

Adopting a Zero Trust approach is a technology and business imperative

A Zero Trust strategy is more than a technological shift for security teams—it's a driver of business agility.

A Zero Trust model is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction; asserts least-privilege access; and relies on intelligence, advanced detection, and real-time response to threats.

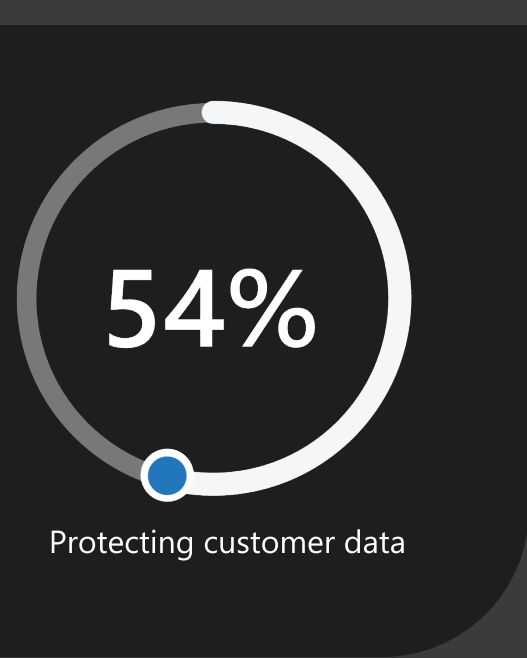
The guiding principles of Zero Trust security are:

- Verify explicitly.
- Use the least-privilege access.
- Assume breach.

When you adopt a Zero Trust approach, you can:

- Support remote and hybrid work.
- Prevent or reduce business damage from a breach.
- Identify and protect sensitive business data and identities.
- Proactively meet regulatory requirements.
- Build confidence in your security posture and programs across your leadership team, employees, partners, stakeholders, and customers.

Benefits captured since implementing Zero Trust¹



- Productivity
- Risk reduction
- Compliance



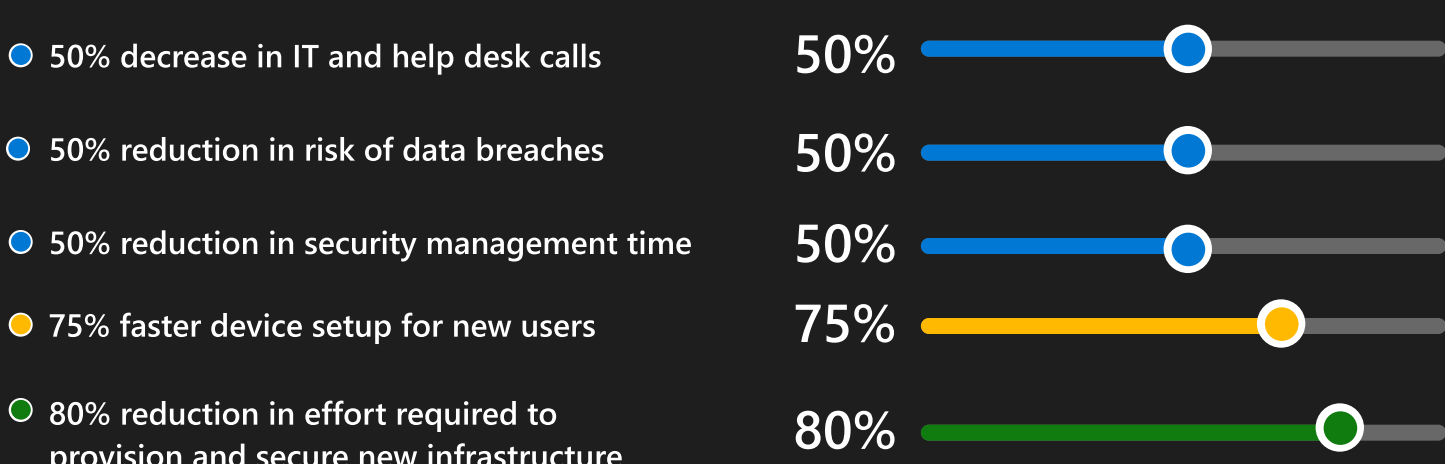
12% of respondents said they were achieving **all** of these benefits.

Around 66% of survey respondents said they were capturing benefits from most aspects of their projects within a year.¹

Value of Zero Trust security across your organization

Microsoft customers have seen an average of 92 percent return on investment within less than six months of implementing a Zero Trust approach.²

Other trends² reported include:



Over **\$7 million** in reduced spending on legacy software and infrastructure

Get started

With a Zero Trust strategy, you can deliver improved and modernized security while driving tangible business results.

Reach out to your Microsoft representative or visit aka.ms/zerotrusted.