Microsoft (introduction-zero-trust-best-practice-frameworks)

▼ Introduction to best practices

This module covers the article of Zero Trust and best practice frameworks for Microsoft cybersecurity capabilities.

Imagine you're a cybersecurity architect in a large organization. You have been tasked with modernizing the organization's cybersecurity. You know that best practices are essential to achieve this goal, but you aren't sure which framework to use. You have heard about Zero Trust and its potential benefits, but you aren't sure how to get started. This module helps you understand best practices and how to use them as a cybersecurity architect. You'll also learn about the concept of Zero Trust and how to get started with it in an organization.

The module is divided into five units:

- Introduction to best practices
- Introduction to Zero Trust
- Zero Trust Initiatives
- Zero Trust Technology Pillars Part 1
- Zero Trust Technology Pillars Part 2

By the end of this module, you are able to understand how to use best practices as a cybersecurity architect, understand the concept of Zero Trust and how it can be used to modernize an organization's cybersecurity, and understand when to use different best practice frameworks like MCRA, CAF, and WAF.

▼ Learning objectives

Upon completion of this module, the learner is able to:

- Understand how to use best practices as a cybersecurity architect.
- Understand the concept of Zero Trust and how it can be used to modernize an organizations cybersecurity.
- Understand when to use different best practice frameworks like MCRA, CAF and WAF.

The content in the module helps you prepare for the certification exam SC-100: Microsoft Cybersecurity Architect.

▼ Prerequisites

- Conceptual knowledge of security policies, requirements, zero trust architecture, and management of hybrid environments
- Working experience with zero trust strategies, applying security policies, and developing security requirements based on business goals

▼ Best practices

Best practices are recommended ways to do things that have been found to be most effective or efficient. Best practices help you avoid mistakes and ensure that your resources and effort

aren't wasted.

Best practices come in many forms:

- exact instructions on what to do, why to do it, who should do it, and how to do it
- high level principles to help with different types of decisions and actions
- guidelines that are part of a reference architecture that describes components that should be included in a solution and how to integrate them together

Microsoft has embedded security best practices in various forms of guidance including:

- Microsoft Cybersecurity Reference Architectures
- Microsoft cloud security benchmark
- the Cloud Adoption Framework (CAF)
- the Azure Well-Architected Framework (WAF)
- Microsoft security best practices

▼ Antipatterns

An **antipattern** is a common mistake that lead to negative outcomes. It's the opposite of a best practice. Many best practices are designed to help you avoid antipatterns.

An example of a best practice that helps you overcome

An example of a best practice that helps you overcome numerous antipatterns is applying security patches regularly. Microsoft has observed multiple antipatterns that get in the way of regularly applying this basic and critically important security best practice:

- **We don't patch (unless it's critical)** - This antipattern avoids patch installation because of an implicit assumption that patches aren't important. Another version of this is that 'It won't happen to us', a belief that unpatched vulnerabilities won't be exploited because it hasn't happened before (or hasn't been detected).
- **Waiting for patch perfection instead of building resilience** - This antipattern avoids patching because of a fear that something could go wrong with the patches. This antipattern also increases likelihood of downtime from attackers.
- **Broken accountability model** - This antipattern holds security accountable for the negative outcomes of patches. This accountability model leads to other teams de-prioritize security maintenance
- **Over-customizing patch selection** - This antipattern uses unique criteria for patching instead of applying all manufacturer recommended patches. This customization effectively creates custom builds of Windows, Linux, and applications which have never been tested in that exact configuration.
- **Focusing only on operating systems** - This antipattern patches only servers and workstations without also addressing containers, applications, firmware, and IoT/OT devices

▼ How architects use best practices

Security best practices must be integrated into people's skills and habits, organizational processes, and technology architecture and implementation.

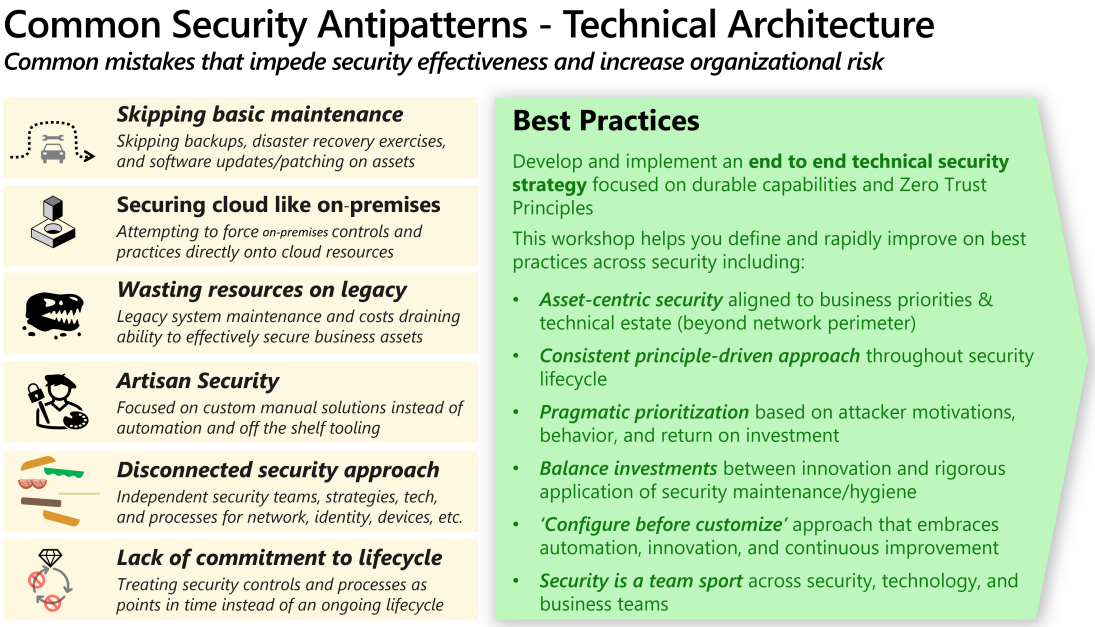
Cybersecurity architects help integrate security best practices and make them actionable by doing the following:

- Integrating best practices into security architecture and policy
- Advising security leaders on how to integrate best practices into business processes, technical processes, and culture.
- Advising technical teams on implementing best practices, and which technology capabilities make best practices easier to implement.
- Advising others in the organization such as Enterprise Architects, IT Architects, application owners, developers, and more on how to integrate security best practices in their areas of ownership.

Follow best practices unless you have a reason to avoid them. Organizations should follow well-defined and well-reasoned best practices unless there is a specific reason to avoid them. While some organizations can ignore certain best practices for good reasons, organizations should be cautious before ignoring high quality best practices like those provided by Microsoft. Best practices aren't perfectly applicable to all situations, but they've been proven to work elsewhere so you shouldn't ignore or alter them without good reason.

Adapt but don't over-customize - Best practices are general guidance that work across most organizations. You may need to adapt best practices to the unique circumstances of your organization. You should be careful not to customize them to the point where the original value is lost. An example of this is adopting passwordless and multi-factor authentication, but making exceptions for the highest impact business and IT accounts that attackers value most.

Adopting best practices will reduce common mistakes and improve overall security effectiveness and efficiency. The following diagram summarizes important antipatterns and best practices.



▼ Which framework should I choose?

Framework	Summary	When to use	Audience	Organizations	Materials
Zero Trust RaMP initiatives	Zero Trust guide based on initiatives designed to provide quick wins in high-impact areas. Plans organized chronologically and identify key stakeholders.	When you want to get started with Zero Trust and make progress quickly.	Cloud architects, IT professionals, and Business decision makers	Early stage cloud and Zero Trust adopters	Project plans with checklists
Zero Trust deployment objectives	Zero Trust guide with detailed configuration steps for each of the technology pillars. More comprehensive than RaMP initiatives.	When you want a more comprehensive guide on rolling out Zero Trust.	Cloud architects, IT professionals	Organizations who have made some progress with Zero Trust and want detailed guidance to make the most out of the technology.	Deployment plans with primary and secondary objectives.
MCRA	The MCRA is a set of diagrams that includes many best practices related to the access control modernization initiative in Zero Trust RaMP	When you want: a starting template for a security architecture, a comparison reference for security capabilities, to learn about Microsoft capabilities, to learn about Microsoft's integration investments	Cloud architects, IT professionals	Early stage cloud and zero trust adopters	PowerPoint slides with diagrams
MCSB	A framework for assessing the security posture of an organization's cloud environment against industry standards and best practices.	Looking for guidance on how to implement security controls and monitor them for compliance.	Cloud architects, IT professionals	All	Detailed specifications of controls and service baselines
CAF	A documentation	When you are looking to	Cloud architects, IT	Organizations who need	Best practices, documentation,

	and implementation framework for best practices throughout the cloud adoption lifecycle, providing a step-by-step approach to cloud migration and management using Azure.	create and implement business and technology strategies for the cloud.	professionals, and Business decision makers	technical guidance for Microsoft Azure	and tools
WAF	A framework designed to help customers build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads in Azure, using five pillars: cost optimization, operational excellence, performance efficiency, reliability, and security.	When you are looking to improve the quality of a cloud workload.	Cloud architects, IT professionals	All	Azure Well-Architected Review, Azure Advisor, Documentation, Partners, Support, and Services Offers, Reference architectures, Design principles

▼ Introduction to Zero Trust

A Zero Trust approach to security is required to be effective at keeping up with threats, changes to cloud platforms, and changes in business models responding to a rapidly evolving world. You can find best practices for adopting a Zero Trust approach to security throughout the Microsoft Cybersecurity Reference Architecture (MCRA) and Microsoft cloud security benchmark (MCSB).

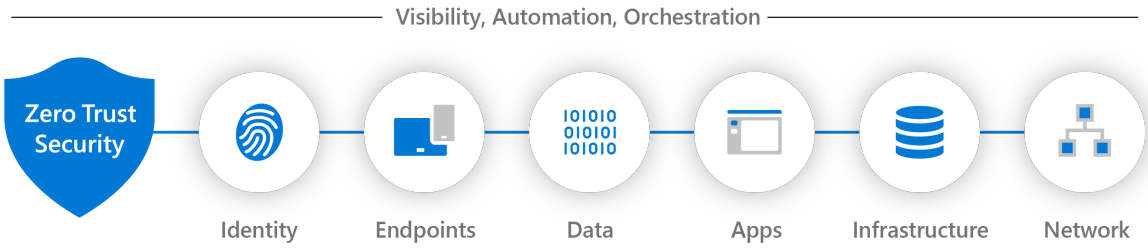
Microsoft Zero Trust approach to security is based on three principles: **assume breach, verify explicitly, and least privilege**.

Guiding principles of Zero Trust

- **Verify explicitly** - Always authenticate and authorize based on all available data points.
- **Use least privilege access** - Limit user access with Just-In-Time and Just-Enough-Access (**JIT/JEA**), risk-based adaptive policies, and data protection.
-

Assume breach - Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

This is the core of **Zero Trust**. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "**never trust, always verify**."
It is designed to adapt to the complexities of the modern environment that embraces the mobile workforce, protects people, devices, applications, and data wherever they are located.
A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements. Each of these is a source of signal, a control plane for enforcement, and a critical resource to be defended.



Different organizational requirements, existing technology implementations, and security stages all affect how a Zero Trust security model implementation is planned. Using our experience in helping customers to secure their organizations, as well as in implementing our own Zero Trust model, we've developed the following guidance to assess your readiness and to help you build a plan to get to Zero Trust.

These principles apply across the technical estate and are usually applied to a Zero Trust transformation through a series of either modernization initiatives (RaMP) or technology pillars (with deployment guidance for each pillar).

▼ Zero Trust initiatives

▼ Zero Trust initiatives

As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, **Rapid Modernization Plan (RaMP)** guidance is based on initiatives and gives you a set of deployment paths to more quickly implement key layers of protection.

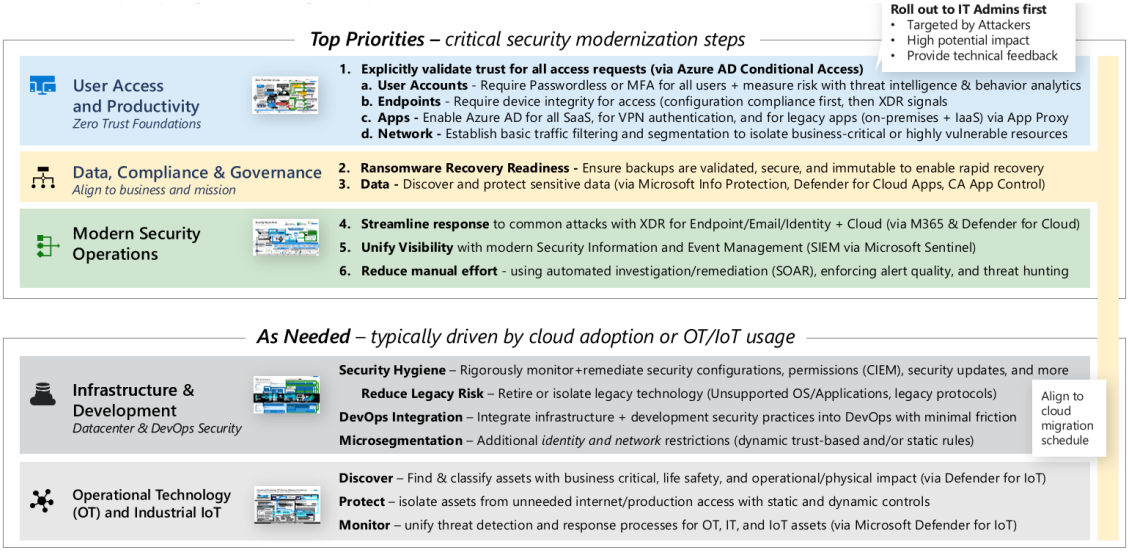
RaMP guidance takes a project management and checklist approach:

- **By providing a suggested mapping of key stakeholders, implementers, and their accountabilities, you can more quickly organize an internal project and define the tasks and owners to drive them to conclusion.**
- **By providing a checklist of deployment objectives and implementation steps, you can see the bigger picture of infrastructure requirements and track your progress.**

▼ RaMP initiatives for Zero Trust

Zero Trust is a major transformation of a security program, so it's critical to start with the most impactful items that get you the most security and productivity increases with the least amount of time and resources.

The Zero Trust Rapid Modernization Plan (RaMP) is included in the Microsoft Cybersecurity Reference Architecture (MCRA) and provides best practices that help you prioritize your security modernization. This RaMP identifies the most effective controls for the most relevant and common attacks that require the least amount of investment of time, effort, and resources.



The Zero Trust RaMP aligns to the recommended security modernization initiatives, including the following:

- **Secure Identities and Access** - These quick wins focus on using cloud-based security capabilities like Microsoft Entra ID, Intune, Microsoft Defender for Endpoints, and Microsoft Entra application proxy to rapidly modernize access control to increase productivity and security assurances.
- **Data Security and Governance, Risk, Compliance (GRC)** - These quick wins focus on ensuring the organization can rapidly recover from a ransomware/extortion attack without paying attackers and protecting the most valuable business critical data.
- **Modern Security Operations** - These quick wins focus on streamlining responses to common attacks, getting end to end visibility across the enterprise, and automating manual tasks that slow down analysts and cause exhaustion/burnout.
- **Infrastructure and Development Security** - These quick wins focus on security hygiene, reducing legacy risk, integrating security into DevOps and development processes, and applying the microsegmentation concepts to identity and network access control.
- **Operational Technology (OT) and Internet of Things (IoT) security** - These quick wins focus on quickly discovering, protecting, and monitoring these systems for attacks.

▼ Zero Trust technology pillars part 1

▼ Visibility, automation, and orchestration with Zero Trust

With each of the other technical pillars of Zero Trust generating their own relevant alerts, we need an integrated capability to manage the resulting influx of data to better defend against threats and validate trust in a transaction.

If an investigation results in actionable learnings, you can take remediation steps. For example, if an investigation uncovers gaps in a zero trust deployment, policies can be modified to address these gaps and prevent future unwanted incidents. Whenever possible it is desirable to automate remediation steps, because it reduces the time it takes for a SOC analyst to address the threat and move onto the next incident.

▼ Visibility, automation, and orchestration Zero Trust deployment objectives

When implementing an end-to-end Zero Trust framework for visibility, automation, and orchestration, we recommend you focus first on these **initial deployment objectives**:

I. Establish visibility.

II. Enable automation.

After these are completed, focus on these **additional deployment objectives**:

III. Enable additional protection and detection controls.

▼ Securing identity with Zero Trust

Before an identity attempts to access a resource, organizations must:

- **Verify the identity with strong authentication.**
- **Ensure access is compliant and typical for that identity.**
- **Follows least privilege access principles.**

Once the identity has been verified, we can control that identity's access to resources based on organization policies, on-going risk analysis, and other tools.

▼ Identity Zero Trust deployment objectives

When implementing an end-to-end Zero Trust framework for identity, we recommend you focus first on these initial deployment objectives:

I. Cloud identity federates with on-premises identity systems.

II. Conditional Access policies gate access and provide remediation activities.

III. Analytics improve visibility.

After these are completed, focus on these additional deployment objectives:

IV. Identities and access privileges are managed with identity governance.

V. User, device, location, and behavior is analyzed in real time to determine risk and deliver ongoing protection.

VI. Integrate threat signals from other security solutions to improve detection, protection, and response.

▼ Applications

To get the full benefit of cloud apps and services, organizations must find the right balance of providing access while maintaining control to protect critical data accessed via applications and APIs.

The **Zero Trust** model helps organizations ensure that apps, and the data they contain, are protected by:

- **Applying controls and technologies to discover Shadow IT.**
- **Ensuring appropriate in-app permissions.**
- **Limiting access based on real-time analytics.**
- **Monitoring for abnormal behavior.**
- **Controlling user actions.**
- **Validating secure configuration options.**

▼ Applications Zero Trust deployment objectives

Before most organizations **start the Zero Trust journey**, their on-premises apps are accessed through physical networks or VPN, and some critical cloud apps are accessible to users.

When implementing a Zero Trust approach to managing and monitoring applications, we recommend you focus first on these **initial deployment objectives**:

I. Gain visibility into the activities and data in your applications by connecting them via APIs.

II. Discover and control the use of shadow IT.

III. Protect sensitive information and activities automatically by implementing policies.

After these are completed, focus on these **additional deployment objectives**:

IV. Deploy adaptive access and session controls for all apps.

V. Strengthen protection against cyber threats and rogue apps.

VI. Assess the security posture of your cloud environments

▼ Zero Trust technology pillars part 2

▼ Secure data with Zero Trust

The three core elements of a data protection strategy are:

1. **Know your data** - If you don't know what sensitive data you have on-premises and in cloud services, you can't adequately protect it. You need to discover data across your entire organization and classify all data by sensitivity level.
2. **Protect your data and prevent data loss** - Sensitive data needs to be protected by data protection policies that label and encrypt data or block over-sharing. This ensures only authorized users are able to access the data, even when data travels outside of your corporate environment.
3. **Monitor and remediate** - You should continuously monitor sensitive data to detect policy violations and risky user behavior. This allows you to take appropriate action, such as revoking access, blocking users, and refining your protection policies.

▼ Data Zero Trust deployment objectives

An information protection strategy needs to encompass your organization's entire digital content. As a baseline, you need to define labels, discover sensitive data, and monitor the use of labels and actions across your environment.

When implementing an end-to-end Zero Trust framework for data, we recommend you focus first on these **initial deployment objectives**:

I. Access decisions are governed by encryption.

II. Data is automatically classified and labeled.

After these are completed, focus on these **additional deployment objectives**:

III. Classification is augmented by smart machine learning models.

IV. Access decisions are governed by a cloud security policy engine.

V. Prevent data leakage through DLP policies based on a sensitivity label and content inspection.

▼ Secure endpoints with Zero Trust

Zero Trust adheres to the principle, "Never trust, always verify." In terms of endpoints, that means always verify *all* endpoints. That includes not only contractor, partner, and guest devices, but also apps and devices used by employees to access work data, regardless of device ownership.

In a Zero Trust approach, the same security policies are applied regardless of whether the device is corporate-owned or personally-owned through bring your own device (BYOD); whether the device is fully managed by IT, or only the apps and data are secured. The policies apply to all endpoints, whether PC, Mac, smartphone, tablet, wearable, or IoT device wherever they are connected, be it the secure corporate network, home broadband, or public internet.

▼ Endpoint Zero Trust deployment objectives

When implementing an end-to-end Zero Trust framework for securing endpoints, we recommend you focus first on these **initial deployment objectives**:

I. Endpoints are registered with cloud identity providers. In order to monitor security and risk across multiple endpoints used by any one person, you need visibility in all devices and access points that may be accessing your resources.

II. Access is only granted to cloud-managed and compliant endpoints and apps. Set compliance rules to ensure that devices meet minimum security requirements before access is granted. Also, set remediation rules for noncompliant devices so that people know how to resolve the issue.

III. Data loss prevention (DLP) policies are enforced for corporate devices and BYOD. Control what the user can do with the data after they have access. For instance, restrict file saving to untrusted locations (such as local disk), or restrict copy-and-paste sharing with a consumer communication app or chat app to protect data.

After these are completed, focus on these **additional deployment objectives**:

IV. Endpoint threat detection is used to monitor device risk. Use a single pane of glass to manage all endpoints in a consistent way, and use a SIEM to route endpoint logs and transactions such that you get fewer, but actionable, alerts.

V. Access control is gated on endpoint risk for both corporate devices and BYOD. Integrate data from Microsoft Defender for Endpoint, or other Mobile Threat Defense (MTD) vendors, as an information source for device compliance policies and device Conditional Access rules. The device risk will then directly influence what resources will be accessible by the user of that device.

▼ Secure infrastructure with Zero Trust

Azure Blueprints, Azure Policies, Microsoft Defender for Cloud, Microsoft Sentinel, and Azure Sphere can greatly contribute to improving the security of your deployed infrastructure and

enable a different approach to defining, designing, provisioning, deploying, and monitoring your infrastructure.

▼ Infrastructure Zero Trust deployment objectives

When implementing an end-to-end Zero Trust framework for managing and monitoring your infrastructure, we recommend you focus first on these **initial deployment objectives**:

I. Workloads are monitored and alerted to abnormal behavior.

II. Every workload is assigned an app identity—and configured and deployed consistently.

III. Human access to resources requires Just-In-Time.

After these are completed, focus on these **additional deployment objectives**:

IV. Unauthorized deployments are blocked, and alert is triggered.

V. Granular visibility and access control are available across workloads.

VI. User and resource access segmented for each workload.

▼ Secure networks with Zero Trust

Instead of believing everything behind the corporate firewall is safe, an end-to-end Zero Trust strategy assumes breaches are inevitable. That means you must verify each request as if it originates from an uncontrolled network—identity management plays a crucial role in this.

▼ Network Zero Trust deployment objectives

When implementing an end-to-end Zero Trust framework for securing networks, we recommend you focus first on these **initial deployment objectives**:

I. Network segmentation: Many ingress/egress cloud micro-perimeters with some micro-segmentation.

II. Threat protection: Cloud native filtering and protection for known threats.

III. Encryption: User-to-app internal traffic is encrypted.

After these are completed, focus on these **additional deployment objectives**:

IV. Network segmentation: Fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation.

V. Threat protection: Machine learning-based threat protection and filtering with context-based signals.

VI. Encryption: All traffic is encrypted.