The ROI of Zero Trust

5 ways reducing your attack surface with a Zero Trust security strategy saves your business time and money

CLOUDFLARE

01

Reduce attack surface

Based on Gartner's assumptions, organizations that isolate high-risk browsing from end user systems and isolate application access from networks will achieve a 91% reduction in attacks that can reach their environment.[1]

02

Reduce breach costs

With less attack surface comes greater protection from destructive data breaches. According to IBM's Cost of a Data breach report, organizations with mature Zero Trust adoption levels pay less to recover from data breaches, with mature Zero Trust organizations paying $3.28M compared to $5.04M for organizations without a Zero Trust strategy.[2]

03

Accelerate onboarding

When adopting Zero Trust goes hand in hand with replacing legacy remote access approaches like the VPN and IP-based controls, organizations like Cloudflare customer eTeacher Group report that they spend less time onboarding new users, reducing the amount of time it takes to grant access to a new user by as much as 60%.

04

Reduce IT tickets

When users don't have to deal with a VPN client on their device, organizations start to see a big drop in the amount of time they spend addressing access-related tickets, with some organizations reporting an up to 80% reduction in time spent servicing user issues.

05

Reduce latency

Adopting Zero Trust approaches to Internet browsing and application access significantly impacts your business connectivity speed. It avoids hairpinning traffic to a data center far away from users or resources, and when users connect to resources through Cloudflare's network rather than default Internet routes, public and private web apps load 30% faster and TCP connection's round trip time is 17% faster.

Start in under 30 minutes

Scale effortlessly

Finish with an industry-best ROI-to-time ratio

Reduce Attack Surface

Reduce Breach Costs

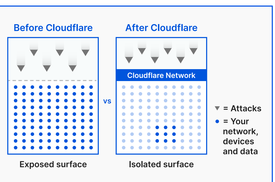
Accelerate Onboarding

Reduce IT Tickets

Reduce Latency

That means built-in layers of protection against:

- malware lateral movement
- ransomware
- phishing
- VPN vulnerabilities
- supply chain or MFA bypass attacks

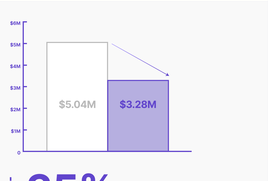


91%

Minimizes successful attacks by up to 91%

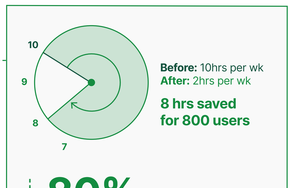
30%

Makes it 30% faster to connect to apps and services



35%

Reduces the average cost of a data breach by 35%, from $5.04M to $3.28M



80%

Decreases time spent addressing remote access IT tickets by up to 80%

60%

Accelerates new employee onboarding time by up to 60%

01

Start in under 30 minutes

Cloudflare's Zero Trust security platform increases visibility, eliminates complexity, and reduces risks as employees connect to applications and the Internet. It takes as little as 30 minutes of setup time to get started.

02

Scale effortlessly

Quickly scale Zero Trust security policies to new users around the globe, because Cloudflare's Zero Trust services are deployed consistently in every one of our 250+ cities around the world.

03

Finish with an industry-best ROI-to-time ratio

Support your vast range of application types and protocols, with fast and easy onboarding. You'll never manually manage bandwidth, or pay more as your requests increase.

Ready to start?

Click here

[1]Combines assumptions from two Gartner publications — Innovation Insight for Remote Browser Isolation, 8 March 2018, and It's Time to Isolate Your Services From the Internet Cesspool, 17 November 2017

[2]IBM, Cost of a Data Breach Report, 2021