confidenciais.

Isso levanta questões urgentes nos níveis de diretoria e de alto escalão. Como concedemos acesso seguro para as ferramentas aos dados corporativos? Como garantimos que um complemento de IA de aparência inócua não é um gateway para exfiltração de dados? As consequências para a empresa e a reputação são reais e estão aumentando.

O que não estamos detectando: IA oculta e pontos cegos na governança

Um grande ponto cego é a disseminação não controlada de ferramentas de IA por toda a empresa. Os funcionários estão adotando a IA muito antes da política formal, muitas vezes sem saber dos riscos. Essas implantações de "IA oculta" evitam as análises tradicionais, criando superfícies de ataque invisíveis e novos riscos de conformidade.

Poucas organizações mapeiam onde a IA é usada. Sem essa visibilidade, é quase impossível gerenciar a exposição de dados ou responder a incidentes de forma eficaz.

O que vem a seguir: controle proativo e escrutínio regulatório aprimorado

Nos próximos doze a dezoito meses, a segurança corporativa mudará da detecção de ameaças reativa para a governança proativa do acesso e uso da IA. O escrutínio regulatório vai se intensificar, exigindo transparência, supervisão operacional e fortes práticas de proteção de dados.

As organizações que avançarem rapidamente, formando equipes de governança multifuncionais, definindo políticas de uso de IA e implementando controles de acesso para ferramentas e usuários, reduzirão o risco e se posicionarão como líderes.

O futuro da resiliência não consiste apenas em detectar ameaças, mas em controlar como e onde a IA toca os seus dados.

"Os funcionários estão **adotando a IA muito antes da política formal**, muitas vezes sem saber dos riscos."

2

Além do perímetro: Zero Trust, identidade e a nova fronteira de segurança

Além do perímetro: Zero Trust, identidade e a nova fronteira de segurança

A mudança para ambientes multinuvem, plataformas SaaS e arquiteturas baseadas em API criou um cenário de segurança fragmentado, onde configurações incorretas, riscos de identidade e TI invisível expõem as empresas a ameaças cibernéticas crescentes. Nesse ambiente, a segurança Zero Trust substituiu os modelos desatualizados baseados em perímetros para se tornar a base para proteger aplicativos em nuvem, cargas de trabalho e dados com abordagens de verificação contínua e centradas na identidade.

Para acompanhar o ritmo, as organizações devem aplicar os princípios Zero Trust em plataformas em nuvem e SaaS.

O Zero Trust substitui as VPNs tradicionais

Agora, os agentes de ameaças visam ativamente os provedores de VPN com explorações de dia zero e tentativas de quebra de senha com força bruta para obter acesso à rede.[10] À medida que os perímetros de rede entram em colapso, as organizações estão mudando para uma segurança centrada na identidade, aplicando a verificação contínua, o acesso com menor privilégio e a autenticação contextual em todas as cargas de trabalho em nuvem e aplicativos SaaS.

O acesso à rede Zero Trust (ZTNA) agora é essencial, substituindo as VPNs legadas que deixam as empresas vulneráveis a ataques baseados em credenciais, movimento lateral e ameaças internas. Sem o Zero Trust, as empresas correm o risco de se expor ao acesso não autorizado, credenciais comprometidas e vulnerabilidades da cadeia de suprimentos.

APIs: o vetor de ataque emergente

Com 60% do tráfego da internet agora baseado em APIs, as APIs desprotegidas se tornaram um alvo principal para invasores.[11] Muitas organizações não conseguem rastrear e proteger APIs, deixando-as vulneráveis à exfiltração de dados, abuso de credenciais e ataques de injeção. A análise baseada em aprendizado de máquina da Cloudflare descobriu que as organizações subnotificam os endpoints de API em um fator de quatro, criando um ponto cego de segurança significativo.[12]

Para mitigar os riscos, as empresas devem adotar a descoberta automatizada de APIs, a aplicação de autenticação e a detecção de anomalias orientada por IA para evitar violações e vazamentos de dados.

A análise baseada em aprendizado de máquina da Cloudflare descobriu que **as organizações subnotificam os endpoints de API em um fator de quatro**

TI invisível e serviços em nuvem não gerenciados aumentam o risco

A rápida adoção de serviços em nuvem não sancionados torna cada vez mais difícil para as equipes de TI monitorar e proteger os ambientes em nuvem de forma eficaz. Os funcionários frequentemente usam ferramentas de colaboração não aprovadas, expondo dados confidenciais e contornando as políticas de segurança corporativa.

Agentes de segurança de acesso à nuvem (CASBs), ferramentas de descoberta com tecnologia de IA e aplicação automatizada de políticas agora são essenciais para obter visibilidade em tempo real, garantir a conformidade e evitar a exposição não autorizada de dados.

Segurança centrada em identidade: o fim das senhas

À medida que as ameaças cibernéticas se tornam mais sofisticadas, a identidade continua sendo o principal vetor de ataque. Vinte e cinco por cento dos contratos de resposta a incidentes da Cisco estão relacionados a usuários que aceitam notificações push de autenticação multifator (MFA) fraudulentas no primeiro trimestre de 2024.[13] Credenciais comprometidas também levaram a violações significativas, como a segmentação de pelo menos 160 clientes da Snowflake, incluindo o Grupo Santander, Ticketmaster e Advanced Auto Parts.[14]

Os cibercriminosos cada vez mais contornam a MFA, sequestram sessões ativas e roubam credenciais, expondo as empresas a violações generalizadas e controles de contas.

Desafios:

- **A reutilização de credenciais coloca as empresas em risco – Quarenta** e seis porcento de todas as tentativas de login humano envolvem credenciais comprometidas, um número que sobe para 60% para as organizações empresariais.[15] Os invasores automatizam o preenchimento de credenciais, obtendo acesso a sistemas corporativos com mínimo esforço.
- **Os ataques de credenciais automatizados estão escalando rapidamente – Noventa** e quatro por cento das tentativas de login usando credenciais vazadas vêm de bots, testando milhares de senhas roubadas por segundo.[16] Sem mitigação de bots e autenticação adaptativa em tempo real, as organizações permanecem altamente vulneráveis a violações em larga escala.
- **As senhas são insuficientes** – senhas estáticas e até mesmo métodos básicos de MFA são cada vez mais ineficazes contra as ameaças modernas, que incluem desvio de MFA, sequestro de sessão e roubo de credenciais em ambientes com proteção contra phishing. Para combater esses riscos, as organizações devem adotar autenticação sem senha, impor controles de acesso Zero Trust e implantar chaves de segurança compatíveis com FIDO2 para eliminar a dependência de credenciais estáticas.

46%
de todas as tentativas de login humano envolvem **credenciais comprometidas**

94%
das tentativas de login usando credenciais vazadas vêm de bots, testando **milhares de senhas roubadas por segundo**

PERGUNTAS PARA O ALTO ESCALÃO

Proteger a nuvem e repensar a autenticação

À medida que a adoção da nuvem é acelerada, as organizações precisam repensar a segurança e a autenticação para se protegerem contra ameaças em evolução. Uma abordagem Zero Trust, visibilidade orientada por IA e uma forte proteção de identidade são essenciais para proteger serviços em nuvem, aplicativos SaaS e APIs. **Determine o nível de proatividade de sua organização ao enfrentar esses desafios com perguntas como:**

P1

Estamos aplicando a segurança Zero Trust em nuvens, aplicativos SaaS e APIs?

Temos verificação contínua, acesso com privilégio mínimo e autenticação baseada em risco em todos os ambientes?

P2

Temos visibilidade total da TI invisível e dos serviços em nuvem não gerenciados?

Estamos usando ferramentas de descoberta orientadas por IA para detectar aplicativos não autorizados e aplicar políticas de segurança?

P3

Nossas APIs estão protegidas contra acesso não autorizado e violações de dados?

Estamos implementando descoberta automatizada de APIs, controles de autenticação e detecção de anomalias orientada por IA?

P4

Eliminamos as vulnerabilidades baseadas em senhas em nossa estratégia de autenticação?

Estamos adotando autenticação sem senha, MFA resistente a phishing e proteção de identidade adaptável?

P5

Estamos preparados para detectar e responder a ataques de credenciais automatizados?

Podemos implantar mitigação de bots orientada por IA, análise comportamental e revogação automatizada de credenciais para evitar o acesso não autorizado?

PERSPECTIVAS DE EXECUTIVOS

Zero Trust para um futuro resiliente

Corey Mahan
Vice President,
Product Management,
Cloudflare

No momento, o maior desafio que as organizações enfrentam é equilibrar segurança com usabilidade. O trabalho híbrido veio para ficar, a adoção da nuvem está acelerando e os usuários esperam acesso sem atrito, independentemente de onde estejam ou que dispositivo estejam usando. Mas as arquiteturas tradicionais não conseguem acompanhar. Estamos vendo muitas empresas que dependem de um conjunto desconexo de soluções pontuais que não escalam bem, levando a interrupções, latência e usuários frustrados.

Os executivos estão fazendo uma pergunta essencial: como oferecemos acesso seguro sem desacelerar os negócios? Essa pressão é o que está trazendo o Zero Trust para a vanguarda, não apenas como modelo de segurança, mas como facilitador de negócios.

Armadilhas comuns

Muitas organizações começam com a intenção certa, mas depois ficam presas. Uma armadilha comum é pensar que comprar uma "solução Zero Trust " é igual a implementar uma estratégia. Não é assim. O Zero Trust é uma mudança de mentalidade e de arquitetura.

Outra questão é assumir que unificado significa integrado. Muitas das chamadas plataformas são apenas produtos emendados que não compartilham dados, políticas ou mesmo back-ends. Isso cria pontos cegos, especialmente em ambientes modernos, como APIs em nuvem, pipelines de DevOps e aplicativos de IA.

E também há a TI invisível, ferramentas que os funcionários usam e que as equipes de TI não sabem, o que cria sérias lacunas de governança.

O que vem a seguir (doze a dezoito meses)

No próximo ano, veremos o Zero Trust evoluir de controles isolados para uma camada fundamental que abrange toda a empresa. O foco mudará do gerenciamento seguro e de acesso remoto apenas para a unificação de políticas de identidade, dados e tráfego em todos os ambientes. Os líderes já estão mudando para plataformas resilientes por design, que são globais por padrão, automatizam respostas e oferecem visibilidade em tempo real. É aí que está o valor real: não apenas reduzir o risco, mas permitir agilidade.

As organizações que avançam são as que incorporam o Zero Trust em sua base digital, tornando-o parte de como elas criam, escalam e inovam com segurança.

“Uma **armadilha comum** é pensar que comprar uma ‘solução Zero Trust’ equivale a implementar uma estratégia.”

3

Mais forte, não apenas mais segura: escalar a proteção na infraestrutura, nos ecossistemas e na supervisão

Mais forte, não apenas mais segura: escalar a proteção na infraestrutura, nos ecossistemas e na supervisão

Criar resiliência entre redes, cadeias de suprimentos e estruturas de conformidade é essencial para manter a integridade operacional e a vantagem competitiva.

No entanto, as ameaças cibernéticas, como os ataques de DDoS, hoje são mais rápidas, maiores e mais complexas, indo além do alcance das defesas tradicionais. Ao mesmo tempo, as cadeias de suprimentos digitais estão expondo vulnerabilidades ocultas, enquanto o ambiente regulatório se torna mais exigente e fragmentado.

Para se manterem competitivas, as organizações devem reformular a segurança cibernética de uma questão de TI para uma estratégia de resiliência de negócios, que escala em infraestrutura, ecossistemas e supervisão.

Os ataques de DDoS estão aumentando em escala e sofisticação

Os ataques de DDoS evoluíram para ferramentas de precisão usadas por cibercriminosos, hacktivistas e estados-nação para interromper operações e gerar consequências regulatórias e para a reputação. Os ataques de DDoS estão prejudicando empresas em todos os setores. Em 2024, a Cloudflare bloqueou 20,9 milhões de ataques de DDoS, um aumento de 50% em relação a 2023.[17]

A escala e a sofisticação dos ataques de DDoS estão aumentando, com os invasores aproveitando botnets, dispositivos de IoT e automação orientada por IA para lançar ataques persistentes e de alto impacto em serviços digitais críticos.

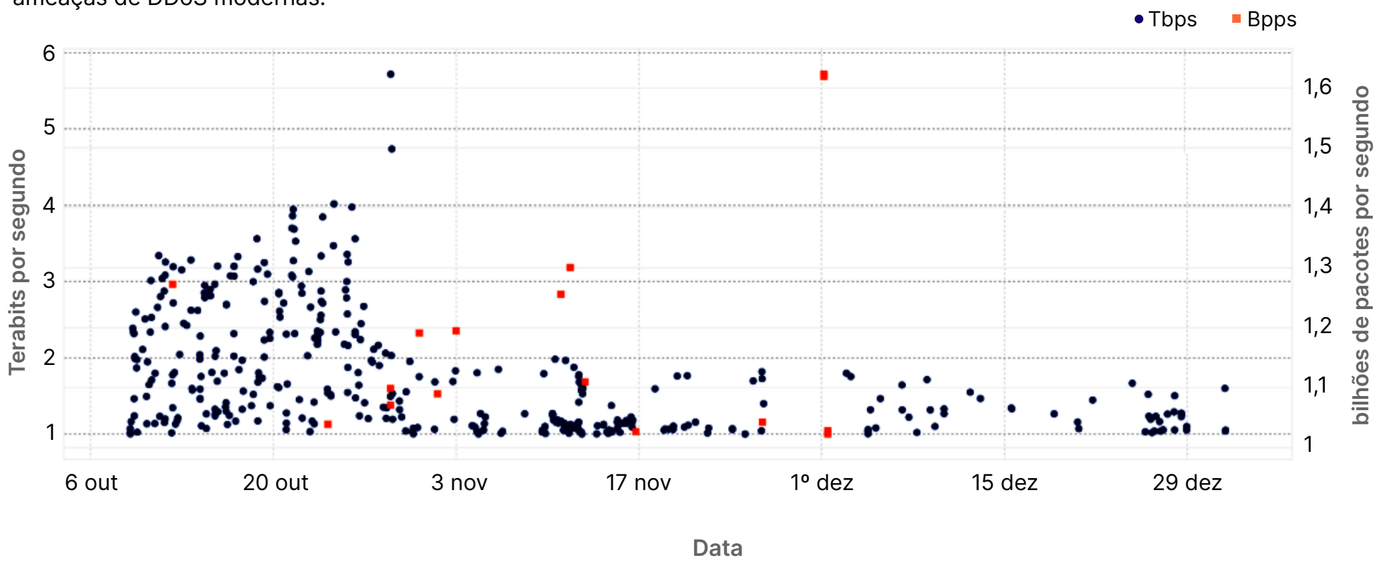
Em 2024, a Cloudflare bloqueou **20,9 milhões** de ataques de DDoS, um **aumento de 50% em relação a 2023**

Ataques de DDoS 2024

O aumento dos ataques de DDoS hipervolumétricos

T4 de 2024

No quarto trimestre de 2024, os ataques hipervolumétricos na camada de rede aumentaram para níveis sem precedentes. O número de ataques superiores a 1 Tbps aumentou 1.885% em relação ao trimestre anterior, enquanto os ataques que ultrapassam 100 milhões de pacotes por segundo (pps) aumentaram 175% no trimestre. Notavelmente, 16% dos ataques superiores a 100 milhões de pps também ultrapassaram 1 bilhão de pps, destacando a crescente intensidade e escala das ameaças de DDoS modernas.[18]



Dados da Cloudflare mostram que uma organização empresarial média usa **pelo menos vinte scripts de terceiros**

Escalada dos ataques à cadeia de suprimentos

De acordo com o Fórum Econômico Mundial, 54% das grandes empresas identificam a gestão de riscos de terceiros como seu principal desafio de resiliência cibernética.[19] Os ataques a cadeias de suprimentos de software, plataformas em nuvem e integrações de terceiros estão aumentando drasticamente. Em 2024, 15% das violações envolveram um terceiro.[20]

Além disso, há uma crescente concentração de risco em alguns provedores de nuvem dominantes. Uma única vulnerabilidade ou interrupção em um desses provedores pode se espalhar por todos os setores, como evidenciado pelas grandes interrupções de TI em 2024, que causaram bilhões em perdas e expuseram a fragilidade dos ecossistemas digitais hiperconectados. Esses incidentes foram um lembrete claro de que, no ambiente interdependente de hoje, um único ponto de falha pode paralisar operações inteiras.

Uma área particularmente vulnerável são os ataques do lado do cliente, onde as empresas dependem regularmente de scripts de terceiros para acelerar o desenvolvimento de aplicativos web. Esses scripts são códigos incorporados, geralmente JavaScript, originários de um servidor externo.

Embora esses scripts aumentem a eficiência, eles também criam vulnerabilidades de segurança significativas: cada conexão com funções externas aumenta o risco de ataques à cadeia de suprimentos baseados em navegador.

Dados da Cloudflare mostram que uma organização empresarial média usa pelo menos vinte scripts de terceiros, enquanto algumas, sem saber, têm centenas de milhares, cada um representando um possível ponto de entrada para os invasores.

Uma grande organização de comércio eletrônico tinha mais de 340 mil scripts de terceiros anexados ao seu site.[21]

Regulamentos como a Lei de Resiliência Cibernética da UE e o padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS 4.0) ajudam a abordar a segurança da cadeia de suprimentos, mas sua aplicação continua sendo um desafio.

Regulamentações de segurança cibernética estão proliferando

As regulamentações de segurança cibernética estão se expandindo em um ritmo rápido, colocando maiores demandas sobre as empresas para aprimorar a segurança, a transparência e os relatórios de incidentes. A Comissão de Valores Mobiliários dos EUA (SEC) agora exige que as empresas públicas divulguem incidentes importantes de segurança cibernética e detalhem suas estratégias de gerenciamento de riscos. O Regulamento Geral sobre a Proteção de Dados (RGPD) da UE continua sendo uma das leis de privacidade de dados mais rigorosas, impondo penalidades de até 4% da receita global pelo não cumprimento. A CPS 234 da Australian Prudential Regulation Authority (APRA) exige que as instituições financeiras mantenham medidas robustas de segurança da informação, enquanto a Digital Operational Resilience Act (DORA) da UE define padrões unificados de segurança cibernética para o setor financeiro.

Em outras palavras, a conformidade não é mais uma reflexão para o futuro. As organizações que navegam com sucesso nesse cenário incorporarão a conformidade em suas operações, aproveitando a automação para agilizar os relatórios e garantir o alinhamento contínuo com as regulamentações em evolução.

Instalação de automação de conformidade

A automação de conformidade está emergindo como uma tendência essencial à medida que as organizações enfrentam uma crescente complexidade regulatória e riscos operacionais. Com mais de 52 requisitos de denúncia de incidentes cibernéticos atualmente ativos ou propostos apenas nos EUA e estruturas globais como o RGPD, DORA e PCI DSS 4.0 expandindo em escopo, os processos de conformidade manuais não são mais sustentáveis.[22] Uma pesquisa da Deloitte descobriu que 62% das organizações globais planejam aumentar o investimento em automação de conformidade, citando a fragmentação regulatória e a necessidade de resposta em tempo real.[23]

Para atender aos requisitos de dados jurisdicionais sem sacrificar o desempenho, as empresas estão adotando a localização estratégica de dados, roteando o tráfego por meio de nós regionais e implantando ferramentas de auditoria automatizadas para verificar a conformidade. Ao mesmo tempo, a linha entre conformidade e segurança está se confundindo: as empresas estão implementando estruturas integradas que alinham a detecção de ameaças, a aplicação de políticas e a prontidão para auditorias.

Essa convergência permite que as empresas reduzam riscos, respondam mais rapidamente às mudanças regulatórias e escalem a governança além das fronteiras. As organizações que automatizarem e operacionalizarem a conformidade ganharão uma vantagem estratégica, acelerando a entrada em mercados regulamentados, aumentando a confiança do cliente e minimizando a exposição financeira e de reputação.

O crescente cenário regulatório

A estrutura regulatória global para segurança cibernética e proteção de dados continua a evoluir rapidamente, com as organizações agora navegando em uma complexa rede de requisitos de conformidade em todas as jurisdições.

Por exemplo:

Regras de segurança cibernética da SEC

A SEC dos EUA implementou requisitos abrangentes de divulgação de segurança cibernética para empresas públicas. Essas regras exigem relatórios em tempo hábil de incidentes de segurança importantes e divulgações detalhadas sobre estratégias de gerenciamento de riscos, governança e perícia.

NIS2

A diretiva NIS2 da UE define requisitos de segurança mais rigorosos em 18 setores críticos. Ela exige medidas de resiliência, gerenciamento de riscos, resposta a incidentes e relatórios, com supervisão aprimorada e penalidades pela não conformidade.

APRA CPS 234

O padrão de segurança da informação CPS 234 da Prudential Regulation Authority da Austrália exige que as instituições financeiras mantenham recursos robustos de segurança da informação proporcionais ao tamanho e à extensão das ameaças aos seus ativos de informação.

DORA

A DORA representa a abordagem abrangente da Europa à resiliência operacional digital no setor financeiro. Ela estabelece requisitos uniformes para a segurança de redes e sistemas de informação que apoiam as operações das entidades financeiras.

PERGUNTAS PARA O ALTO ESCALÃO

Continuidade e conformidade reimaginadas

Em um cenário de ameaças moldado por ataques de DDoS em larga escala, cadeias de suprimentos opacas e regulamentações globais complexas, a verdadeira resiliência vai além da defesa. Significa projetar sistemas que continuam a operar sob pressão e tratar a conformidade como uma proteção e um facilitador estratégico. **Essas cinco perguntas ajudam os CXOs a avaliar a prontidão de sua organização para resistir e se adaptar à disrupção.**

P1

Nossa infraestrutura consegue absorver ataques de DDoS em larga escala e manter o tempo de atividade sob pressão?

A capacidade de mitigação deve exceder tanto o pico de tráfego legítimo quanto os maiores ataques registrados. Organizações resilientes implementam infraestrutura geograficamente redundante e planos de failover com reconhecimento de conformidade e testam regularmente os procedimentos de recuperação para garantir o tempo de atividade e o alinhamento regulatório.

P2

Temos visibilidade em tempo real de nossas dependências de terceiros mais críticas?

As vulnerabilidades da cadeia de suprimentos são uma das principais causas de incidentes de segurança. Organizações voltadas para o futuro monitoram continuamente fornecedores e serviços externos, impõem requisitos contratuais de segurança e integram insights de riscos de terceiros em processos de governança mais amplos.

P3

Automatizamos os fluxos de trabalho de conformidade para acompanhar as regulamentações globais?

Com tantas estruturas regulatórias evoluindo rapidamente, uma abordagem manual para a conformidade não consegue escalar. Empresas de alto desempenho usam auditoria automatizada, monitoramento em tempo real e roteamento de dados com reconhecimento de jurisdição para manter o alinhamento contínuo e reduzir a sobrecarga.

P4

Nossas funções de segurança e conformidade estão totalmente integradas?

Equipes isoladas criam ineficiências e lacunas. Plataformas unificadas que alinham a detecção de ameaças com relatórios regulatórios simplificam os processos de auditoria, melhoram a visibilidade e reduzem os riscos em toda a empresa.

P5

Testamos nossa postura de resiliência completa, desde a detecção de incidentes até a recuperação e a emissão de relatórios?

As organizações proativas desenvolvem manuais que vinculam controles técnicos aos requisitos regulatórios, simulam interrupções regularmente e adaptam arquiteturas de conformidade para escalar entre jurisdições.

PERSPECTIVAS DE EXECUTIVOS

As novas regras de prontidão

Emily Hancock
Chief Privacy Officer, Cloudflare

Proteger o futuro: regulamentação, risco e prontidão

A regulamentação de segurança cibernética está entrando em uma nova era definida por requisitos mais rigorosos, maior escrutínio e responsabilização mais ampla. Desde as divulgações obrigatórias de incidentes da SEC até as rigorosas penalidades de privacidade do RGPD e novos padrões como DORA e APRA CPS 234, os reguladores globais estão criando expectativas em relação à proteção de dados, continuidade operacional e transparência. Para as equipes executivas, a conformidade não é mais apenas uma obrigação legal, é uma prioridade estratégica.

Ao mesmo tempo, novas tecnologias e modelos de ameaças em evolução estão desafiando as abordagens tradicionais de segurança. À medida que a inovação se acelera, os reguladores e as partes interessadas estão prestando mais atenção à gestão de riscos no longo prazo, especialmente no que diz respeito a dados confidenciais. As organizações devem demonstrar que podem proteger não apenas os ativos atuais, mas também os dados e sistemas que sustentarão a confiança digital do futuro.

O que estamos deixando passar: equívocos e lacunas negligenciadas

Muitas organizações ainda tratam a segurança e a conformidade como funções isoladas, gerenciadas por equipes técnicas sem coordenação multifuncional. Isso cria pontos cegos, particularmente para entender onde residem os dados confidenciais, como a criptografia é aplicada e onde estão as vulnerabilidades nos sistemas de terceiros.

Sem uma estrutura clara de inventário e governança, as organizações correm o risco de ficar para trás tanto em relação aos reguladores quanto aos invasores.

Outra lacuna está na minificação de dados. Muitas vezes, as empresas retêm dados pessoais de que não precisam mais, aumentando a exposição sem benefício comercial. A incorporação de princípios de privacidade por design, limitando a coleta de dados, automatizando a exclusão e criando controles no nível da arquitetura, pode reduzir o risco e melhorar o alinhamento regulatório.

O que vem a seguir: uma mudança em direção à conformidade incorporada

Nos próximos doze a dezoito meses, esperamos que os reguladores e órgãos de padronização coloquem mais ênfase em práticas de segurança proativas e verificáveis. Isso inclui controles mais fortes sobre governança de dados, criptografia e risco de terceiros. As empresas que agirem desde o início, adotando plataformas integradas, automatizando fluxos de trabalho de conformidade e incorporando a segurança às operações essenciais, vão reduzir a complexidade, evitar remediações dispendiosas e se posicionar como líderes confiáveis.

A mudança é clara: a conformidade, a continuidade e a segurança devem ser projetadas desde o início. As organizações que internalizarem essa mentalidade não vão apenas acompanhar a regulamentação, elas vão liderar um mundo que exige responsabilidade, transparência e confiança.

“Sem uma estrutura clara de inventário e governança, **as organizações correm o risco de ficar para trás tanto em relação aos reguladores quanto aos invasores.**”

4

Quebrar o código: privacidade preparada para o futuro na era quântica

Quebrar o código: privacidade preparada para o futuro na era quântica

A computação quântica promete avanços transformadores na ciência e na indústria, mas também representa uma ameaça fundamental à segurança digital. Quando os sistemas quânticos em larga escala amadurecerem, eles serão capazes de quebrar criptosistemas de chave pública amplamente utilizados para proteger a internet. Isso inclui criptografia TLS, VPNs, assinatura de código e sistemas de blockchain.

O perigo não é hipotético. Os agentes de ameaças já estão coletando dados criptografados hoje, apostando que os futuros computadores quânticos serão capazes de descriptografá-los, uma estratégia conhecida como “Colher agora, descriptografar depois”. À medida que a adoção da criptografia pós-quântica é acelerada, a visibilidade dos sistemas criptográficos, a aplicação automatizada de políticas e um caminho de migração claro definirão a prontidão organizacional.

As ameaças quânticas já estão em movimento

O Instituto Nacional de Padrões e Tecnologia (NIST) alertou que as organizações devem agir agora para evitar serem pegas desprevenidas.[24] Agentes de estado-nação e adversários sofisticados estão coletando ativamente tráfego criptografado, propriedade intelectual e segredos de estado para descriptografar posteriormente. As comunicações que exigem confidencialidade por uma década (ou mais), como registros de saúde, inteligência militar e contratos legais, já estão vulneráveis se não forem protegidas com um acordo de chave resistente a ataques quânticos.

A adoção da PQC aumentou, mas existem lacunas

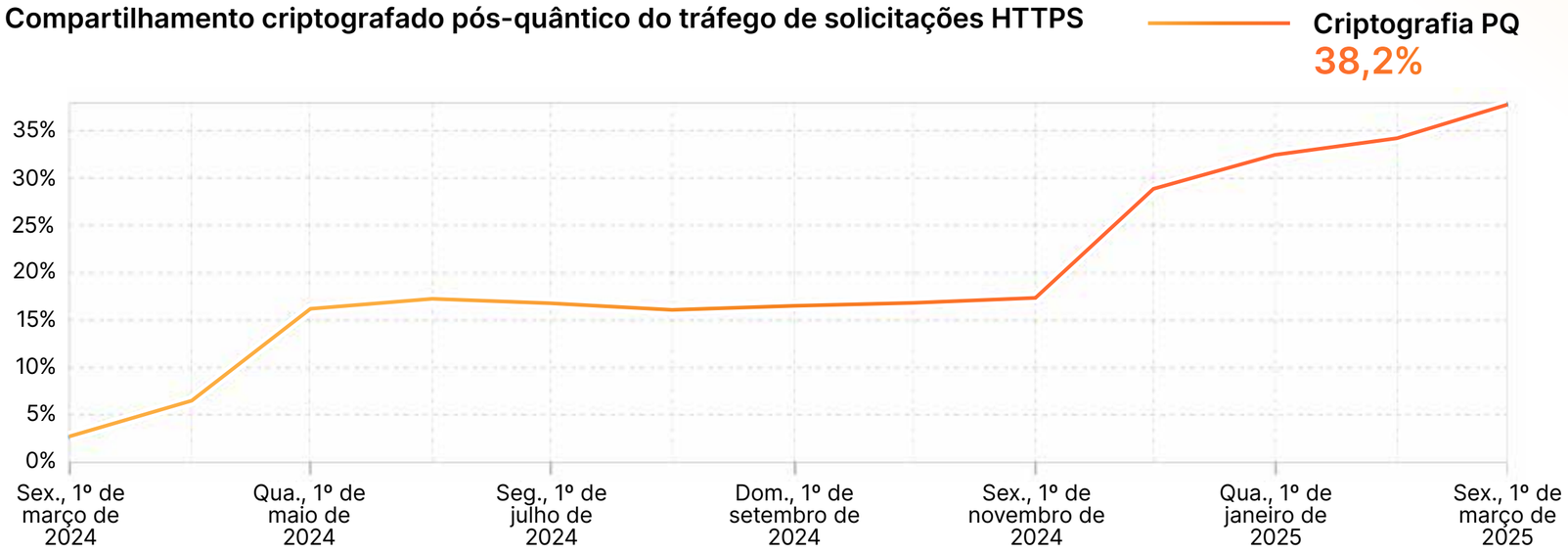
A criptografia pós-quântica (PQC) passou da pesquisa teórica para a implementação da produção. As principais empresas de tecnologia, incluindo a Cloudflare, estão liderando o movimento em direção à adoção da PQC.

No início de 2024, a Cloudflare relatou que apenas 3% do tráfego HTTPS era criptografado usando algoritmos pós-quânticos. Em março de 2025, esse número atingiu 38%, após o lançamento do TLS pós-quântico híbrido por padrão pela Cloudflare e o suporte aos navegadores Chrome, Edge e Firefox.[25]

Ainda assim, a adoção é desigual. A maioria dos ambientes empresariais está no início das fases de descoberta ou piloto e a expansão criptográfica complica a transição. As empresas que não priorizam a criptografia resistente ao quântico correm o risco de ficar para trás nas exigências regulatórias e expor seus dados a vulnerabilidades no longo prazo.

Adoção de criptografia pós-quântica em todo o mundo

Compartilhamento criptografado pós-quântico do tráfego de solicitações HTTPS



Plano estratégico da migração quântica

1

Comece documentando todos os lugares em que a criptografia é usada.

Crie uma lista de projetos de migração, priorizados por risco e nível de esforço.

2

Torne a prontidão pós-quântica parte do processo de avaliação de seu fornecedor agora.

Nem todos os fornecedores são iguais quando se trata de adotar os padrões mais recentes. Valide a agilidade na criptografia do fornecedor, especialmente seus fornecedores de Zero Trust que fazem o tunelamento do tráfego da rede corporativa.

3

Dê prioridade às migrações de contratos importantes.

Devido à ameaça de coletar agora, descriptografar depois, há um benefício claro em garantir que seu contrato de chave seja resistente ao quântico agora. Os fornecedores convergiram amplamente na transição do TLS 1.3 para ser compatível com o X25519MLKEM768: um híbrido da curva elíptica convencional X25519 junto com o ML-KEM pós-quântico (Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 203).

As migrações de assinatura devem ser documentadas, mas não priorizadas neste momento.

As organizações ainda estão trabalhando para chegar a um consenso sobre a abordagem correta para migrar para assinaturas pós-quânticas. Felizmente, as assinaturas pós-quânticas protegem principalmente contra ataques on-path ativos, tornando essa migração uma prioridade menor.

4

A visibilidade de criptomoedas e a automação orientada por XDR acelerarão a transição

A migração pós-quântica não se trata apenas de implantar novos algoritmos, mas de entender onde a criptografia reside em ambientes em expansão. Isso inclui sistemas incorporados, cargas de trabalho em nuvem, aplicativos legados, APIs e dispositivos de IoT. As equipes de segurança que usam plataformas estendidas de detecção e resposta (XDR) com telemetria profunda de rede e endpoints estão melhor posicionadas para descobrir criptomoedas desatualizadas, detectar comportamentos de fallback inseguro e automatizar fluxos de trabalho de correção.

A agilidade na criptografia do fornecedor se tornará um diferencial de risco

Os órgãos reguladores (por exemplo, NIST, BSI, ANSSI) estão começando a recomendar ou exigir arquiteturas cripto ágeis. As empresas vão avaliar cada vez mais a prontidão pós-quântica em RFPs e auditorias da cadeia de suprimentos. No entanto, nem todos os fornecedores estão avançando no mesmo ritmo. Aqueles que não oferecerem suporte à criptografia híbrida ou quântica segura podem enfrentar a desqualificação, especialmente nos setores governamentais, de serviços financeiros e de defesa.

PERGUNTAS PARA O ALTO ESCALÃO

Preparação para riscos quânticos

À medida que os invasores adotam táticas de colher agora e descriptografar depois e os reguladores avançam em direção aos mandatos pós-quânticos, as organizações devem começar a se preparar hoje. Os executivos que lideram essa transição não apenas preparam sua infraestrutura para o futuro, mas também ganham uma vantagem estratégica em confiança, conformidade e resiliência. **Considere sua prontidão para a era de riscos quânticos no curto prazo, fazendo estas perguntas:**

P1

Temos visibilidade total de onde a criptografia é usada em nosso ambiente, de nuvens e aplicativos a sistemas incorporados e ferramentas de terceiros?

Os sistemas criptográficos geralmente são profundamente enraizados e mal documentados. Sem visibilidade total, as organizações correm o risco de deixar sistemas críticos desprotegidos ou, sem saber, expostos a ameaças da era quântica.

P2

Priorizamos a migração para protocolos de acordo de chave pós-quânticos, especialmente para sistemas que protegem dados confidenciais ou de longa vida útil?

Os ataques colher agora, descriptografar depois visam dados que devem permanecer confidenciais por anos. Migrar mecanismos de troca de chaves, como handshakes TLS, é uma etapa urgente e de alto impacto na garantia da confidencialidade futura.

P3

Nossas ferramentas de detecção e monitoramento de ativos são capazes de identificar criptografias desatualizadas ou vulneráveis em toda a empresa?

As plataformas XDR, SIEM e de descoberta de ativos devem ajudar a detectar desvios criptográficos, bibliotecas legadas e protocolos de fallback. Isso é essencial para evitar configurações incorretas e orientar as prioridades de migração.

P4

Estamos avaliando a cripto agilidade de nossos fornecedores e parceiros como parte de nosso processo de aquisição e análise de risco?

Os fornecedores que não possuem um roteiro para prontidão pós-quântica podem se tornar elos fracos. Incorporar o alinhamento da PQC na due diligence ajuda a reduzir a exposição downstream e garante resiliência no longo prazo.

P5

Temos uma estratégia de migração baseada em riscos e em fases que inclui governança, automação e visibilidade executiva?

A migração pós-quântica é uma jornada complexa, que dura vários anos. Um roteiro claro com responsabilidade, automação para implantação e métricas em tempo real para o progresso é essencial para manter o impulso e a confiança no nível do conselho.

PERSPECTIVAS DE EXECUTIVOS

Esclarecendo a confusão criptográfica

Wesley Evans
Senior Product Manager, Cloudflare

As organizações estão enfrentando um aumento na complexidade criptográfica. Onde antes tínhamos alguns padrões bem definidos, agora temos um ecossistema fragmentado de algoritmos e modelos de implantação. Essa rápida evolução, juntamente com a crescente pressão regulatória e operacional para adotar a criptografia quântica segura, cria confusão no nível empresarial.

Os líderes são instruídos a adotar a criptografia e se preparar para a resiliência quântica, mas a maioria não possui um inventário claro de onde e como a criptografia é usada. Sem visibilidade, o planejamento se torna uma adivinhação. Paralisações no orçamento. A propriedade não é clara. E isso torna mais fácil para os executivos não priorizarem a ação, mesmo quando os riscos são bem conhecidos.

Armadilhas comuns

Um grande ponto cego é a suposição de que as organizações ainda não foram comprometidas. Os ataques colher agora, descriptografar depois são reais e ativos, especialmente para dados com valor no longo prazo, como registros de saúde, propriedade intelectual e informações de segurança nacional. Se seus dados se enquadrarem nessas categorias, eles já podem estar nas mãos de um agente de ameaças, esperando pela capacidade de descriptografá-los.

Outro equívoco é que o risco quântico será precedido por um marco claro, como uma descoberta pública no algoritmo de Shor. Mas os invasores não precisam de resultados instantâneos.

Se levar semanas ou meses para quebrar uma chave e a recompensa for significativa, eles farão esse investimento. Esse atraso na percepção contribui para uma perigosa sensação de complacência.

Direção futura

Duas mudanças estão chegando rapidamente. Primeiro, os avanços na correção de erros quânticos vão fazer com que a ameaça da descriptografia quântica pareça real, não teórica. Isto irá desencadear um aumento da pressão por parte dos reguladores, conselhos e do público. Em segundo lugar, as organizações começarão a implementar sistemas cripto ágeis. Isso significa, finalmente, fazer um balanço de onde reside a criptografia, como ela é usada e quem a possui.

Não será fácil. A maioria das equipes está entrando nisso como uma visita há muito esperada ao dentista criptográfico. Espere incômodo, custos e surpresas. Mas esperar só piora as coisas. A prioridade agora não é substituir tudo da noite para o dia, mas criar visibilidade, atribuir responsabilidades e iniciar o caminho de atualização. Aqueles que agirem desde o início estarão mais bem posicionados para gerenciar a mudança pós-quântica, antes que se torne uma crise.

“Os avanços na correção de erros quânticos **farão com que a ameaça da descriptografia quântica** pareça real, não teórica.”

5

Mudando o equilíbrio: governança, geopolítica e ética

Mudando o equilíbrio: governança, geopolítica e ética

À medida que a dinâmica do poder global muda, a intersecção entre segurança cibernética, geopolítica e ética está redefinindo as responsabilidades da liderança. Hoje, os ataques cibernéticos são ferramentas de influência geopolítica, os órgãos reguladores estão responsabilizando os executivos pessoalmente e a IA está introduzindo dilemas éticos que desafiam a supervisão tradicional.

Com alterações como o mandato da SEC em 2023 para divulgação rápida de incidentes cibernéticos e relatórios generalizados de operações cibernéticas patrocinadas por estados, os líderes devem incorporar governança robusta, ética de IA transparente e gerenciamento de riscos ágil em sua estratégia.

A governança de segurança passa da orientação para a responsabilidade

A supervisão regulatória está se tornando mais rigorosa. Em 2023, a SEC determinou que empresas de capital aberto divulguem incidentes cibernéticos em até quatro dias, marcando uma mudança em direção à responsabilização forçada. Quase 72% das empresas agora priorizam o conhecimento em segurança cibernética em seus conselhos, com 71% apresentando-a em pelo menos uma biografia de diretor, em comparação com apenas 34% em 2018.[26] Os conselhos reconhecem cada vez mais que negligenciar a segurança cibernética pode levar a graves consequências operacionais, legais e de reputação.

A geopolítica e a guerra cibernética afetam diretamente a empresa

Agentes de estado-nação e grupos hacktivistas estão cada vez mais aproveitando as operações cibernéticas como armas estratégicas. Nos últimos anos, campanhas apoiadas pelo estado visaram os setores financeiro, de energia e tecnologia para causar disrupção nas cadeias de suprimentos globais e influenciar a dinâmica do mercado. Por exemplo, o agente de ameaças com motivação política, LameDuck, realizou mais de 35 mil ataques de DDoS confirmados no período de um ano, levando a interrupções operacionais em organizações como Microsoft, OpenAI e Scandinavian Airlines.[27] Mesmo organizações aparentemente neutras podem ser envolvidas em conflitos geopolíticos.

Os executivos devem ser tratados como superfícies de ataque

Os líderes de alto escalão enfrentam ameaças cibernéticas diretas. Golpes de deepfake e esquemas de falsificação de executivos de alto perfil aumentaram exponencialmente, com vários CEOs supostamente sendo alvo de mensagens de áudio e vídeo fraudulentas projetadas para enganar as partes interessadas.[28] Tais incidentes ressaltam como a liderança é vulnerável ao risco cibernético e a ataques financeiros e de reputação direcionados.

A fragmentação regulatória e a incerteza na cadeia de suprimentos estão se intensificando

As empresas globais agora navegam por um labirinto de leis divergentes de segurança cibernética, IA e soberania de dados. Restrições comerciais e controles de exportação forçaram empresas a reavaliar relacionamentos com fornecedores e reconfigurar cadeias de suprimentos. Por exemplo, as mudanças nas tarifas e a diretiva NIS2 da UE interromperam os protocolos estabelecidos da cadeia de suprimentos, aumentando os custos de conformidade e o risco de atrasos operacionais.

A ética da IA e a IA oculta exigem governança em escala

A explosão da IA generativa no local de trabalho está ultrapassando o controle organizacional. A McKinsey relata que 65% das empresas agora usam a GenAI em pelo menos uma função de negócios, contra um terço em 2023.[29] O AI Gateway da Cloudflare processou mais de cinco bilhões de solicitações entre outubro de 2024 e fevereiro de 2025, um aumento de 60% em apenas cinco meses.[30] A adoção é extremamente rápida: em janeiro de 2025, a DeepSeek AI alcançou a 3ª posição na lista de serviços de IA do Cloudflare Radar nove dias após o lançamento de seu modelo R1.[31]

Essa adoção popular está alimentando a ascensão da IA oculta, ferramentas não autorizadas usadas por funcionários sem supervisão. Essas ferramentas representam sérios riscos: vazamento de dados, não conformidade regulatória e exposição de informações confidenciais a modelos públicos.

Para responder, as organizações devem ir além das declarações básicas de políticas. A governança eficaz requer estruturas de aprovação claras, registro de prompts, filtragem de URLs e monitoramento de uso. Sem aplicação ativa, a ética e a segurança da IA permanecerão teóricas.

> Agentes de estado-nação e grupos hacktivistas estão cada vez mais aproveitando as operações cibernéticas como **armas estratégicas.**

PERGUNTAS PARA O ALTO ESCALÃO

Navegar pelo risco ético e geopolítico

À medida que as ameaças cibernéticas se tornam geopolíticas, a ética da IA se torna mais complexa e as expectativas regulatórias se tornam mais rígidas, as equipes executivas precisam ir além dos controles técnicos. **Essas perguntas podem ajudar os líderes a avaliar se suas estratégias de governança, inteligência e resposta são adequadas para um mundo onde a própria liderança faz parte da superfície de ameaças.**

P1

Temos uma responsabilidade clara no nível do conselho pela segurança e resiliência digital, com funções definidas e liderança com conhecimento cibernético?

Como os reguladores agora responsabilizam os executivos pessoalmente, como visto nos requisitos de divulgação rápida da SEC, garantir que o conselho esteja equipado com experiência cibernética dedicada é fundamental para mitigar riscos legais e de reputação.

P2

Estamos monitorando mudanças geopolíticas e seu impacto em nosso cenário de ameaças, incluindo ataques cibernéticos patrocinados por estados e campanhas de ativistas?

Com as recentes operações apoiadas pelo estado interrompendo as cadeias de fornecimento e visando setores críticos do mercado, ter inteligência em tempo real sobre o risco geopolítico é essencial para proteger as operações e a liderança globais.

P3

Temos um plano de resposta proativo para ataques direcionados a executivos, como golpes de deepfake e campanhas de falsificação?

À medida que a liderança enfrenta riscos crescentes de desinformação e falsificação impulsionados pela IA, as estratégias de resposta devem incluir protocolos de resposta a incidentes direcionados e medidas contínuas de gerenciamento de reputação.

P4

Nossas políticas e controles de segurança são robustos o suficiente para detectar e gerenciar o uso não autorizado de IA em nossa força de trabalho?

Com mais organizações aproveitando a GenAI e o aumento dos relatos de IA oculta, é necessário um monitoramento granular e a aplicação de diretrizes rígidas para evitar vazamentos de dados e garantir a conformidade regulatória.

P5

Estamos alinhando nossas estratégias de segurança cibernética e de IA com a evolução das regulamentações regionais sobre soberania de dados e IA ética e estamos usando esse alinhamento como uma vantagem estratégica?

Estruturas regulatórias divergentes, como a diretiva NIS2 da UE e as leis de soberania de dados regionais, exigem que as políticas de segurança sejam ágeis e com visão de futuro. Esse alinhamento reduz o risco legal e aumenta a confiança do mercado e o posicionamento competitivo.

PERSPECTIVAS DE EXECUTIVOS

Governança e responsabilidade em um mundo de policrise

Ramy Houssaini
Chief Cyber Solutions Officer, Cloudflare

As organizações devem navegar em um cenário de policrise onde riscos geopolíticos, econômicos e tecnológicos se interceptam. O mandato de divulgação de incidentes cibernéticos da SEC exemplifica a mudança das orientações de segurança cibernética para a responsabilidade executiva. As organizações devem desenvolver recursos de detecção e resposta a violações em tempo real. A não conformidade acarreta penalidades severas, enquanto os danos à reputação podem corroer a confiança das partes interessadas. Os conselhos devem incorporar experiência em segurança cibernética e gerenciamento proativo de riscos para permanecerem resilientes.

Pontos cegos: riscos geopolíticos, de IA e da cadeia de suprimentos

Um ponto cego importante é subestimar as ameaças cibernéticas geopolíticas. Muitas empresas assumem a neutralidade, mas os ataques patrocinados por estados prejudicam cada vez mais os setores financeiros, tecnológicos e de energia, deixando as cadeias de abastecimento vulneráveis.

Outro risco negligenciado é a IA oculta, ferramentas de IA não autorizadas usadas sem supervisão. Sem um monitoramento robusto, os dados confidenciais podem ser expostos, levando a penalidades regulatórias e desvantagens competitivas.

Além disso, fornecedores de quarta e quinta partes introduzem vulnerabilidades ocultas. Embora as empresas se concentrem em fornecedores diretos, os ecossistemas ampliados de fornecedores muitas vezes não têm visibilidade, tornando-os suscetíveis a ameaças cibernéticas e interrupções operacionais.

Desenvolvimentos futuros e preparação estratégica

Nos próximos doze a dezoito meses, as organizações devem antecipar:

- **Expansão regulatória:** a diretiva NIS2 da UE e estruturas semelhantes intensificarão os requisitos de conformidade. Os líderes devem estabelecer forças-tarefa regulatórias para permanecer à frente.
- **Aceleração da governança de IA:** com o aumento da IA oculta, os reguladores vão impor controles mais rígidos. As empresas devem aplicar estruturas de monitoramento e governança para mitigar os riscos.
- **Executivos como alvos:** os golpes de deepfake e os ataques de personificação se tornarão mais sofisticados, aumentando os riscos de fraude e desinformação. As organizações devem implantar sistemas de detecção orientados por IA e aprimorar o treinamento de segurança para executivos.
- **Resiliência da cadeia de suprimentos:** as ameaças cibernéticas e a instabilidade geopolítica continuarão a afetar as cadeias de suprimentos. As empresas devem fortalecer as avaliações de risco, cumprir as obrigações de segurança e melhorar o monitoramento dos fornecedores.

Para ter sucesso nesta era de policrise, os líderes devem integrar a segurança cibernética à governança, avaliar riscos geopolíticos, impor a supervisão da IA e criar cadeias de suprimentos resilientes. Agilidade e gerenciamento de riscos superiores serão essenciais para navegar pelas regulamentações em evolução e garantir a estabilidade no longo prazo.

“Os conselhos devem **incorporar experiência em segurança cibernética e gerenciamento proativo de riscos** para permanecerem resilientes.”

CONCLUSÃO

Movimentos do alto escalão que criam resiliência em escala

A natureza da segurança cibernética mudou e agora ela atinge todos os setores da empresa. Em 2025, ataques com tecnologia de IA, riscos geopolíticos, complexidade regulatória e interdependências da cadeia de suprimentos exigem uma resposta coordenada e multifuncional. Proteger o futuro significa mais do que reagir às ameaças; significa incorporar a resiliência na forma como as organizações operam, inovam e crescem. Essas chamadas para a ação são projetadas para que os CXOs criem resiliência como uma capacidade estratégica, juntos.

1 Tornar a resiliência um mandato estratégico compartilhado

Crie propriedade multifuncional para a segurança cibernética, garantindo que o alto escalão se alinhe em conjunto com a postura de segurança, alocação de recursos e plano de contingência. A resiliência não é o trabalho de uma equipe, é uma capacidade empresarial que deve escalar entre funções e regiões geográficas.

2 Automatizar e integrar para garantir escalabilidade

A conformidade manual e as defesas fragmentadas não conseguem acompanhar as ameaças habilitadas por IA e a expansão dos requisitos regulatórios. Invista em automação para detecção de ameaças, fluxos de trabalho de conformidade e resposta a incidentes. Integre ferramentas de conformidade, risco e segurança para eliminar silos e melhorar a visibilidade.

3 Repensar a governança cibernética como uma vantagem competitiva

Com o aumento da responsabilidade executiva, garanta que seu conselho e o alto escalão incluam uma liderança com conhecimento cibernético e funções formalizadas para a supervisão do risco digital. Incorpore o risco cibernético às estruturas de risco corporativo e trate o alinhamento regulatório como um diferencial competitivo.

4 Preparar-se para o futuro agora, não mais tarde

Comece sua migração para criptografia pós-quântica (PQC) e prontidão para a governança de IA hoje. Os líderes que esperarem vão se tornar vulneráveis a ameaças do tipo "colher agora, descriptografar depois" ou à expansão descontrolada da IA. Visibilidade, agilidade na criptografia de fornecedores e estratégias de migração em fases são fundamentais.

5 Testar para falhas em escala

Resiliência não é evitar falhas; é operar apesar delas. Simule crises do mundo real, desde ataques de DDoS hipervolumétricos ao uso indevido de insiders ou ataques direcionados a executivos, e teste sua capacidade de detectar, conter e recuperar. Considere conformidade, comunicações e cadeia de suprimentos em seus cenários.

6 Integrar a IA no ataque e na defesa

A IA não deve mais ser tratada apenas como uma ferramenta. Ao invés disso, é uma capacidade estratégica dentro do alto escalão, impulsionando a agilidade, a resiliência e a inovação em toda a empresa. Ao aproveitar os insights com tecnologia de IA, as organizações podem se adaptar rapidamente às mudanças do mercado, antecipar riscos e otimizar a tomada de decisões em tempo real.

A IA aumenta a resiliência automatizando a detecção de ameaças, simplificando a resposta a crises e fortalecendo as posturas de segurança cibernética contra riscos em evolução. Além disso, alimenta a inovação ao descobrir novos fluxos de receita, acelerando a P&D e personalizando as experiências do cliente em escala. À medida que a IA se torna profundamente integrada às principais funções das empresas, ela transforma as organizações em empresas mais adaptáveis e prontas para o futuro, permitindo que os líderes naveguem na complexidade com confiança.

Proteger o futuro significa mais do que reagir às ameaças; significa **incorporar a resiliência na forma como as organizações operam, inovam e crescem.**

Resiliência na Cloudflare: os fundamentos para permitir um futuro mais escalável

RESILIÊNCIA NA CLOUDFLARE

Uma rede única e programável, diferente de qualquer outra

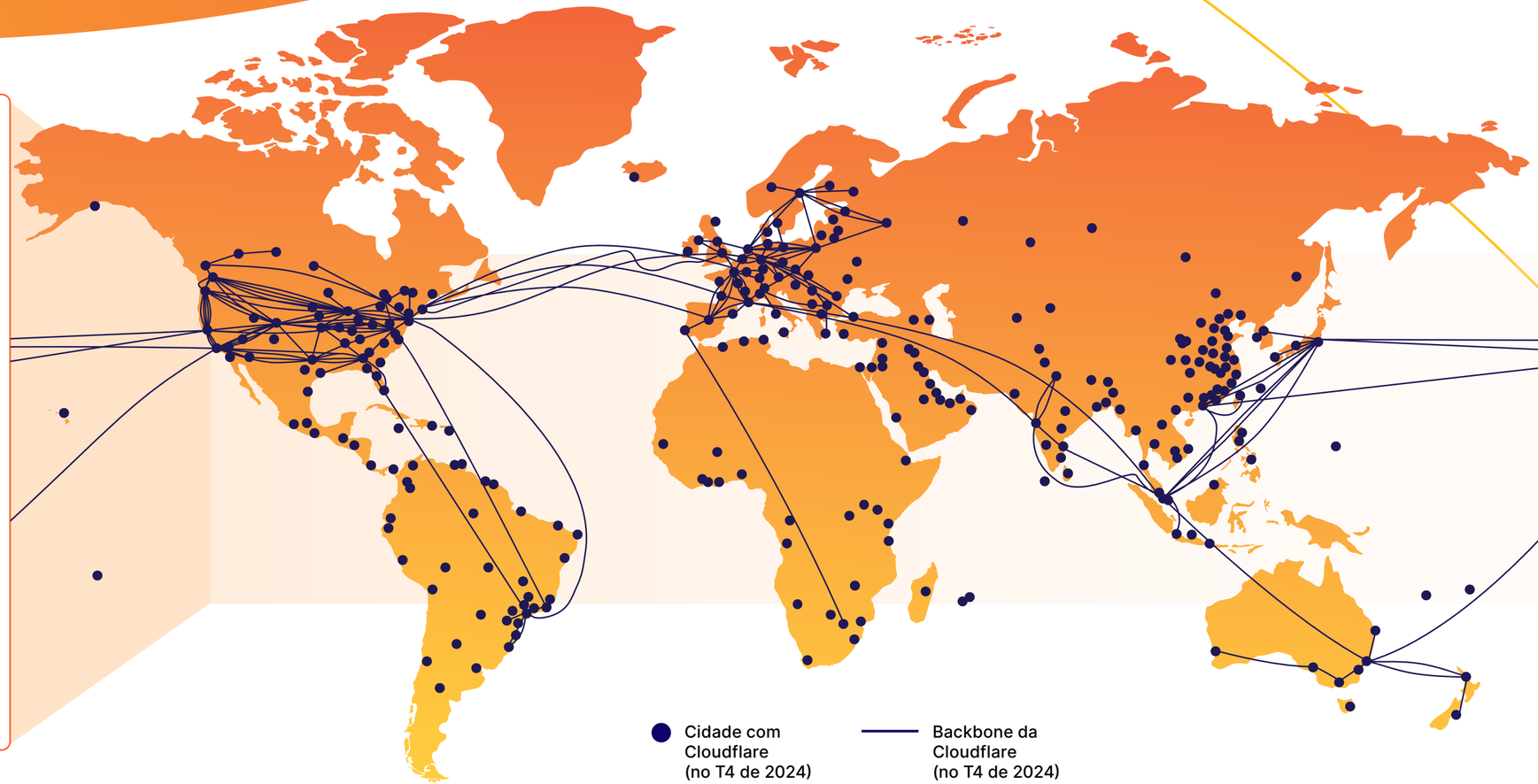
Mais de 335 cidades
em mais de 125 países, incluindo a China Continental

↳ **c/ + de 190 cidades**
para inferência de IA alimentada por GPUs

aprox. 50 ms
de aprox. 95% da população mundial conectada à internet

aprox. 13.000 redes
conectam-se diretamente à Cloudflare, incluindo provedores de internet, de nuvem e grandes empresas

348 Tbps
de capacidade de rede e continua aumentando



RESILIÊNCIA NA CLOUDFLARE

Cloudflare Workers

A melhor plataforma para desenvolvedores criarem e escalarem inferências e agentes de IA

Custo e escalabilidade

Escalar e reduzir até zero

Execute modelos de IA em GPUs sem ter que pagar por recursos pré-provisionados com meses de antecedência, no pico. Só pague pelo que você usar.

Sem computação = sem cobranças de uso

Preços baseados em computação significam que você não é cobrado quando sua função está ociosa e aguardando E/S. (Os aplicativos podem passar até **dez vezes** mais tempo esperando por E/S do que realmente usando a CPU).

Desempenho

Implante a partir da região: Terra

O código é executado dentro de 50 ms de aproximadamente 95% da população global conectada à internet.

Orquestração e execução em um só lugar

O Workers pode interagir com APIs, LLMs e serviços externos ou internos, onde quer que seja mais eficiente para ser executado.

Experiência do desenvolvedor

Todos os produtos de que você precisa

Acesse inferência, gerenciamento de estado, implantação de IU ou fluxos de trabalho em uma única plataforma.

Da ideia à produção em segundos

Experiência de desenvolvimento fácil, incluindo desenvolvimento local e implantação rápida.

Economize tempo

Sem necessidade de ajustes. Posicionamento automático para desempenho ideal.

Você escreve o código. Nós cuidamos do resto.

RESILIÊNCIA NA CLOUDFLARE

Uma única plataforma de segurança. Da rede para a nuvem. Aplicativos para IA.

Permitir que as organizações:

- Recuperem o controle operacional
- Melhorem a postura de segurança
- Acelerem a consolidação de fornecedores
- Aprimorem a experiência do usuário e a produtividade
- Alcancem a governança e a conformidade dos dados

RESILIÊNCIA NA CLOUDFLARE

A Cloudflare foi criada para o que vem a seguir

Uma plataforma combinável

Segurança unificada

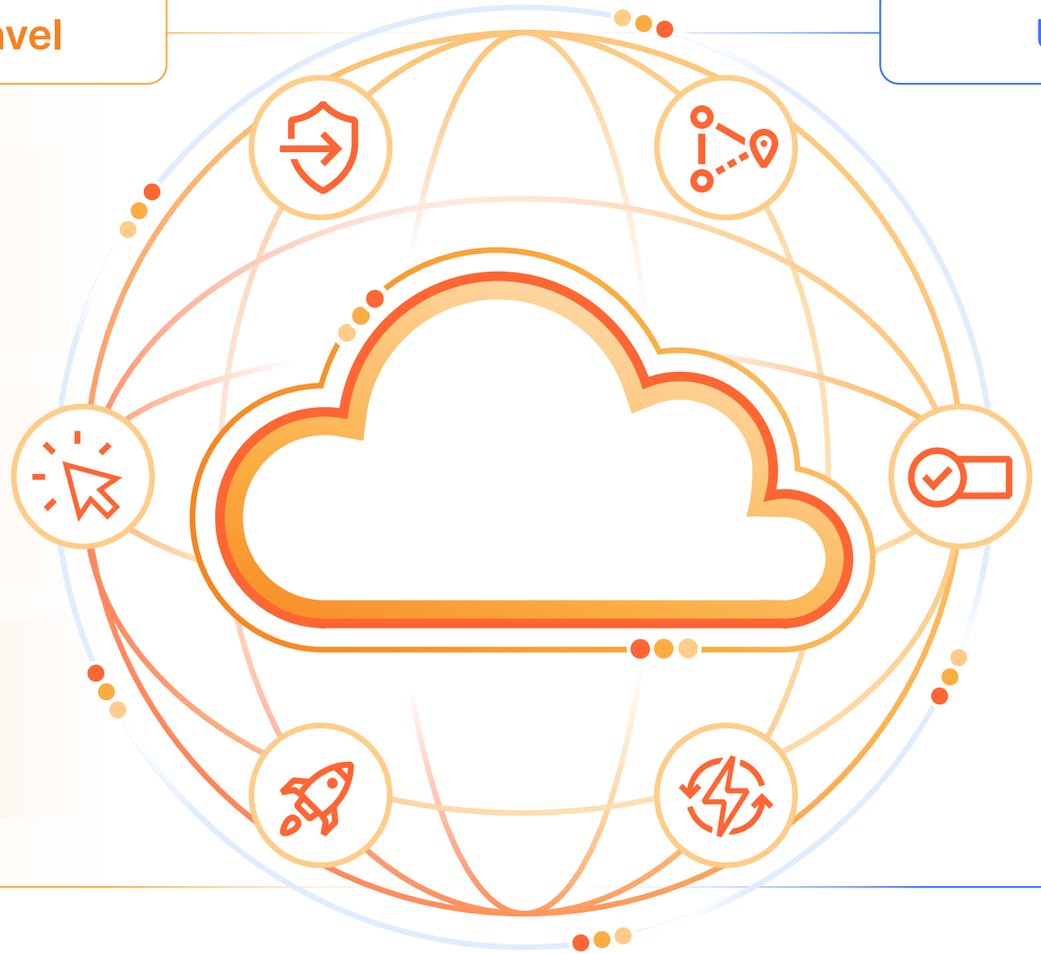
para sistemas externos e recursos internos

Conectividade any-to-any

para usuários, aplicativos, filiais, data centers e nuvens

Flexibilidade

para personalizar a plataforma com ferramentas full stack para desenvolvedores



Uma rede programável

Mais eficaz

simplificando a conectividade e o gerenciamento de políticas

Mais produtiva

garantindo experiências do usuário rápidas, confiáveis e consistentes em qualquer lugar

Mais ágil

inovando rapidamente para atender aos requisitos de segurança em constante evolução

RESILIÊNCIA NA CLOUDFLARE

Execute tarefas de inferência no Workers AI, a primeira plataforma de inferência de IA sem servidor distribuída globalmente

mais de 335 cidades

em mais de 125 países, incluindo a China Continental

O código é executado dentro de 50 ms de aproximadamente 95% da população global conectada à internet

mais de 190 cidades

com GPUs

Constelação crescente de cidades para inferência de IA alimentada por GPUs

Implante a partir da região:

Terra

RESILIÊNCIA NA CLOUDFLARE

Lutando pela internet aberta

A internet é um milagre. A conexão de diversas redes com padrões comuns nos permite trocar dados em todo o mundo de uma forma resiliente, interoperável e acessível a qualquer pessoa. Hoje, dependemos dela para o crescimento econômico e a inovação, o acesso à informação e liberdade de expressão, bem como o estado de direito e os princípios democráticos.

A Cloudflare tem orgulho de fazer parte da comunidade global que defende a internet.

- Defender a neutralidade da rede
- Monitorar locais onde a internet não é aberta
- Proteger os direitos humanos e as instituições democráticas
- Implantar padrões que melhoram a privacidade e a segurança dos fluxos de dados
- Participar do desenvolvimento de padrões da internet
- Apoiar a governança da internet multisetorial

CLOUDFLARE

2025

Relatório sobre sinais da Cloudflare

Saiba mais

Resiliência em escala

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-6966.2025APR24

Notas

As conclusões deste relatório se baseiam, principalmente, nos padrões de tráfego agregados observados em toda a rede global da Cloudflare entre 2 de janeiro de 2024 e 31 de dezembro de 2024.

1. https://www.darktrace.com/blog/survey-findings-ai-cyber-threats-are-a-reality-the-people-are-acting-now/
2. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html
3. Análise do Cloudflare Radar, 2024
4. https://www.cnbc.com/2025/02/24/chegg-sues-google-for-hurting-traffic-as-it-considers-alternatives.html; https://www.theguardian.com/gnm-press-office/2025/feb/25/make-it-fair
5. Análise do Cloudflare Radar, 2024
6. https://nationalcioreview.com/wp-content/uploads/2024/07/2023_Insider_Threat_Report-16d8d8f7.pdf
7. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai
8. https://www.verizon.com/business/resources/T1e3/reports/2024-dbir-data-breach-investigations-report.pdf
9. Análise do Cloudflare Radar, 2024. https://radar.cloudflare.com/bots
10. https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials/; https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
11. Análise do Cloudflare Radar, 2024
12. Análise do Cloudflare Radar, 2024
13. https://blog.talosintelligence.com/how-are-attackers-trying-to-bypass-mfa/
14. https://therecord.media/advance-auto-parts-data-breach-2million
15. Análise do Cloudflare Radar de 12 de outubro de 2024 a 31 de dezembro de 2024.
16. Análise do Cloudflare Radar de 12 de outubro de 2024 a 31 de dezembro de 2024. https://radar.cloudflare.com/security/application-layer
17. Análise do Cloudflare Radar, 2024. https://blog.cloudflare.com/tag/ddos-reports/
18. Análise do Cloudflare Radar, 2024. https://radar.cloudflare.com/reports/ddos-2024-q4
19. https://reports.weforum.org/docs/WEF_Global_Cyber security_Outlook_2025.pdf
20. https://www.verizon.com/business/resources/Tdd6/reports/2024-dbir-data-breach-investigations-report.pdf
21. Análise do Cloudflare Radar, 2024
22. https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf
23. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-survey-findings-on-esg-disclosure-and-preparedness.pdf
24. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
25. Análise do Cloudflare Radar, 2024. https://radar.cloudflare.com/adoption-and-usage
26. https://www.ey.com/en_us/board-matters/cyber-disclosure-trends
27. https://www.cloudflare.com/threat-intelligence/research/report/inside-lameduck-analyzing-anonymous-sudans-threat-operations/
28. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam
29. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024
30. Análise do Cloudflare Radar, outubro de 2024 a fevereiro de 2025
31. Análise do Cloudflare Radar, janeiro de 2025