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.

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 shift in the way we think about security. A Zero Trust approach is a practical, purpose-driven approach to security across all layers of the digital estate that explicitly and continuously verifies every action, whether that action is from inside or outside the perimeter. Zero Trust addresses security at its core, not just any access points to the network.

The guiding principles of Zero Trust security are:

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

Benefits captured since implementing Zero Trust:

- Continuity of access and authentication: 71%
- Managing access to cloud apps and devices: 62%
- Facilitating the move to remote work: 62%
- Securing access with least-privilege access: 49%
- Reducing the complexity of integration: 47%
- Reducing time to breach: 42%
- Enhancing both security and user experience: 41%
- Efficiently mitigating information discovery: 37%

17% 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.

Value of Zero Trust security across your organization:

- Over $7 million in reduced spending on legacy software and infrastructure.
- Microsoft customers have seen an average of 92% return on investment within less than six months of implementing a Zero Trust approach.
- On average, 50% reduction in help desk calls.
- 50% reduction in security management time.
- 75% faster device setup for new users.
- 80% reduction in effort required to provision and secure new infrastructure.
- 50% productivity increase.

Adopting a Zer o T r ust ap pr o ach is a te chnology and bus iness imperativ e.

A Z er o T r ust strat egy is mor e than a te chnological shif t for se curi ty teams—it’ s a driver of bus iness agility.

A Z er o T r ust model is a proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every action, whether that action is from inside or outside the perimeter. Zero Trust addresses security at its core, not just any access points to the network.

The guiding principles of Zero Trust security are:

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

Benefits captured since implementing Zer o Trust:

- Continuity of access and authentication: 71%
- Managing access to cloud apps and devices: 62%
- Facilitating the move to remote work: 62%
- Securing access with least-privilege access: 49%
- Reducing the complexity of integration: 47%
- Reducing time to breach: 42%
- Enhancing both security and user experience: 41%
- Efficiently mitigating information discovery: 37%

17% 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.

Value of Zero Trust security across your organization:

- Over $7 million in reduced spending on legacy software and infrastructure.
- Microsoft customers have seen an average of 92% return on investment within less than six months of implementing a Zero Trust approach.
- On average, 50% reduction in help desk calls.
- 50% reduction in security management time.
- 75% faster device setup for new users.
- 80% reduction in effort required to provision and secure new infrastructure.
- 50% productivity increase.

Get started

With a Zero Trust strategy, you can deliver improved and secure user experience while enabling agility across your organization.

Microsoft Security
www.microsoft.com/security