CLOUDFLARE

BUSINESS IMPACT

Top 10 Productivity Improvements

96% of security leaders say developing a Zero Trust strategy is their #1 priority.[1] Find out how Zero Trust delivers value for organisations.

Zero Trust unlocks productivity across the organization

For IT and security administrators

65%	of IT decision makers and security professionals say Zero Trust increases the productivity of IT security teams [2]
↓80%	decreased time spent addressing remote work IT tickets with Zero Trust vs VPN access [3]
↑50%	average increased operational efficiency of security teams across five sample orgs implementing Zero Trust [4]
35%	increased likelihood to report strong SecOps among orgs with mature implementations of Zero Trust / SASE [6]
↓29%	reduction in solution complexity and the # of integration points with a Zero Trust platform vs. legacy architecture [7]

Productivity drivers

- Granular controls without additional overhead
- Simplified initial deployment, ongoing policy management, and scaling across users and apps
- Reduced complexity by consolidating point services onto a single Zero Trust cloud platform
- Less time spent fixing problems and vulnerabilities with legacy systems

For end users

53%	of IT decision makers and security professionals say Zero Trust improves the user experience [2]
↑60%	accelerated time for new employee onboarding by provisioning Zero Trust vs. VPN access to applications [3]
85%	of IT leaders agree that an improved employee experience translates to higher revenue [5]
3 days	saved annually by enabling secure BYOD and Zero Trust access to key resources for frontline workers [4]
65%	of employees believe they would be more productive if they had better technology at their disposal [8]

Productivity drivers

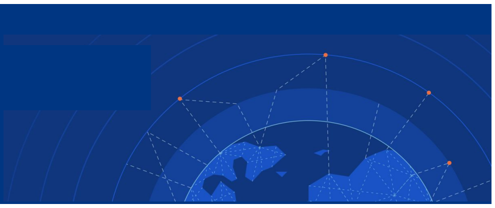
- More transparent, less intrusive security checks
- Faster onboarding / offboarding of employees, contractors, suppliers, and third parties
- Simplified authentication workflows without any backhauling traffic through on-pem appliances
- Reduced idle time because of issues related to connectivity, access, or security policies

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

Request a consultation



Not yet ready for your consultation?

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

1. “Microsoft Zero Trust Adoption Report,” July 2021 (Link)
2. “Global Study on Zero Trust Security for the Cloud,” Ponemon Institute LLC, July 2022 (Link)
3. Cloudflare case studies (Link)
4. “The Total Economic Impact ^{TM} of Zero Trust Solutions from Microsoft,” Forrester Research, December 2021 (Link)
5. Loomis, Amy and Webber, Alan, “Driving Bottom-Line Value by Linking Customer Experience to Employee Experience,” IDC Research, January 2022 (Link)
6. “Security Outcomes Study,” Cisco, December 2021 (Link)
7. “Realizing Cybersecurity Value,” Palo Alto Networks, September 2022, (Link)
8. “The need for improved digital employee experience: How technology enables better employee retention and productivity,” Ivanti, 2022, (Link)