Zero Trust phase grid tracker

Microsoft Zero Trust adoption framework

aka.ms/zero-trust-adopt

A blueprint for Zero Trust architecture

At Microsoft, there's no one-size-fits-all list of tasks that results in Zero Trust, like other roadmaps attempt to do, Instead, Microsoft helps you create a strategy and map to address your unique organization risks and business priorities.

The Microsoft Zero Trust adoption framework:

- Shows you how to get started.
- Helps you identify your risks and develop your strategy.
- Gives you the flexibility to make progress based on your unique risks, business priorities, and resources.
- Provides paths to help you move from starting point to maturity.

Support your strategy with Zero Trust business scenarios

Zero Trust business scenarios align the strategy and technical work of Zero Trust to business outcomes your leaders care about. Each scenario leads you through a staged approach to building strategy and maturing your security posture. Each scenario addresses specific technical pillars of Zero Trust architecture.

How to use this Zero Trust phase grid tracker

This guide provides a blueprint for building Zero Trust architecture. You decide which paths are most strategic for your business. This tracker provides an at-a-glance view.

Customize your journey

To customize this tracker:

- Download the Visio file.
- Re-order or customize the goals.
- Plug in your own security tools.
- Create your own custom path using the template on the **Customization** page.

Other Zero Trust trackers

The Zero Trust journey is highly collaborative and involves many stakeholders. Microsoft provides Zero Trust trackers for your different audiences. Each of these trackers can be adapted to fit your organization's strategy and objectives:

- **Grid tracker** (what you see here)
- **Business leader tracker** (PowerPoint)
- **Implementer tracker** (Excel)
- **Microsoft Security Exposure Management, Zero Trust Initiative** (a dashboard)
- **Zero Trust Assessment** (an automated Excel file)

For information about these trackers, see aka.ms/zero-trust-trackers.

Zero Trust business scenarios help you work together with your C-suite and other business leaders to gain buy in and track progress

Business scenario	Identities	Endpoints	App data	Apps	Privileged access	Threat protection	Security operations	Network	Infrastructure	Backup & restore
Secure remote and hybrid work	✓	✓						✓		
Identify and protect sensitive business data			✓	✓				✓		
Implement threat protection and XDR						✓	✓	✓		
Implement security breach prevention and recovery infrastructure					✓			✓	✓	✓
Meet regulatory and compliance requirements			✓	✓						

Contact

Name: Firstname Lastname
Phone: (555) 555-5555
Email: example@contoso.com

Name: Firstname Lastname
Phone: (555) 555-5555
Email: example@contoso.com

Zero Trust business scenario		Stage 1		Stage 2		Stage 3		Stage 4	
Rapidly modernize your security posture	**Security enhanced for...**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**
	Overall posture Digital assets IT and IoT assets User awareness SecOps processes	Identify risks to your organization	▮▮	Develop a response readiness plan	▮▮	Visualize your security posture using audience-appropriate dashboards	▮	Continuously educate your users	▮▮
		Capture your initial Secure Score status	▮	Inventory your digital estate	▮▮▮	Document and manage shadow IT using Microsoft Defender for Cloud Apps	▮▮	Evolve your organization's SecOps capabilities	▮▮
		Identify regulatory requirements	▮▮	Update your status for Secure Score	▮▮				
		Set leadership expectations	▮	Capture your status in Compliance Manager	▮	Develop a patching and updating methodology	▮▮	Continue to manage risk	▮▮
Secure remote and hybrid work	**Security enhanced for...**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**
	User account credentials Endpoints Applications Application data Networks	Verify and secure every identity with strong authentication	▮▮	Register devices with Microsoft Entra ID	▮▮	Enroll devices in your device management solution and apply recommended security protections	▮▮	Monitor device configuration drift	▮▮
		Integrate SaaS apps with Microsoft Entra ID for single sign-on	▮▮	Implement **Starting point** Zero Trust identity and device access policies	▮▮				
		Use modern authentication for all new applications	▮▮	Use application proxy with on-premises apps for single sign-on	▮▮	Allow only compliant and trusted devices to access data	▮▮	Implement password-free authentication	▮▮
Identify and protect sensitive business data	**Security enhanced for...**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**
	Sensitive data in the cloud and on-premises SaaS apps Network communication External access Microsoft Teams for highly-sensitive projects	Discover and identify sensitive business data	▮▮▮	Develop and test a classification schema	▮▮	Add protection to specific labels (encryption and other protection settings)	▮▮	Extend labels and protection to data in SaaS apps, including DLP	▮▮
		Discover non-sanctioned SaaS apps	▮▮	Apply labels to data across Microsoft 365	▮▮	Introduce automatic and recommended labeling in Office apps and services	▮▮	Extend automated classification to all services	▮▮
		Encrypt network communication	▮	Introduce basic DLP policies	▮▮	Extend DLP policies across Microsoft 365 services	▮	Extend labels and protection to data at-rest in on-premises repositories	▮▮
				Set up secure Microsoft Teams for sharing data internally and externally with business partners	▮	Implement key insider risk management policies	▮▮	Protect organization data in your cloud infrastructure	▮▮

Zero Trust business scenario		Stage 1		Stage 2		Stage 3		Stage 4	
Implement security breach prevention and recovery infrastructure	**Security enhanced for...**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**
	Privileged accounts Networking infrastructure Attack distraction and deception Patching infrastructure Risk management BCDR infrastructure	Secure privileged accounts	▮▮	Implement Microsoft 365 Backup and Azure Backup for **critical** business data	▮▮	Implement Microsoft 365 Backup and Azure Backup for **all** business data	▮▮	Discontinue legacy network security technology	▮▮
		Segment your network	▮▮	Implement a patching plan	▮▮▮	Implement Azure Site Recovery for **all** workloads	▮▮▮		
		Implement Azure Site Recovery for **critical** workload continuity	▮▮	Create honeypot resources	▮	Gain visibility to network traffic	▮	Practice threat and BCDR response	▮▮
		Encrypt network communication	▮	Get started with Microsoft Purview Insider Risk Management	▮	Design your threat and business continuity/disaster recovery (BCDR) response	▮▮		
Implement threat protection and XDR	**Security enhanced for...**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**
	Incident response Proactive hunting Automatic detection and response SecOps processes and procedures Business critical monitoring	Turn on XDR tools: • Defender for Endpoint • Defender for Office 365 • Microsoft Entra ID Protection • Defender for Identity • Defender for Cloud Apps	▮▮	Turn on Defender for Cloud	▮	Turn on Defender for IoT	▮	Evolve SecOps as a discipline in your organization	▮▮
		Investigate and respond to threats using Microsoft Defender XDR	▮▮	Define internal process for SecOps	▮▮	Design a Microsoft Sentinel workspace and ingest XDR signals	▮▮		
				Monitor business critical and honeypot resources with XDR tools	▮▮	Proactively hunt for threats	▮▮	Leverage automation to reduce load on your SecOps analysts	▮▮
Meet regulatory and compliance requirements	**Security enhanced for...**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**	**Goals**	**Effort**
	Sensitive and regulated data	Identify applicable regulatory requirements	▮	Use Microsoft Purview to identify regulated data, assess its risk, and define custom classifiers	▮▮	Extend data lifecycle management policies with automation	▮	Use Microsoft Sentinel to continuously assess and inventory your information compliance status	▮
		Use Compliance Manager to identify regulations, assess compliance with the requirements, and plan remediation	▮▮	Assess information protection requirements and then implement basic protection and data governance policies using retention and sensitivity labels	▮▮▮	Set up partitioning and isolation controls using sensitivity labels, DLP, and information barriers	▮▮		
		Review current guidance for applicable regulations	▮▮	Implement basic DLP policies to control the flow of regulated information	▮▮	Expand information protection policies with container labeling, automatic and mandatory labeling, and stricter DLP policies	▮▮	Use Compliance Manager to remediate gaps and meet new or updated regulations	▮▮
				Implement communication compliance policies if required by regulations	▮▮	Reassess compliance using Compliance Manager to identify and remediate remaining gaps	▮		

Zero Trust adoption resources

Adoption scenario plan phase grid

Microsoft

Customization

Use this template to customize your own business scenario journey.
Download the Visio file from this page: aka.ms/zero-trust-trackers

Scenario

You can create more granular scenarios for your organization and map the work across the stages. For example, prepare your environment for Microsoft Copilot.

Goals

Adjust the template for the number of goals per stage. Stage the work according to your organization's starting point, timeline, and current maturity.

Level of effort

You decide the level of effort based on how much effort you estimate it takes for your organization to accomplish a goal.

Resources

Zero Trust adoption framework

Zero Trust trackers

Zero Trust for AI companions

Zero Trust deployment plan with Microsoft 365

Zero Trust for Azure services

Scenario	Security enhanced for...	Goals	Effort	Goals	Effort	Goals	Effort	Goals	Effort
	Text	Text		Text		Text		Text	
		Text		Text					
		Text				Text			
		Text		Text					