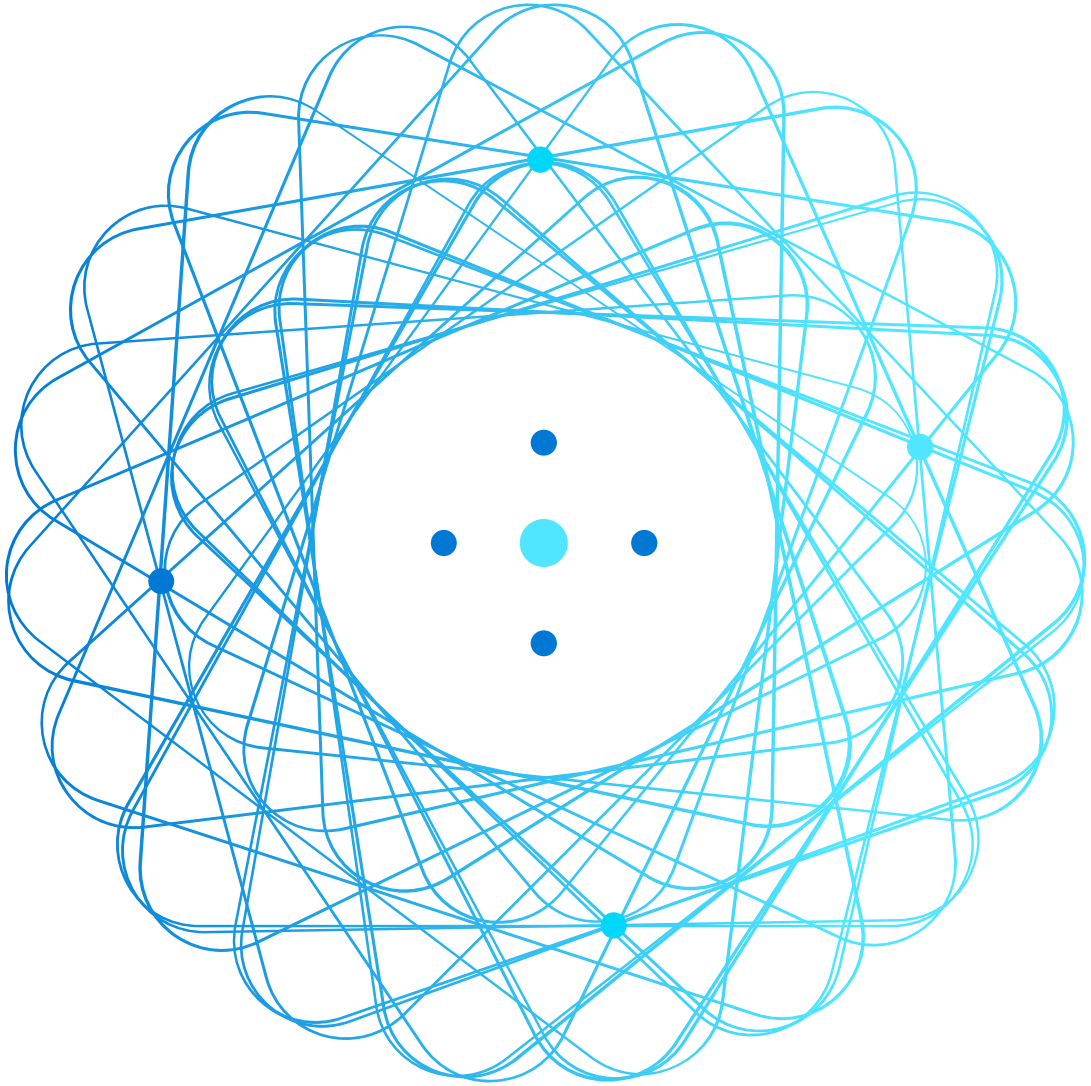
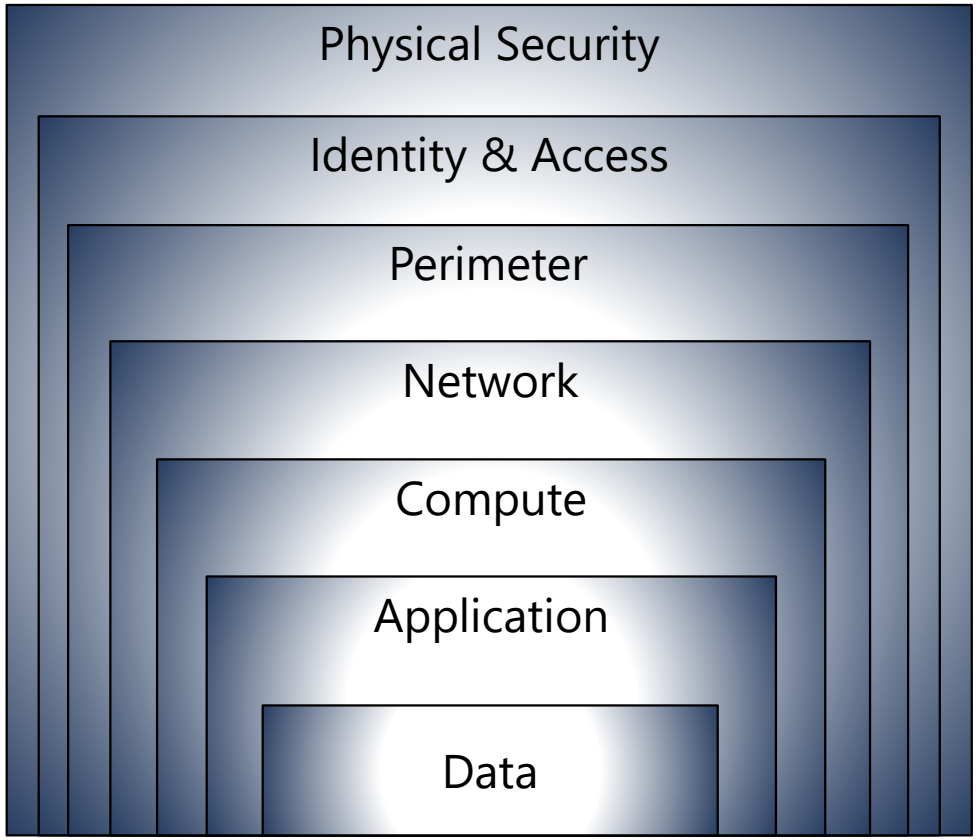
Microsoft Azure

Security & Monitoring Basics

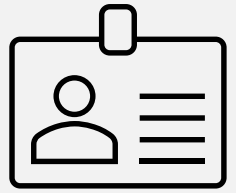


Defense in depth

- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Core Azure identity services



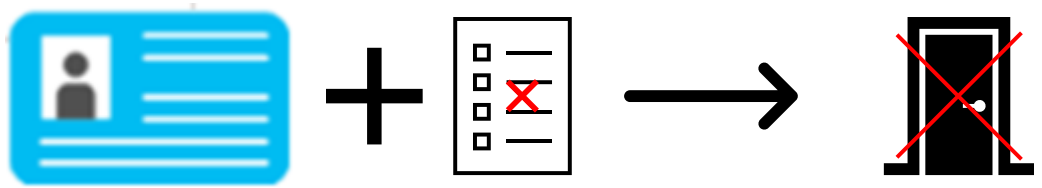
Compare Authentication and Authorization

Authentication

- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.

Authorization

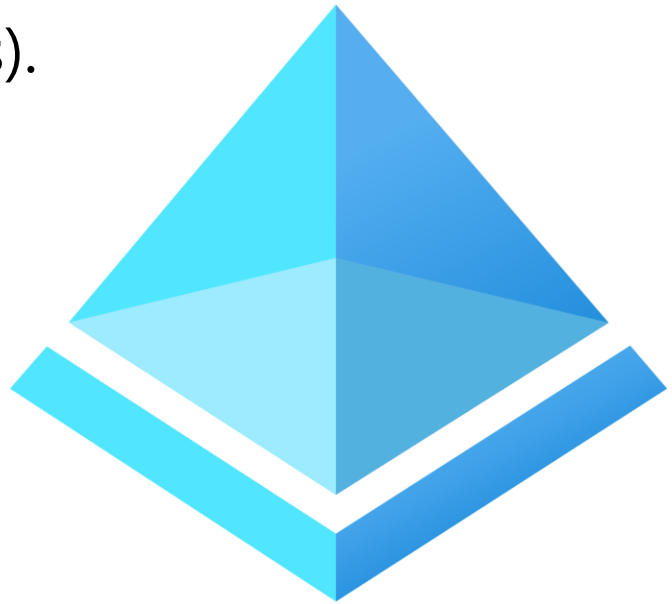
- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.



Azure Active Directory (AAD)

Azure Active Directory (AAD) is Microsoft Azure's cloud-based identity and access management service.

- Authentication (employees sign-in to access resources).
- Single sign-on (SSO).
- Application management.
- Business to Business (B2B).
- Business to Customer (B2C) identity services.
- Device management.



Azure Multi-Factor Authentication

Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know ←→ Something you possess ←→ Something you are

Role-based access control (RBAC)

Fine-grained access management control over your Azure resources.

Available to *all* Azure subscribers, at no additional cost.

Example uses of Azure RBAC :

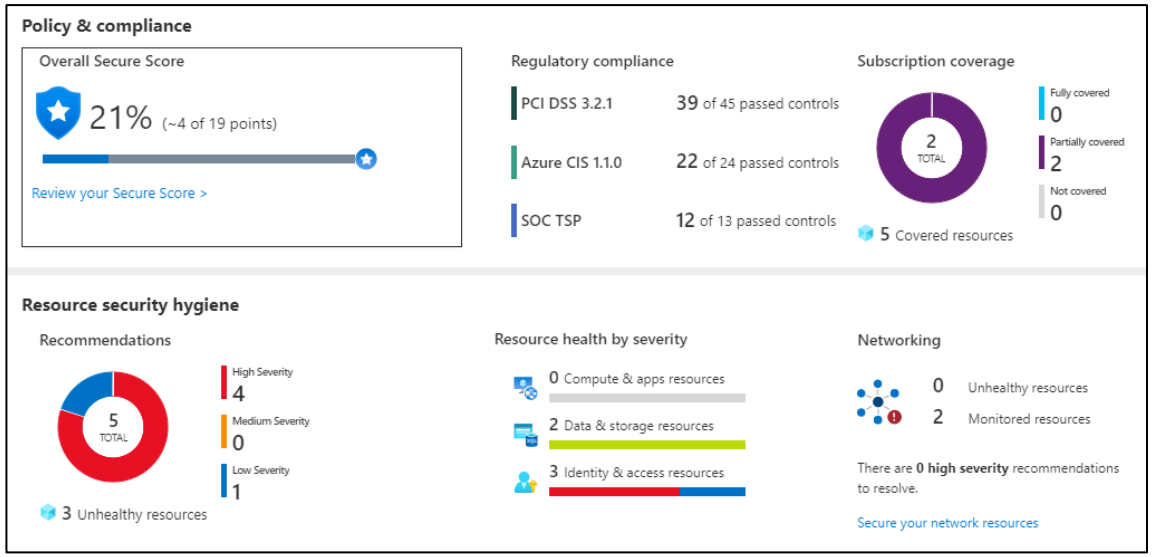
- Grant specific access rights to particular users for certain jobs. One user can manage VMs, while another manages virtual networks.
- Allocate particular database types to certain database administration groups.

Security tools and features

Azure Security Center

Azure Security Center is a monitoring service that provides threat protection across both Azure and on-premises datacenters.

- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports



Azure Security Center - capabilities

Policy Compliance

Run policies across management groups, subscriptions, or tenants.

Continuous Assessments

Assess new and deployed resources to ensure that they are configure properly.

Tailored Recommendations

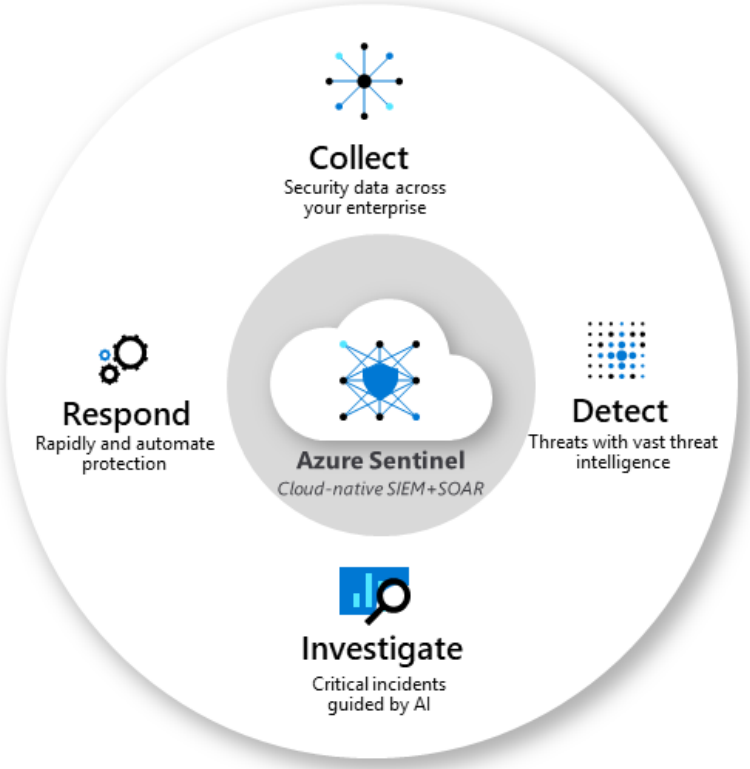
Recommendations based on existing workload with instructions on how to implement them.

Threat Protection

Analyze attempted threats through alerts and impacted resource reports.

Azure Sentinel

Azure Sentinel is a security information management (SIEM) and security automated response (SOAR) solution that provides security analytics and threat intelligence across an enterprise.



Connector and Integrations:

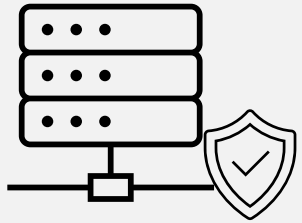
- Office 365
- Azure Active Director
- Azure Advanced Threat Protection
- Microsoft Cloud App Security

Azure Key Vault

Azure Key Vault stores application secrets in a centralized cloud location in order to securely control access permissions and access logging.

- Secrets management.
- Key management.
- Certificate management.
- Storing secrets backed by hardware security modules (HSMs).

Secure network connectivity



Shared Security

- Migrating from customer-controlled to cloud-based datacenters shifts the responsibility for security.
- Security becomes a shared concern between cloud providers and customers.

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Network Security Groups (NSGs)

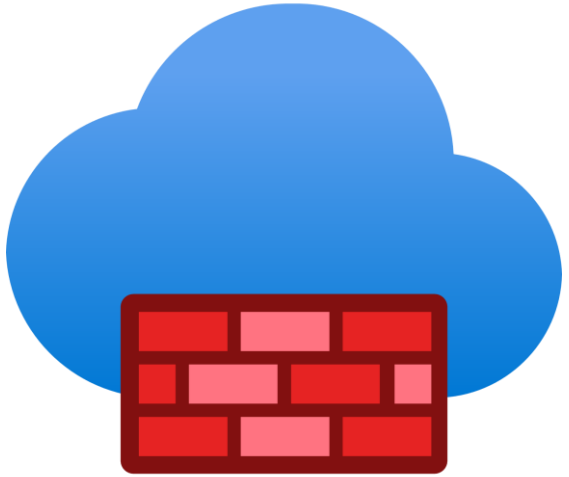
Network Security Groups (NSGs) filter network traffic to and from Azure resources on Azure Virtual Networks.

- Set inbound and outbound rules to filter by source and destination IP address, port, and protocol.
- Add multiple rules, as needed, within subscription limits.
- Azure applies default, baseline security rules to new NSGs.
- Override default rules with new, higher priority rules.

Azure Firewall

A stateful, managed Firewall as a Service (FaaS) that grants/denies server access based on originating IP address, in order to protect network resources.

- Applies inbound and outbound traffic filtering rules
- Built-in high availability
- Unrestricted cloud scalability
- Uses Azure Monitor logging



Azure Application Gateway also provides a firewall, Web Application Firewall (WAF). WAF provides centralized, inbound protection for your web applications.

Azure Distributed Denial of Service (DDoS) protection

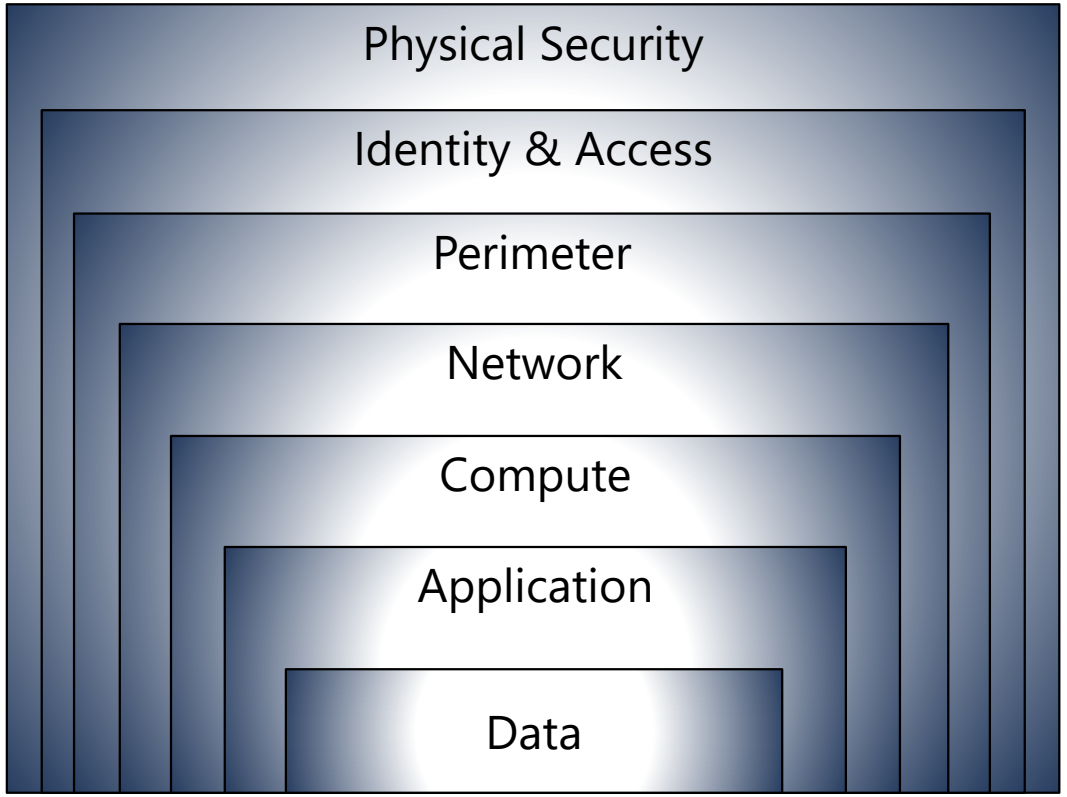
DDoS attacks overwhelm and exhaust network resources, making apps slow or unresponsive.

- Sanitizes unwanted network traffic before it impacts service availability.
- Basic service tier is automatically enabled in Azure.
- Standard service tier adds mitigation capabilities that are tuned to protect Azure Virtual Network resources.

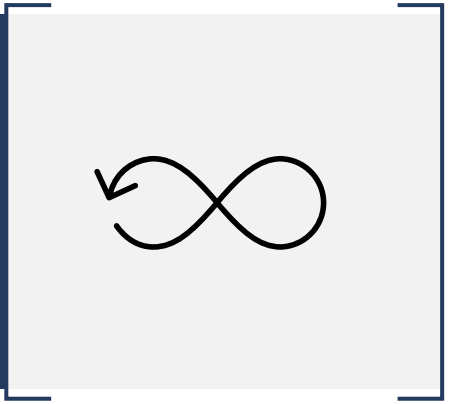
Defense in Depth Reviewed

Combining network security solutions

- **NSGs** with **Azure Firewall** to achieve defense in depth.
- **Perimeter layer** protects your network boundaries with Azure DDoS Protection and Azure Firewall.
- **Networking layer** only permits traffic to pass between networked resources with Network Security Group (NSG) inbound and outbound rules.

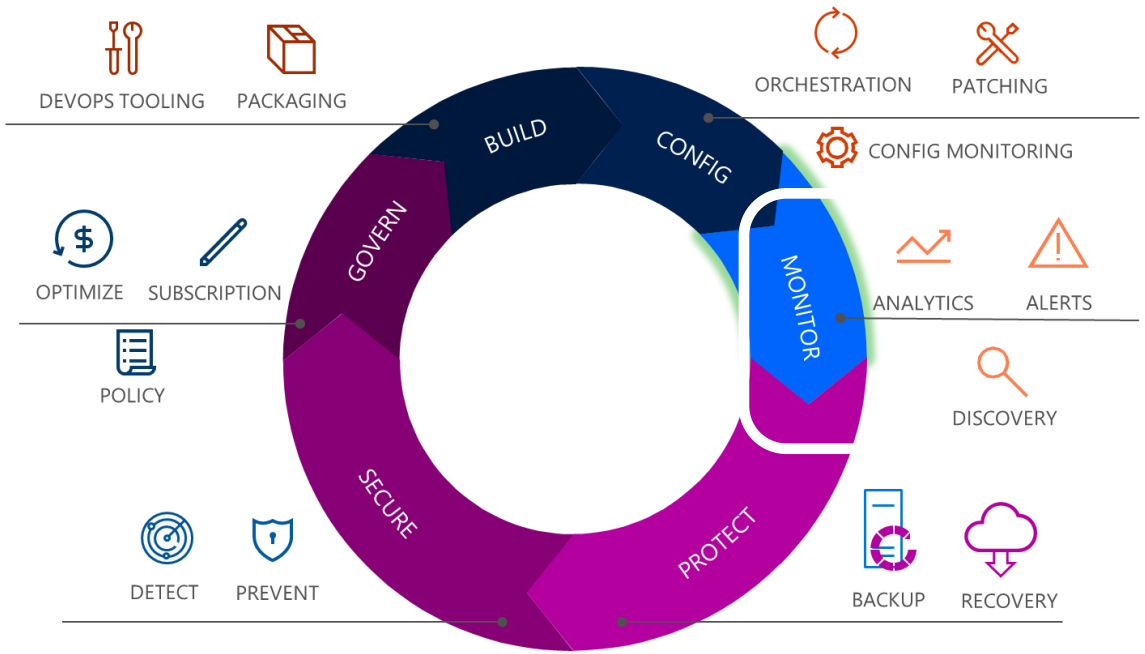


Monitoring



Azure Monitoring Toolset overview

Modern Cloud Management



Azure Service Health

Get personalized guidance and support for when issues in Azure services affect you

Azure Advisor

Your personalized Azure best practices recommendation engine

Azure Monitor

Highly granular and real-time monitoring data for any Azure resource

Log Analytics

Collect, search, and visualize machine data from on-premises and cloud

Application Insights

Detect, triage, and diagnose issues in your web apps and services

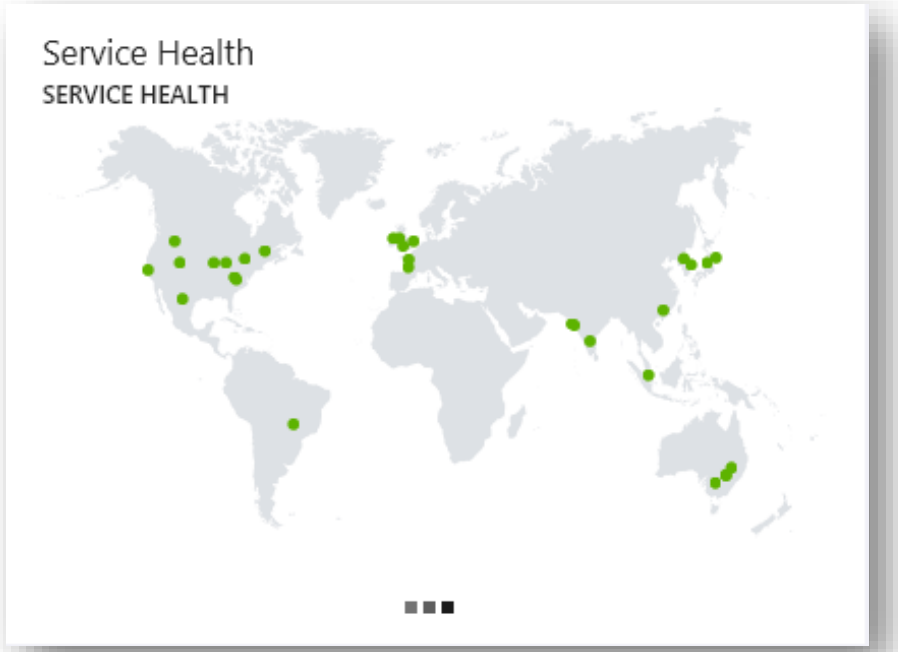
Azure Monitoring Tools – Service Health

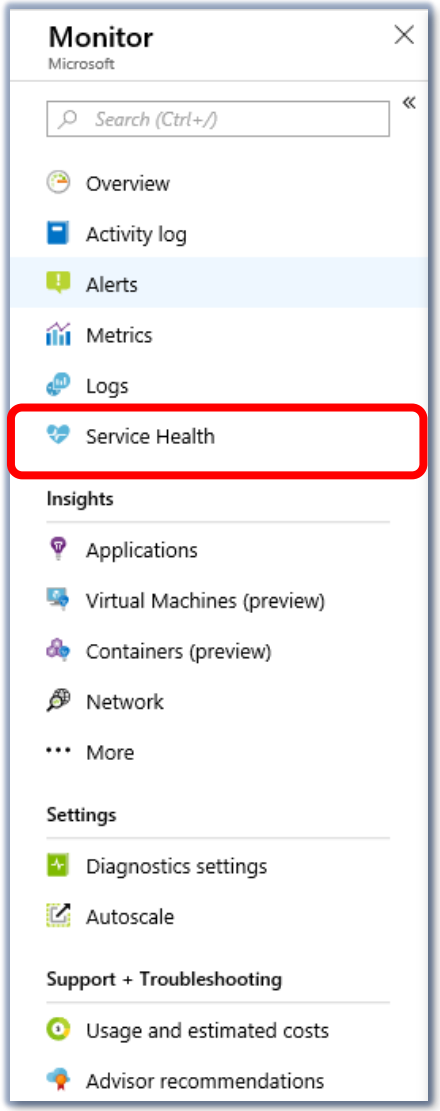
Azure Service Health

- Suite of experiences
- Provide personalized guidance and support when issues in Azure services affect you

Azure Service Health is composed of:

- Azure status – a global view of the health of Azure services
- Service Health – a personalized view of the health of your Azure services
- Resource Health – a deeper view of the health of the individual resources provisioned to you by your Azure services





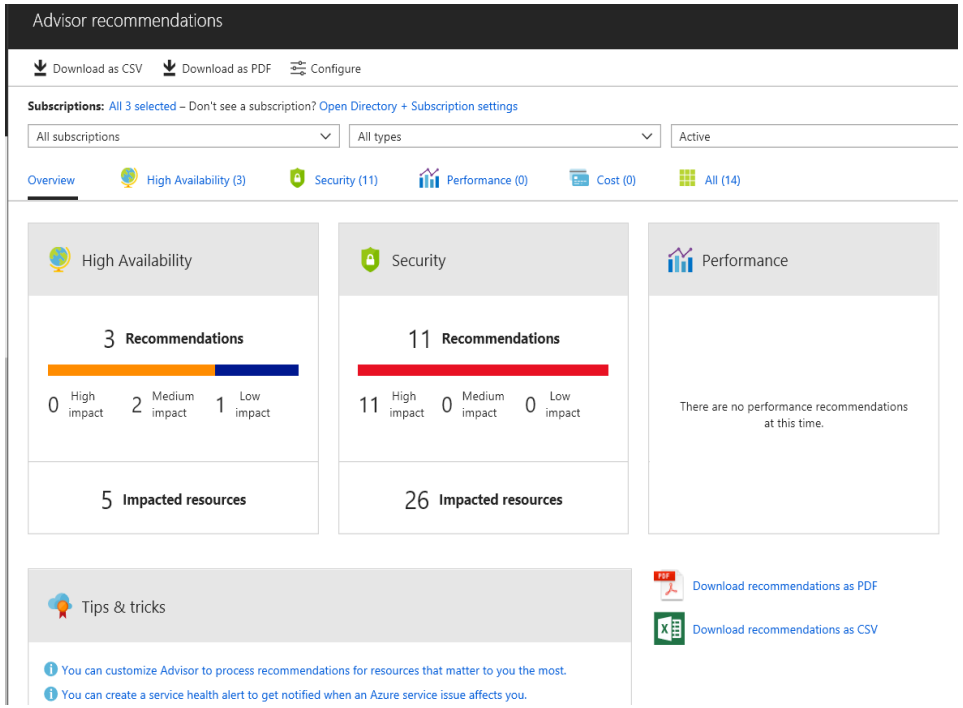
Azure Monitoring Tools – Azure Advisor

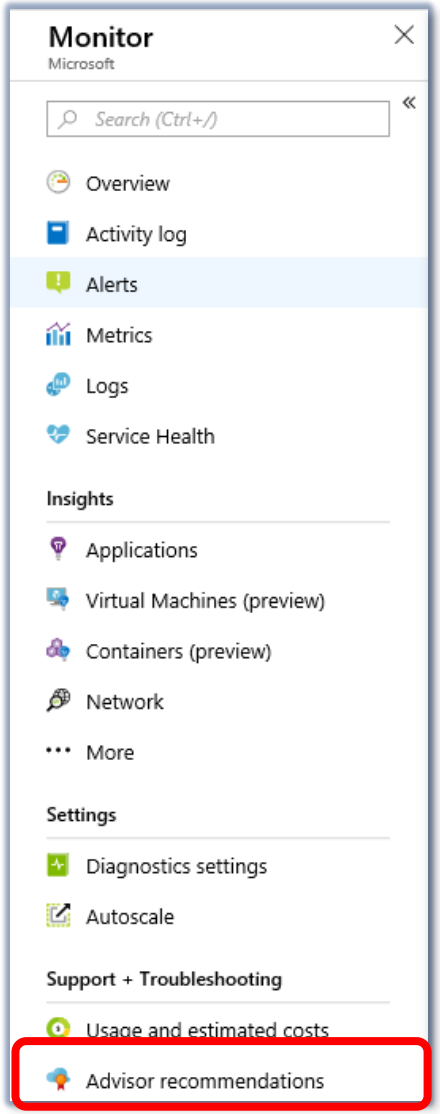
What is Azure Advisor?

- Advisor is a personalized cloud consultant
- Helps to follow best practices
- Analyzes resource configuration and usage telemetry
- Recommends solutions to improve Azure resources

With Azure Advisor you can …

- Get proactive, actionable, and personalized best practices and recommendations
- Improve performance, security, and high availability of your resources
- Get recommendations with proposed actions inline





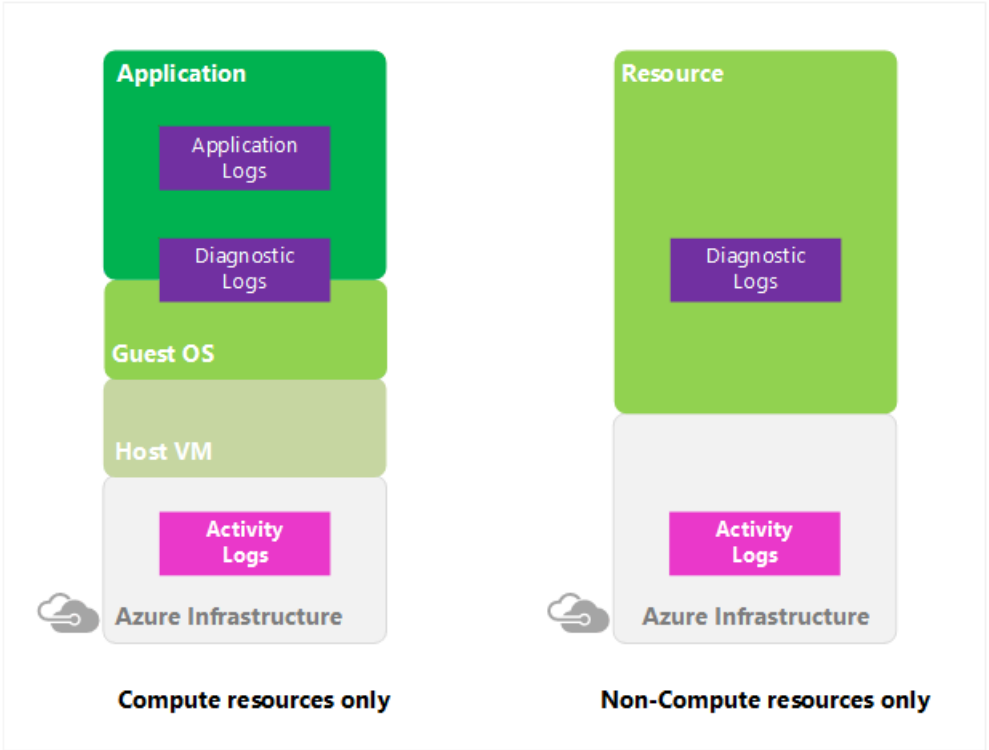
Azure Monitoring Tools – Activity Log

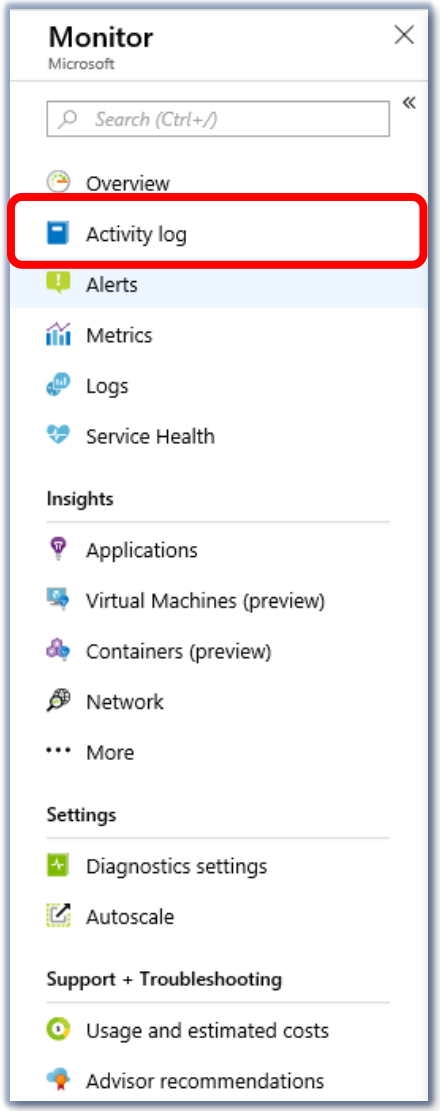
What is Azure Activity Log?

- Provides insight into subscription-level events
- Includes a range of data:
  - Azure Resource Manager
  - Azure operational data
  - Service Health events

With Azure Activity Log you can …

- Analyze events generated by ARM
- Review alerts fired
- Generate Alerts for specific critical events





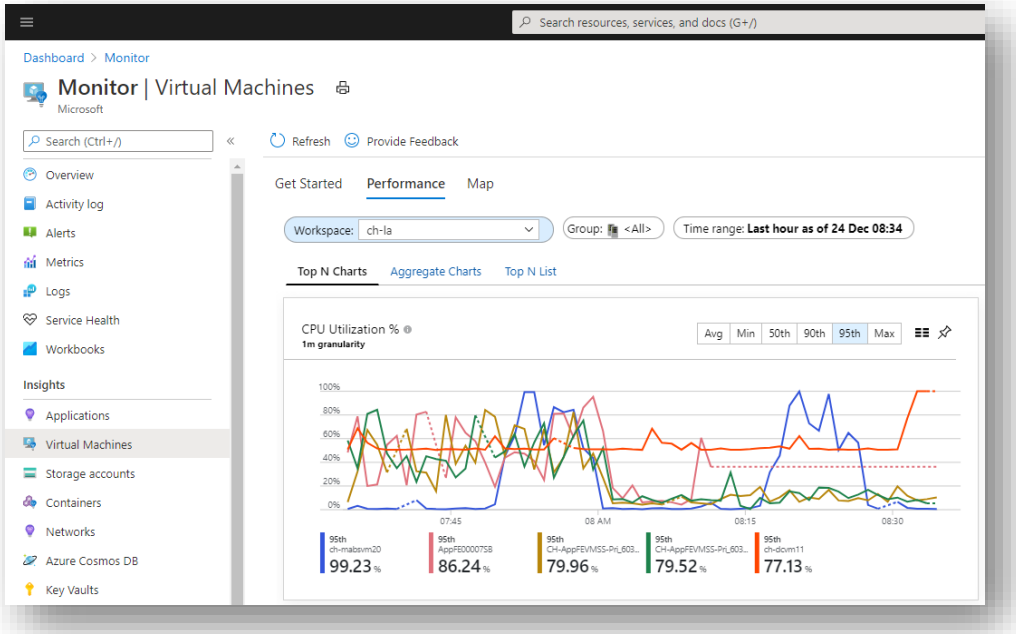
Azure Monitoring Tools – Azure Monitor

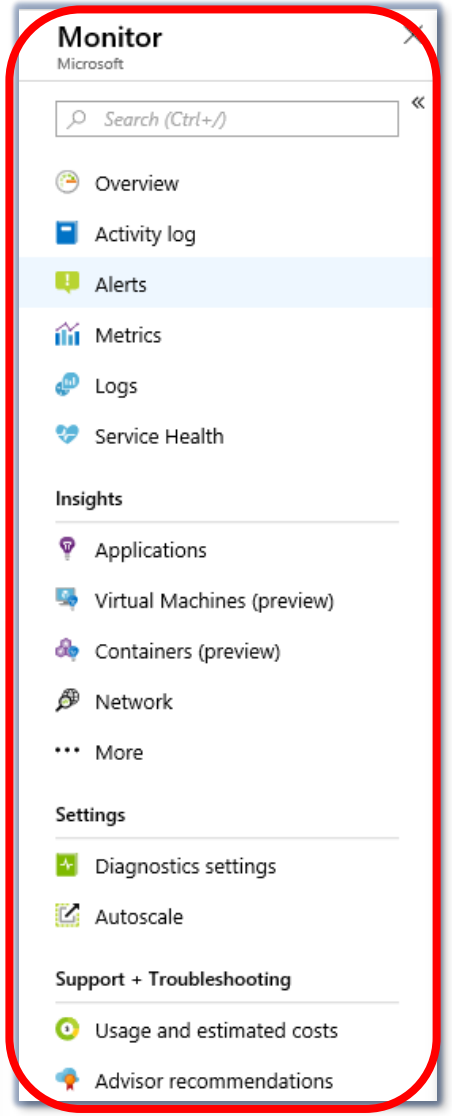
Monitor Overview

- Unified and centralized tool for all Azure Monitoring topics
- Helps to discover and access monitoring services and capabilities
- Out-of-the-box insights on Activity Logs
- Integrated overview from premium monitoring services as a jumping-off point

Compute Resource Health Monitoring

- Focused on cross-resource monitoring for the compute ecosystem
- Correlated events and Azure health issues integrated with performance metrics
- Link into topology views in context

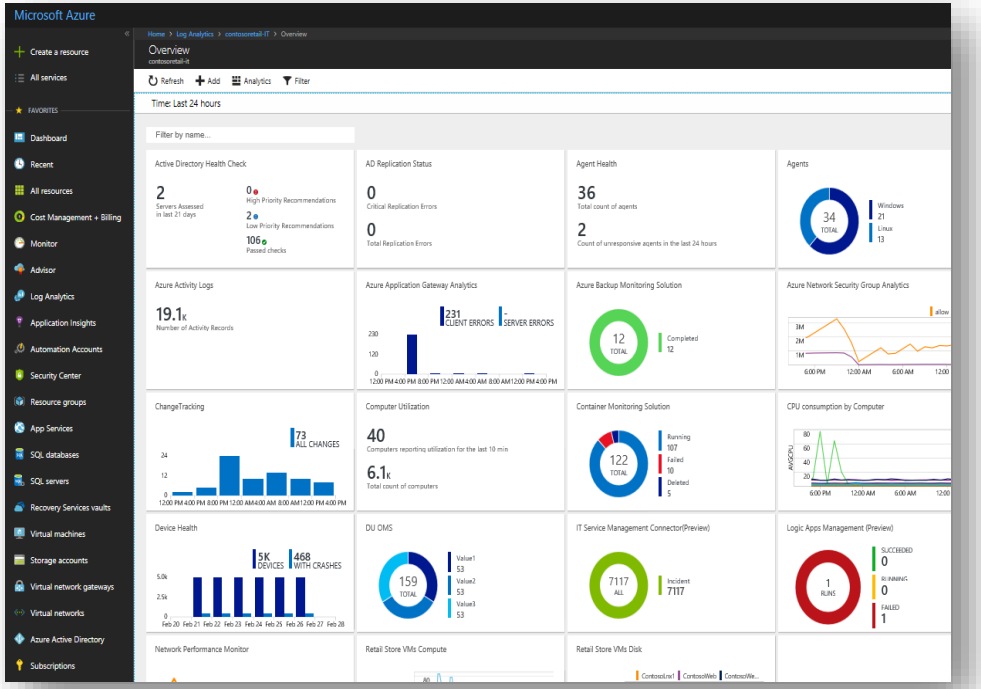


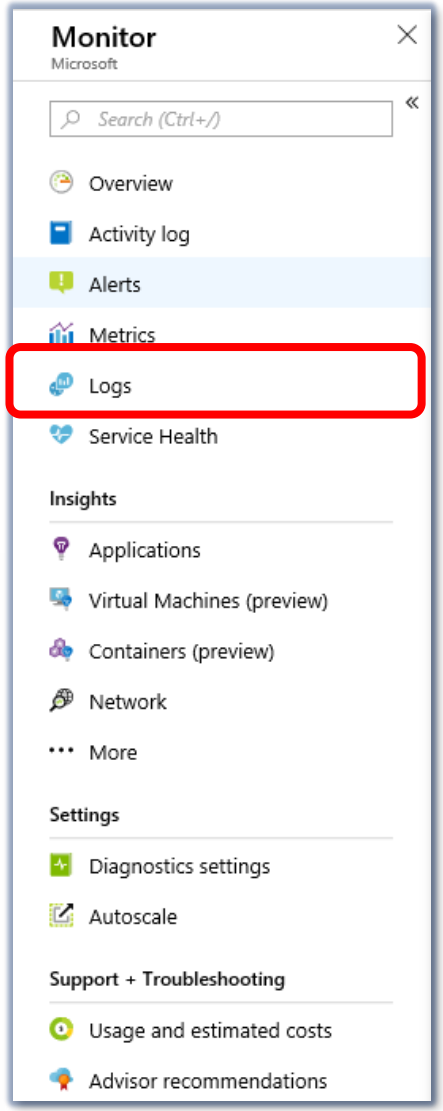


Azure Monitoring Tools – Azure Log Analytics

Azure Log Analytics

- Monitors cloud and on-premises environments to maintain availability and performance
- Get insights across various workloads and systems
- Collects telemetry and other data from a variety of sources, both on-premises and cloud
- Provides many solutions (e.g. AD, DNS, Container, Service Map, Wire Data)
- Correlates data from different types and sources
- Alerts based on query results

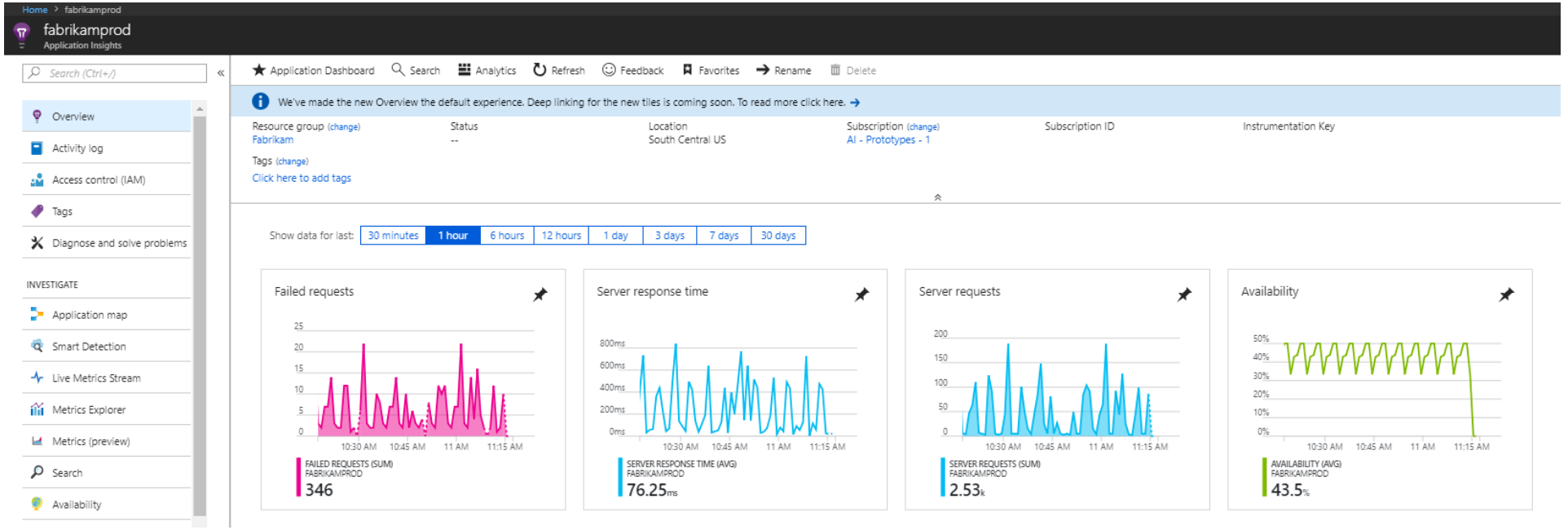


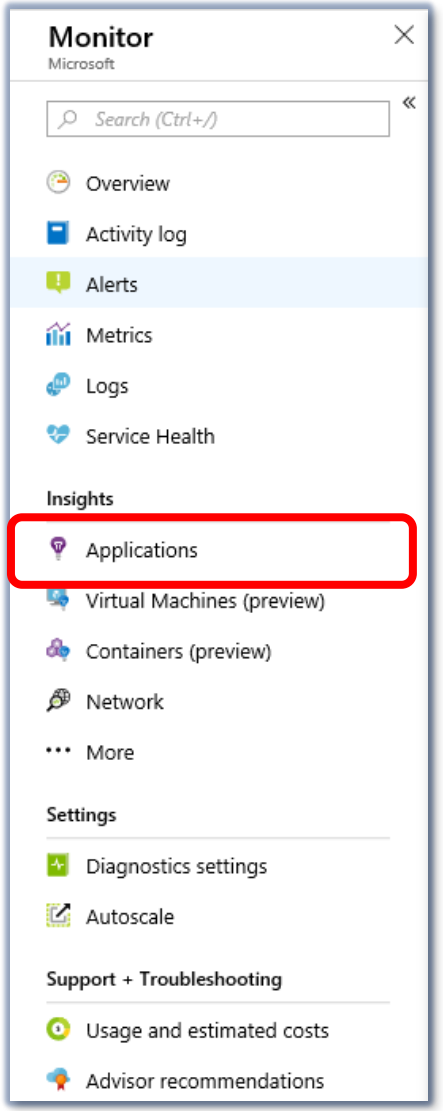


Azure Monitoring Tools – Application Insights

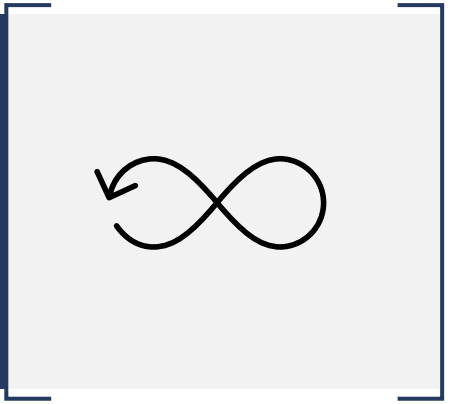
Azure Application Insights

- Extensible Application Performance Management (APM) service for web developers
- Use to monitor live web applications
- Automatically detect performance anomalies
- Includes powerful analytics tools to diagnose issues and understand what users actually do with the web application

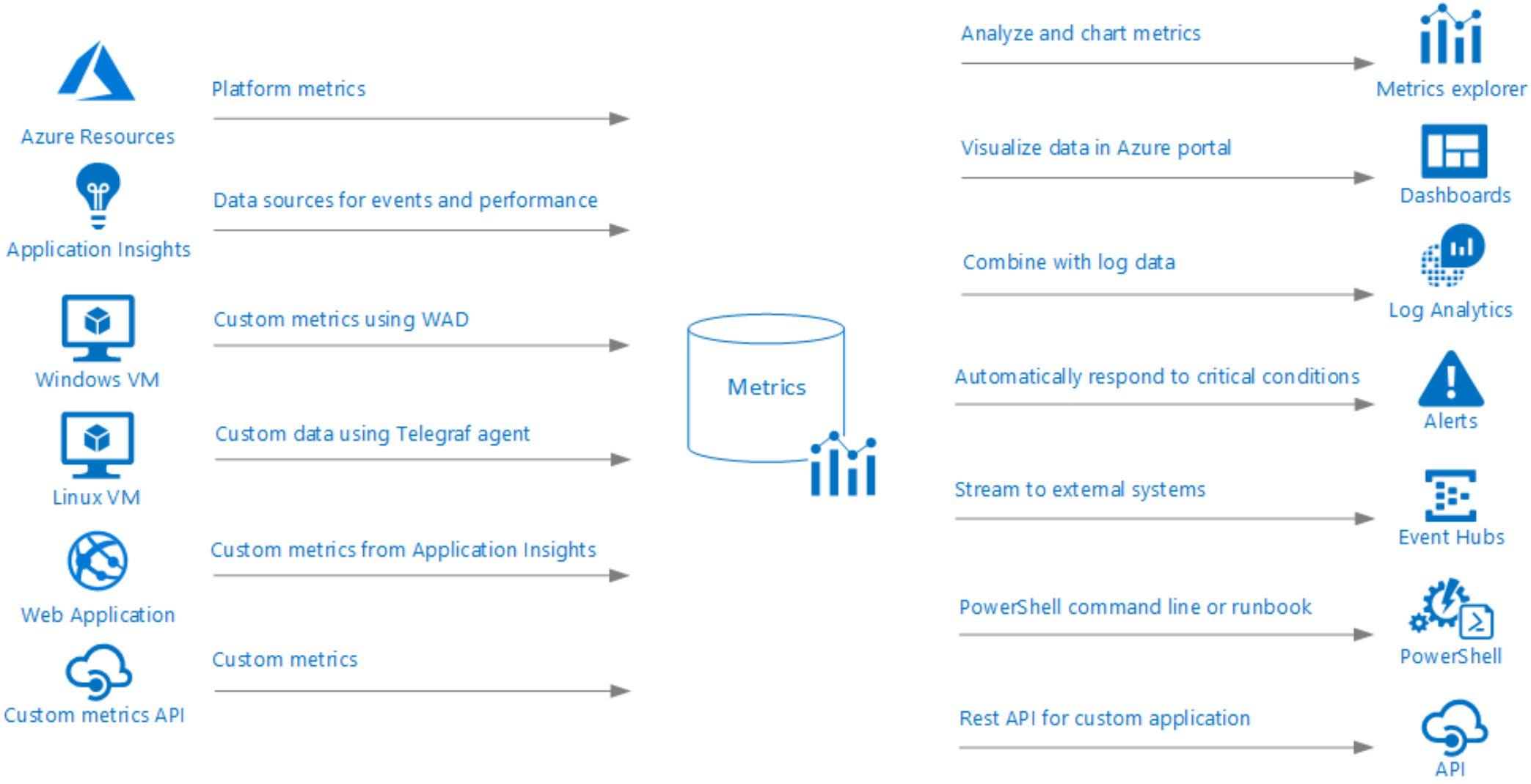




Monitoring - Appendix



Data collected by Azure Monitor – Metrics sources



Data collected by Azure Monitor – Log Sources