Cloud Infrastructure Week#7

Emrah Mutlu

January 2024

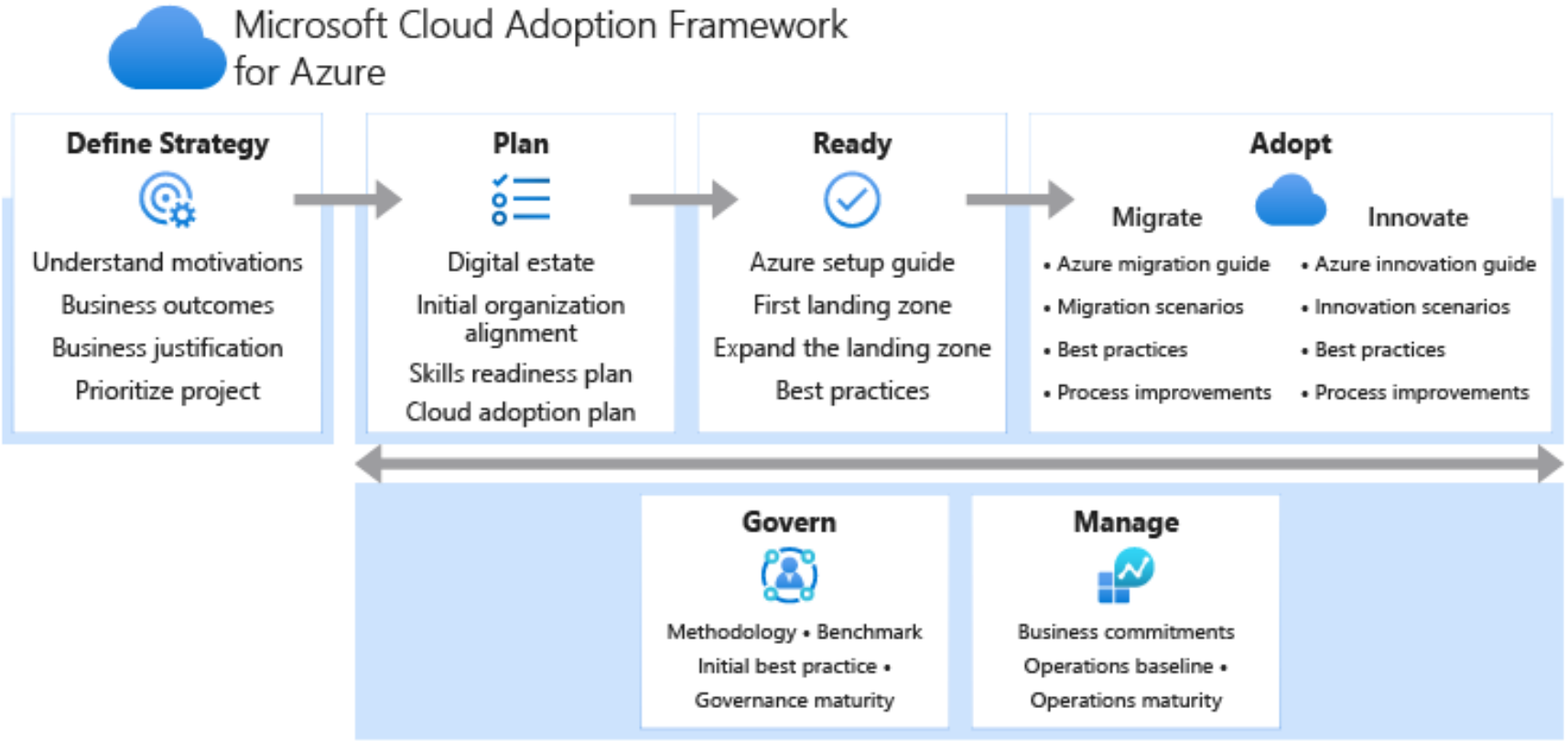
AGENDA – WEEK#7

- Cloud Governance
  - Azure CAF (Cloud Adoption Framework)
  - Governance Foundations
  - RBAC, Azure AD, Policy, Blueprints
  - Resource Locks and Tags
- Cloud Monitoring
  - Azure Monitor
  - Azure Dashboard
  - Azure Security Center
  - Azure Sentinel
  - Azure App. Insights
- Cloud Security
  - OWASP TOP 10
  - Security Posture
  - Defense in Depth & Zero Trust Strategy
  - Microsoft Defender for Cloud
  - JIT VM Access
  - DDoS Protection
  - Microsoft Intune
- Case Study
- Certs & Future Concepts
- Homework

Orion Innovation

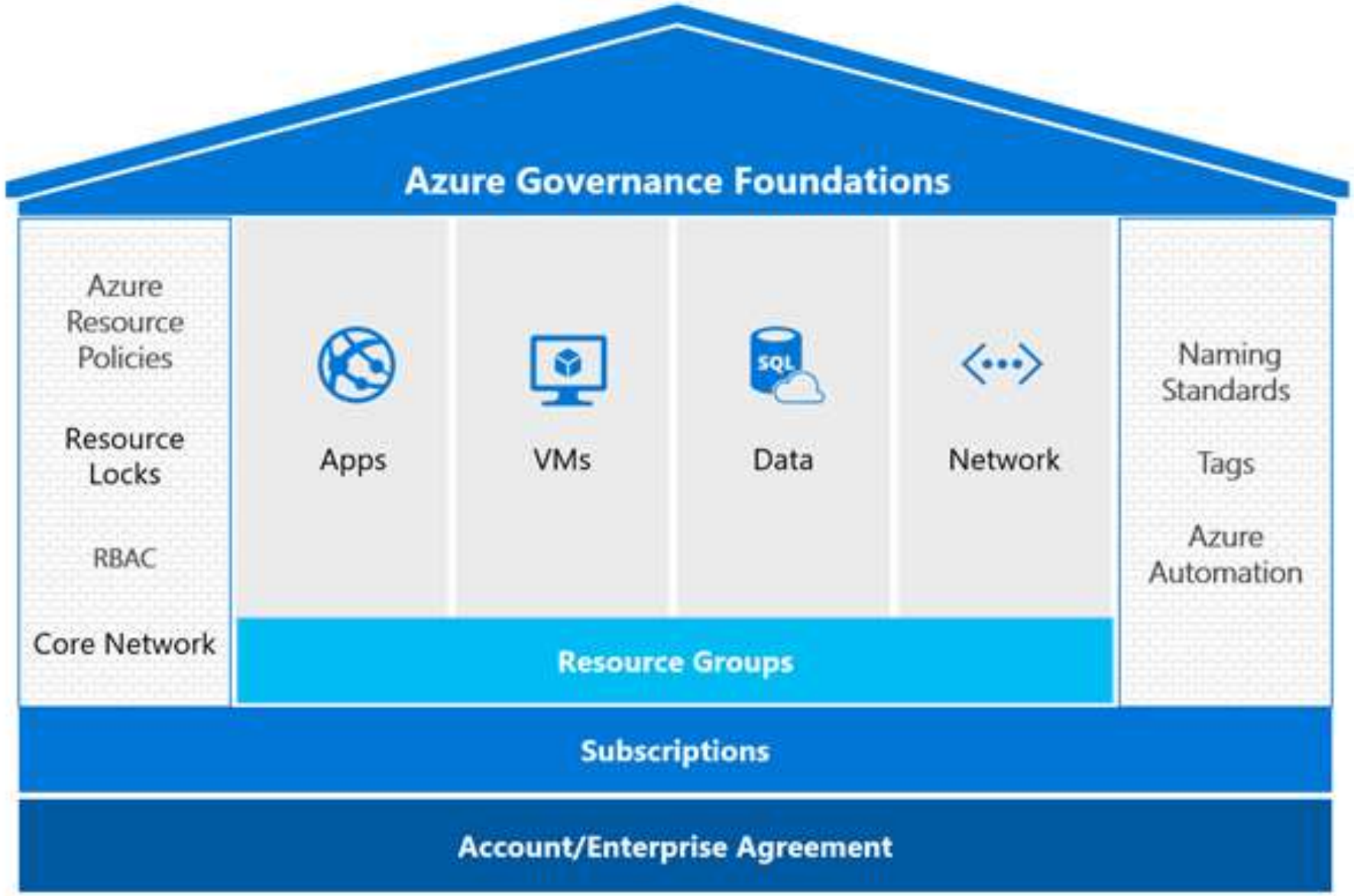
Cloud Governance

- The term ***governance*** describes the general process of establishing rules and policies and ensuring that those rules and policies are enforced.
- **Azure CAF** ensures a smooth cloud migration with the help of all parties and shared responsibilities which is determined by the RACI (Responsible, Accountable, Consulted, Informed) templates.



RACI Template

GOVERNANCE FOUNDATIONS

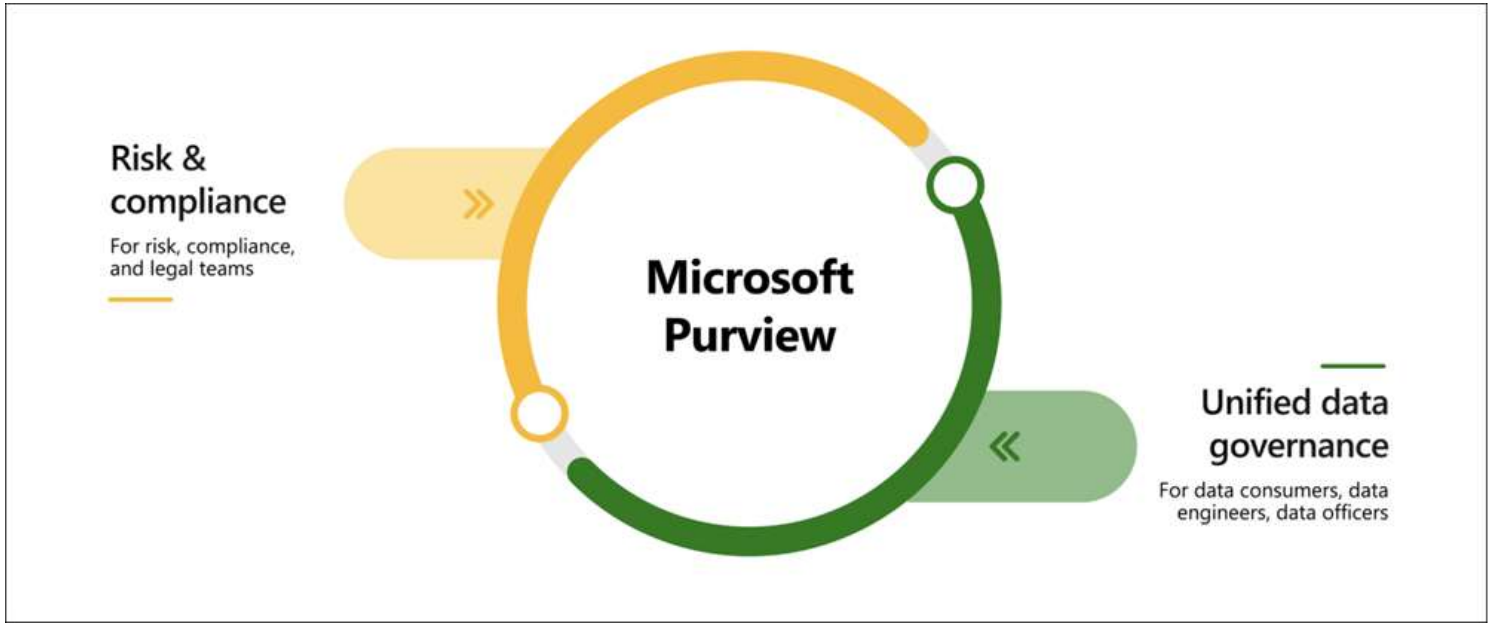


Purview provides **Risk & Compliance solutions** like:

- Protect sensitive data across clouds, apps, and devices.
- Get started with regulatory compliance.
- Identify data risks and manage regulatory compliance requirements.

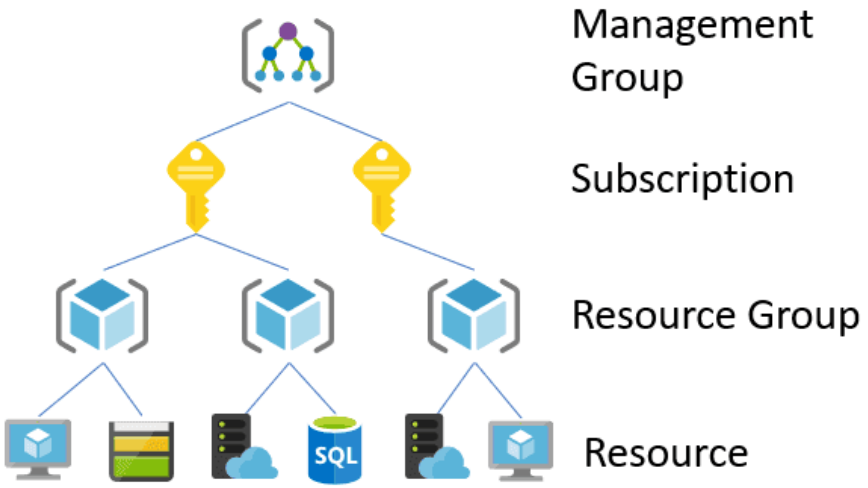
Unified **data governance solutions** like:

- Create an up-to-date map of your entire data estate that includes data classification and end-to-end lineage.
- Identify where sensitive data is stored in your estate.
- Create a secure environment for data consumers to find valuable data.
- Generate insights about how your data is stored and used.
- Manage access to the data in your estate securely and at scale.



AZURE RBAC (ROLE BASED ACCESS CONTROL)

- Azure RBAC (Role-Based Access Control) is the system that allows control over **who has access to which Azure resources**, and **what those people can do with those resources**.
- Some built-in roles are:
  - **Owner**: Has full access to all resources, including the ability to delegate access to other users.
  - **Contributor**: Can create and manage Azure resources.
  - **Reader**: Can view only existing Azure resources.
  - **User Access Administrator**: Can manage access to Azure resources

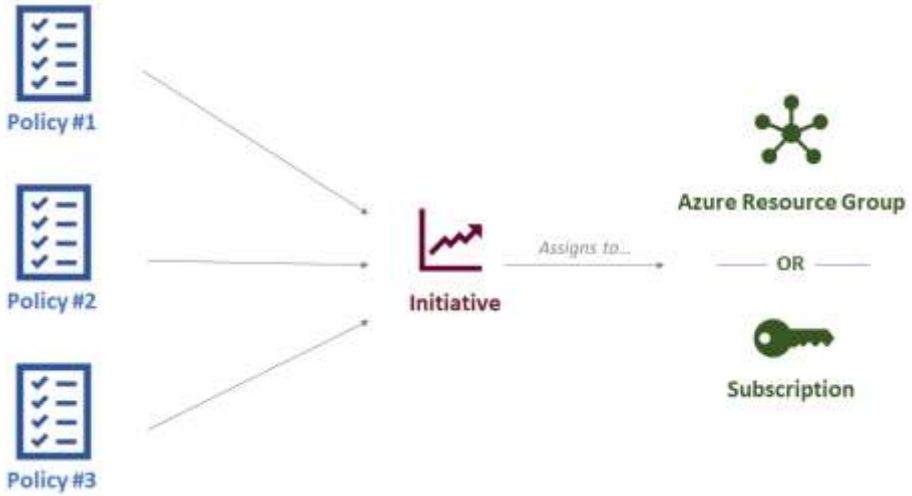


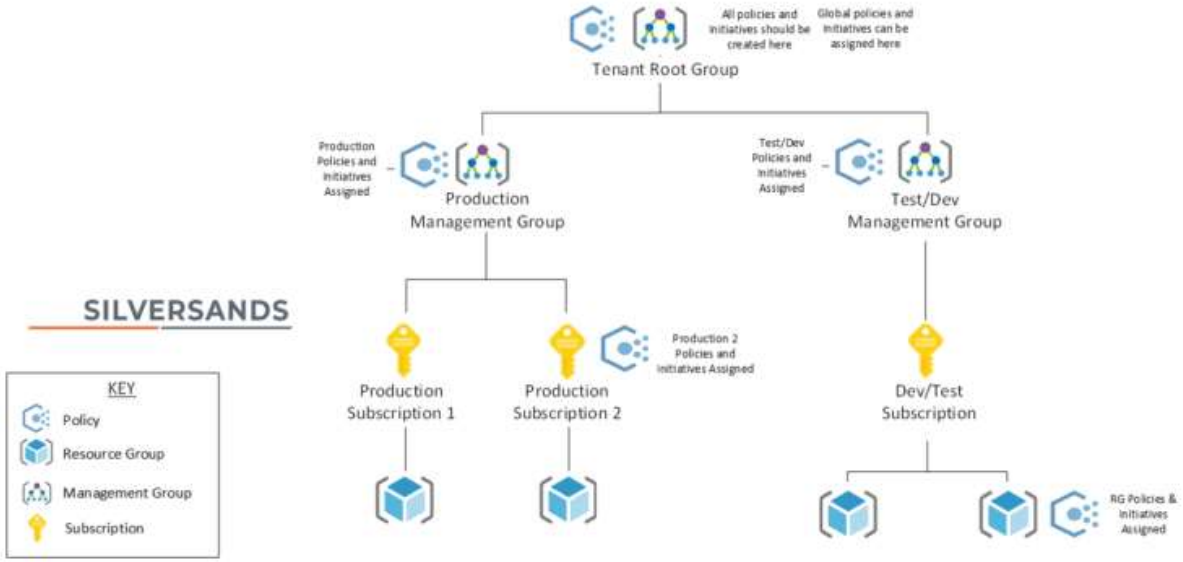
AZURE AD (ENTRA ID) ROLES AND RESPONSIBILITIES

Global Administrator: Can manage access to administrative features in Azure AD. A person in this role can grant administrator roles to other users, and they can reset a password for any user or administrator.
User Administrator: Can manage all aspects of users and groups, including support tickets, monitoring service health, and resetting passwords for certain types of users.
Billing Administrator: Can make purchases, manage subscriptions and support tickets, and monitor service health. Azure has detailed billing permissions in addition to Azure RBAC permissions.

AZURE POLICY

- **Azure Policy** is a free Azure service that allows you to create policies, assign them to resources, and receive alerts or take action in cases of non-compliance with these policies. **Azure Policy** allows you to define both individual policies and groups of related policies, known as ***initiatives*.**
- The basic elements of Azure Policy are **Policy Definition, Initiatives,** and **Initiative or Policy assignments.**
- **Policy Definition** explains resource compliance (**following a rule order**) and what effect to take when resources are non-compliant (**failing to act in accordance with rules or regulations**). Example: Restrict the list of locations where users can deploy resources.
- The **initiative** is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind. Example: All policies that relate to billing can be grouped in one initiative.
- **Policy or initiative assignment:** Describes where the policy is applied. Can be a resource group or subscription. Example: The policy to limit the list of locations where users can deploy resources is applied only to the finance team's resource group, and not to the Dev team's resource group.

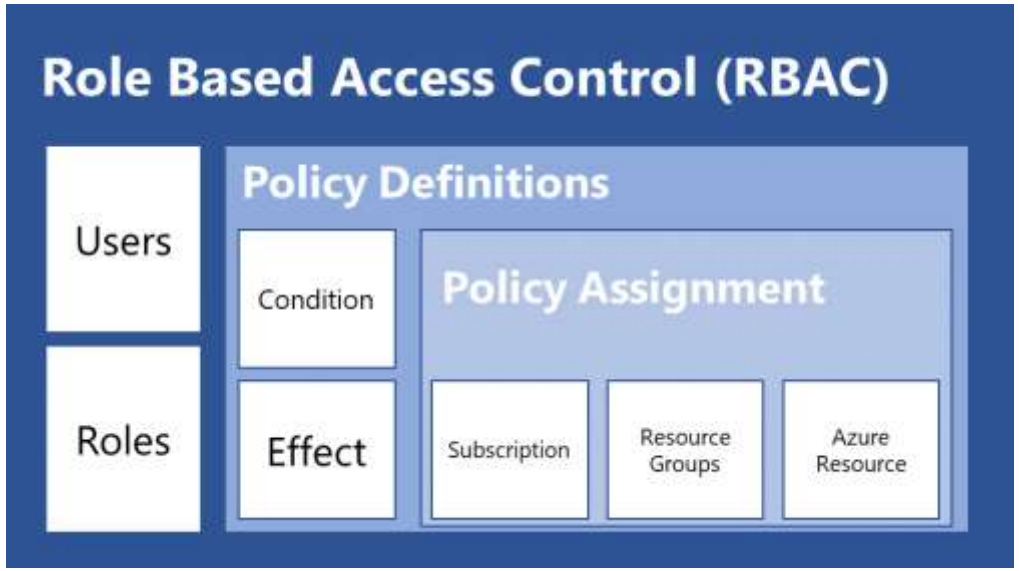




- GENEL- PUBLIC

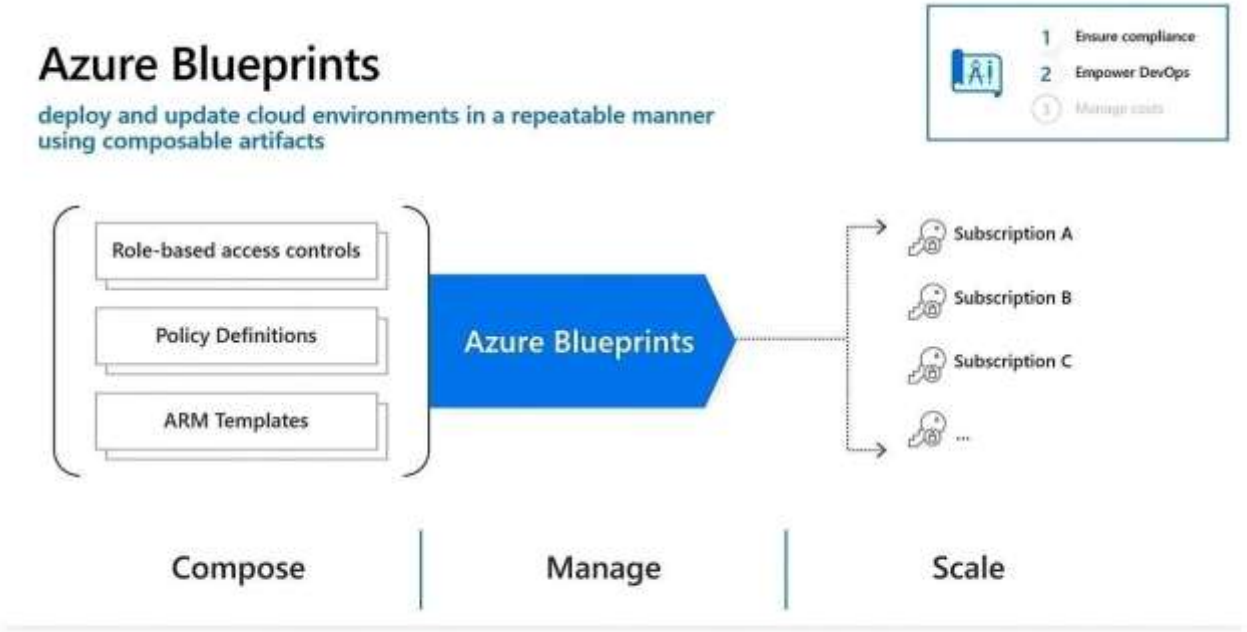
AZURE POLICY AND RBAC

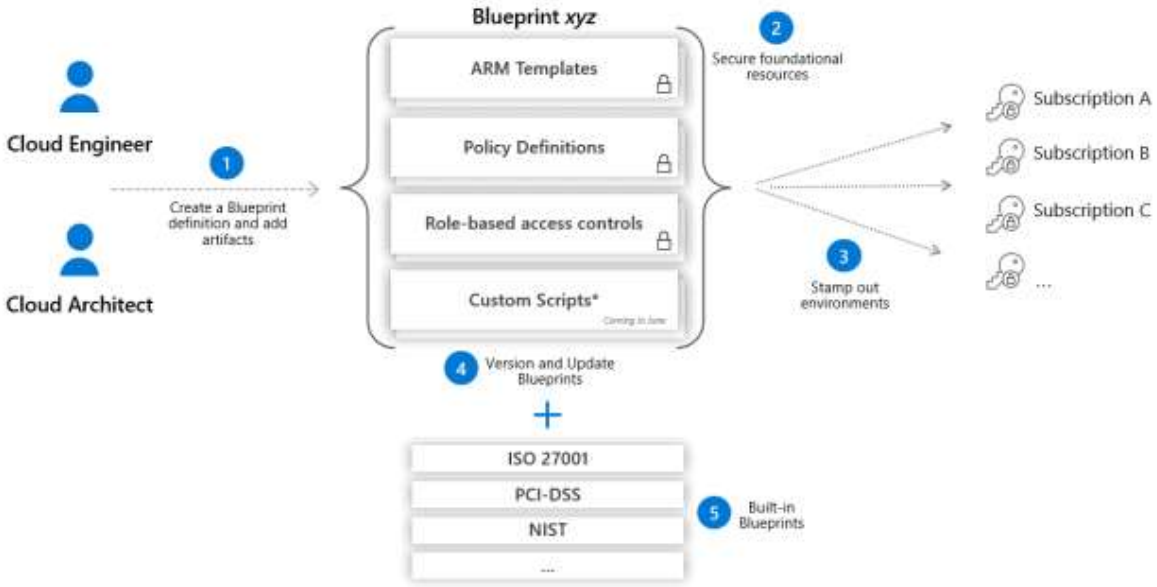
- Azure Policies and RBAC, both services work hand-in-hand to provide governance around your environment. **Azure Policy** is based on how scope works in **Azure Resource Manager**. **RBAC** grants **access** to users or groups within a subscription whereas **policy** is defined **within the resource group or subscription**. **RBAC** focuses on **what resources** the users can access and the **policy** is focused on the **properties of resources**.
- **Azure Policy** is used to prevent users from creating resources that violate **organizational standards**. Policies are rules that define what resources are allowed or disallowed in your Azure environment. Policies can be created at a **management group**, **subscription**, or **resource group** level. These policies can then be assigned to **specific scopes**, such as management groups or subscriptions.
- **Azure Policy** can be used to enforce a variety of resource configuration settings, such as **resource tags**, **required resource types**, **required resource locations**, and **minimum resource sizes**. Policies can also be used to **enforce compliance** with **regulatory** requirements such as HIPAA, PCI-DSS, and GDPR.



AZURE BLUEPRINTS

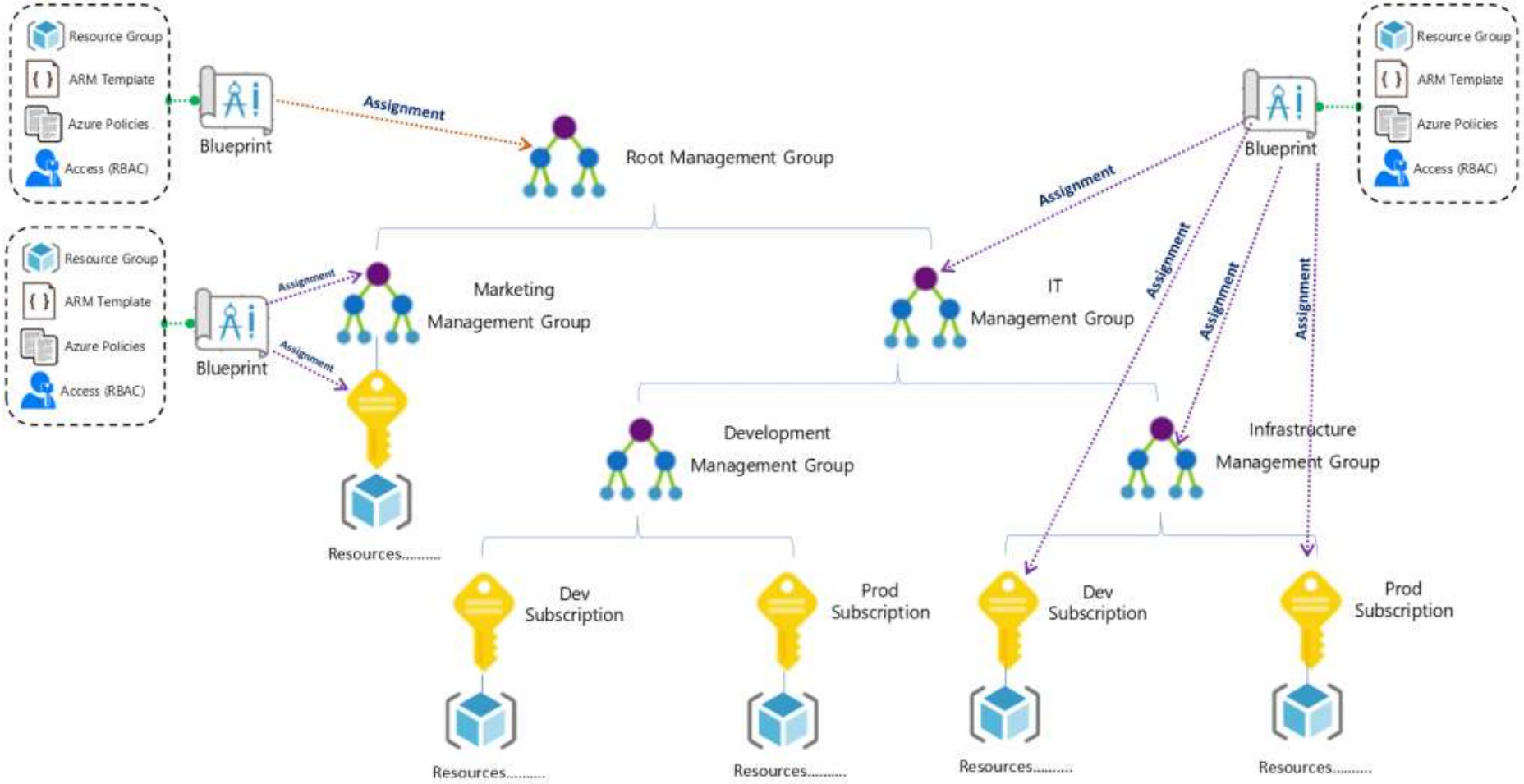
- **Azure Blueprints,** a blueprint is a package or container for composing focus-specific sets of standards, patterns, and requirements related to the implementation of Azure cloud services, security, and design that can be reused to maintain consistency and compliance.





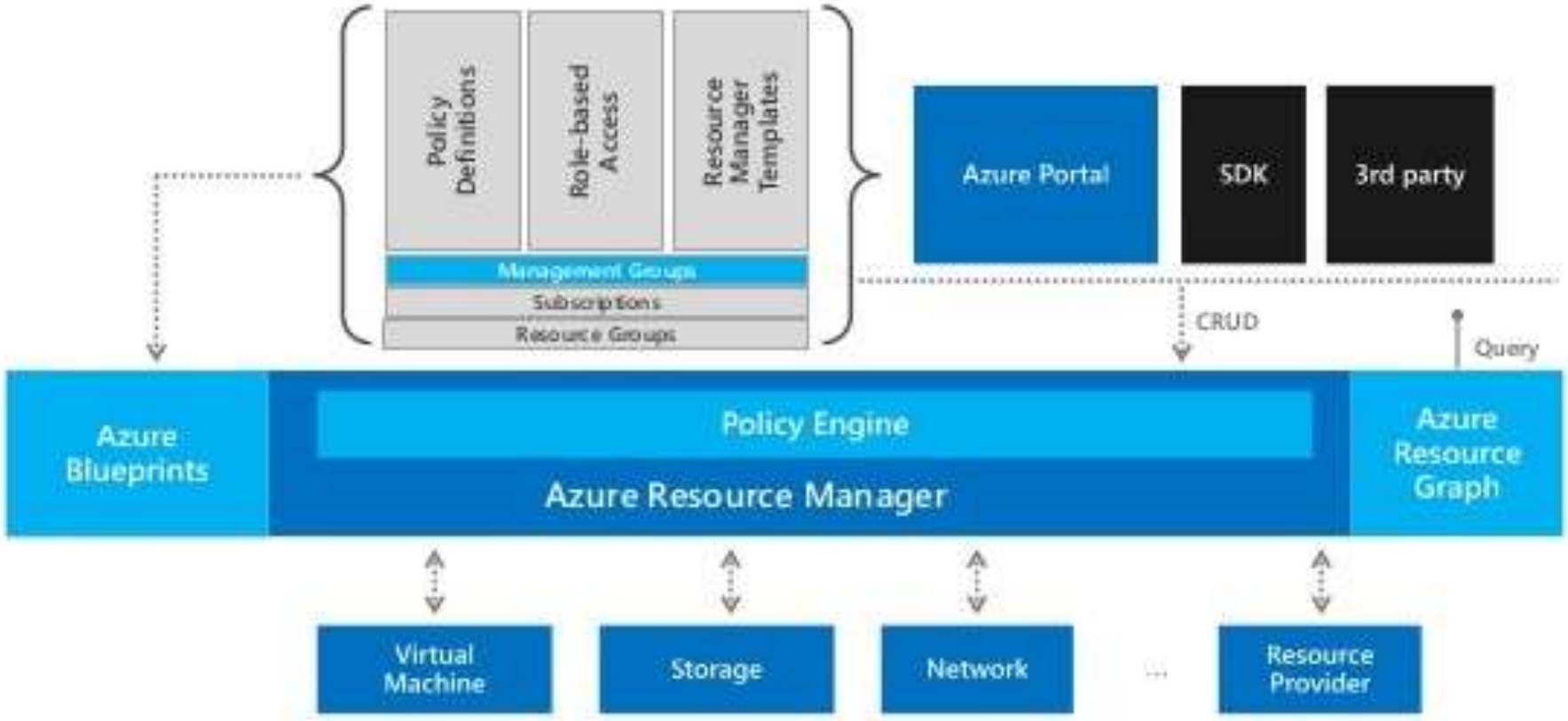
AZURE BLUEPRINTS

- **Azure Blueprint** allows you to create a way to package all these components together and makes it super easy to "**stamp**" your blueprint on any **environment** dev, test, prod, or other.



- GENEL- PUBLIC

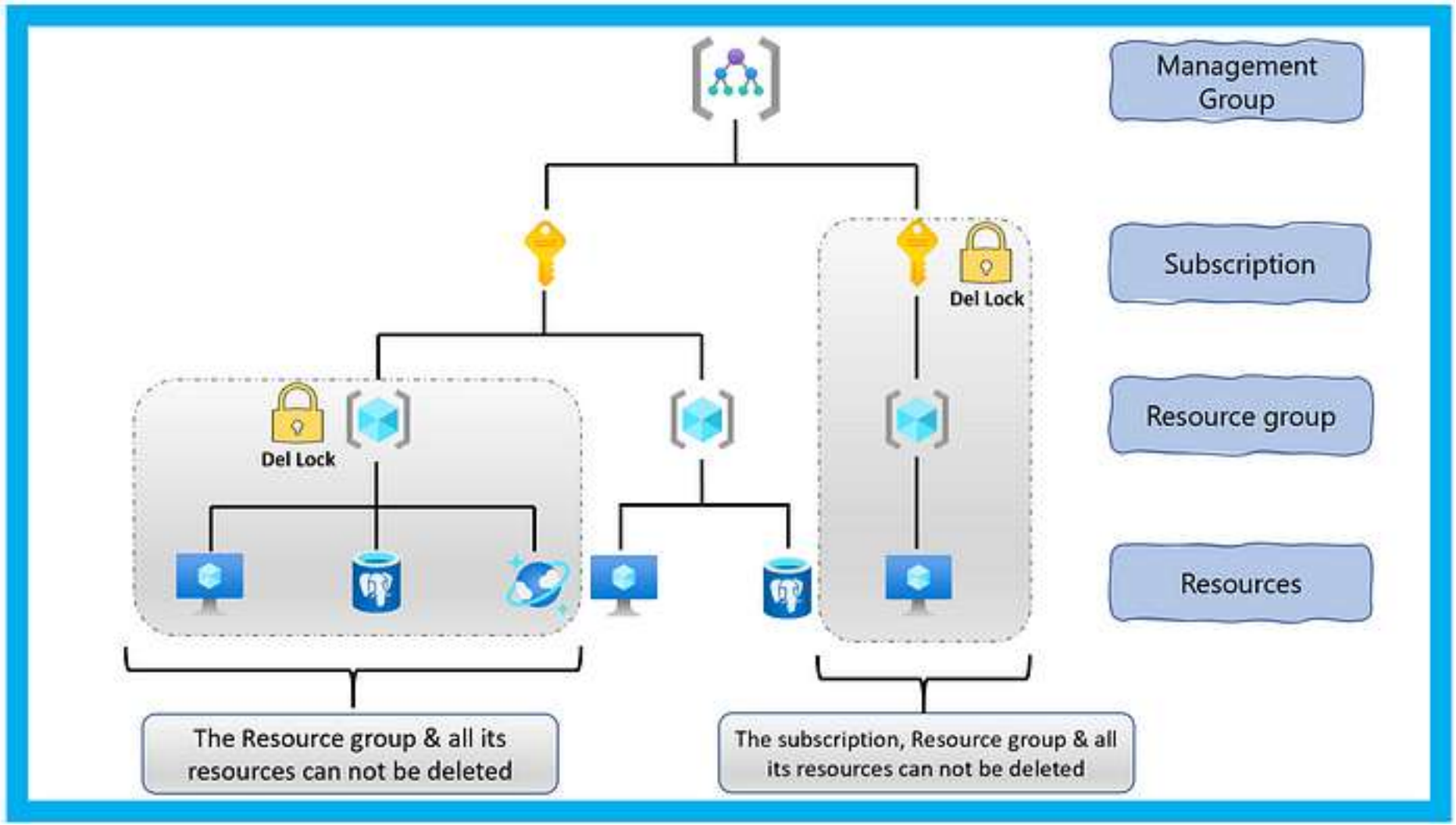
Cloud blueprints are much like the blueprints used in the construction industry. They contain all the key information and **bill of materials** to successfully build and deploy applications in the cloud including server, software, storage, network, images, and firewall details, and most importantly how they all relate together.



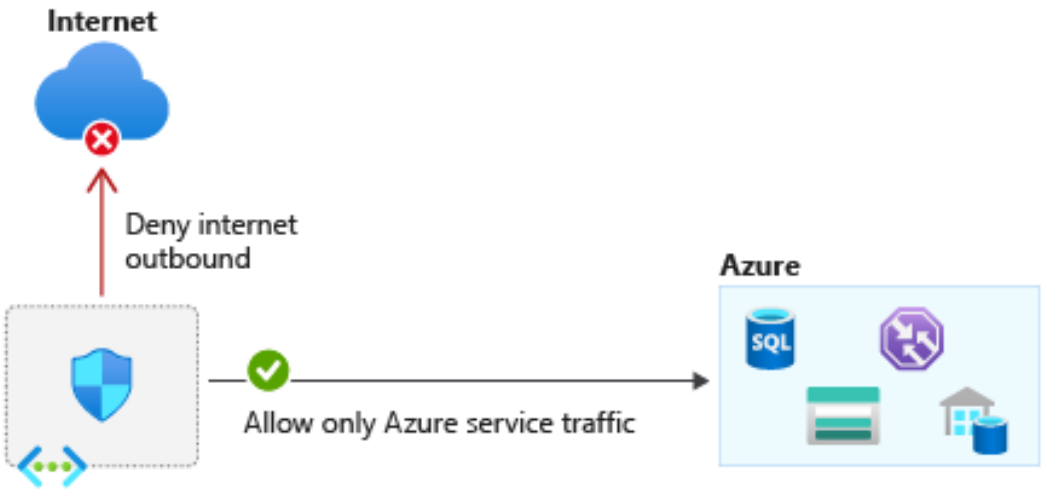
COMPARISION OF POLICY, BLUEPRINT AND RBAC

Topics	Azure RBAC	Azure Policy	Azure Blueprints
Focus	• RBAC focuses on what resources the users can access.	• The policy is focused on the properties of resources.	• Focuses on specific sets of standards, patterns, and requirements related to the implementation of Azure cloud services, security, and design.
Scope	• Grant access to users or groups within a subscription.	• Policy within the resource group or subscription.	• Assigned to a subscription in a single operation that can be audited and tracked.
Integration	• All three services work hand-in-hand to provide governance around your environment.		

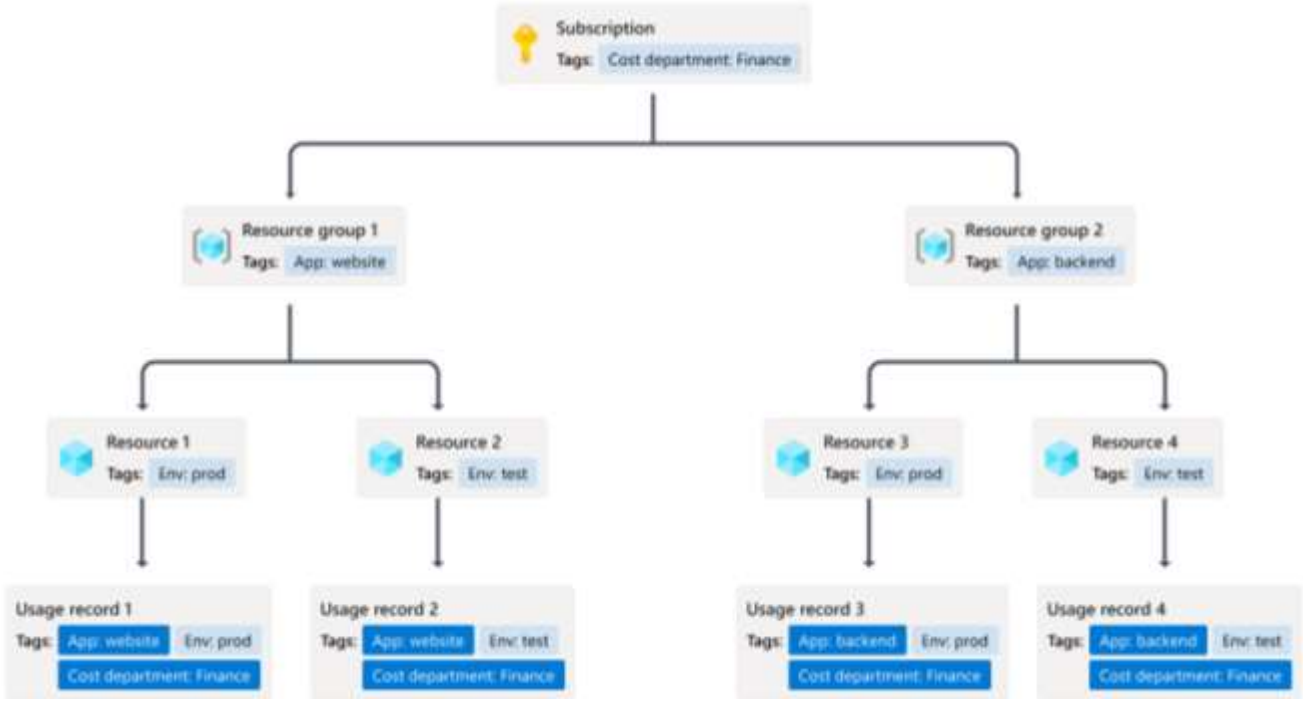
A **resource lock** prevents resources from being accidentally deleted or changed.



Resource tags provide extra information, or metadata, about your resources to manage resources based on these tags.



Network Security Group (NSG)				
Action	Name	Source	Destination	Port
Allow	AllowStorage	VirtualNetwork	**Storage**	Any
Allow	AllowSQL	VirtualNetwork	**Sql.EastUS**	Any
Deny	DenyAllOutBound	Any	Any	Any

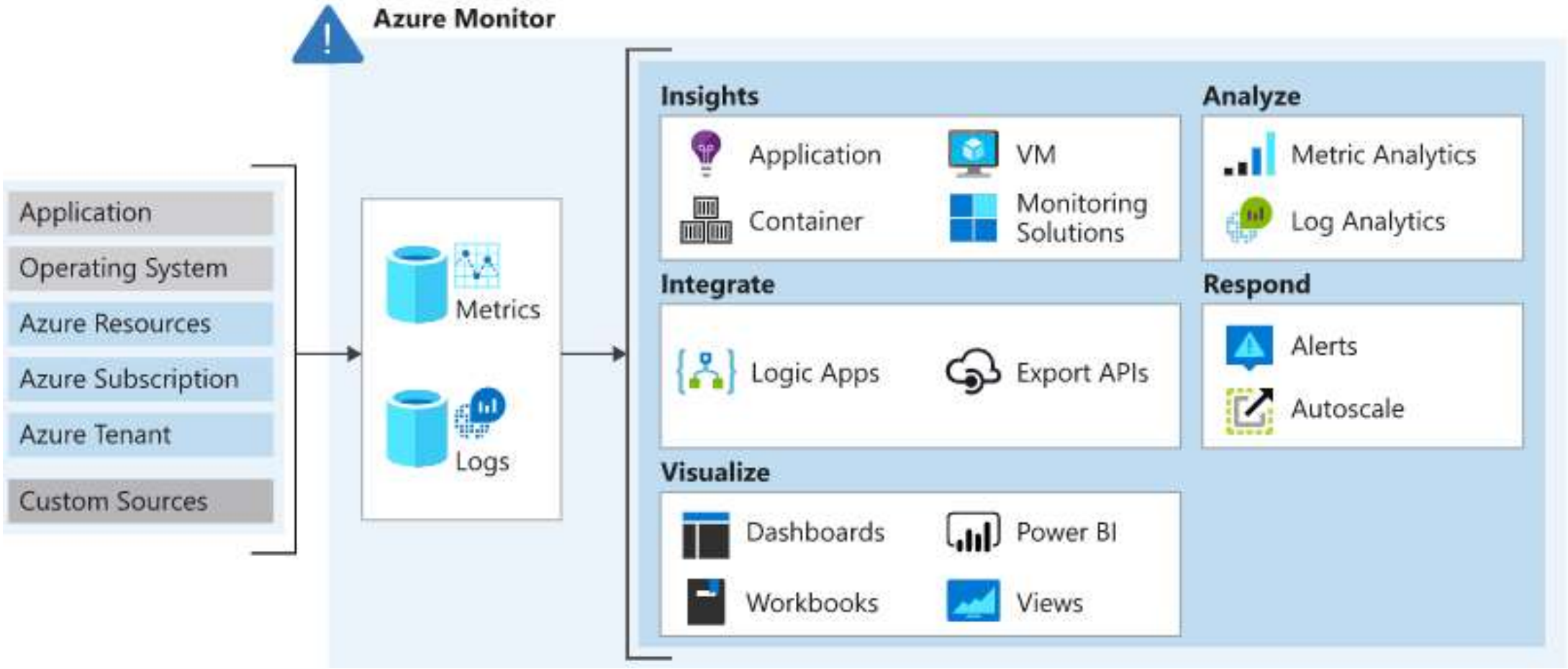


Additional Info:
Service Tag List:
https://learn.microsoft.com/en-us/azure/virtual-network/service-tags-overview#available-service-tags
Azure IP Ranges and Service Tags (JSON):
https://www.microsoft.com/en-us/download/details.aspx?id=56519

Orion Innovation

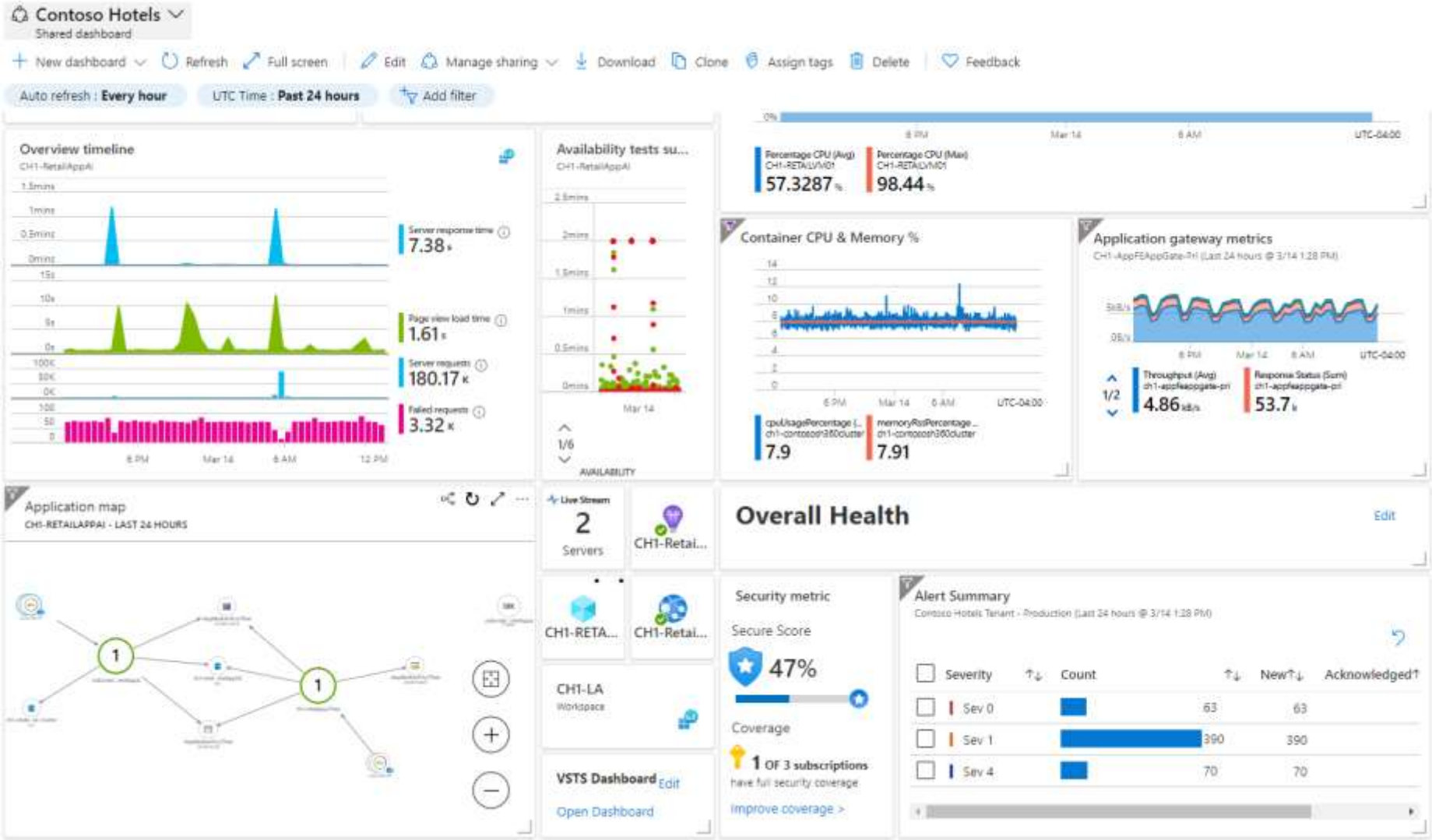
Cloud Monitoring

Azure Monitor is a service for collecting, analyzing, and acting on **telemetry** from your cloud and on-premises environments.

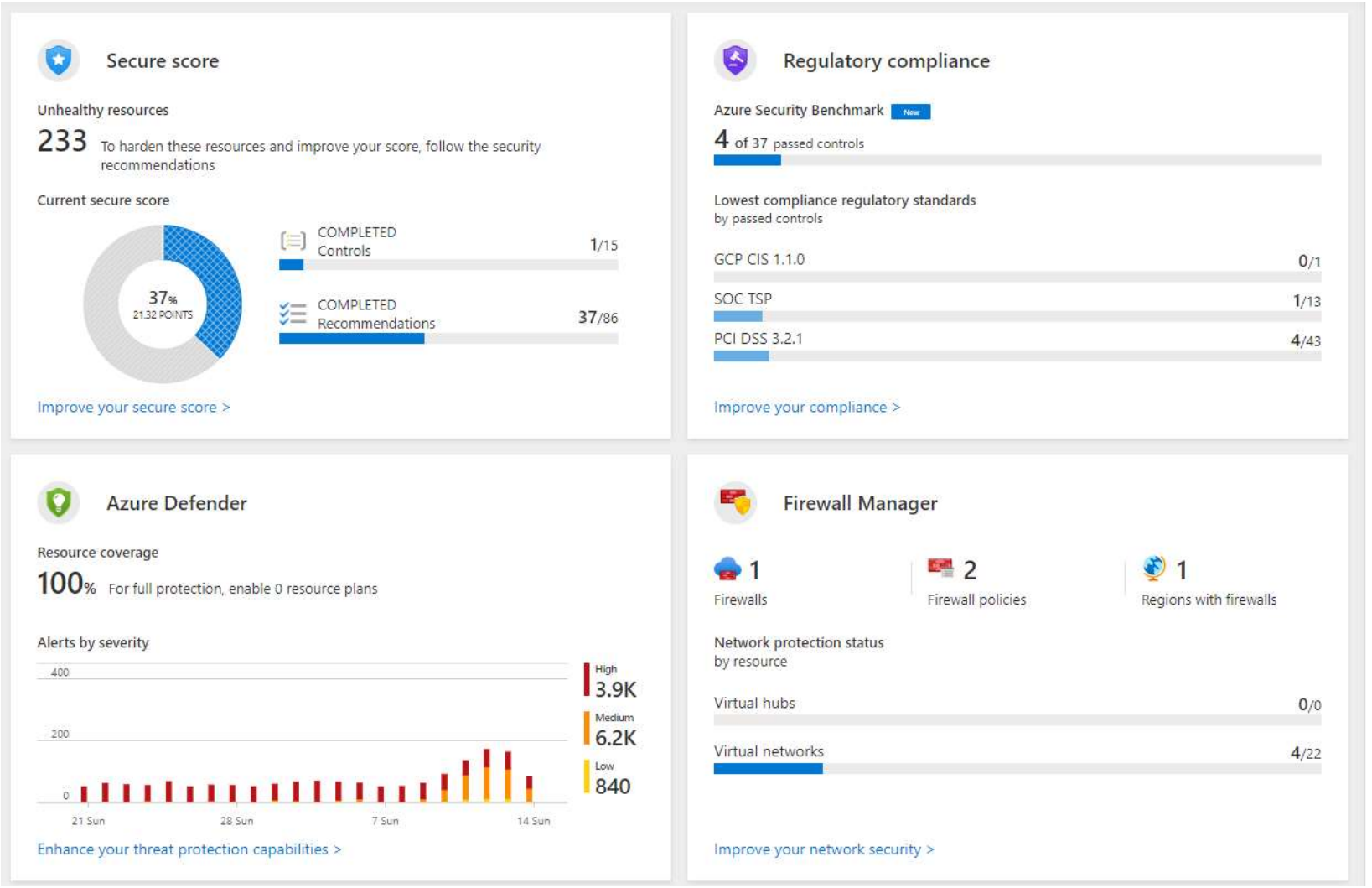


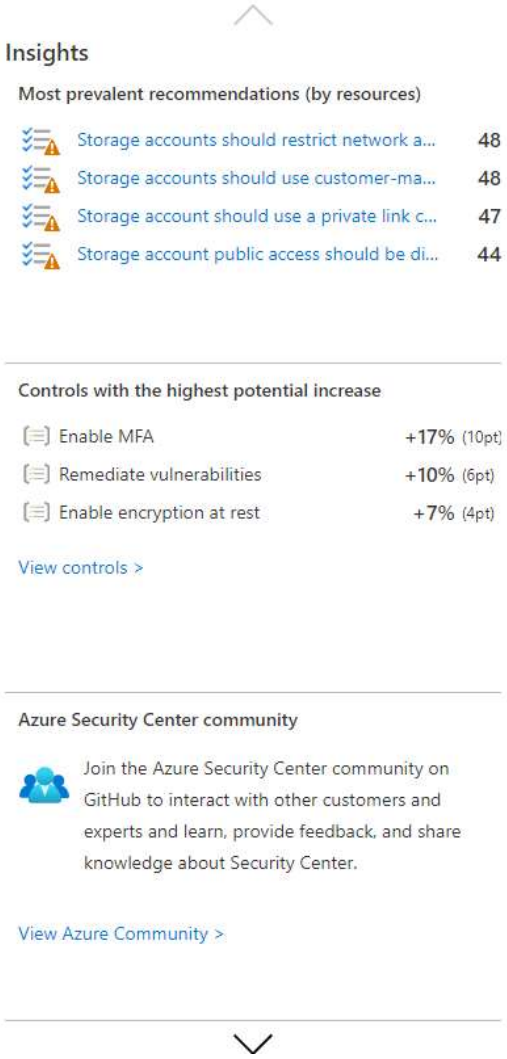
AZURE DASHBOARD

You may visualize the data yourself with **Azure dashboards** in Portal, create business views with Power BI, or create interactive reports using workbooks.

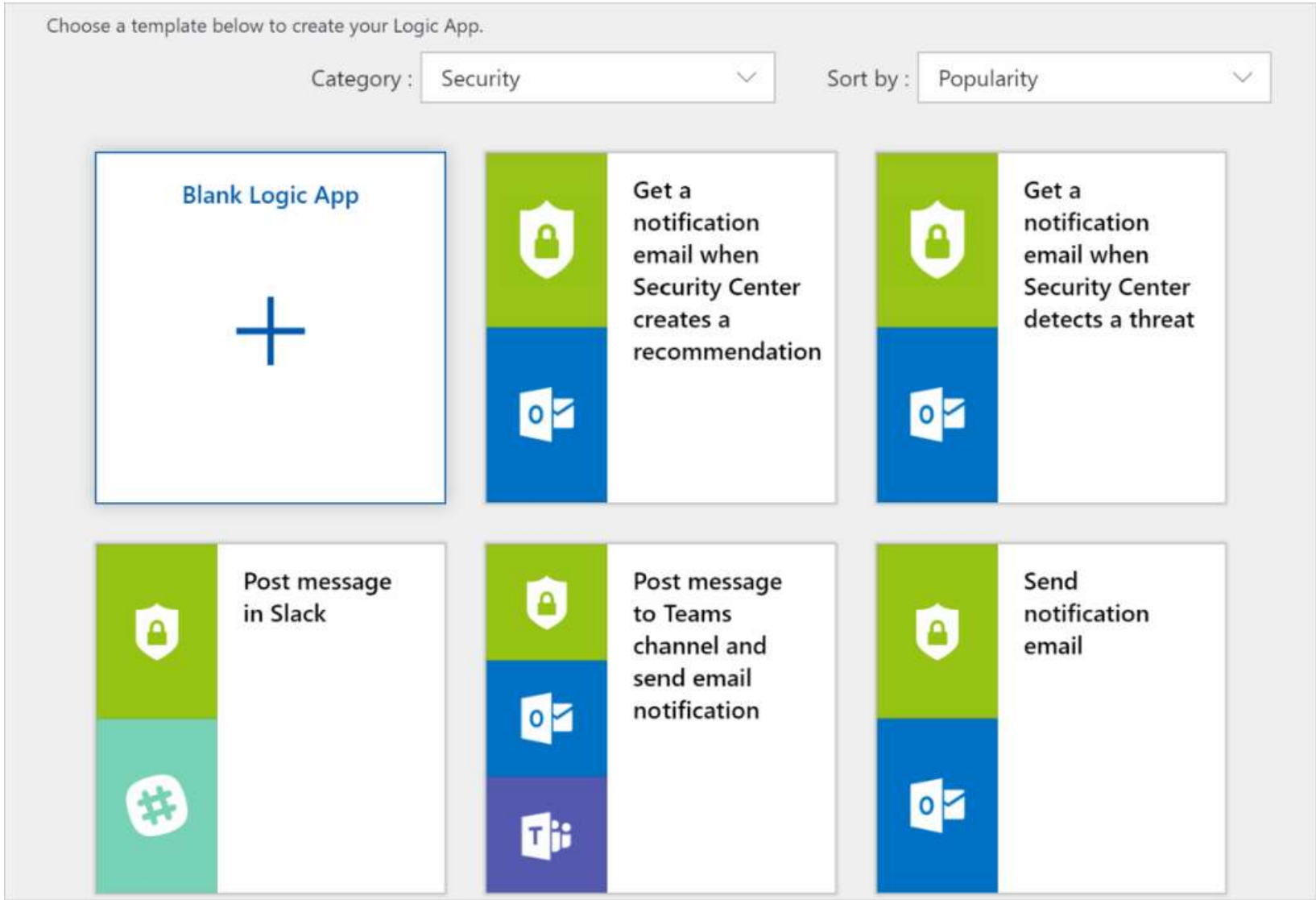


Azure Security Center is a service that manages the security of your infrastructure from a centralized location. Use Security Center to monitor the security of your workloads, whether they're on-premises or in the cloud.



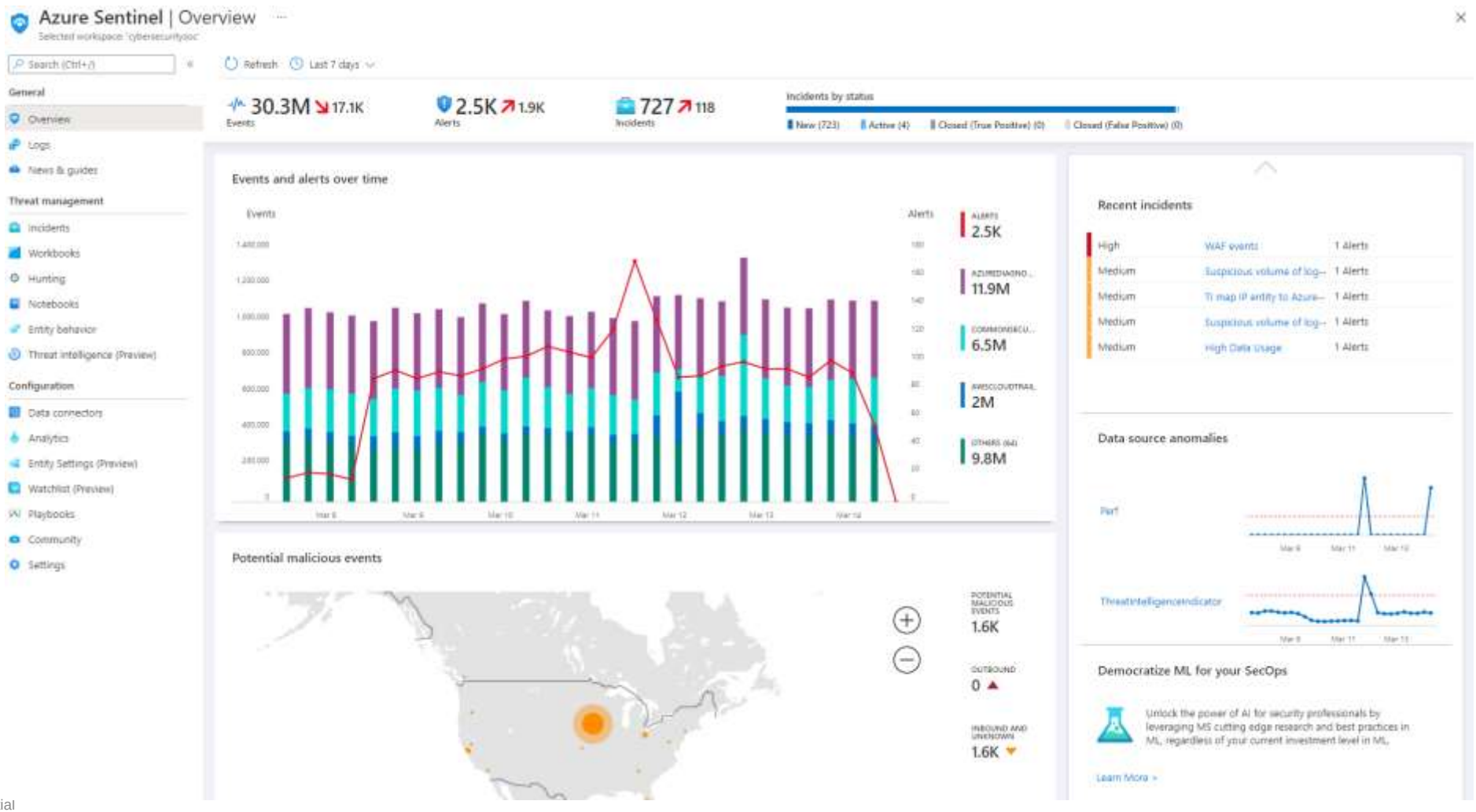


AZURE SECURITY CENTER / LOGIC APP INTEGRATION TO RESPOND THREATS

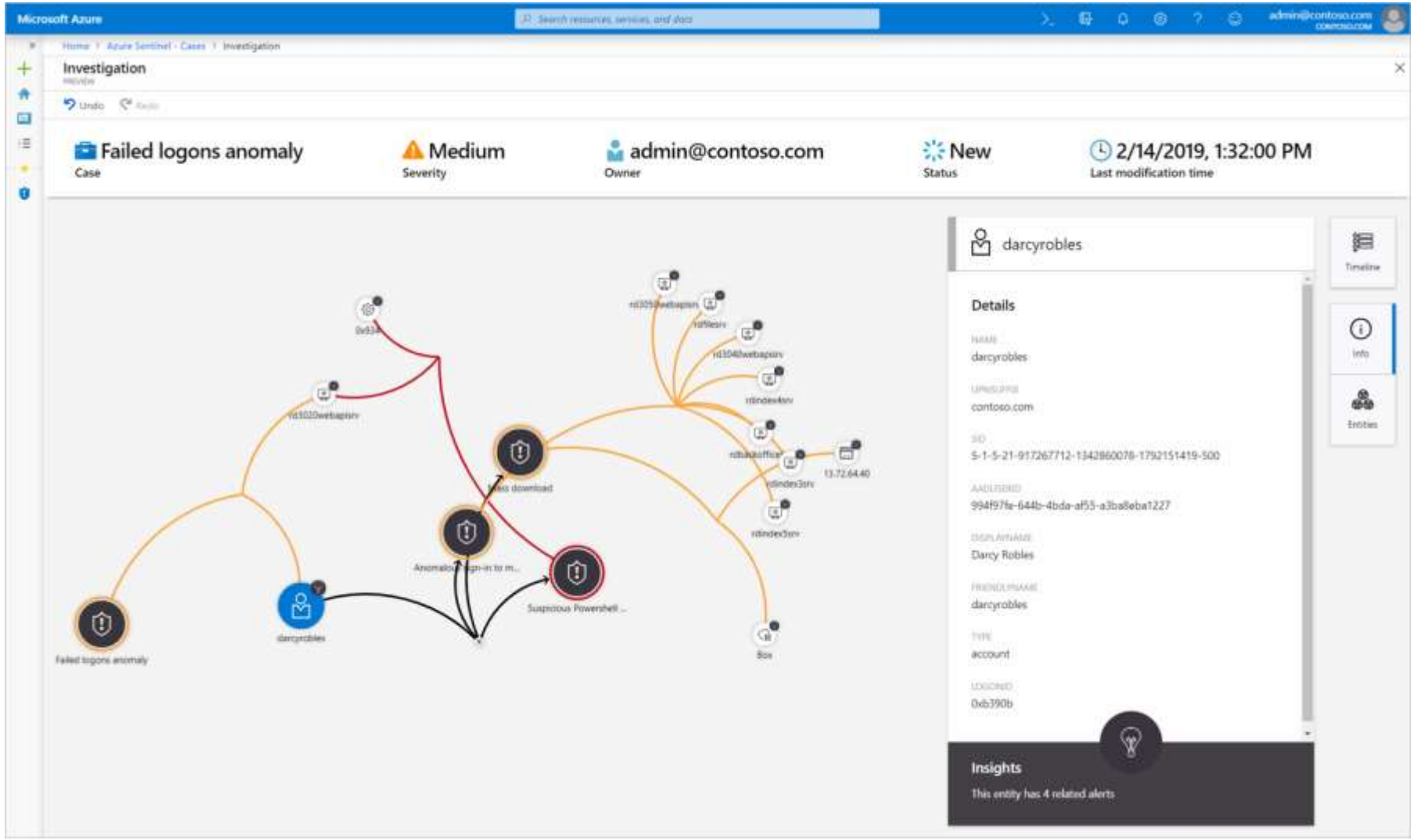


AZURE SENTINEL

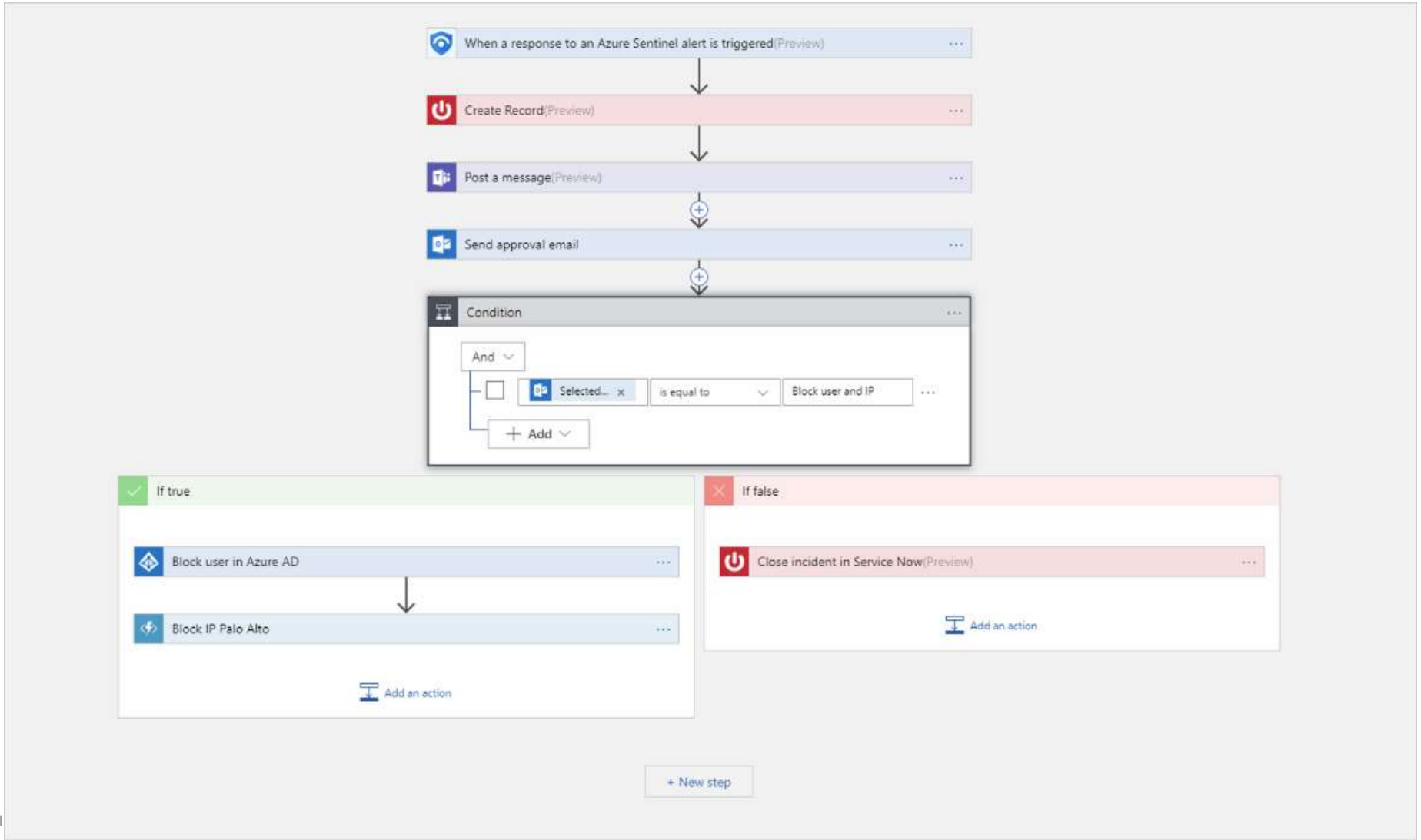
You use **Azure Sentinel** to collect data on the devices, users, infrastructure, and applications across your enterprise**. Built-in threat intelligence** for detection and investigation can help **reduce false positives**. Use Sentinel to proactively hunt for threats and anomalies, and respond by using orchestration and automation.



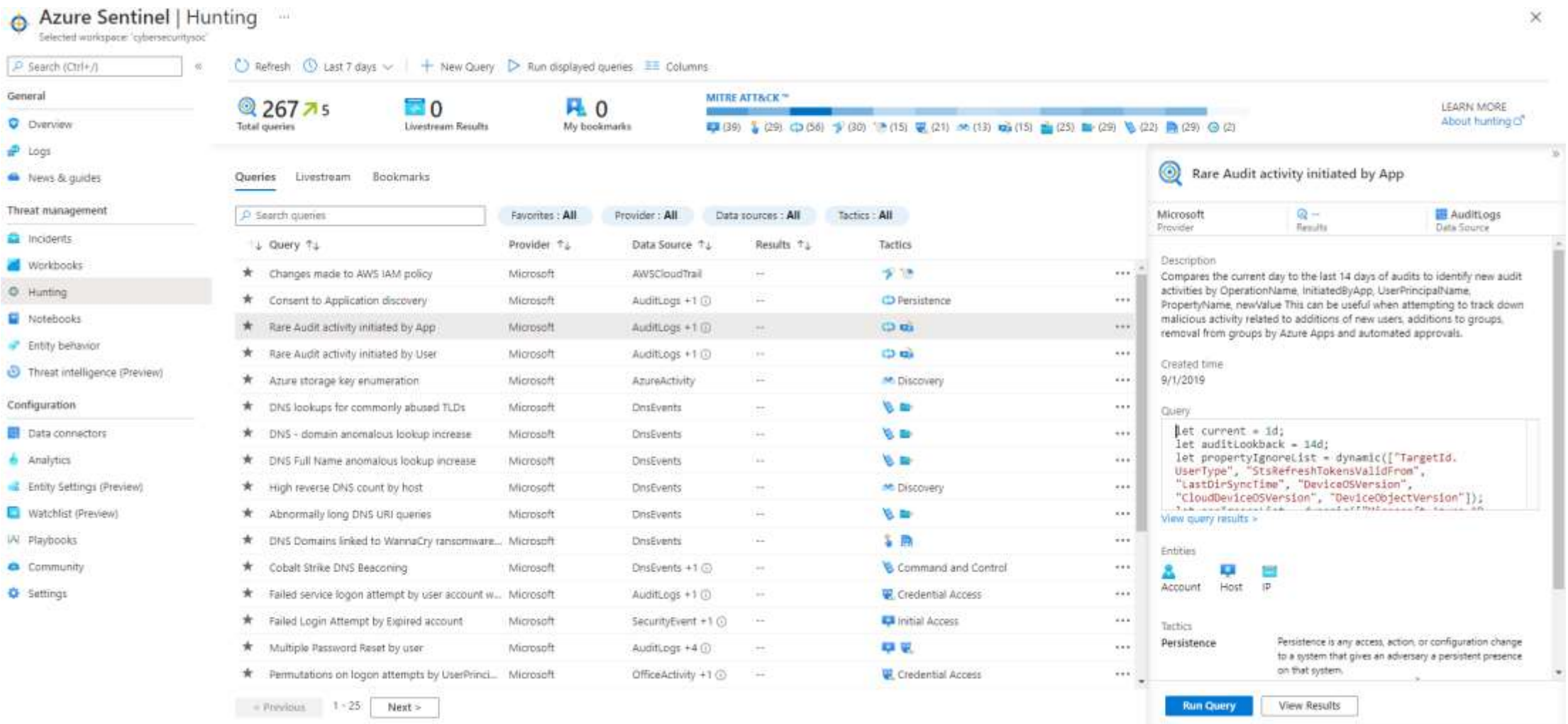
Incidents help you group and combine alerts that are related. You use incidents to reduce the noise generated because of the scale of the data. Incidents also help you to further investigate any anomalous activities or threats that have raised alerts.



Use **playbooks** to automate your response to alerts in Sentinel. You configure playbooks by using Azure Logic Apps. Your playbook details the steps to take when an alert is triggered in Sentinel.



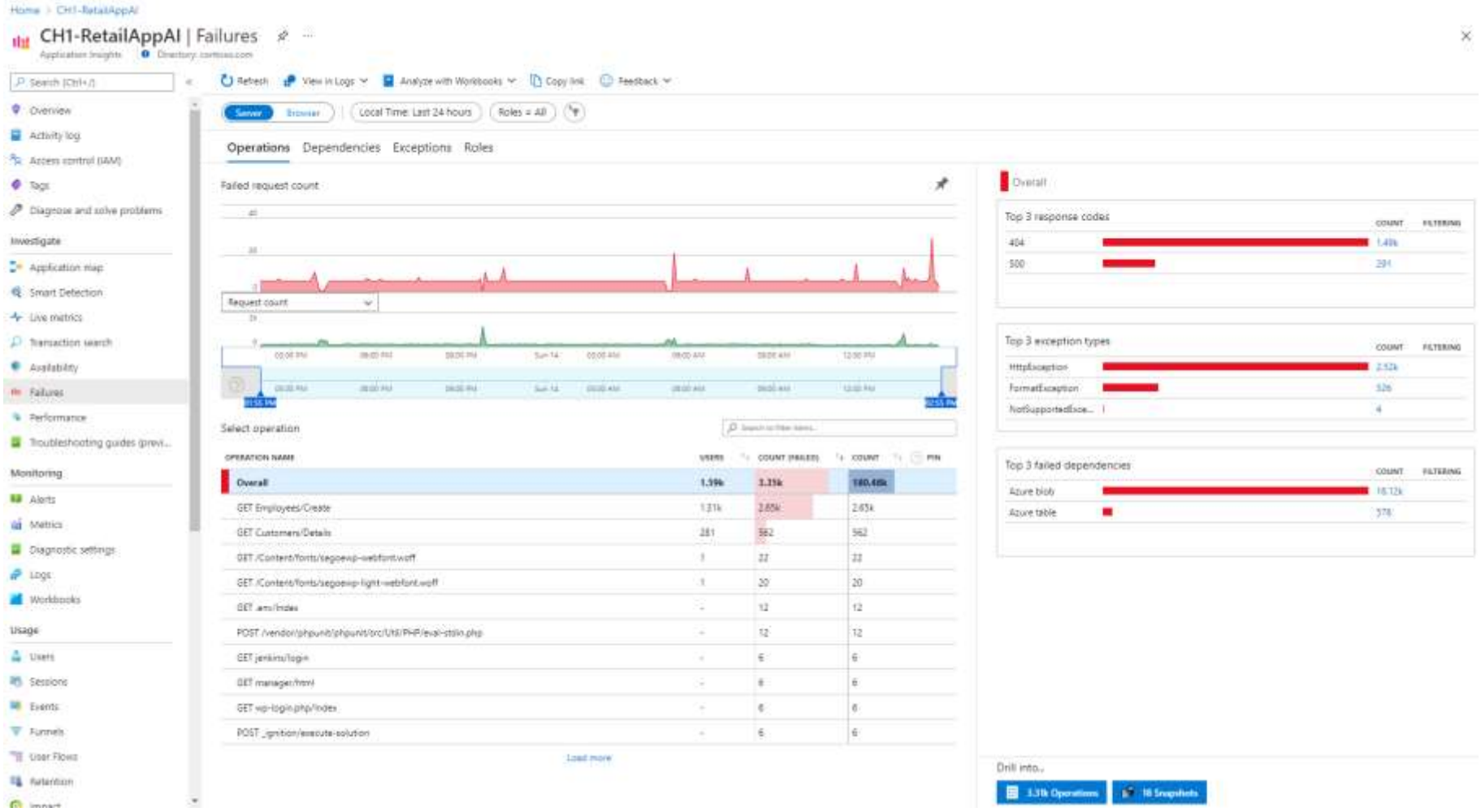
Use **hunting queries** to look for threats across your enterprise before alerts are raised. Microsoft security researchers maintain built-in hunting queries that act as a base for you to build your own queries.



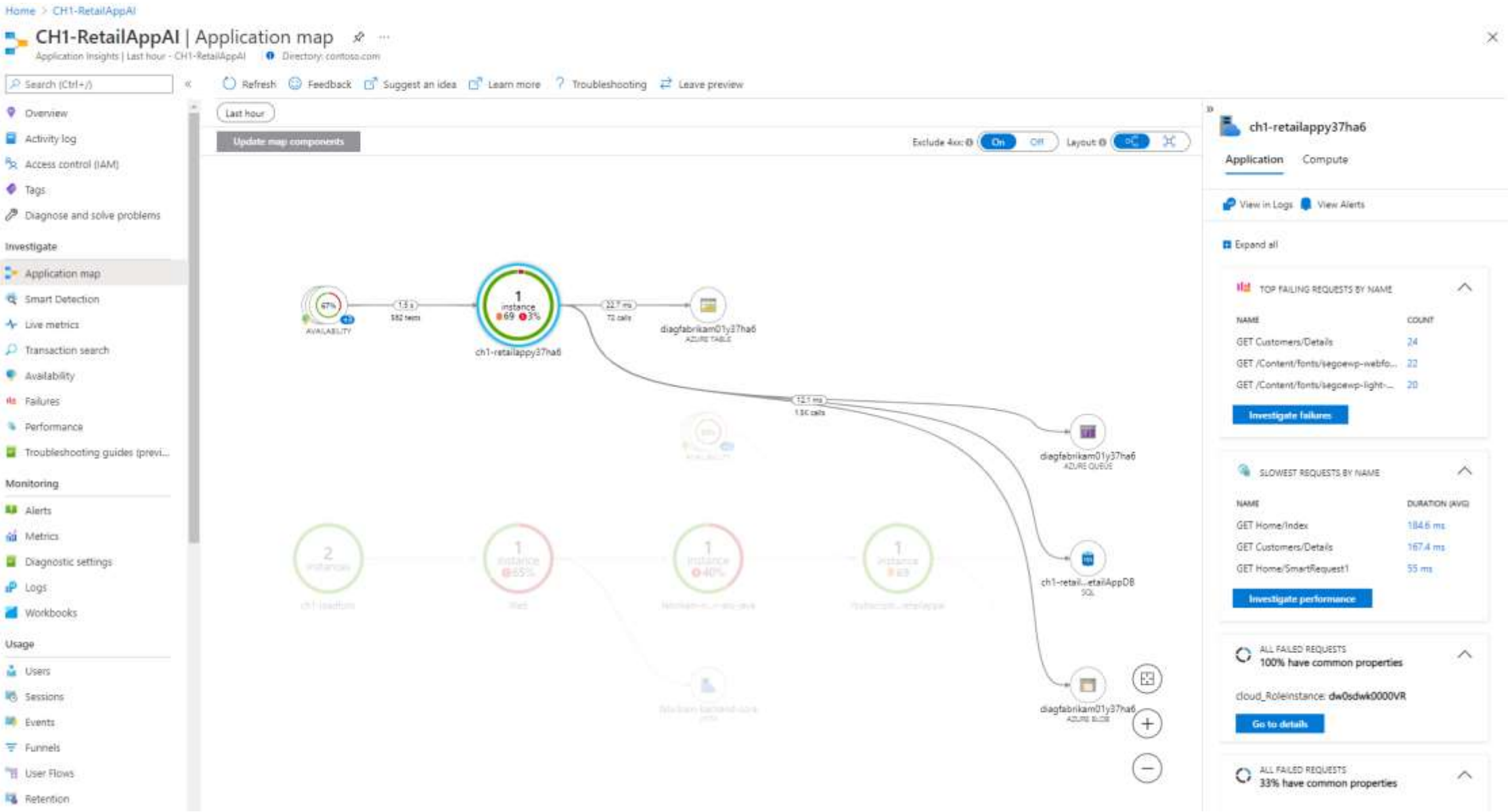
AZURE APPLICATION INSIGHTS

You use Application Insights to:

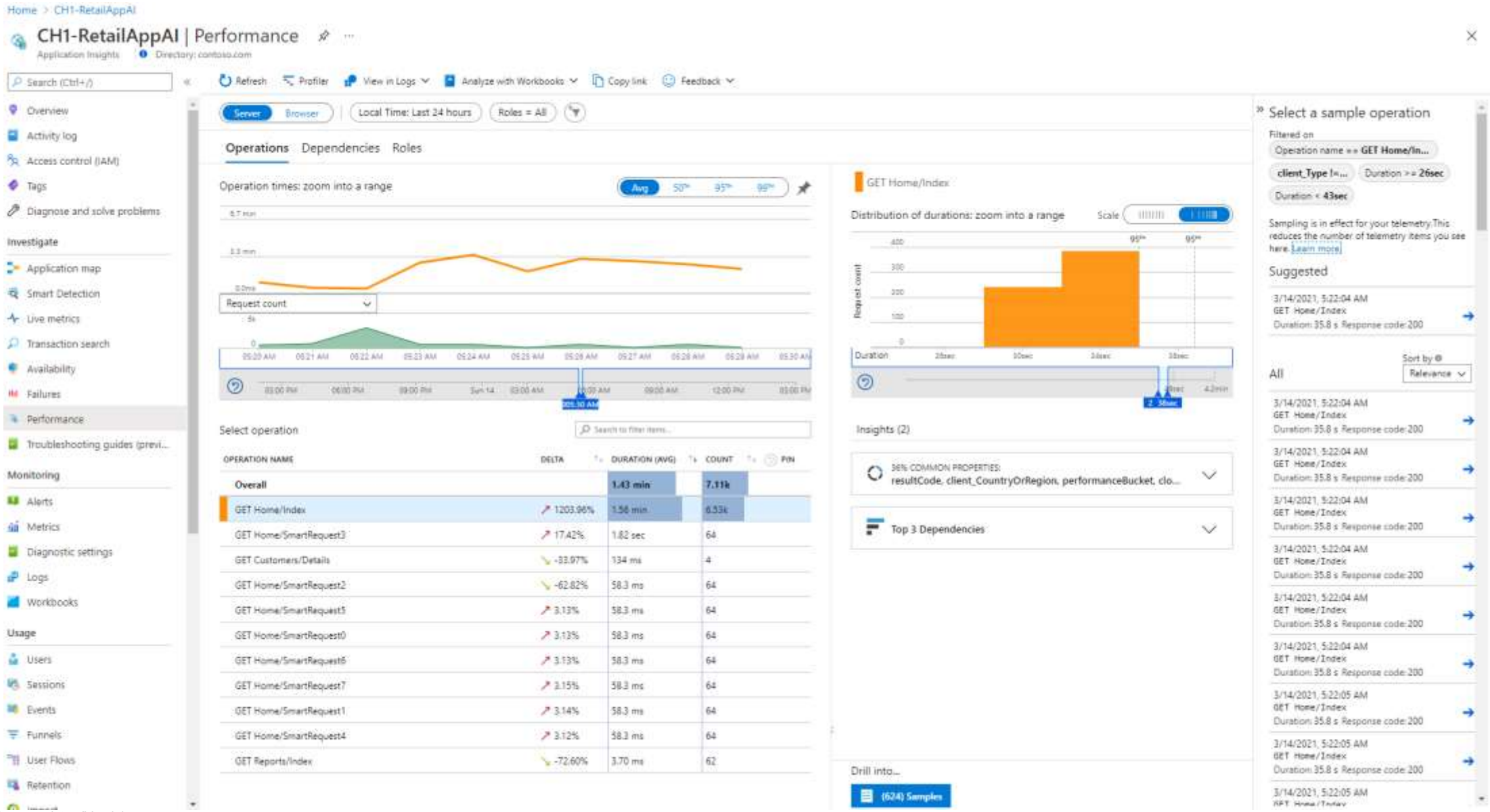
- Analyze and address issues and problems that affect your application's health and performance.
- Improve your application's development lifecycle.
- Measure your user experience, and analyze users' behavior.



AZURE APPLICATION INSIGHTS / APP DEPENDENCIES



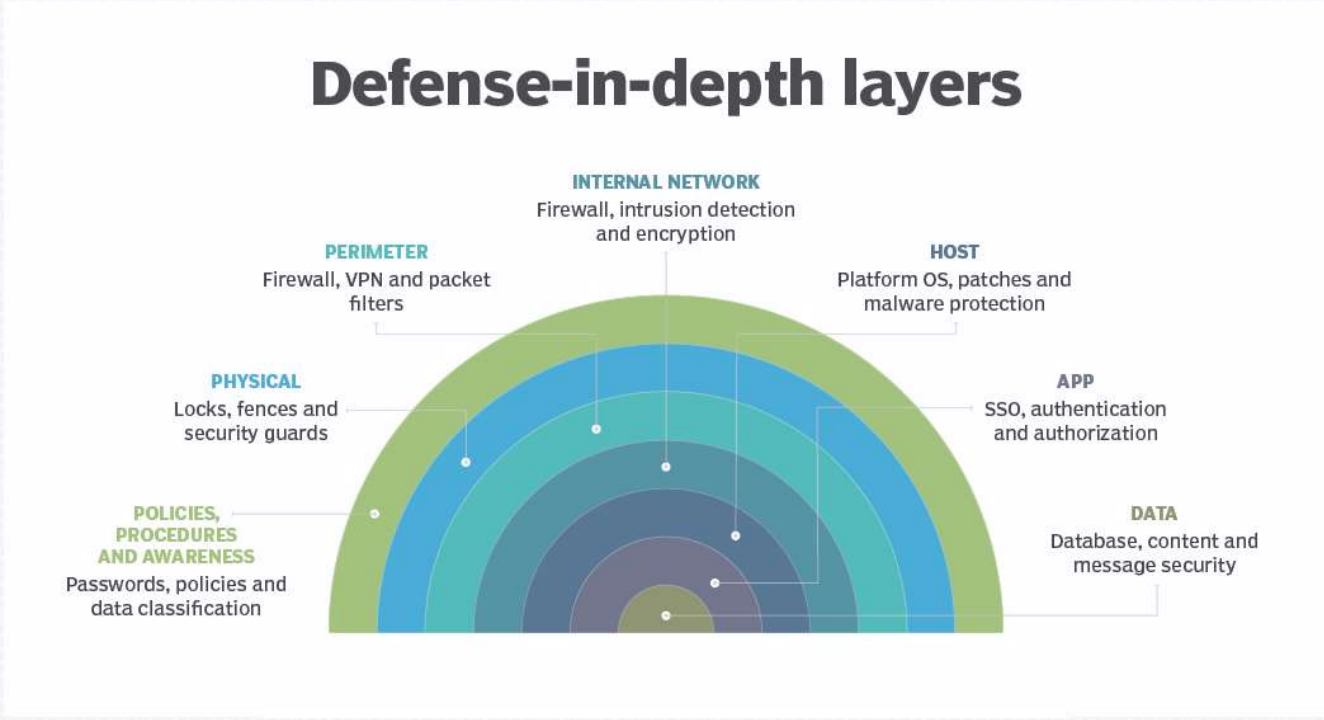
AZURE APPLICATION INSIGHTS / APP PERFORMANCE



Orion Innovation

Cloud Security

OWASP TOP10



Broken Access Control

- Bypass access control checks
- Unauthorized access to accounts
- Unauthorized creation, reading, updating and deletion of data
- Elevation of privilege

- Privacy and regulatory impacts
- The biggest breaches and largest costs

34 CWEs	Found in 3.8% apps	Weighted Exploit: 6.9
19k CVEs	Occurred 318k times	Weighted Impact: 5.9

Cryptographic Failures

- Covers
  - Some facets of “Sensitive Data Exposure”
  - Missing or ineffective data at rest controls
  - Missing or ineffective TLS
  - Missing or ineffective configuration

- Includes CWEs for hard coded passwords
- Mostly found during code reviews or static code analysis

29 CWEs	Found in 4.5% apps	Weighted Exploit: 7.3
3075 CVEs	Occurred 234k times	Weighted Impact: 6.8

Injection

- Moving down from A1 … at last
- Now covers XSS and JavaScript injection due to safer view frameworks

- Easily - but now rarely - found using tools
- Still quite exploitable

- Adopt better frameworks and more secure paved roads
- Provide observability to development teams if they use less secure alternatives
- Help by providing paved roads and gold standard support for safer frameworks

33 CWEs	Found in 3.4% apps	Weighted Exploit: 7.3
32k CVEs	Occurred 274k times	Weighted Impact: 7.2

Insecure Design

NEW

- New category obtained from data
  - Broad category, but it's NOT a catch all bucket!

- Insecure design directly impacts application security
- Insecure design is easily the costliest to fix later (up to 100x)

- **Really shift left**! Earlier integration with the development and teams
- **Threat model** Where are controls needed? Are they there? Do they work?
- **Adopt better frameworks!** Create secure paved roads **with** dev teams
- **Test, test, and test!** Create unit, integration, and other tests

40 CWEs	Found in 3.0% apps	Weighted Exploit: 6.5
2691 CVEs	Occurred 262k times	Weighted Impact: 6.8

Security Misconfiguration

- Cloud infrastructure as code == slight jump to A5
- Covers unhardened, misconfigured, and default configurations

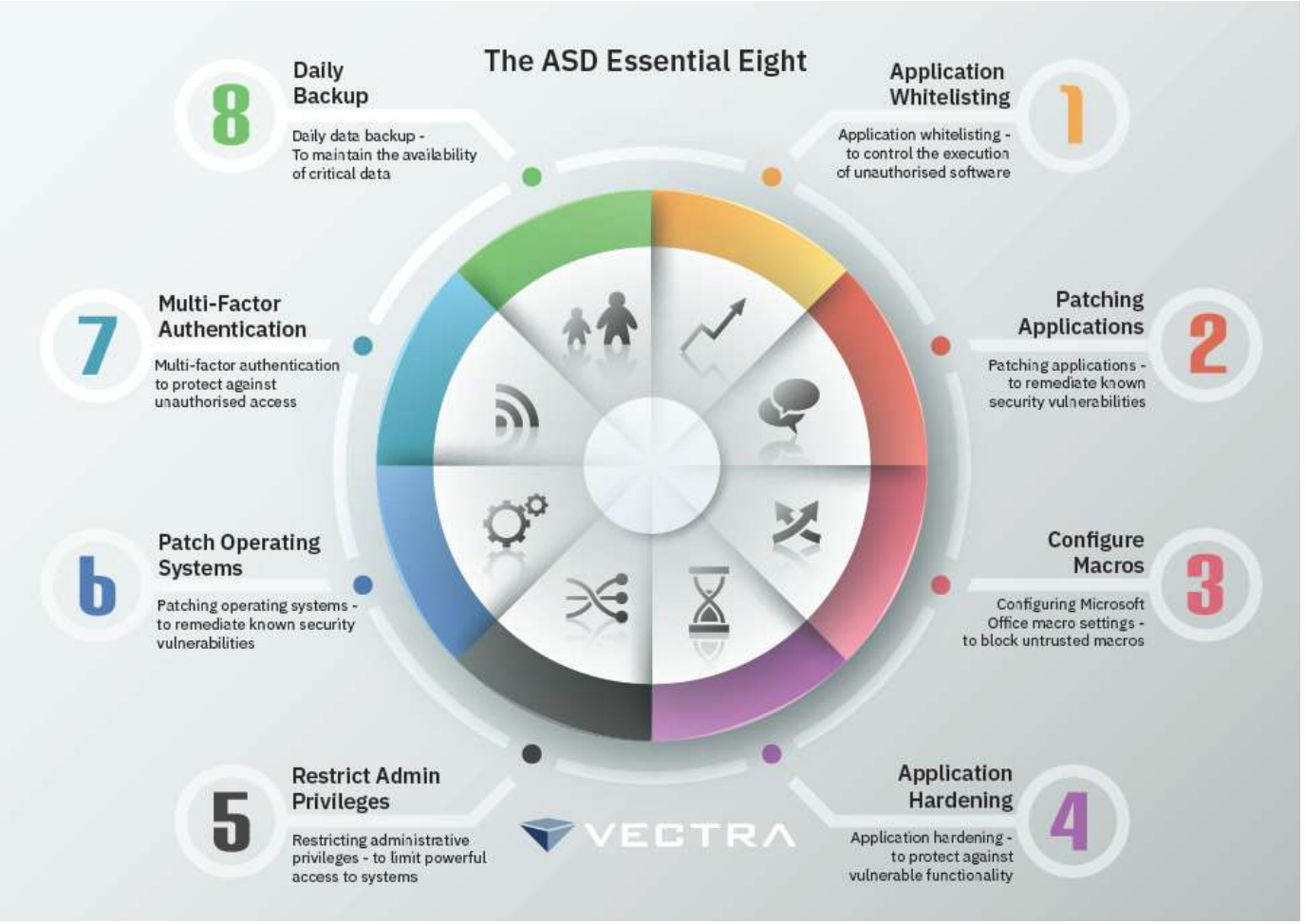
- Eliminate the risk: Build “paved road” pre-hardened development and production frameworks, components, and build configurations
- Surface the risk: Build tools to identify weakly or insecurely configured components and applications

20 CWEs	Found in 4.5% apps	Weighted Exploit: 8.1
789 CVEs	Occurred 208k times	Weighted Impact: 6.6

Vulnerable and Outdated Components

TOP 10

- Root cause of the LARGEST and MOST COSTLY breach of all time
- Covers the USG Executive Order for supply chain security
- Covers “Patching Applications” of the ASD Essential 8



- Recommend using CI/CD tools to warn for outdated components
- Strongly recommend breaking the build for vulnerable components

3 CWEs	Found in 8.8% apps	Weighted Exploit: 5.0
0 CVEs	Occurred 30k times	Weighted Impact: 5.0

Identification and authentication failures

- Includes authentication and session management issues
- CWEs cover nearly all the ASVS (Application Security Verification Standard) V2 and V3 at Level 1
- ASVS: https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

- Protect against re-used, breached, and weak passwords
- Add MFA to all the things
- Use the ASVS to improve authentication of your apps
- Consider a “paved road” secured and shared authentication service

22 CWEs	Found in 2.6% apps	Weighted Exploit: 7.4
3897 CVEs	Occurred 132k times	Weighted Impact: 6.5

Software and Data Integrity Failures

NEW

- Integrity of business or privacy critical data
- Lack of integrity of includes from content data networks
- Software updates without integrity
- CI/CD pipelines without check in or build checks, unsigned output

- Improve the integrity of the build process
- Use SBOM (Software Bill of Materials) to identify authentic builds and updates
- Use sub-resource integrity if using CDN for web page includes
- Consider how you vet and ensure npm, maven, repos are legit

10 CWEs	Found in 2.0% apps	Weighted Exploit: 6.9
1152 CVEs	Occurred 47.9k times	Weighted Impact: 7.9

Security Logging and Monitoring Failures

- Critical to reduce the breach window, response time, and cleanup
- Necessary if you have breach disclosure laws
- Critical if you intend to prosecute

- Interview or code review the best review technique
- Static code analysis can’t find the absence
- Still difficult to dynamically test

4 CWEs	Found in 6.5% apps	Weighted Exploit: 6.9
242 CVEs	Occurred 53.6k times	Weighted Impact: 5.0

Server-Side Request Forgery (SSRF)

TOP 10

- Everyone needs to learn how to test
  - Developers
  - AppSec Professionals
- Frameworks need to protect against SSRF by default
- IDEs (and frameworks though *doc) need to highlight potential SSRF

1 CWEs	Found in 2.7% apps	Weighted Exploit: 8.2
385 CVEs	Occurred 9.5k times	Weighted Impact: 6.7

Next Steps

- OWASP Top 10 is the MINIMUM
- There’s always something that nearly makes it in
- Include these in any coding standard or testing

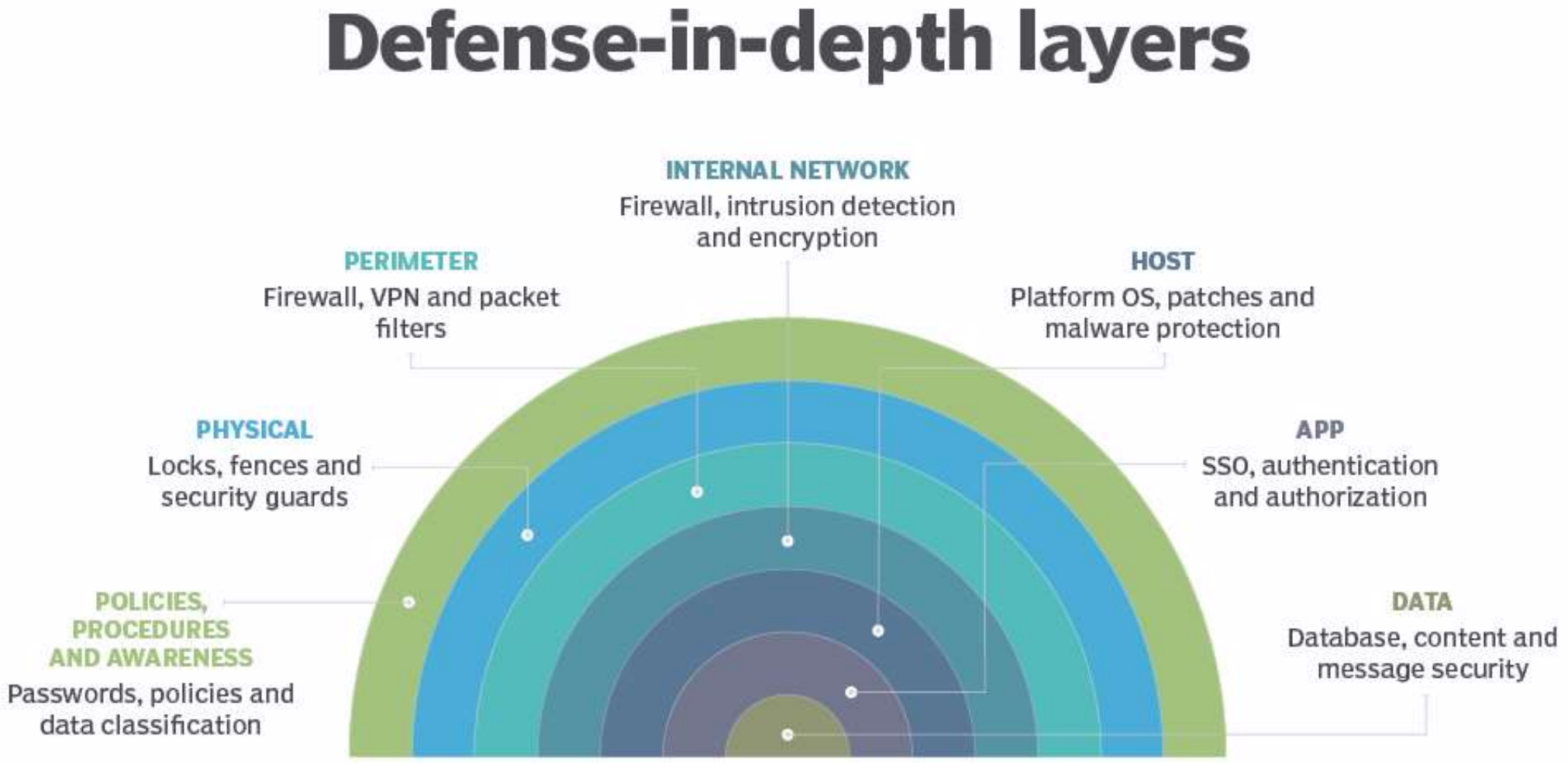
- **Code Quality issues**
- **Denial of Service**
- **Memory Management Errors**

SECURITY POSTURE

Security posture refers to an organization's **overall cybersecurity strength** and how well it can **predict, prevent and respond** to ever-changing cyberthreats.

Suggestions:

- **Create a cybersecurity framework.** Companies should align their security requirements with the goals and objectives of the business.
- **Perform a risk assessment.** A cybersecurity risk assessment identifies the level of vulnerability across an organization's assets. The results enable organizations to determine what they need to do to improve their security postures. They also help identify the security controls that should be put in place to protect the business against future attacks.
- **Prioritize risk.** After identifying the asset vulnerabilities, enterprises should then rank them based on the overall risk they pose to the business and determine what to work on first.
- **Implement automated cybersecurity tools.** Using automated tools can help reduce incident response times and prevent hackers from infiltrating the network.
- **Educate workers.** Security awareness training should be part of the onboarding process. In addition, companies should regularly test employees on their knowledge of the organization's cybersecurity policies, including ones related to social media.
- **Control administrative access privileges.** Organizations should only grant administrative access privileges to a small group of employees, like security teams. Letting too many people modify hardware and operating system settings can be disastrous to companies' security postures.
- **Track security metrics.** Security metrics enable companies to accurately measure the effectiveness of their cybersecurity posture. Security metrics can also help organizations uncover ways to mitigate risk, as well as help with prioritizing future potential risks. To be effective, a security metrics program depends heavily on what enterprises decide to measure. Consequently, companies must track the metrics that affect the business from an operational and strategic perspective.

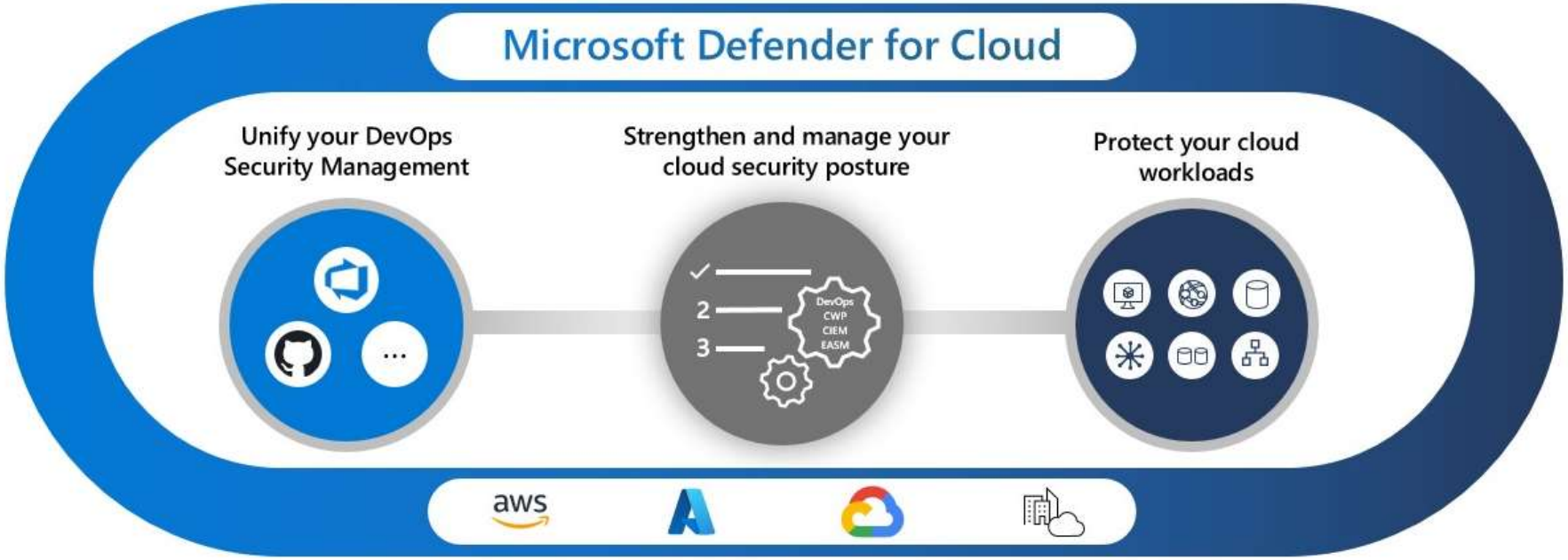


- Zero Trust is a security model that assumes the **worst-case scenario** and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.
- To address this new world of computing, Microsoft highly recommends the **Zero Trust security model**, which is based on these guiding principles:
  - **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. Use analytics to get visibility, drive threat detection, and improve defenses.
- Traditionally, corporate networks were restricted, protected, and generally assumed safe. Only managed computers could join the network, VPN access was tightly controlled, and personal devices were frequently restricted or blocked.
- The Zero Trust model flips that scenario. Instead of assuming that a device is safe because it’s within the corporate network, it **requires everyone to authenticate**. Then **grants access based on authentication** rather than location.

MICROSOFT DEFENDER FOR CLOUD

Microsoft Defender for Cloud is a cloud-native application protection platform (**CNAPP**) that is made up of security measures and practices that are designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

- A development security operations (**DevSecOps**) solution that unifies security management at the code level across multicloud and multiple-pipeline environments
- A cloud security posture management (**CSPM**) solution that surfaces actions that you can take to prevent breaches
- A cloud workload protection platform (**CWPP**) with specific protections for servers, containers, storage, databases, and other workloads



JIT VM ACCESS

Just in time VM access protect your virtual machines by only accessed based on audited access that you configure.

Home > Security Center > Just-in-time VM access >

JIT VM access configuration

ADFSHIR

+ Add Save Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range
22 *(Recommended)*	Any	Per request	N/A
3389 *(Recommended)*	Any	Per request	N/A
5985 *(Recommended)*	Any	Per request	N/A
5986 *(Recommended)*	Any	Per request	N/A

Add port configuration

Port *

Protocol

Any | TCP | UDP

Allowed source IPs

Per request | CIDR block

IP addresses

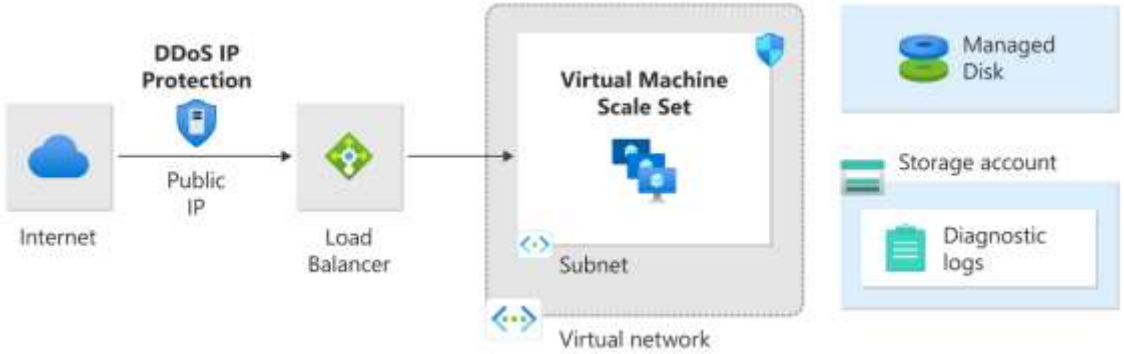
Max request time

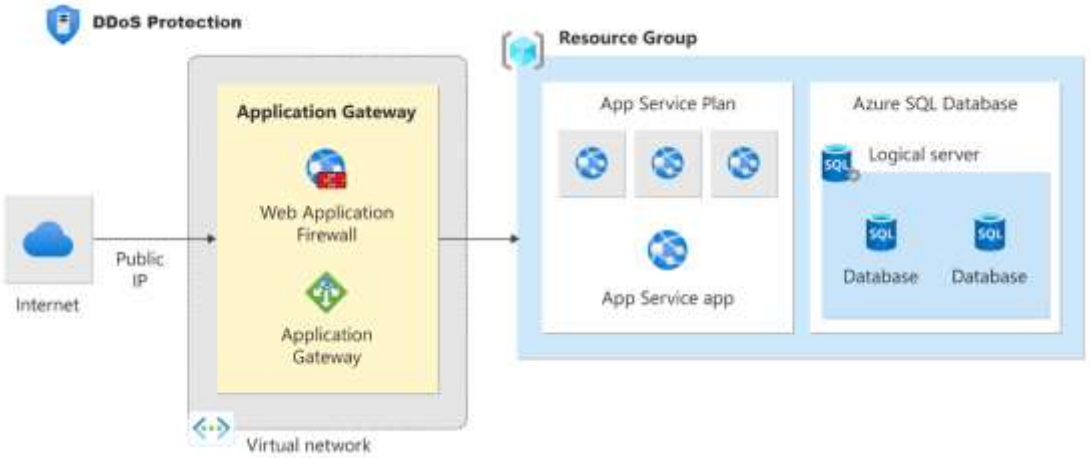
3

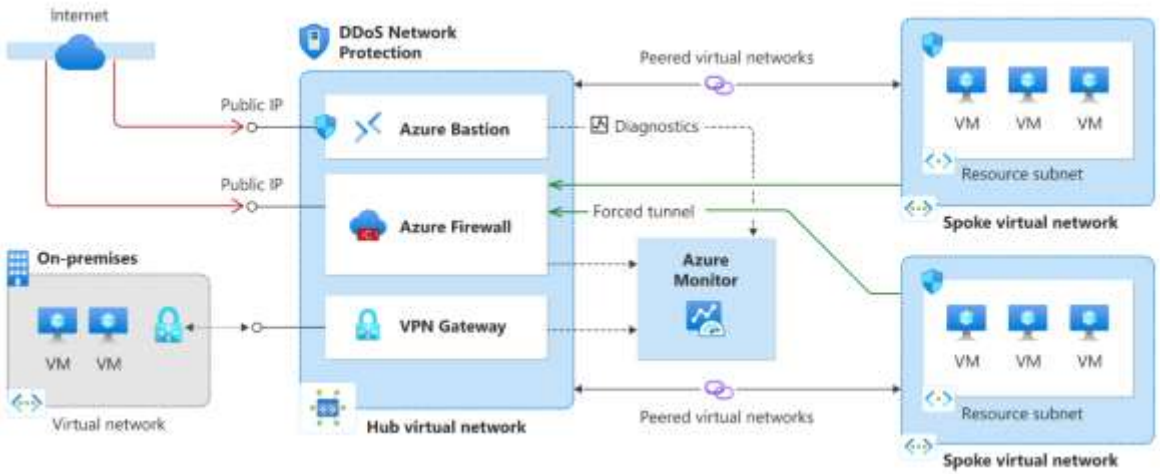
(hours)

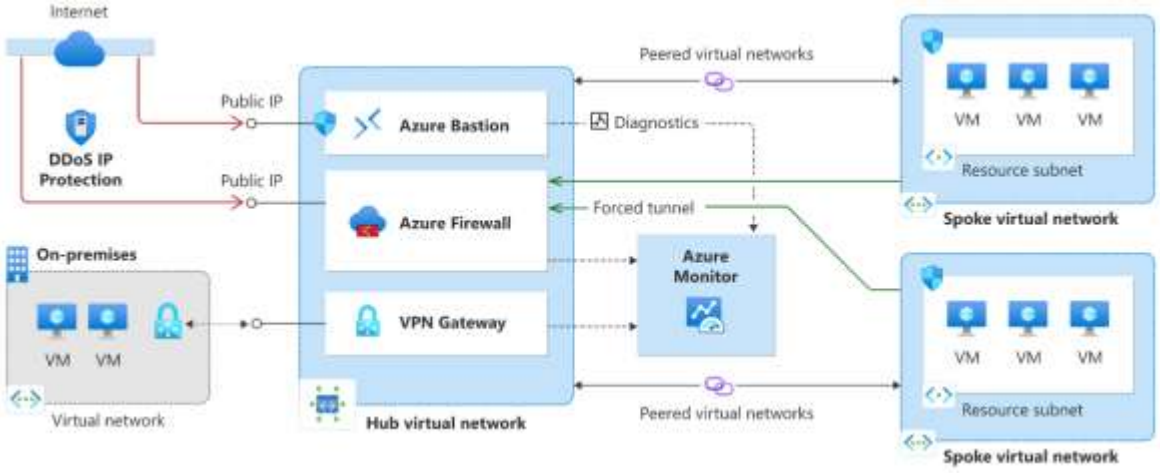
AZURE DDOS PROTECTION

Azure DDoS Protection, combined with application design best practices, provides enhanced **DDoS mitigation features** to defend against DDoS attacks. It's **automatically tuned** to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it **requires no application or resource changes**.









MICROSOFT INTUNE

Microsoft Intune is a cloud-based **endpoint management solution**. It manages user access to organizational resources and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.

CASE STUDY: DESIGNING A CLOUD SECURITY INFRASTRUCTURE

Background: Contoso, headquartered in Dallas, Texas, is a **medium-sized insurance provider**, with a customer base across the mid- and western United States. Its products include accident and health insurance, life insurance, as well as travel, home, and auto coverage. The company deals with various data, including **confidential customer records and contracts**, **frequently updated marketing information**, and **large amounts of historical content** that must be retained for **compliance** purposes. Customer records and contracts are created by using **Microsoft Office products**, marketing information is typically stored in the **Adobe Acrobat format**, and historical content is commonly **compressed as ZIP-based archives**.

Contoso uses its **on-premises infrastructure** to provide **storage** and implement **backups**. All data is hosted on **file servers** running **Windows Server 2016**, using both **local and iSCSI attached devices**. Storage devices are close to reaching their capacity. Backups are implemented by using several **tape libraries**, which are approaching their end-of-life. The operational team handling backups found them to be relatively **unreliable** due to frequently **failing restores** and **data corruption** issues. To remediate these issues, users commonly **maintain multiple copies** of the same data across different file servers. Unfortunately, this further exacerbates the storage capacity issues.

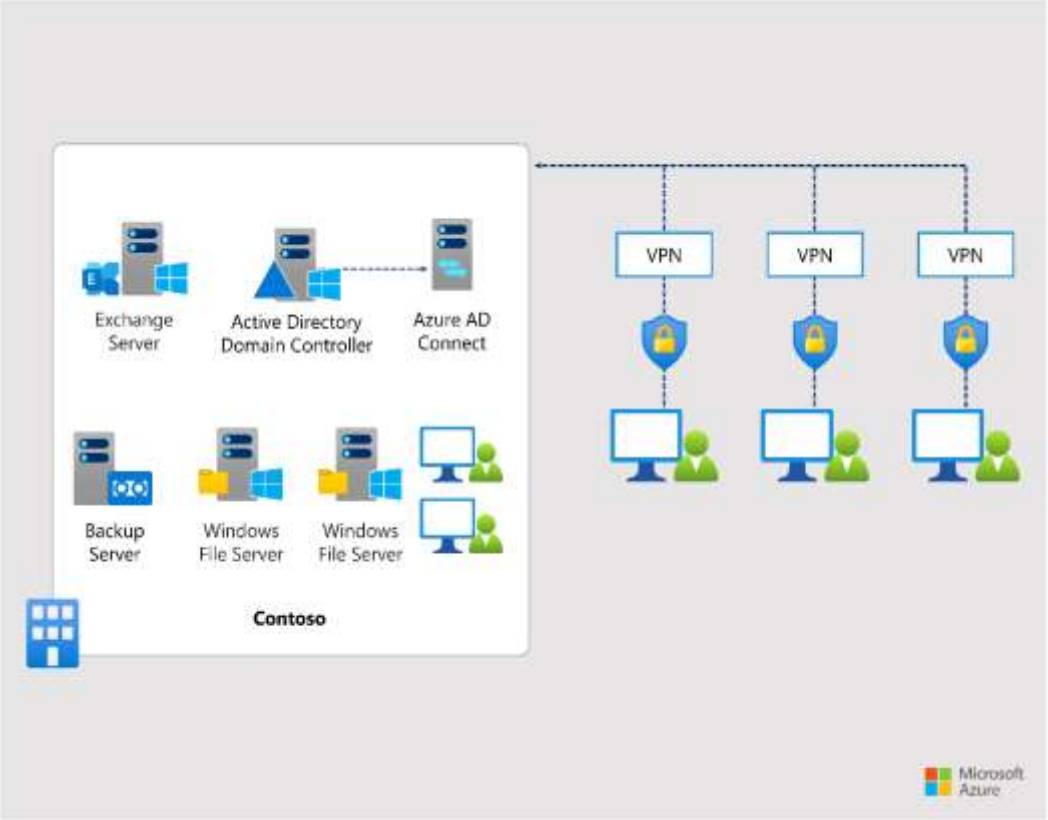
Contoso relies extensively on **remote workforce**, with insurance sales staff using their personal devices to occasionally establish **VPN connections** to headquarters. The lack of oversight of the remote devices has been assessed by the company's Information Security (**InfoSec**) team as a significant **vulnerability**. This assessment was proven fully justified by a recent incident that involved a **malware** transmitted through the company's on-premises Microsoft Exchange email. The malware managed to compromise one of the privileged **Active Directory Domain Services (AD DS) accounts** and attempted to **encrypt data** on one of the file servers. This attempt was detected and blocked by the **Microsoft Defender Antivirus** running on all of the company owned Windows computers but prompted Contoso's CIO to start considering a cloud-based strategy for data storage and protection.

The **CIO intends** to **migrate** most the company's data to **Microsoft 365 and Azure** and to rely on cloud-based services to implement **both short-term backups and long-term data retention**. This approach to data storage must include provisions **mitigating the risk of malware**, with a particular focus on **ransomware protection**. The risk mitigation should address the issue of **unsupervised devices used by remote workers**. In addition, the new cloud-based architecture should deliver **comprehensive monitoring and detection of cyberthreats**, allowing the InfoSec team to detect, track, and block their exploits before they impact critical data assets.

Requirements:

- Minimize the footprint of on-premises storage infrastructure.
- Minimize the footprint of on-premises backup infrastructure.
- Ensure that the data protection solution addresses the need for short-term backups.
- Ensure that the data protection solution addresses the need for long-term backups supporting 7-year retention required due to compliance reasons.
- Deliver continuous security protection and monitoring of remote devices.
- Control access to the company's assets based on a wide range of conditions, including the state of users' devices and dynamically evaluated risk, relying on heuristics and globally collected security-related telemetry.
- Protect backups against accidental or malicious deletions.

Initial Setup:



- **Minimize the footprint of on-premises storage infrastructure**

  Data Types:

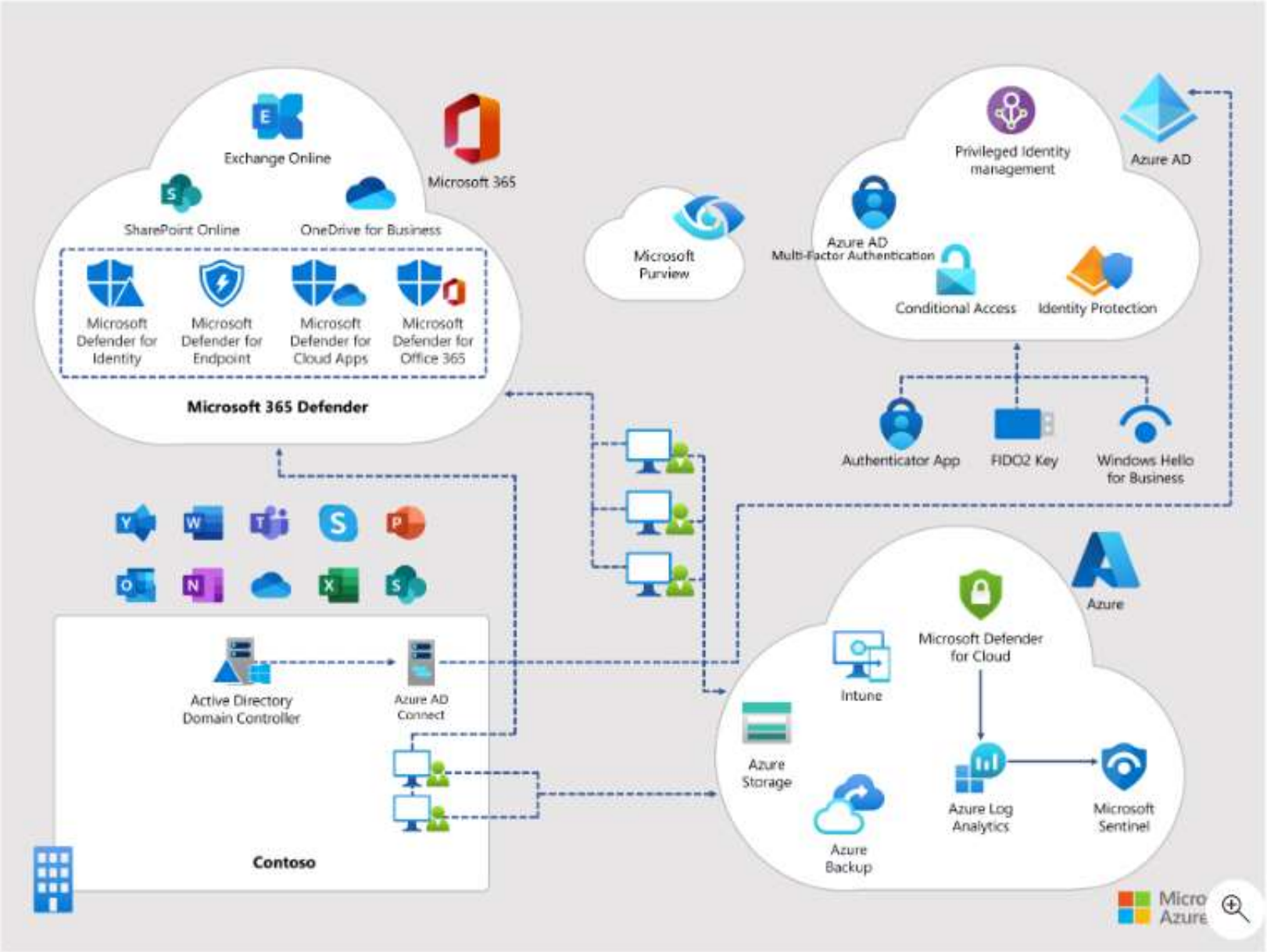
  - Confidential customer records and contracts in the Microsoft Office format
    - SharePoint Online and OneDrive
  - Frequently updated marketing information in the Adobe Acrobat format
    - Azure Files
  - Large amounts of historical content in the ZIP-based format that must be retained for compliance purposes
    - Azure Blob Storage
- **Minimize the footprint of on-premises backup infrastructure**
  - Microsoft 365 native data protection features combined with Azure Backup and Azure Blob Storage support for soft delete, versioning, and immutability could serve as a replacement for on-premises tape backups.
- **Ensure that the data protection solution addresses the need for short-term backups**
  - For short-term data retention, Contoso can use the native features of **SharePoint Online, OneDrive for Business, Exchange Online, Azure Blob Storage, and Azure Files**. SharePoint Online and OneDrive offer **built-in data protection** through versioning, recycle bin, and Files Restore, which provide short-term backup functionality.
  - **Azure Files** support snapshots and **soft delete** for file shares. Snapshots are read-only, **point-in-time copies of Azure Files shares**. Soft delete transitions deleted shares to a soft deleted state instead of removing them permanently.

- **Ensure that the data protection solution addresses the need for long-term backups supporting 7-year retention required due to compliance reasons.**
  - Azure Storage offers the ability to protect its blobs long-term by using immutable storage. Immutable storage for Azure Blob Storage would allow Contoso to store its data that is subject to compliance-related retention requirements in the WORM (Write Once, Read Many) state. While in the WORM state, data can't be modified or deleted for a user-specified interval.
  - Azure Backup supports backups of Azure Files shares, which Contoso can use to host the marketing information. The retention period depends on the total number of recovery points, but the maximum retention with yearly recovery points is 10 years.
  - Microsoft Purview retention policies that automatically retain a designated content.
- **Deliver continuous security protection and monitoring of remote devices.**
  - Microsoft Endpoint Protection
  - Microsoft Intune’s Mobile Device Management (MDM) functionality
  - MFA (Multi-Factor Authentication) via Microsoft Authenticator
  - Passwordless login support via FIDO2 Keys
  - Windows Hello for Business for MFA, Biometric sign-in, face recognition, iris recognition, hardware requirement support

- **Control access to the company's assets based on a wide range of conditions, including the state of users' devices and dynamically evaluated risk, relying on heuristics and globally collected security-related telemetry.**
  - Microsoft Entra (Azure AD) Conditional Access policies
    - Sign-in frequency
    - Sign-in location
    - Persistent browser session
    - Require multifactor authentication
    - Require authentication strength
    - Require device to be marked as compliant
    - Require approved client app
    - Require app protection policy
    - Require password change

- **Protect backups against accidental or malicious deletions.**
  - Restricting access to backups by using Azure role-based access control (**RBAC**). Azure Backup supports segregation of duties based on granular, task-based permissions model.
  - Using **Microsoft Entra Privileged Identity Management** to grant time-limited and approval-based role assignments.
  - Ensuring that **soft delete is enabled** to protect backups from accidental or malicious deletions. This feature is enabled by default on all newly created Recovery Services and Backup vaults. It retains backups for 14 days following their deletion.
  - Implementing multiuser authorization (**MUA**) for critical operations on Recovery Services and Backup vaults. MUA for Azure Backup uses the Resource Guard to ensure that critical operations, such as disabling soft delete, stopping and deleting backups, or reducing retention of backup policies, can be performed only when authorized by multiple users.
  - Providing **Just-In-Time access** on Resource Guard by using Microsoft Entra Privileged Identity Management.
  - **Setting up alerts and notifications for critical backup operations.** Azure Backup offers monitoring and notification capabilities for a wide range of scenarios.
  - Ensuring that **network connectivity between backup services and workloads is secure**. For Azure VM, data in transit traverses the Azure backbone network. For Azure Storage, you need to explicitly allow access to Azure services on the trusted services list. For on-premises workloads protected by using Microsoft Azure Recovery Services (MARS) agent or Microsoft Azure Backup Server (MABS), you can use Microsoft peering for ExpressRoute or Virtual Private Network (VPN) to connect to Azure. Private peering supports with private endpoints.
  - **Regularly monitoring backups.** Monitoring solutions, such as Backup Explorer, help identify systems that aren't protected by Azure Backup. They also facilitate monitoring backup items, backup jobs, and policies.

CASE STUDY: PROPOSED SOLUTION ARCHITECTURE



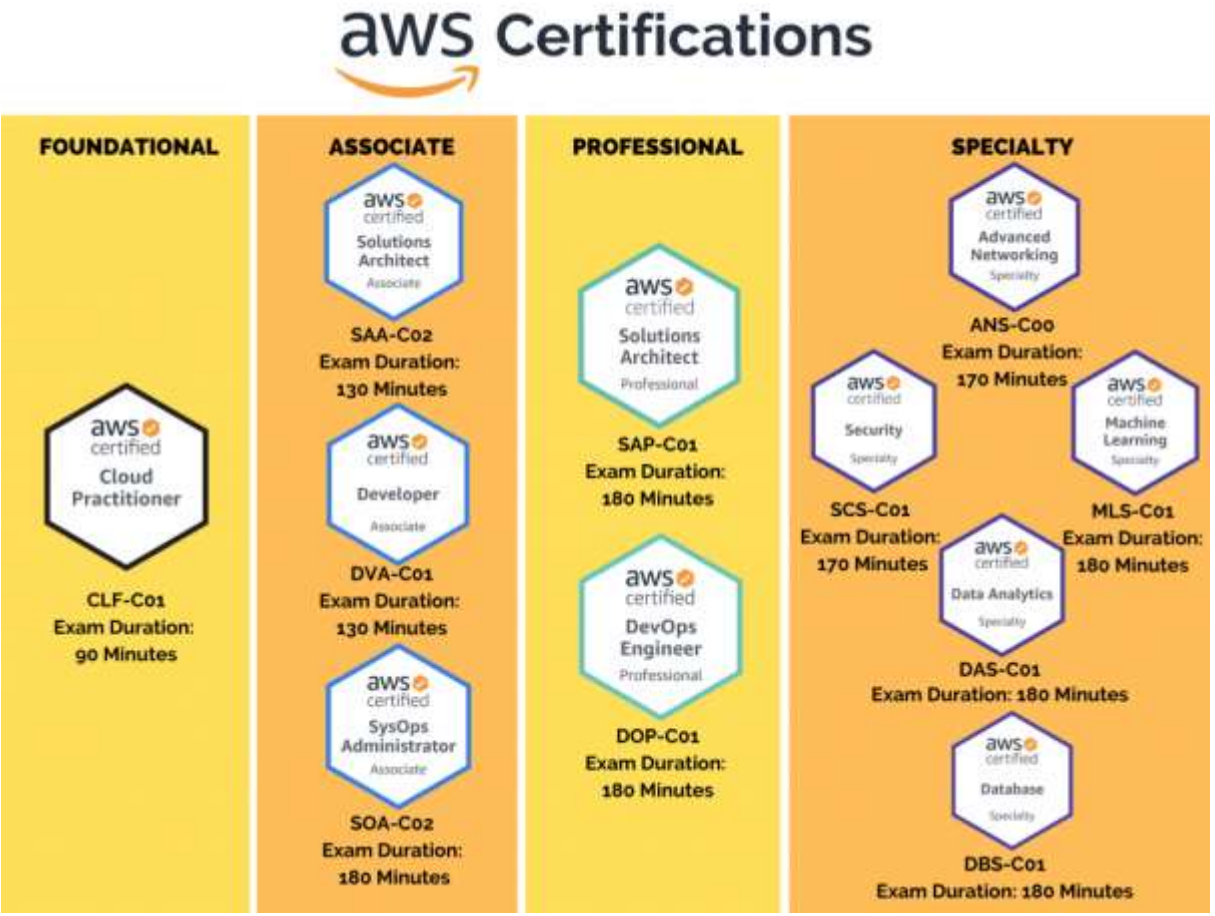
CYBERSEC CERTS

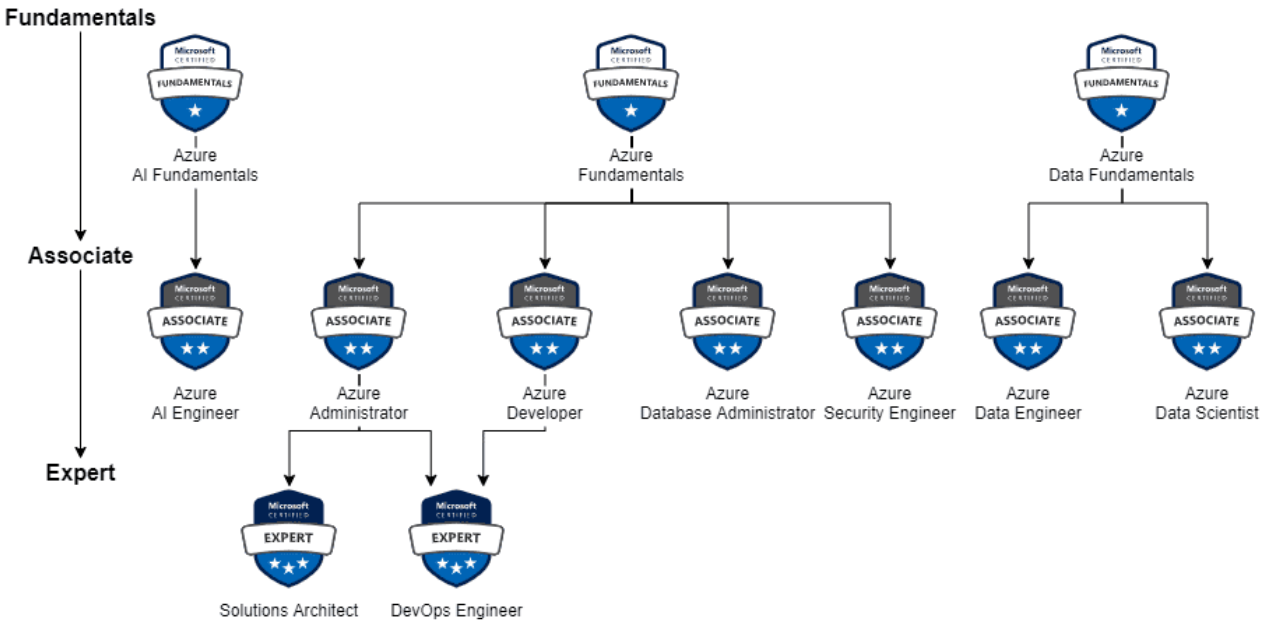
Blue Team

Red Team

1. CASP (CompTIA Advanced Security Practitioner)
2. CISM (Certified Information Security Manager)
3. CHFI (Computer Hacking Forensic Investigator)
4. **CEH (Certified Ethical Hacker)**
5. CAP (Certified Authorization Professional)
6. CompTIA Security+
7. **CISSP (Certified Information Systems Security Professional)**

CLOUD CERTS





HOMEWORK

- Compare AWS and Azure's Security services. Provide a short summary.
- Try to provide a network diagram for the case study in AWS.
- Watch & Learn: https://www.youtube.com/watch?v=imEXuSrP_-I (Playbook w. Sentinel)

Thank You

orioninc.com