Azure RBAC – Key Points

1. **Purpose** - Azure RBAC is designed to ensure that users and services have the right level of access to Azure resources, limiting the risk of unauthorized access or changes to critical resources.

2. **Roles** - Azure provides built-in roles, each with a specific set of permissions that define what users with that role can do. Roles include Owner, Contributor, Reader, and many more.

3. **Custom Roles** - Organizations can create custom roles to tailor access permissions to their specific needs. Custom roles allow for fine-grained control over access.

4. **Scope** - RBAC is applied at different scopes, including the management group, subscription, resource group, or individual resource. This means you can grant different permissions at different levels.

5. **Role Assignment** - Role assignments link users, groups, or service principals to roles at a specific scope. Role assignments define who can do what within a given scope.

Azure RBAC – Key Points

6. **Role Inheritance** - Permissions can be inherited from higher scopes to lower scopes. For example, a role assigned at the subscription level can be inherited by all resource groups and resources within that subscription.

6. **Granular Control** - Custom roles can be created with fine-grained control over permissions. You can specify which actions users can perform on specific resource types.

7. **Least Privilege Principle** - Azure RBAC encourages the principle of least privilege, where users are granted only the permissions necessary to perform their tasks, reducing the risk of unauthorized actions.

8. **Audit and Monitoring** - Azure provides auditing and monitoring capabilities to track role assignments and changes, helping organizations maintain security and compliance.

Concept of Zero Trust

- ✓ Based on the principle of 'never trust, always verify' in cybersecurity.
- ✓ Challenges the traditional network security model, which assumes that once someone or something is inside a network, they can be trusted. In contrast, Zero Trust assumes that no one, whether inside or outside the network, can be inherently trusted.
- ✓ Requires verification and authentication for every user, device, and application attempting to access resources.

Concept of Zero Trust – Key Points

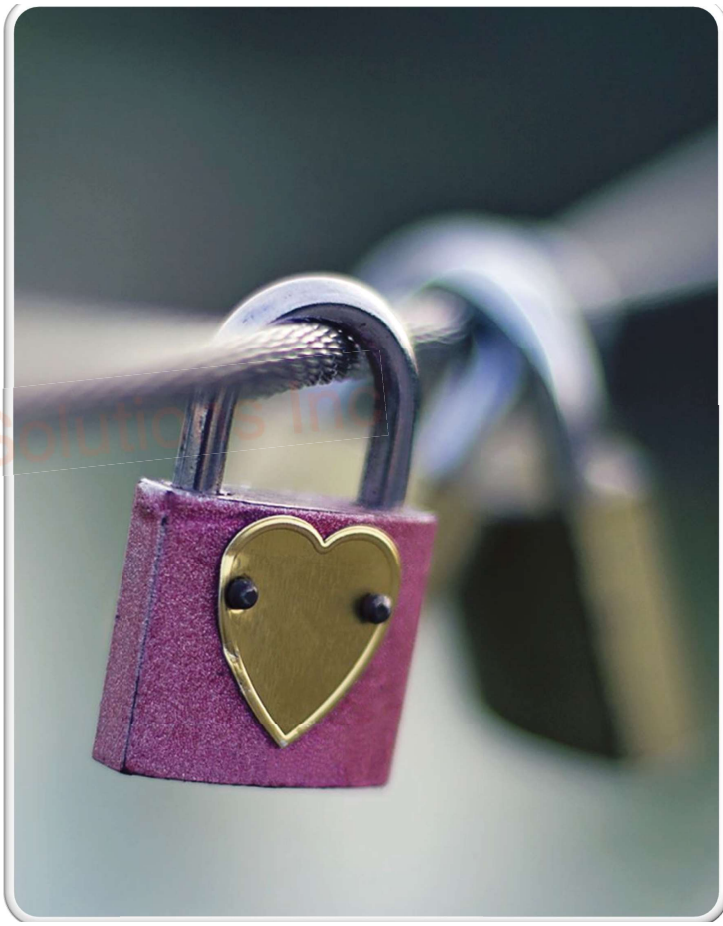
1. **Identity-Centric** – Focus is on verifying the identity of users and devices before granting access to resources. E.g. – Use MFA

2. **Least Privilege** - Means that users and devices should only have the minimum level of access necessary to perform their tasks.

3. **Micro-Segmentation** - Involves segmenting the network into smaller zones. Each segment has its own security policies, limiting scope for attackers.

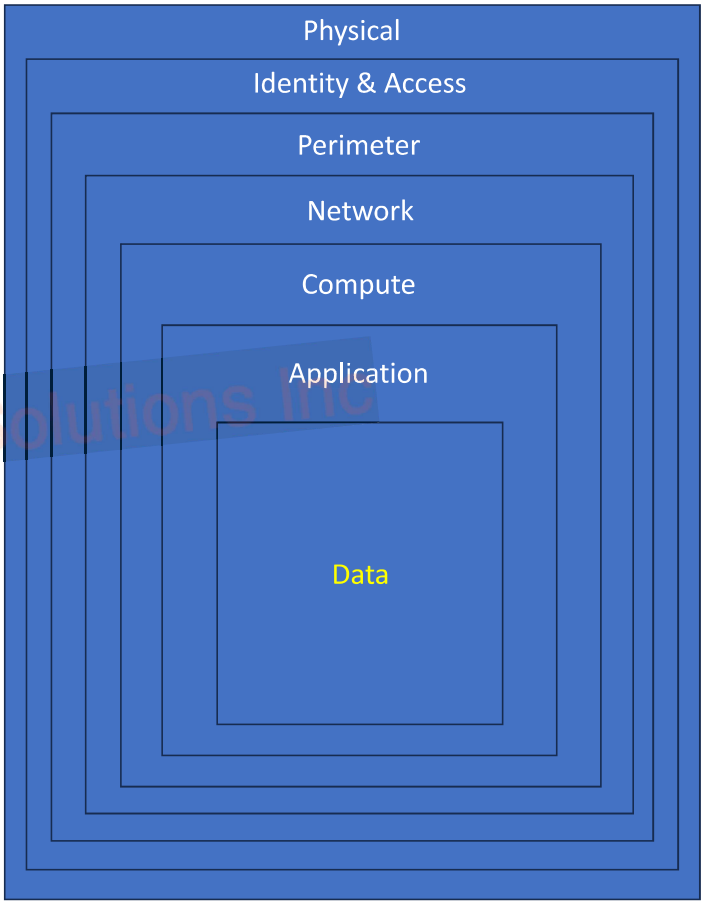
4. **Continuous Monitoring -** This helps in detecting and responding to any unusual or suspicious activities in real-time.

5. **Verification of Trust** - Trust is never assumed, it must be continuously verified. Even after initial access, users and devices are subject to ongoing scrutiny to ensure they remain trustworthy.



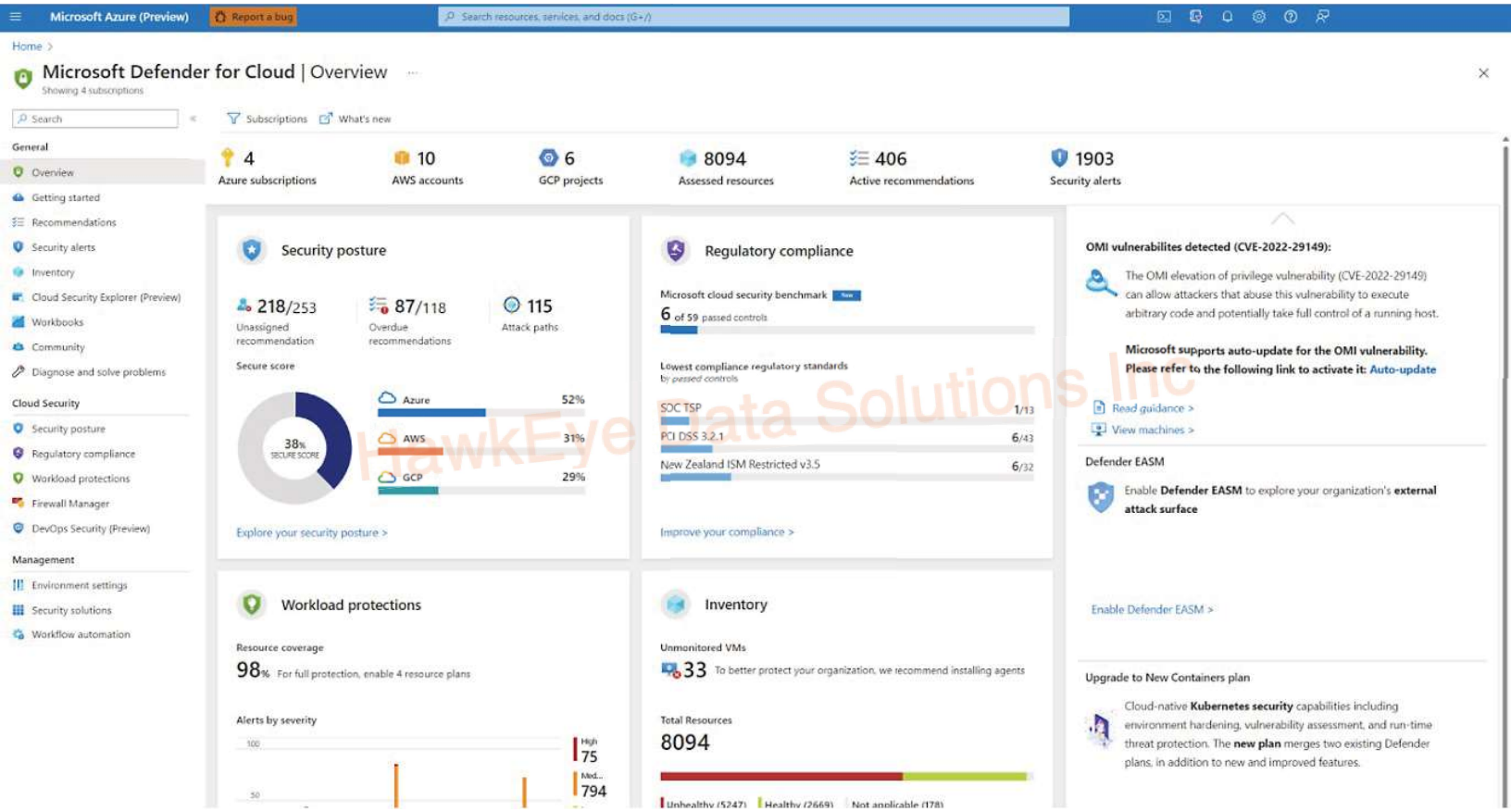
Defense In Depth

- Layering to slow the advance of attackers – multiple layers instead of just one.
- Every layer is a backup (ready to fight) in case one is breached.
- Physical - Datacenters, disks, physical hosts etc.
- Identity & Access – Access to resources & roles / privileges + logging.
- Perimeter – Sniffing for DDoS attacks before they render a service unusable.
- Network – Limiting access between resources through Vnets, Subnets etc. & deny by default.
- Compute – Makes sure that VMs are safe and secure.
- Application – Makes sure that apps are safe & secure – risk assessment, pen-tests, storing credentials separate from code etc.
- Data – The crux: Internal and External data that you're protecting. Need to ensure confidentiality & integrity.



Microsoft Defender for Cloud

- Monitoring tool to assess security posture.
- Can monitor & suggest improvements for both on-prem and cloud deployments!
- Aims to safeguard cloud resources and workloads by providing advanced threat protection, security monitoring, and compliance management
- Azure – Built in support & monitoring for many resources (PaaS mostly). On-prem & multi cloud? Deploy Log Analytics agent to gather information.
- For multi-cloud, the assessment will be done by Defender & a recommendations given for the other CSPs.
- CSD – Continually Assess (recommendations/assessment), Secure (Zero Trust) & Defend (Advanced Threat Protection & Alerts!).

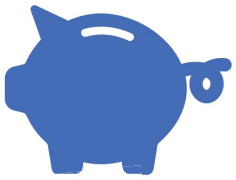


Source : https://azure.microsoft.com/en-ca/products/defender-for-cloud

Factors that can affect cost

- No longer maintaining physical infrastructure.
- Hundreds of managed services at our disposal.
- CapEx -> OpEx model.
- Pay-as-you-go

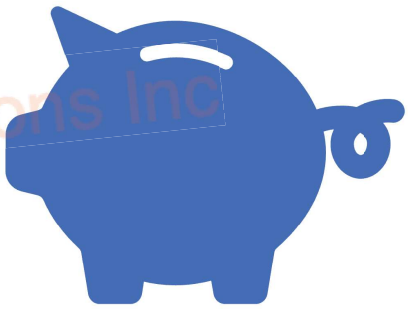
Subscription Type



- Yes, there is a free version that allows access to certain services for 12 months.
- After free trial is over, some services need to be paid for based on consumption.
- Credit can be exhausted.

Resource Type

- E.g. – i3 vs i9.
- OS for VM, size of VM (smaller is generally cheaper and bigger is expensive).
- Access Tier – Hot, Cold, Archive.
- Replication (across regions)



Resource Consumption

- Pay as you go model.
- Amount of network, storage, compute resources used impact costs.
- Use less, pay less. Use more, pay more.
- Reserved resources also available – Up to 72% discounts!
- Committing to using & paying for a certain amount – 1 to 3 years + pay as you go also exists.

Geography

- Choosing the region where the resource is to be deployed.
- Resource cost can be different based on region – labour, maintenanct, taxes etc.
- Moving data between different regions can have different charges.

Network Traffic

- Many inbound transfers (data ingress) into Azure datacenters is free. Some are NOT.
- Data egress is NOT free on many occasions.
- Inter-Region & Inter-Continental transfer is charged.

Azure Marketplace

- Like a shop with pre-built solutions from 3rd party vendors.
- Pay for resources the solutions uses + services of the vendor.
- Solutions are certified with Azure standards.

Pricing Calculator

- ✓ Web-based tool that allows you to estimate the cost of using Azure services based on your specific requirements.
- ✓ You can select the services, configurations, and regions to get cost estimates for your Azure resources.
- ✓ Estimate before you deploy! Free to use.

Total Cost of Ownership (TCO) Calculator

- ✓ Helps organizations assess the cost savings and benefits of migrating their on-premises workloads to Azure.
- ✓ It considers factors like hardware, software, labor, and data center costs to provide a TCO analysis.
- ✓ Tell it what your current infrastructure looks like & it tells how much it costs to run the same in Azure!

Cost Management Tool

- ✓ Like having a friendly piggy-bank manager in Azure - keeps an eye on your spending and helps you make sure your cloud coins are used wisely.
- ✓ Tool within Microsoft Azure that provides organizations with comprehensive insights into their cloud spending.
- ✓ Helps them effectively manage and optimize their Azure costs.

Cost Management Tool – Key Points

- ✓ **Cost Visibility** - Clear and detailed view of an organization's Azure spending. It provides insights into how resources are being utilized and how costs are distributed across different Azure services, subscriptions, and departments.

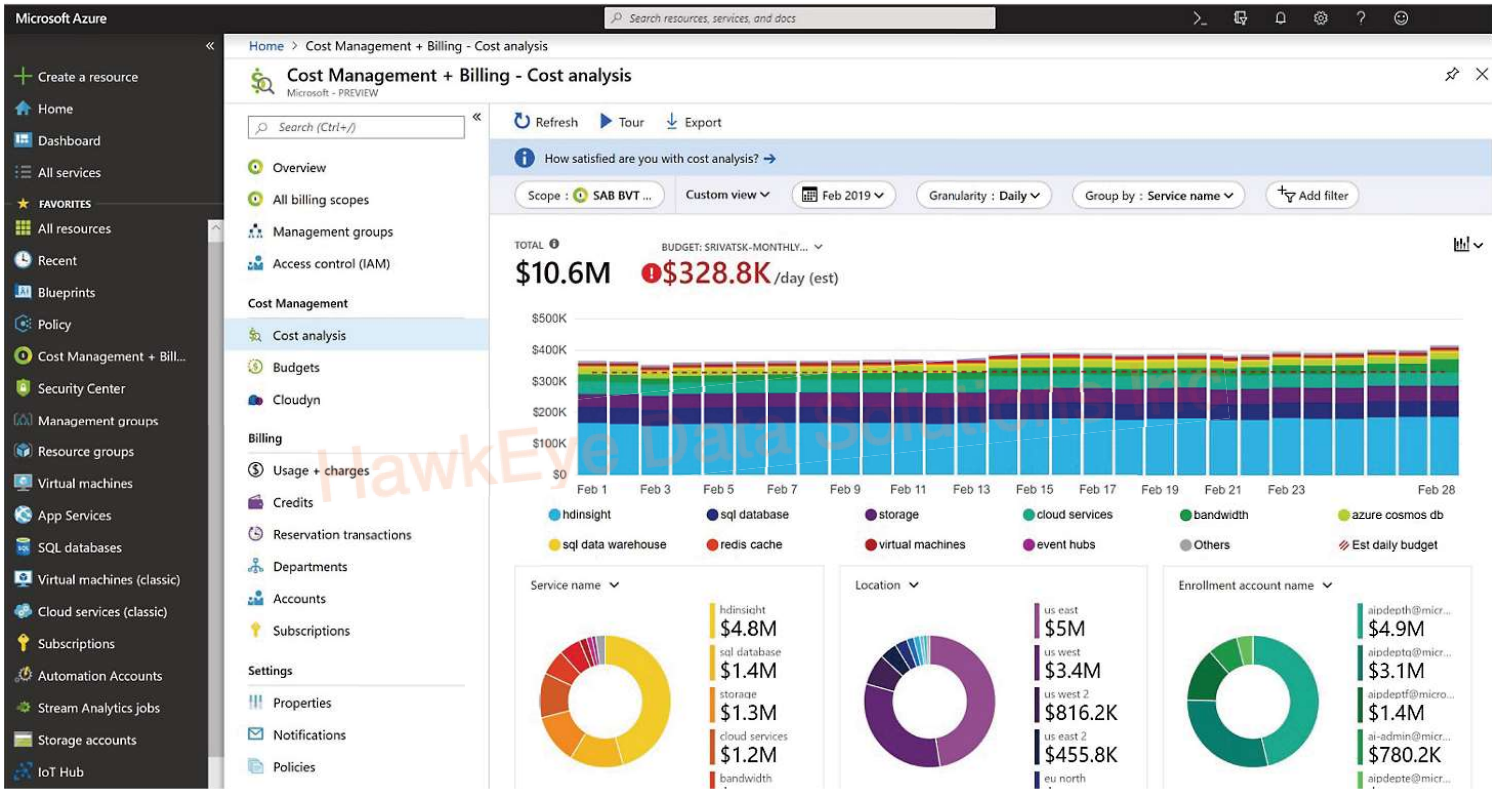
- ✓ **Budgeting and Forecasting** - Set budgets and spending limits using Cost Management. The tool allows users to create budget plans, set alerts, and receive notifications when spending approaches or exceeds defined thresholds. It also offers forecasting capabilities based on historical spending patterns. Department spending quota alerts.

- ✓ **Cost Analysis** - Users can perform in-depth cost analysis to understand spending trends and identify cost optimization opportunities. The tool offers various filters and dimensions to slice and dice spending data, making it easy to analyze costs by resource type, location, tags, and more.

Cost Management Tool – Key Points

- ✓ **Cost Allocation and Chargeback** - Cost Management enables organizations to allocate costs to specific departments, projects, or cost centers. Useful for organizations that want to distribute cloud costs internally or chargeback costs to different teams.

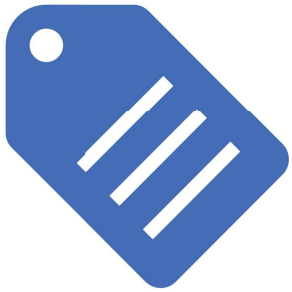
- ✓ **Resource Optimization** - The tool provides recommendations and insights for optimizing Azure resources to reduce costs. It identifies underutilized or idle resources and suggests actions to right-size or decommission them.



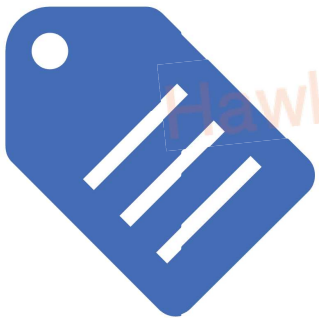
Source: https://azure.microsoft.com/en-us/products/cost-management

Tags

- ✓ Tags allow you to categorize and label cloud resources in a way that makes sense for your organization. You can assign one or more tags to resources, such as virtual machines, storage accounts, and databases.
- ✓ This categorization helps you organize resources based on criteria like department, project, environment (dev, test, prod), owner, or cost center.
- ✓ Add tags using the Azure Portal, Azure CLI, ARM templates, REST APIs etc.



Tags – Key Points



- ✓ **Cost Allocation**: By tagging resources with specific cost center or department information, you can track and attribute cloud costs accurately. This is particularly valuable in organizations where multiple teams share cloud resources - helps allocate expenses to the right teams.

- ✓ **Resource Management**: Tags provide an additional layer of organization and management for your resources. You can use tags to filter and group resources in the Azure Portal, making it easier to find and manage specific resources, especially when you have many of them.

- ✓ **Cost Reporting and Optimization**: Tags are essential for detailed cost reporting and optimization efforts. Azure Cost Management and other cost analysis tools can leverage tags to provide insights into spending patterns. You can create custom reports and dashboards based on tags to track costs by various dimensions, helping identify areas for optimization.

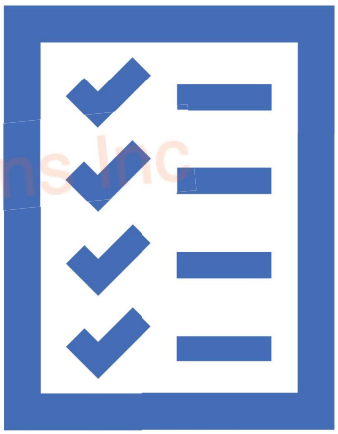
- ✓ **Security and Access Control**: Tags can also be used in conjunction with Azure Role-Based Access Control (RBAC) to control access to resources. You can use tags to define specific access policies and ensure that only authorized users or teams can manage or modify tagged resources.

Azure Policy

- ✓ Like having a superhero for your cloud resources in Microsoft Azure. This superhero makes sure everything in your Azure world follows the rules and stays safe.
- ✓ A set of rules that you can define for your Azure resources.
- ✓ These rules ensure that your resources follow specific guidelines, like having the right security settings or using approved services. It's like setting house rules to keep everything in order and secure in your cloud.
- ✓ Can have both individual policies & group of policies – initiatives. Working towards a larger goal.
- ✓ Non-compliant resources can be denied creation. Existing ones will not be deleted by default.
- ✓ Comes with Built-In policy initiatives.
- ✓ E.g. – Certain # of cores only – will disallow new ones & re-evaluate old ones.

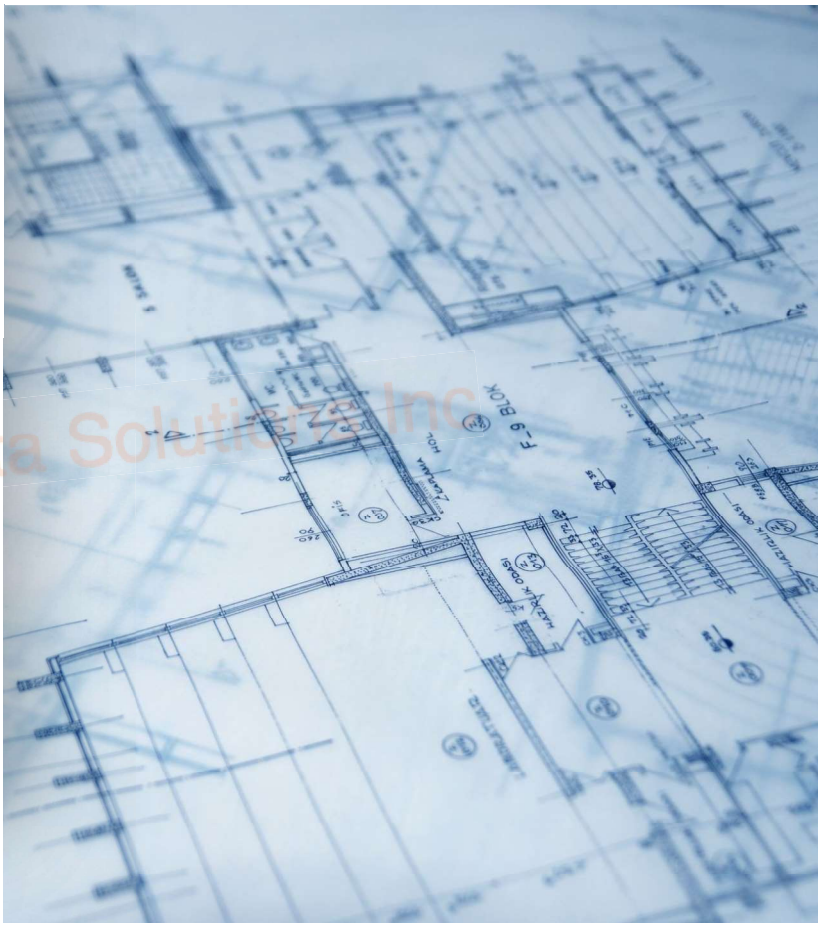
Azure Policy – Key Points

- ✓ **Scalable and Automated**: Can be applied across large numbers of resources automatically, making it scalable for cloud environments.
- ✓ **Enforcement at Scale**: You can apply policies at various levels, such as management groups, subscriptions, or resource groups, to enforce governance consistently.
- ✓ **Built-In and Custom Policies**: It offers a library of built-in policies covering common scenarios, and you can create custom policies tailored to your organization's specific needs.
- ✓ **Monitoring and Reporting**: Azure Policy provides monitoring and reporting on policy compliance, helping you track and audit your resources.
- ✓ **Integration with Azure Services**: It integrates with other Azure services like Azure Monitor and Azure Security Center to enhance governance and security.



Azure Blueprints

- Azure Blueprints is like creating a whole template for your Azure environment.
- It defines a set of resources, configurations, policies, and even roles.
- It's about creating standardized and repeatable Azure environments. Use built-in or custom blueprints!
- Azure Blueprints is like having a blueprint for building an entire house with all its rooms and rules in one go.



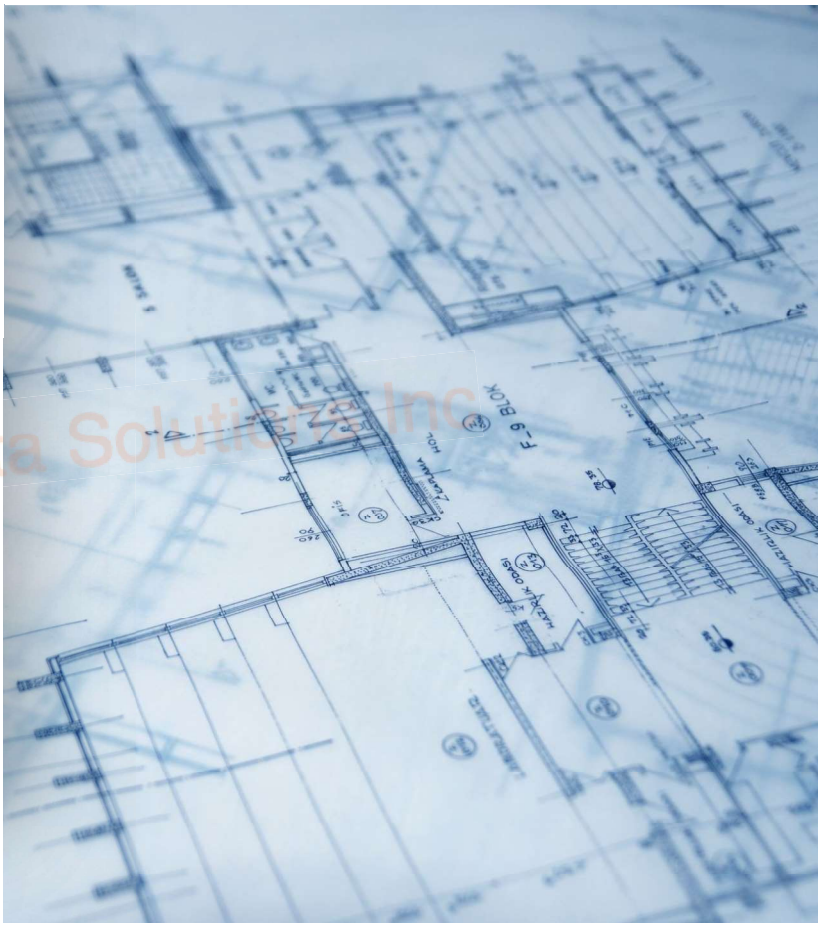
Azure Blueprints – Key Points

1. **Purpose** - Aim to accelerate the creation of compliant and consistent Azure environments by providing a pre-defined set of resources, configurations, and policies.

2. **Resource Templates** - Include Azure Resource Manager templates, which define the infrastructure and resources to be provisioned in an environment.

3. **Compliance and Auditing**: - Azure Blueprints helps organizations maintain compliance with regulatory requirements and industry standards. It also facilitates auditing and reporting by documenting the deployment's configuration.

4. **Blueprint Artifacts** - Blueprints consist of blueprint artifacts, which include resource groups, role assignments, policy assignments, and Resource Manager templates. These artifacts define the environment's structure and policies.



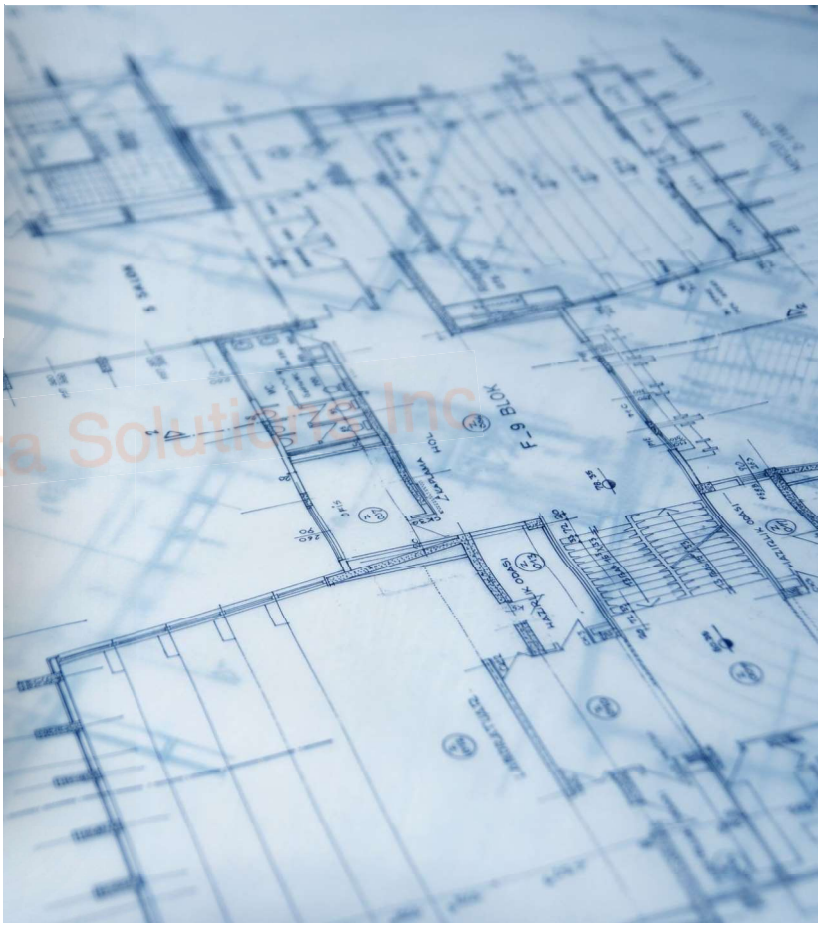
Azure Blueprints – Key Points

5. **Versioning and Revisions** - Support for versioning and revisions : maintain and update blueprints as requirements evolve.

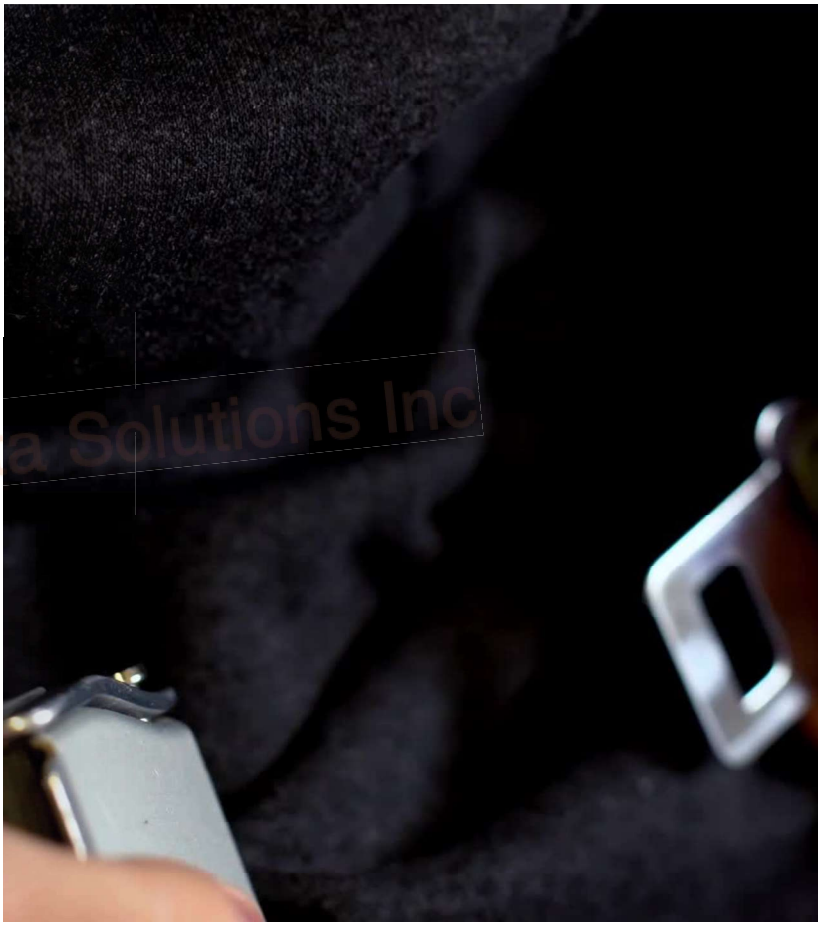
6. **Blueprint Assignments** - Organizations assign blueprints to Azure subscriptions. When assigned, the blueprint artifacts are deployed, and policies are enforced within that subscription.

7. **Scalable and Repeatable** - Enable the creation of repeatable and scalable environments, making it easier to deploy resources consistently across multiple subscriptions.

8. **Integration with Azure Policy** - Azure Blueprints integrates with Azure Policy, allowing organizations to link policy assignments directly to blueprint artifacts for policy enforcement.



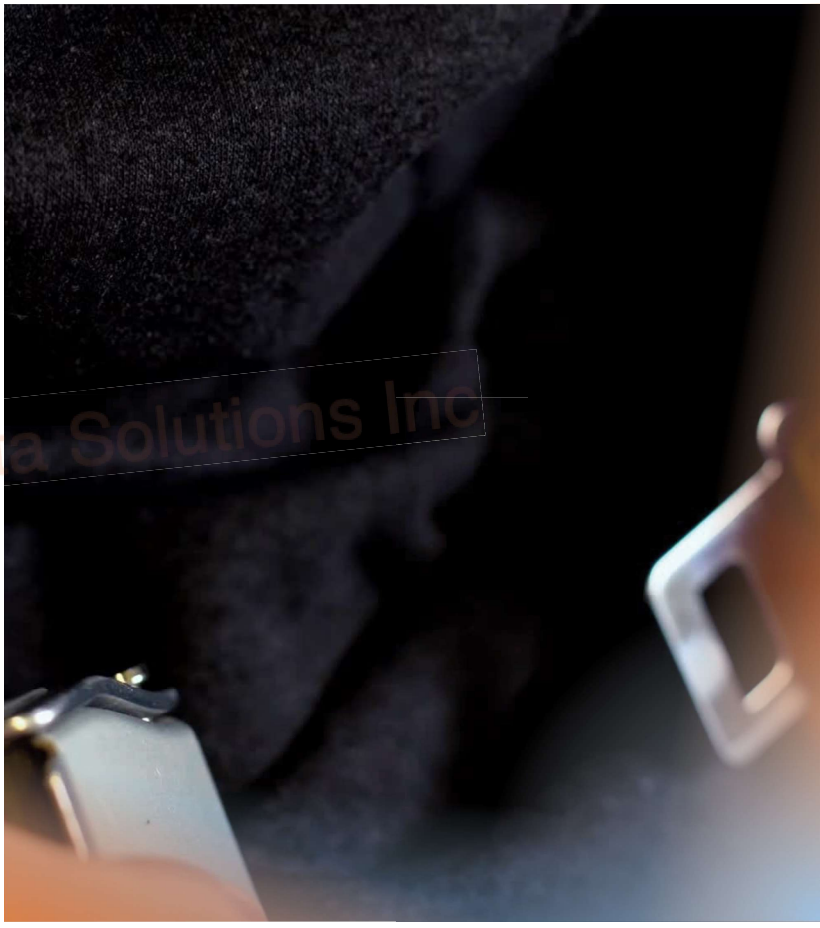
Resource Locks



- ✓ Like seat belts for your cloud resources.
- ✓ They help keep your resources safe and secure from unwanted changes or deletions, just like seat belts help keep you safe in a car.

Resource Locks – Key Points

1. **Prevent Accidents**: Just as a seat belt prevents you from getting hurt in a car accident, resource locks prevent accidental changes or deletions of your critical Azure resources – safety measure.
2. **Two Types of Locks**: There are two types of resource locks: "CanNotDelete" and "ReadOnly."
    1. "CanNotDelete" acts like a seat belt that doesn't let you remove the resource. You can still make changes but can't delete it.
    2. "ReadOnly" is like locking the resource in a glass case. You can't make any changes, like a seat belt that keeps you in your seat.
3. **Simple to Apply**: Just like putting on a seat belt is easy, applying a resource lock is straightforward in the Azure Portal.
4. **Great for Critical Resources**: You'd use resource locks for critical resources that you never want to delete accidentally, like important databases or production servers.
5. **Flexibility**: Resource locks can be applied at different levels, such as a resource group or a single resource.
6. **Remember to Unlock**: Just like you need to unbuckle your seat belt when you're out of the car, you should remember to remove resource locks when they're no longer needed.
7. **Visual Reminder**: When a resource has a lock, it's like seeing a bright-colored seat belt in the car—it reminds you to be cautious.



Azure Service Trust Portal

- ✓ One stop shop to get information relating to Microsoft security, compliance and privacy.
- ✓ This portal is like a mission control center where you can see all the operations and strategies to protect your digital world.
- ✓ **Safety Blueprints**: Just like superheroes have blueprints for their secret hideouts, Azure Service Trust Portal has blueprints for keeping your data safe. These blueprints are called compliance reports.
- ✓ **Safe Data Centers**: This portal shows you how Microsoft builds super-secure data centers, where your digital treasures are stored.
- ✓ **Privacy Shields**: Azure Service Trust Portal has privacy shields (compliance certifications) to ensure that your personal data is handled with care.

Tools for interacting with Azure

- ✓ 3 main ways to manage & maintain your environment – Azure Portal, Azure CLI, Azure PowerShell.
- ✓ **Azure Portal -** Web-based interface that provides a graphical and user-friendly way to manage and monitor your Azure resources. You can create, configure, and monitor resources using this portal. 0 downtime for maintenance activities!
- ✓ **Azure Cloud Shell –** Browser based cloud shell, needs no local installation of configs. Deploy, manage and change environments using the shell of your choice – Azure PowerShell or Azure CLI (Bash based)
- ✓ **Azure Powershell –** Run command-lets (series of commands) on the cloud to deploy or delete resources (one or many). Can be automated. Azure Rest API is called to do it all. Available on Windows, Linux, Mac!
- ✓ **Azure CLI –** Uses Bash commands! An alternative language that's all, everything else is the same as Azure PowerShell.

Azure Resource Manager (ARM)

- ✓ Azure's deployment and management service.
- ✓ Creating, updating, managing resources – ARM will step in.
- ✓ Like having a super organized master planner for building your dream Lego city in the cloud. It helps you assemble all the pieces (resources) together, just the way you want.
- ✓ Lifecycle : Portal, SDK, CLI -> ARM -> Resource -> Request completed.
- ✓ Uses templates (JSON files) instead of scripts! Confident that resource will be created consistently.

Azure Resource Manager (ARM) – Key Points

1. **The Lego Master Planner**: ARM is like the Lego master planner who knows exactly how to build your dream city in the cloud.

2. **Resource Organizer**: It helps you keep all your Lego pieces (resources like virtual machines, databases, and networks) in one neat box, called a resource group.

3. **Resource Relationships**: ARM knows which Lego pieces fit together. It's like having a guide that tells you which resources depend on others.

4. **One-Stop Shop**: You can use ARM to create, update, and delete all your resources in one go. It's like getting everything you need from one store.

5. **Tagging and Sorting**: ARM can also label and sort your Lego pieces. It's like having labels on your Lego bricks so you know which ones belong where.

Azure Resource Manager (ARM) – Templates

- ✓ All about Infrastructure as Code (IaC) – Use code to deploy resources (Portal, PowerShell, CLI).
- ✓ Two main categories – ARM templates & Bicep.
- ✓ ARM – Define the resources in a JSON format. Verified & creation is parallelized.
- ✓ You can be rest assured that the results are repeatable, can be orchestrated & declarative (tell what you want but don't write code).
- ✓ Bicep – Also declarative , but much simpler and concise file. Comes with the benefit of modularity & support for all resources & APIs.

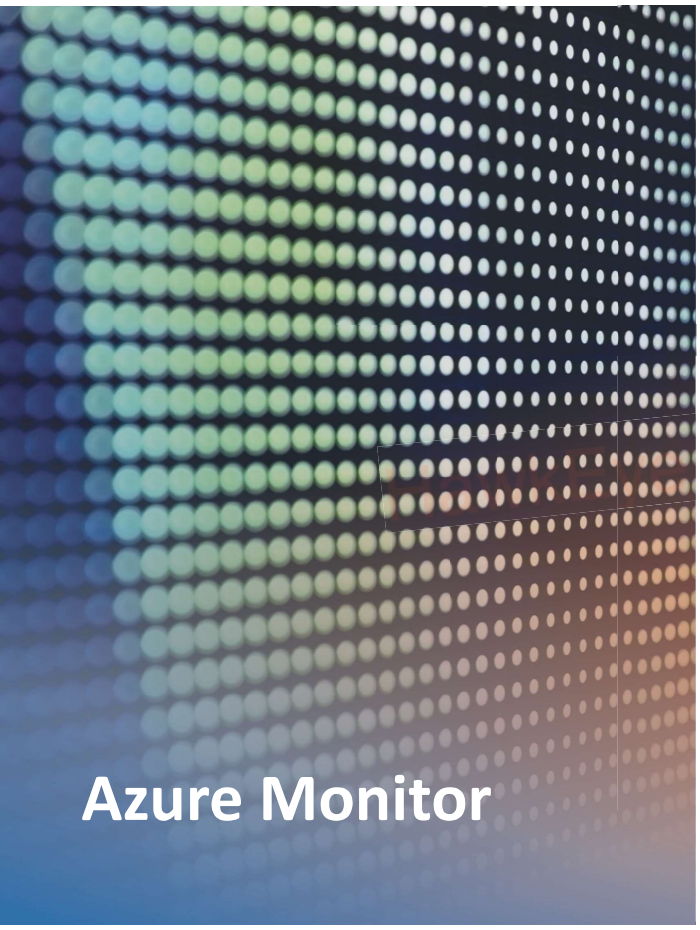
- ✓ **Azure Advisor** is like having a wise and friendly guru in the cloud who helps you save money, improve your cloud efficiency, and follow best practices. It's like getting expert advice for your digital kingdom.

- ✓ Can view these recommendations through portal or API – setup notifications when new suggestions are available. Filtering is also possible to narrow the scope.

- ✓ Recommendations are broken into 5 categories – COPSR (Cost, Operational Excellence, Performance, Security, Reliability).

- ✓ Helps to save money, implement best practices, and optimize resources.

- ✓ **Cost –** To spend less overall.
- ✓ **Operational Excellence –** To implement best practices & achieve maximum efficiency.
- ✓ **Performance –** Improve performance & throughput of applications & overall environment.
- ✓ **Security –** Improve overall security measures & combat security threats.
- ✓ **Reliability -** Ensuring that apps & env. remain available & robust.



- ✓ Azure Monitor is like having superhero senses for your cloud resources. It gives you the ability to see, hear, and feel what's happening in your digital world – Azure, multi-cloud, hybrid!

- ✓ Azure Monitor collects data from various sources, including performance metrics, application logs, infrastructure logs, and more. It can gather data from Azure resources, operating systems, applications, and even custom sources.

- ✓ Put together dashboards (PowerBI) to monitor everything in real-time or even get alerts sent to you through SMS!

- ✓ It provides two main types of data: metrics and logs. Metrics are numerical measurements that describe the performance of a resource, such as CPU usage or network traffic. Logs are textual records of events and activities, which can include error messages, security events, and application traces.

Azure Log Analytics

- ✓ Logs are textual records of events and activities, which can include error messages, security events, and application traces.
- ✓ Serves as a centralized repository for log and telemetry data generated by Azure resources and on-premises systems. It consolidates data from various sources into one location for analysis.
- ✓ It can collect data from a wide range of sources, including virtual machines, containers, Azure services, custom applications, and third-party tools. This data includes logs, metrics, events, and traces.
- ✓ Run queries to analyze the data collected by Azure Monitor. Supports both simple and complex queries.

Azure Monitor Alerts

- ✓ Set thresholds & when they're crossed, get notified!
- ✓ E.g., DB has crossed 85% of total capacity - running out of space.
- ✓ Take corrective action – deploy more if you set it up that way.
- ✓ Action Group – Notification + Action (Who to alert and what to do in response).

Azure Application Insights

- ✓ Monitoring but for Web Apps.
- ✓ All environments supported like Azure Monitor.
- ✓ 2 ways – SDK in your app, or App Insights agent.
- ✓ KPIs like response rates, page load performance, user count etc.
- ✓ **Rich Dashboards**: Application Insights offers customizable dashboards and interactive charts that allow you to visualize data, track performance metrics, and identify bottlenecks.
- ✓ **End-to-End Tracing**: It provides end-to-end tracing capabilities, allowing you to track requests as they flow through different components of your application stack, from the frontend to the backend.

Azure Service Health

- ✓ Like a doctor that tells you the health of your resources individually & the health of Azure's global infrastructure!
- ✓ Azure Status – Health of Azure overall across the world : what services & region is affected, issues & anomalies etc.
- ✓ Service Health – Health of regions and services that YOU are using.
- ✓ Resource Health - Health of your individual resources & whether they are affected.