Microsoft

Zero Trust Business Plan

A practical guide to implementing the Zero Trust framework at your organization

Contents

Digital transformation is shaping the new normal

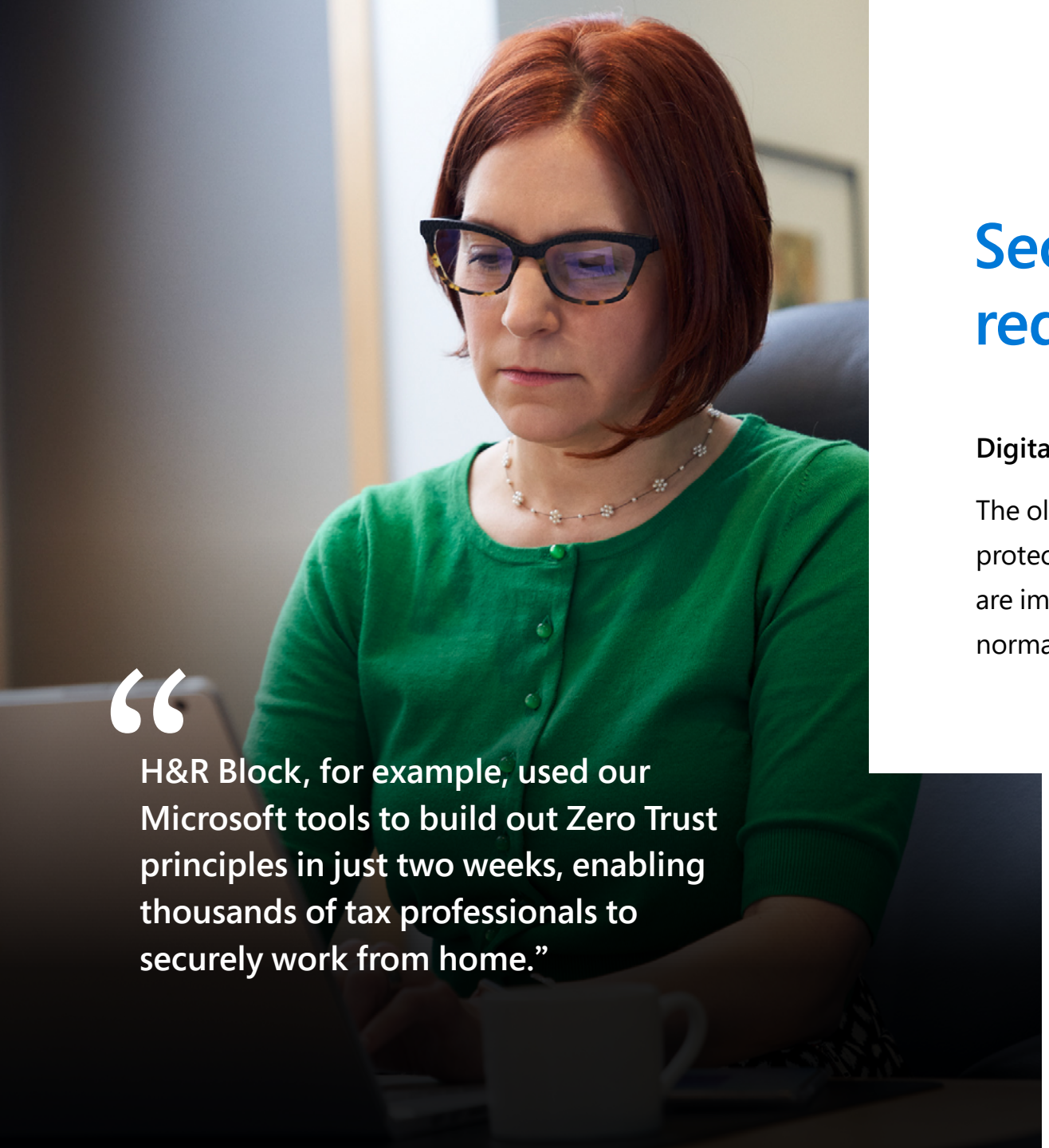
Organizations are embracing digital transformation to manage continuous business environment changes:

- → Shifting business models and partnerships
- → Technology trends
- → Regulatory, geopolitical, and cultural forces

COVID-19 remote work accelerated transformation and often transforms security from a cost-center to a strategic driver for growth.

“COVID taught everyone it’s not going to be all peachy and you’re going to have to be able to adjust very quickly in the future. The closer we get to a zero trust model, it shouldn’t matter whether we are operating out of a garage, the cloud, or a datacenter”

–Manager, Identity & Access Solutions, at financial services company



“H&R Block, for example, used our Microsoft tools to build out Zero Trust principles in just two weeks, enabling thousands of tax professionals to securely work from home.”

Securing digital transformation requires Zero Trust

Digital transformation forces re-examination of traditional security models

The old way of security does not provide business agility, user experiences, and protections needed for a rapidly evolving digital estate. Many organizations are implementing Zero Trust to alleviate these challenges and enable the new normal of working anywhere, with anyone, at any time.

These learnings and best practices are derived from conversations with customers and our own experience implementing Zero Trust at Microsoft.

Pragmatic Zero Trust adoption: Think big, start small, move fast

Develop a multiyear business plan to:

Prioritize quick wins
and incremental progress for each initiative.

Embrace existing technologies
already deployed or licensed.

Structure coherent initiatives
with clear outcomes, benefits, and ownership.

Adopting Zero Trust

We've created an actionable best practices framework to help guide you through your own Zero Trust journey. Each phase includes guidance, best practices, resources, and tools to help you drive your own implementation.

01 Plan

Build a business case focused on the outcomes that are most closely aligned with your organization's risks and strategic goals.

02 Implement

Create a multiyear strategy for your Zero Trust deployment and prioritize early actions based on business needs.

03 Measure

Track the success of your Zero Trust deployment to provide confidence that the implementation of Zero Trust provides measurable improvements.

Zero Trust Plan: What good looks like

Recommended prioritization:

- → **Define a vision** – Zero Trust is a multifaceted journey that can span many years. Clearly **defining** the goals, outcomes, and architectures make organizations more successful than taking a reactive approach.

Note: The benefits and implementation often appear very different depending on your roles and responsibilities.

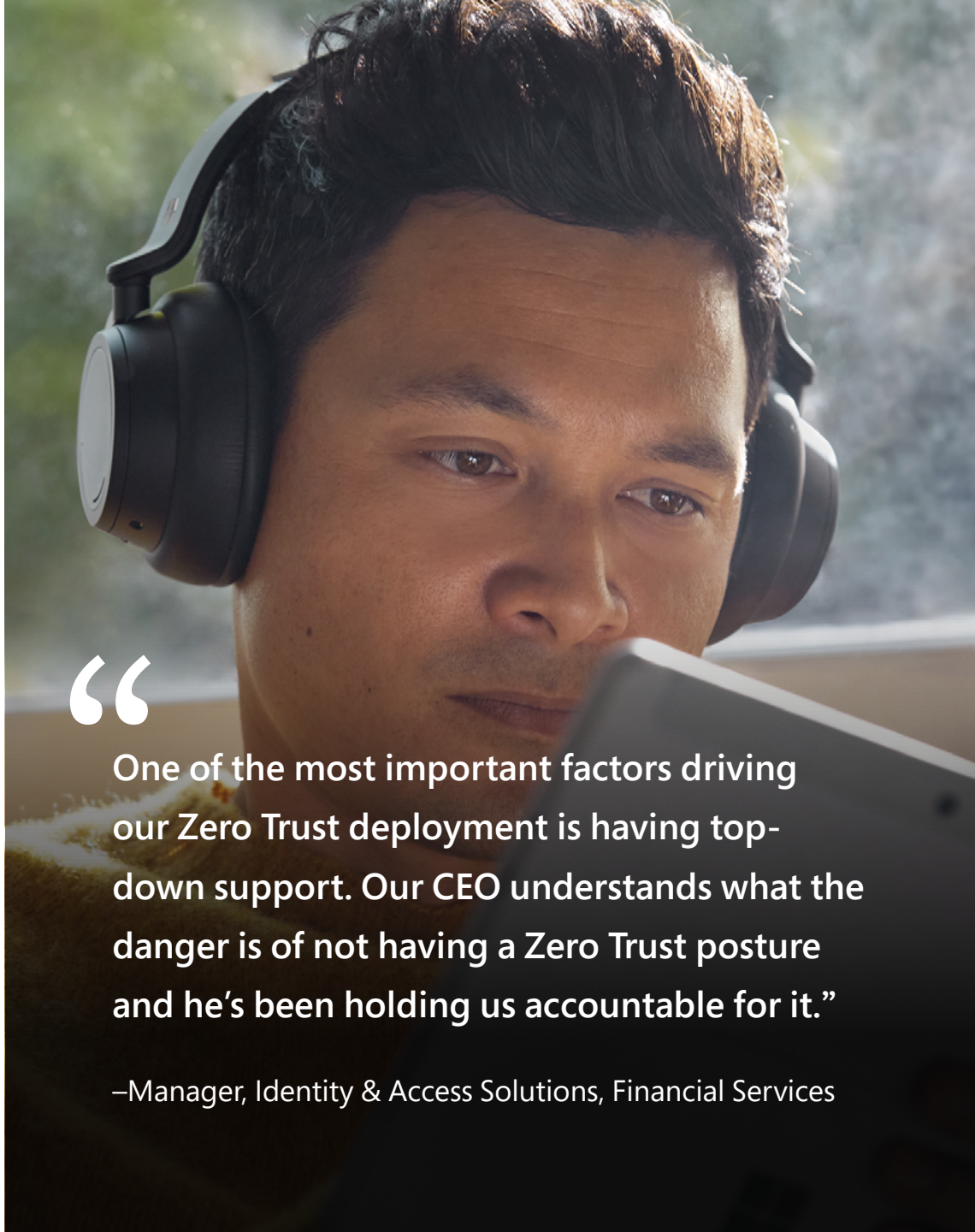
- → **Get buy-in from leadership** – Successful Zero Trust implementations focus on business outcomes to get leadership support for ambitious goals, budget allocations, and internal alignment.
- → **Empower end users** – Zero Trust allows technology teams to engage directly with end users to make security a driving force to improve their experiences and productivity.

Define a vision and get leadership buy-in

The first step in getting leadership support is to ask for and closely listen to business priorities, then developing a vision that focuses on business outcomes.

While you must always tailor this vision to the business priorities and culture, we have seen several common themes emerge across organizations:

- **Business agility** to quickly pursue and capture new opportunities while managing risk, enabling remote work, and migrating to the cloud.
- **Managing complexity** from continuous shifts in business partnerships, competition, and dynamic technical environment.
- **Measurability** to ensure accountability for business and risk outcomes.



> “One of the most important factors driving our Zero Trust deployment is having top-down support. Our CEO understands what the danger is of not having a Zero Trust posture and he’s been holding us accountable for it.”
>
> –Manager, Identity & Access Solutions, Financial Services

Build a strong business case for Zero Trust

A strong business case helps you obtain executive support and drive alignment across business functions. While there are many benefits to a Zero Trust security model, organizations typically see the most success using these four business cases:

- → Support work from anywhere at any time.
- → Enable secure and rapid cloud migration.
- → Realize cost savings through simplification of the security stack.

Focus on the resulting benefits to the business, including:

- → **Proactive risk avoidance** and management.
- → **Risk management for partners** with weak security programs.
- → **Security and compliance agility** to accommodate rapid changes in status of roles and organizations.

PLAN 〉 **IMPLEMENT** 〉 MEASURE

Zero Trust Implementation: What good looks like

Structure the program into clear and coherent initiatives. Microsoft has found that technical strategies and architectures naturally group into these security initiatives:

- Productivity security
- Modern security operations
- Operational technology (OT) and Internet of Things (IoT), *if applicable to the organization*
- Datacenter, services, and API

These are based on Microsoft's experience and other successful customer implementations.

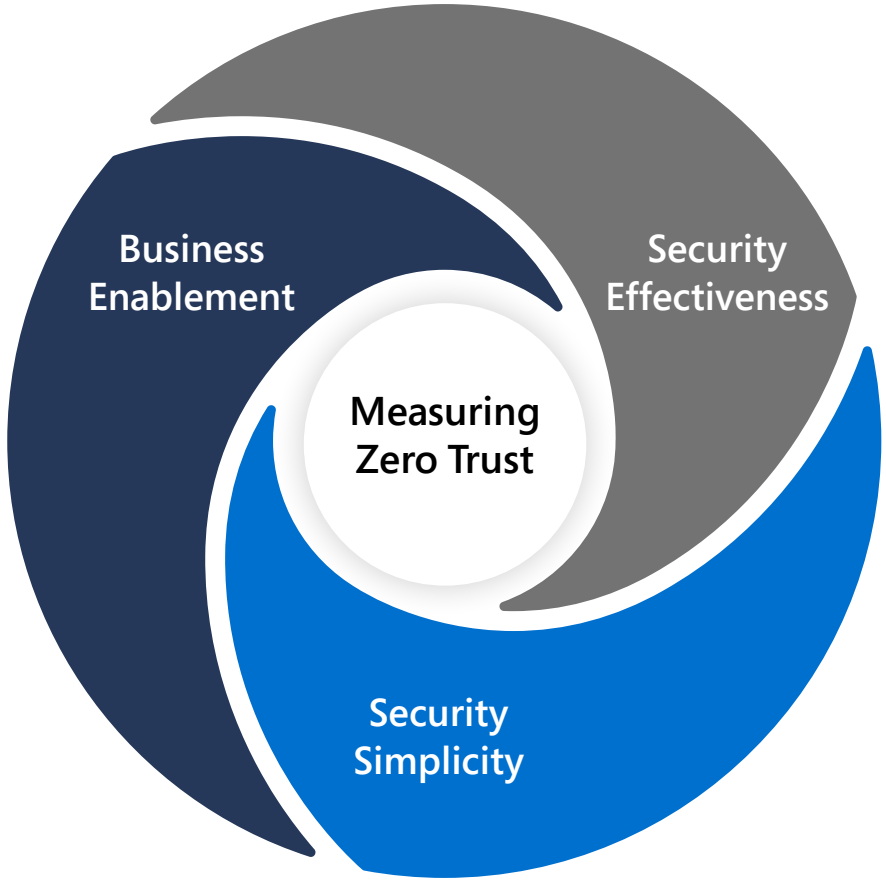
Prioritize and plan the initiatives:

- **Align each initiative to business goals** and evaluate potential positive business impact, friction, and challenges.
- **Make a short term plan.** Start with quick wins and find executive sponsors.
- **Develop a long-term roadmap.**

Measure Progress – What good looks like

Identify key milestones and performance goals for your organization, measure them, and report on success and learnings.

- **Business enablement**—measure friction in the user experience, and how long it takes for internal security approval of initiatives.
- **Security Effectiveness**—identify the reduction in quantity or impact of security incidents after the organization adopts a Zero Trust strategy.
- **Security simplicity**—reduce the number of security vendors that teams have to integrate and lower costs from manual tasks (such as password reset calls).

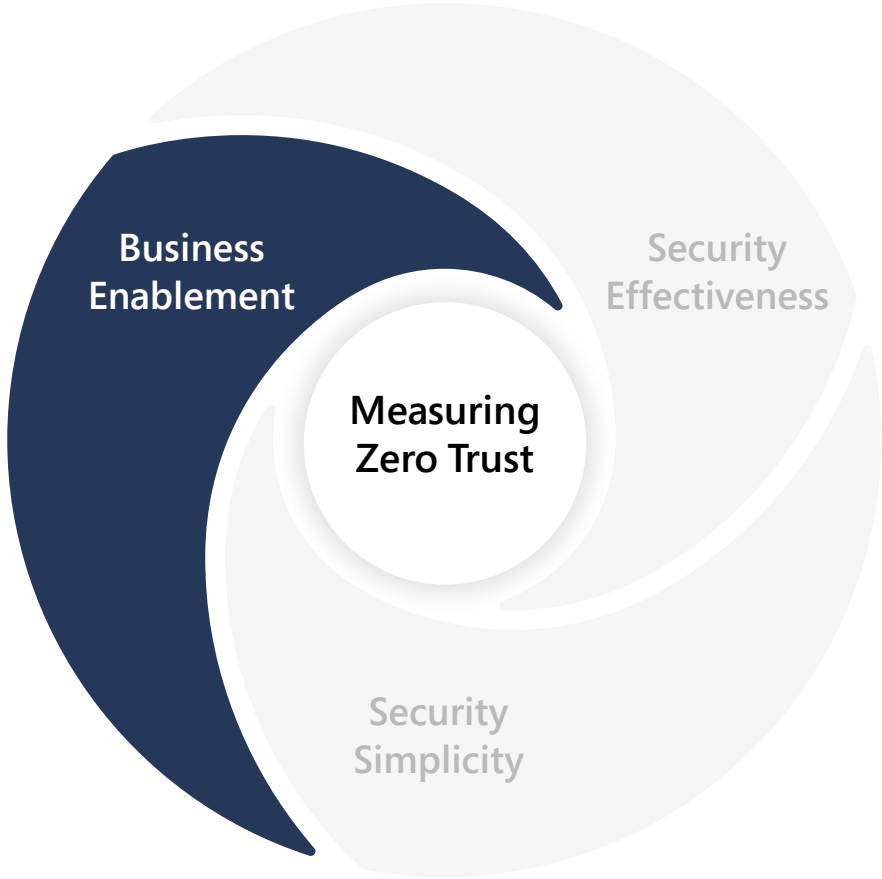


Measure your business enablement improvement

Zero trust should aspire to frictionless user and developer experiences:

- Number of security interruptions in user workflow (such as, multi-factor authentication prompts in a day).
- Deployment milestones (such as percentage of employees accessing apps through single sign-on).
- Visibility milestones (such as drops in app usage due to poor login experience).
- Number of seconds average boot time for managed devices.
- Number of days average for security evaluation of applications.

Don’t forget end-user listening mechanisms, survey users on access ease of use, password resets process, etc.



Measure security effectiveness

Measure your security posture and the resulting impact from security incidents:

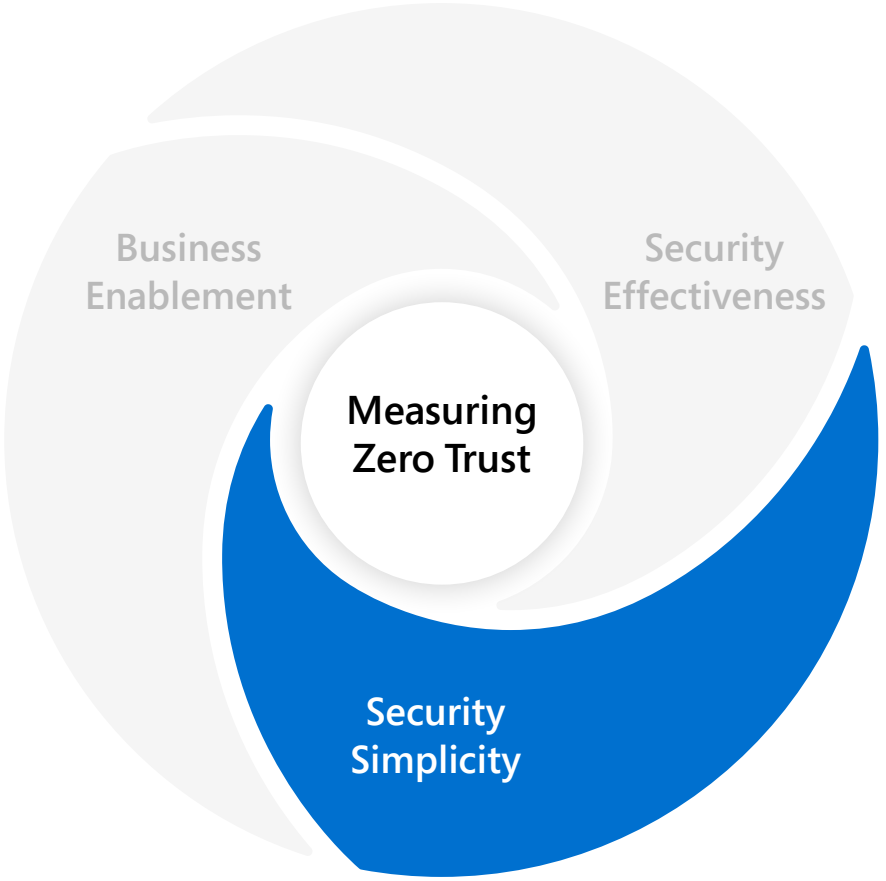
- Number of security incidents (by severity).
- Deployment milestones (such as percentage of employees actively using MFA).
- Visibility milestones (such as percentage of devices/apps that are managed).
- Security posture—track improvements in Microsoft Secure Score.

Keep it in context: As your visibility improves with Zero Trust, you may discover more incidents that were previously missed.

Measure security simplicity

Zero Trust frequently helps simplify the requirements to achieve security

- Number of duplicative security tools that perform similar or identical functions.
- Number of security tools that require custom integration.
- Percentage of time IT help desk spent on low-value activities like password resets.
- Number of manual steps in repetitive workflows (such as investigating common alerts/incidents, manually provisioning users, compliance reporting tasks).
- Percentage of false positive alerts investigated by security teams.
- Ratio of time spent on tool maintenance versus actual incident response.



Zero Trust is a key survival skill for digital transformation

You don’t have to rip and replace technology to get started.

Start by aligning your Zero Trust investments to your current business needs and focusing on getting quick wins. Each win adds incremental value to reduce risk and improving the security posture of your digital estate.

It’s never too late to get started and no scope is too small.

> “Since implementing a Zero Trust strategy using Microsoft 365 technologies, our employees can fulfill their company duties from anywhere in the world while maintaining tight control over core security needs.”

–Igor Tsyganskiy, Chief Technology Officer, Bridgewater Associates

What's next?

Thanks for reviewing our Zero Trust best practices guide. If you haven't already, please check out our Microsoft Zero Trust Maturity Model vision paper (click to download) detailing the core principles of Zero Trust, and our maturity model, which breaks down the top-level requirements across each of the six foundational elements.

We've also compiled useful learnings, technical guidance, and other resources on our external Microsoft Zero Trust site.


Microsoft