

# How Zero Trust Reduces Risk and Improves Technology Efficiency

Secure more – with less overhead

## Quantifying the financial and security impacts of Zero Trust best practices

### Reduce cyber risk

**95%**

attack surface reduction with a SASE architecture, which includes built-in Zero Trust principles <sup>1</sup>

**72%**

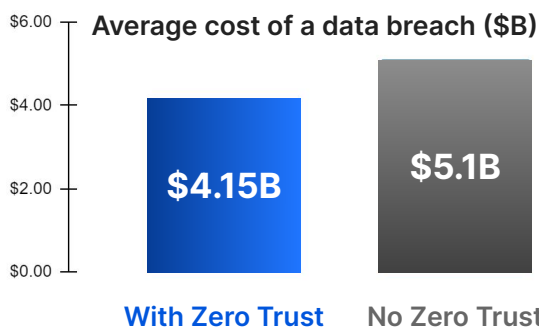
of IT leaders say the top reason for their Zero Trust adoption was to “strengthen data security” <sup>2</sup>

**61%**

of IT / security pros cite “stronger authentication using identity and risk posture” as a benefit <sup>3</sup>

**↓ 23%**

reduced average cost of a data breach at organizations with Zero Trust deployed vs. without <sup>4</sup>



### Drivers

- Reduce excessive trust with identity- and context-based controls for every request
- Enhanced visibility across all users, applications, and devices for faster remediation
- Reduced lateral movement of threats

### Improve technology efficiency

**\$7M**

reduced average spend on legacy security by adopting Zero Trust across five organizations <sup>5</sup>

**\$20 per FTE**

per month saved by replacing redundant security services with a cloud-based Zero Trust platform <sup>5</sup>

**↓ 80%**

reduced effort required to provision and secure new infrastructure <sup>5</sup>

**39%**

of security technologies used by organizations are outdated and can be modernized with Zero Trust <sup>6</sup>

### Top consequences of cybersecurity complexity <sup>7</sup>

**#1**

Financial losses due to successful data breaches or cyber attacks

**#2**

Inability to innovate as quickly as market opportunities allow

**#3**

Lack of operational resilience




### Drivers

- Reduced complexity by consolidating legacy point solutions onto a single cloud platform
- Simplified security workflows without backhauling traffic through on-prem appliances
- Consistent policies across your hybrid workforce

# Zero Trust is a strategic mindset shift for your organization

**Legacy IT security:**  
Perimeter determines trust

**Zero Trust:**  
No perimeter, always verify

Secure perimeter, safe inside network (i.e. "castle & moat")	 Protection	Assume risk, reduce impact (encrypt, inspect, microsegment)
Log only login at the perimeter	 Visibility	Log every login and request everywhere
Default allow, static access based on network location	 Control	Default deny, least privilege based on identity and context

Start unlocking team productivity with Zero Trust

## Not yet ready for your consultation?

- Discover how Zero Trust reduces risk and improves technology efficiency
- Learn more about how peer organizations tackle hybrid work
- Explore a vendor-agnostic roadmap to achieve Zero Trust

1. Based on Cloudflare customer experiences
2. "Capterra's 2022 Zero Trust Survey," August 2022 ([Link](#))
3. "Global Study on Zero Trust Security for the Cloud," Ponemon Institute LLC, July 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, December 2021 ([Link](#))
6. "Security Outcomes Study," Cisco, December 2021 ([Link](#))
7. "2022 Global Digital Trust Insights," PWC, September 2022 ([Link](#))

