CLOUDFLARE

Impacto para a empresa

Como o Zero Trust reduz o risco e melhora a eficiência da tecnologia

Proteja mais – com menos sobrecarga

Quantificar os impactos financeiros e de segurança das melhores práticas do Zero Trust

Reduzir o risco cibernético

95% de redução da superfície de ataque com uma arquitetura SASE, que inclui princípios Zero Trust integrados [1]

72% dos líderes de TI dizem que o principal motivo para a adoção do Zero Trust foi "fortalecer a segurança dos dados" [2]

61% dos profissionais de TI/segurança citam "autenticação mais forte usando identidade e postura de risco" como um benefício [3]

↓23% do custo médio reduzido de uma violação de dados na comparação entre organizações com e sem Zero Trust implantado [4]

Custo médio de uma violação de dados (Bilhões de US$)

Impulsionadores

- Reduzir a confiança excessiva com controles baseados em identidade e contexto para todas as solicitações
- Visibilidade aprimorada de todos os usuários, aplicativos e dispositivos para uma correção mais rápida
- Movimento lateral de ameaças reduzido

Melhorar a eficiência da tecnologia

US$ 7 milhões de redução no gasto médio em segurança legada ao adotar o Zero Trust em cinco organizações [5]

US$ 20 por FTE por mês economizados com a substituição de serviços de segurança redundantes por uma plataforma Zero Trust baseada em nuvem [5]

↓80% de redução do esforço necessário para provisionar e proteger a nova infraestrutura [5]

39% das tecnologias de segurança usadas pelas organizações estão desatualizadas e podem ser modernizadas com o Zero Trust [6]

As principais consequências para as equipes de segurança [7]

Número 1 Perdas financeiras devido a violações de dados ou ataques cibernéticos bem-sucedidos

nº 2 Incapacidade de inovar tão rapidamente quanto as oportunidades de mercado permitem

nº 3 Falta de resiliência operacional

Impulsionadores

- Complexidade reduzida ao consolidar soluções pontuais legadas em uma única plataforma em nuvem
- Fluxos de trabalho de segurança simplificados sem tráfego de backhauling pelos dispositivos no local
- Políticas consistentes para toda a sua força de trabalho híbrida

+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

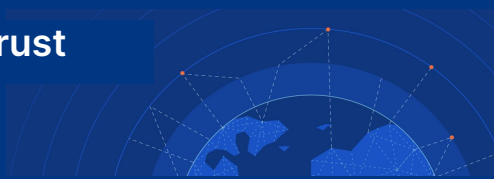
REV:PMM-2022NOV

O Zero Trust é uma mudança de mentalidade estratégica para sua organização

Segurança de TI legada: O perímetro determina a confiança		Zero Trust: Não importa o perímetro, sempre verificar
Perímetro seguro, rede interna segura (ou seja, "castelo e fosso")	TCP e UDP	Assume o risco, reduz o impacto (criptografa, inspeciona, faz microssegmentação)
Permitir o login apenas no perímetro	SIEM	Registra todos os logins e solicitações em todos os lugares
O padrão é permissão, acesso estático com base no local da rede	Controle	O padrão é negação, privilégio mínimo com base na identidade e no contexto

Comece a reduzir o risco cibernético com o Zero Trust

Solicite uma consulta



Ainda não está pronto para sua consulta?

- Descubra como o Zero Trust melhora a produtividade da equipe: leia o resumo
- Saiba mais sobre como organizações semelhantes lidam com o trabalho híbrido: leia o resumo
- Explore um roteiro independente de fornecedor para alcançar o Zero Trust: leia o artigo técnico

1. Com base nas experiências do cliente da Cloudflare
2. "Capterra's 2022 Zero Trust Survey," agosto de 2022 (Link)
3. "Global Study on Zero Trust Security for the Cloud," Ponemon Institute LLC, julho de 2022 (Link)
4. "The Cost of a Data Breach Report," IBM, 2022 (Link)
5. "The Total Economic Impact ™ of Zero Trust Solutions from Microsoft," Forrester Research, dezembro de 2021 (Link)
6. "Security Outcomes Study," Cisco, dezembro de 2021 (Link)
7. "2022 Global Digital Trust Insights," PWC, setembro de 2022 (Link)

+55 (11) 3230.4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:PMM-2022NOV