



Azure Monitor Overview

Maxim Sergeev

Sr. Premier Field Engineer

Monitoring landscape – apps & infrastructure

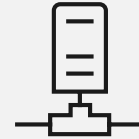
Infrastructure



Apps

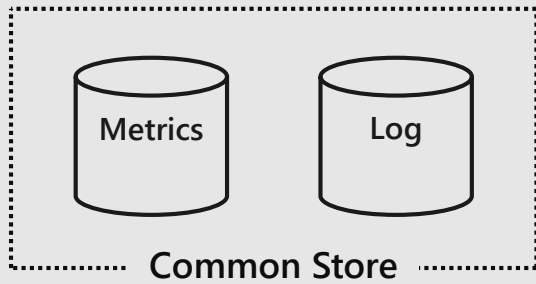


Network



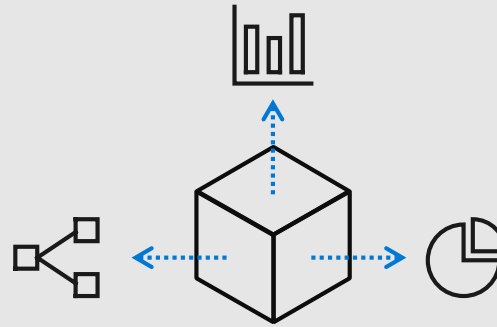
Azure Monitor

Full observability for your infra, app and network



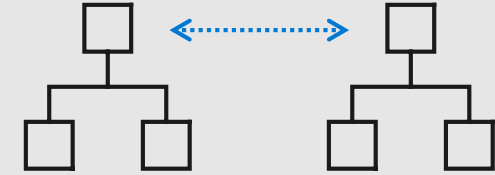
Unified Monitoring

A common platform for all metrics, logs and other monitoring telemetry



Data Driven Insights

Advanced diagnostics and analytics powered by machine learning capabilities



Workflow Integrations

Rich ecosystem of popular DevOps, issue management, SIEM, and ITSM tools

Signals and Sources in Azure

Signals



Metrics



Logs



Alerts

Sources

Application

User telemetry
Application logs

Guest OS (‘user space’)

Linux syslog
Windows Perf Counters

Azure Resources

Virtual Machines
Storage Accounts
Network Security Groups

Azure Subscriptions

Resource Manager
Service Health
Security Center

Azure Tenants

Azure Active Directory



Azure Monitor

Application

Operating System

Azure Resources

Azure Subscription

Azure Tenant

Custom Sources



Insights



Application



Container



VM



Monitoring Solutions

Visualize



Dashboards



Views



Power BI



Workbooks

Analyze



Metrics Explorer



Log Analytics

Respond



Alerts



Autoscale

Integrate



Event Hubs

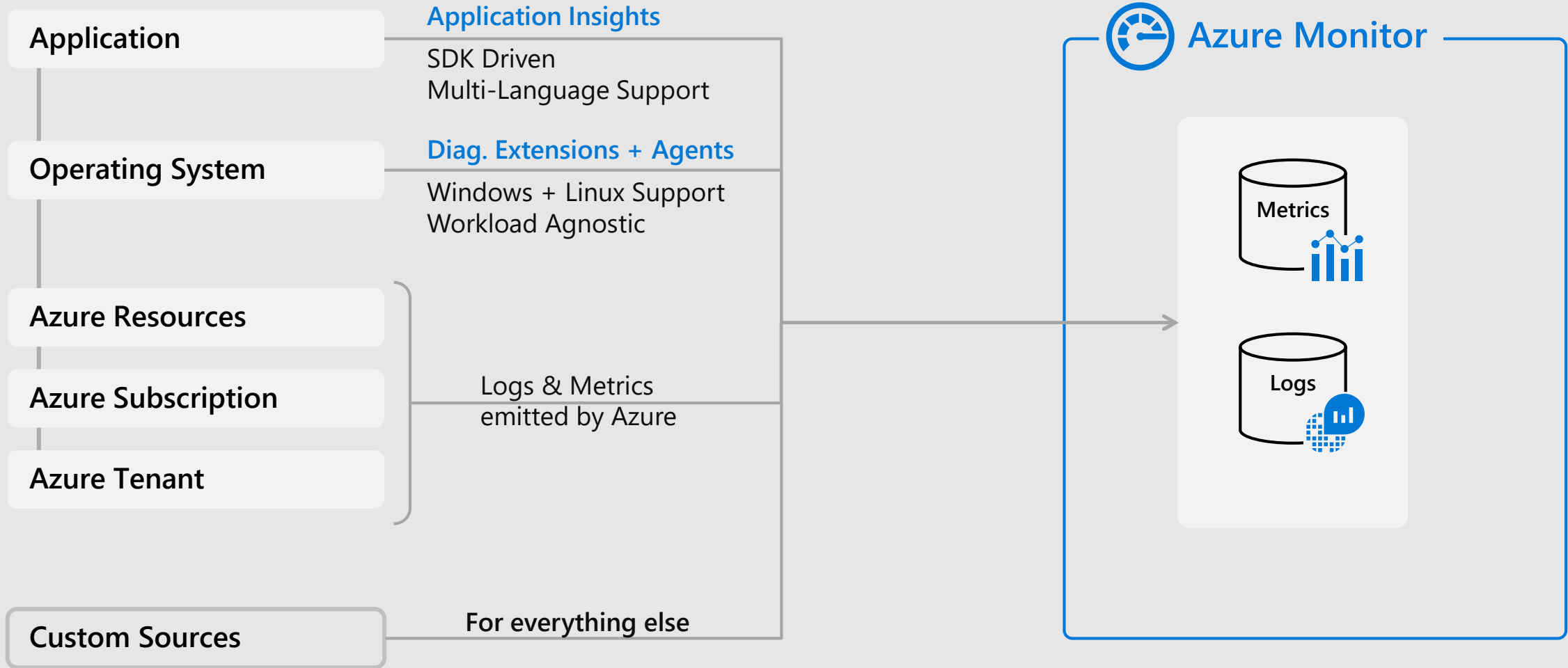


Logic Apps



Ingest & Export APIs

Wiring it all up



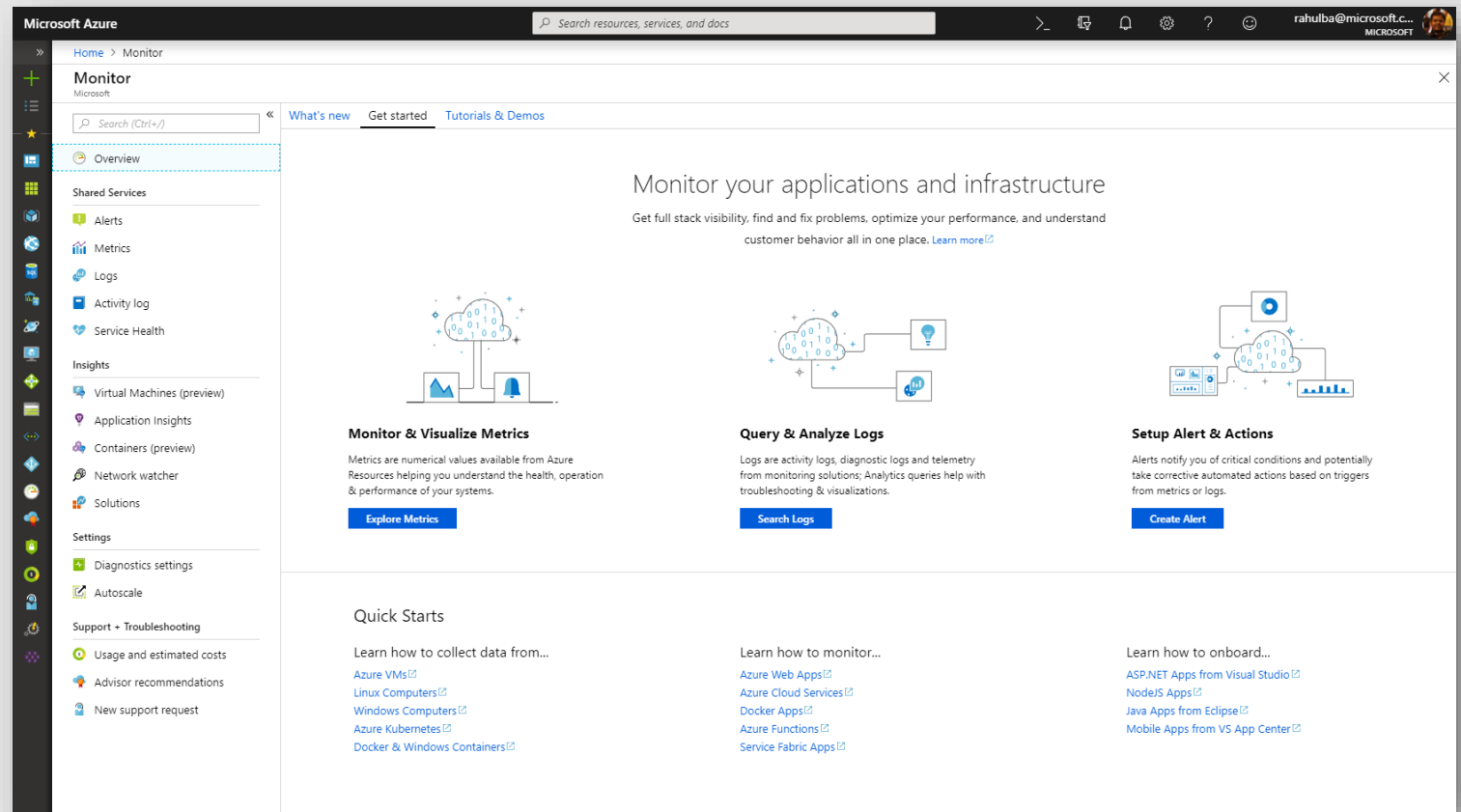
Unified Monitoring



Unified Monitoring



- One Metrics, One Logs, One Alerts across Azure/on-prem resources
- Unified offering with App Insights & Log Analytics as integrated features
- Integration into native Azure resource blades
- Ability to send custom metrics & custom logs



Data Driven Insights



Full Stack Visibility in Resource Groups

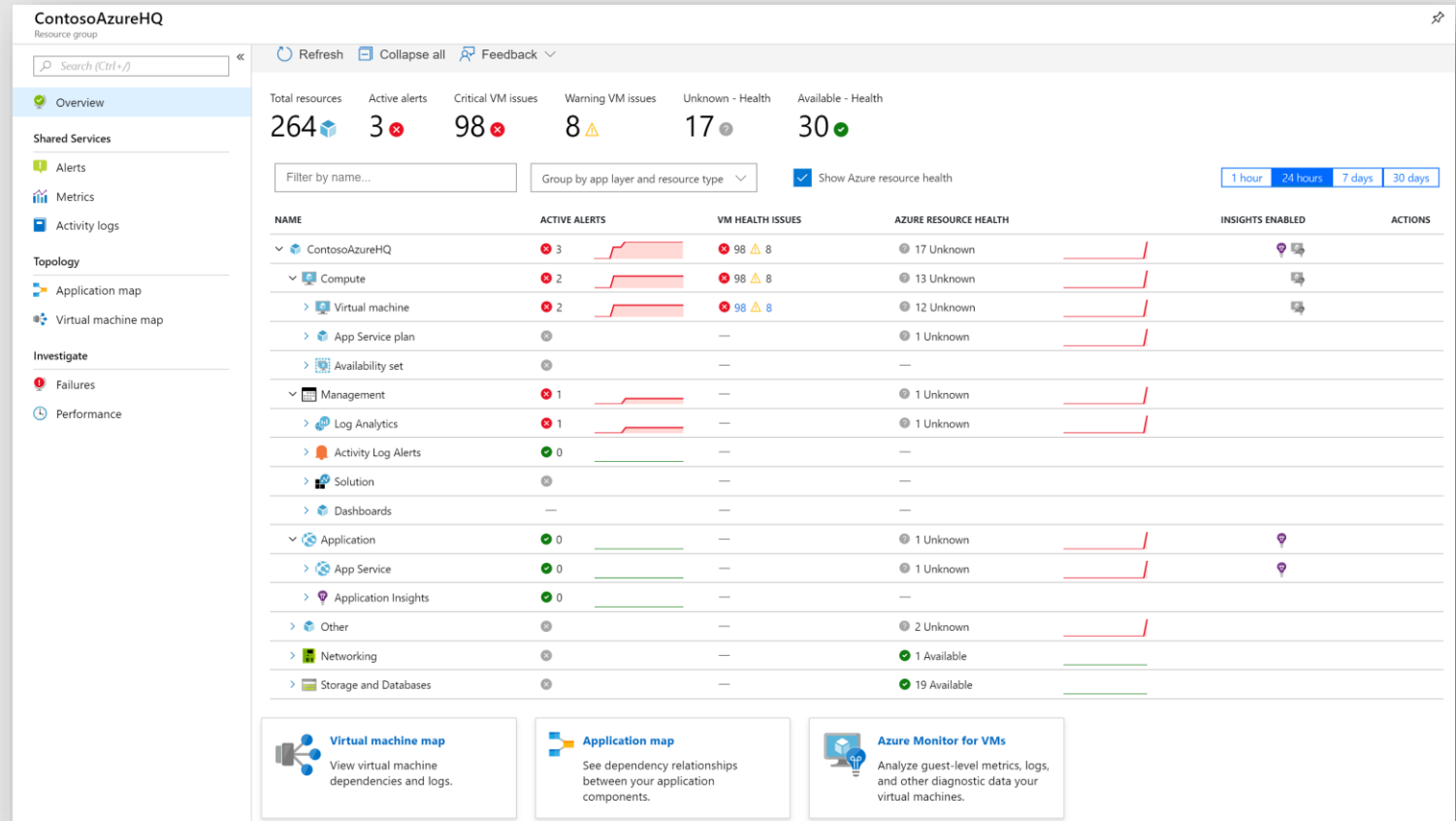


➔ Monitor health state of all resources

➔ See alerts firing across app & infra

➔ Jump to Application Map or VM Map

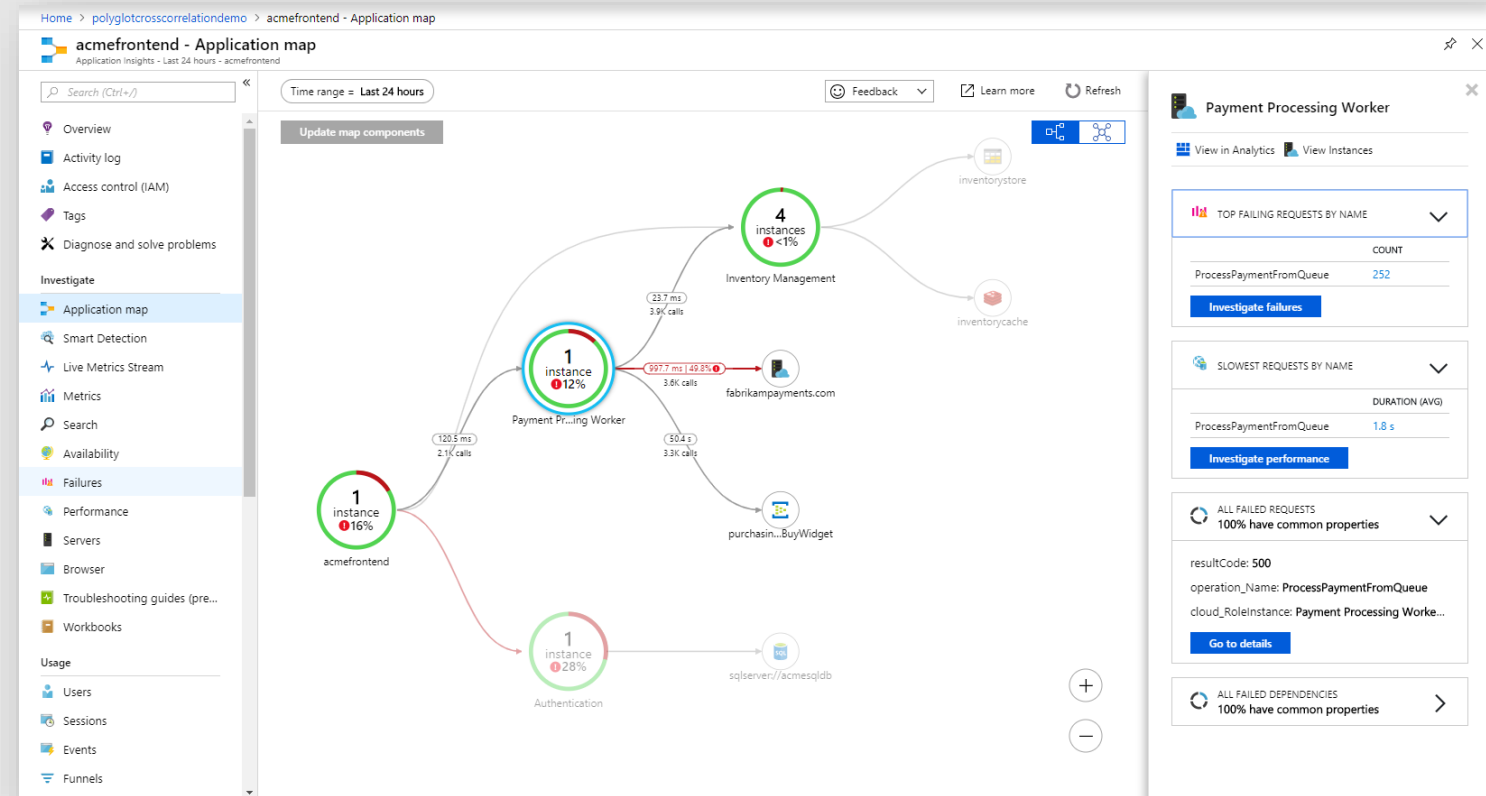
➔ Drill down into failures or perf issues



Diagnose E2E issues with Application Insights



- ➔ Monitor apps in .NET, JS, Java, Node.js or any language with OSS SDKs
- ➔ Visualize server/client connections & dependencies with App Map
- ➔ Track E2E distributed transactions (including for Python & Go) **NEW!**
- ➔ Drill down to code-level with Snapshot Debugging & Profiling
- ➔ Understand end-user cohorts, behavior & engagement for planning

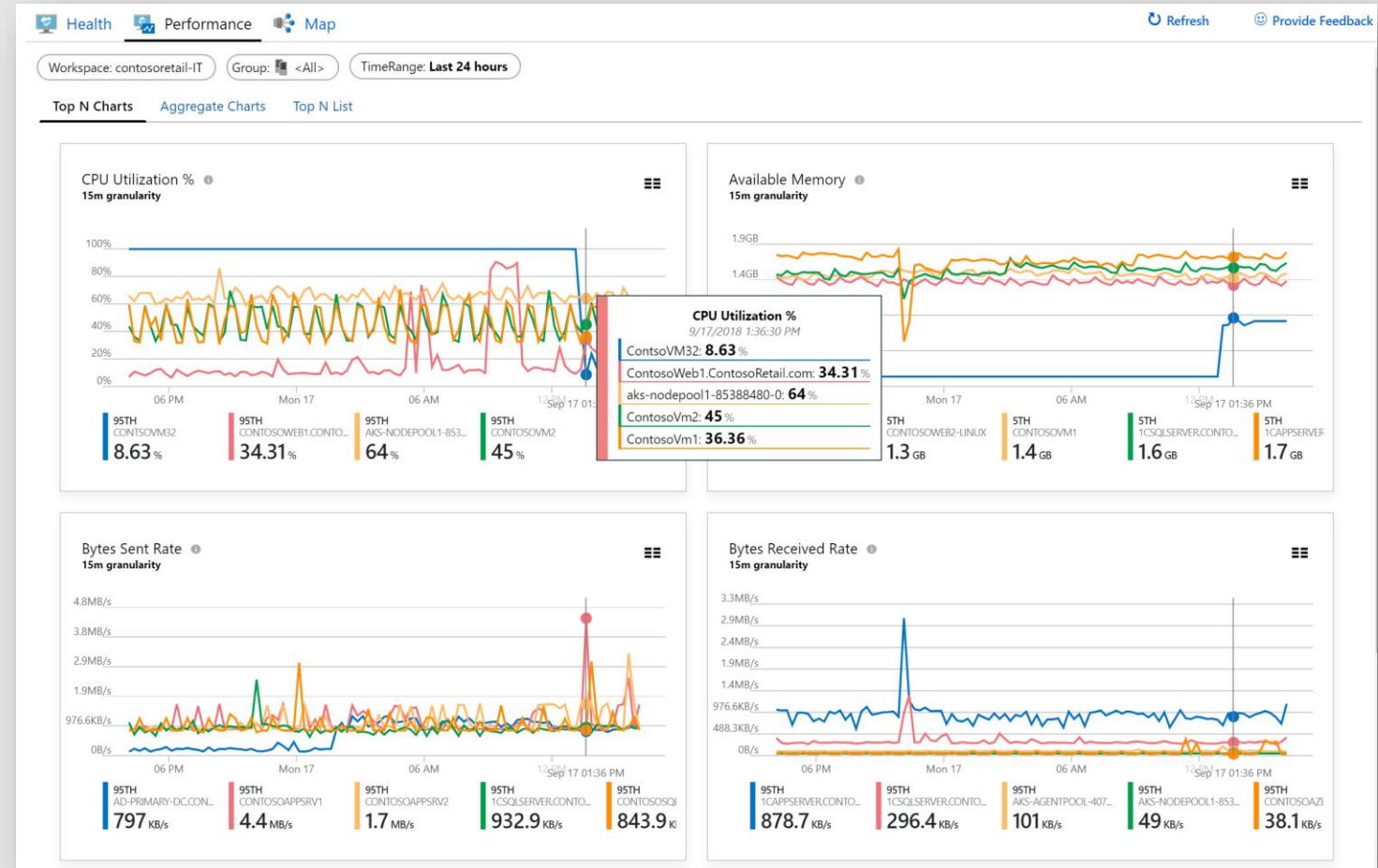


[Learn more](#): BRK3346 (Build the right solution for your business by Continuous DevOps Monitoring and Learning)

Rich Insights for Virtual Machines



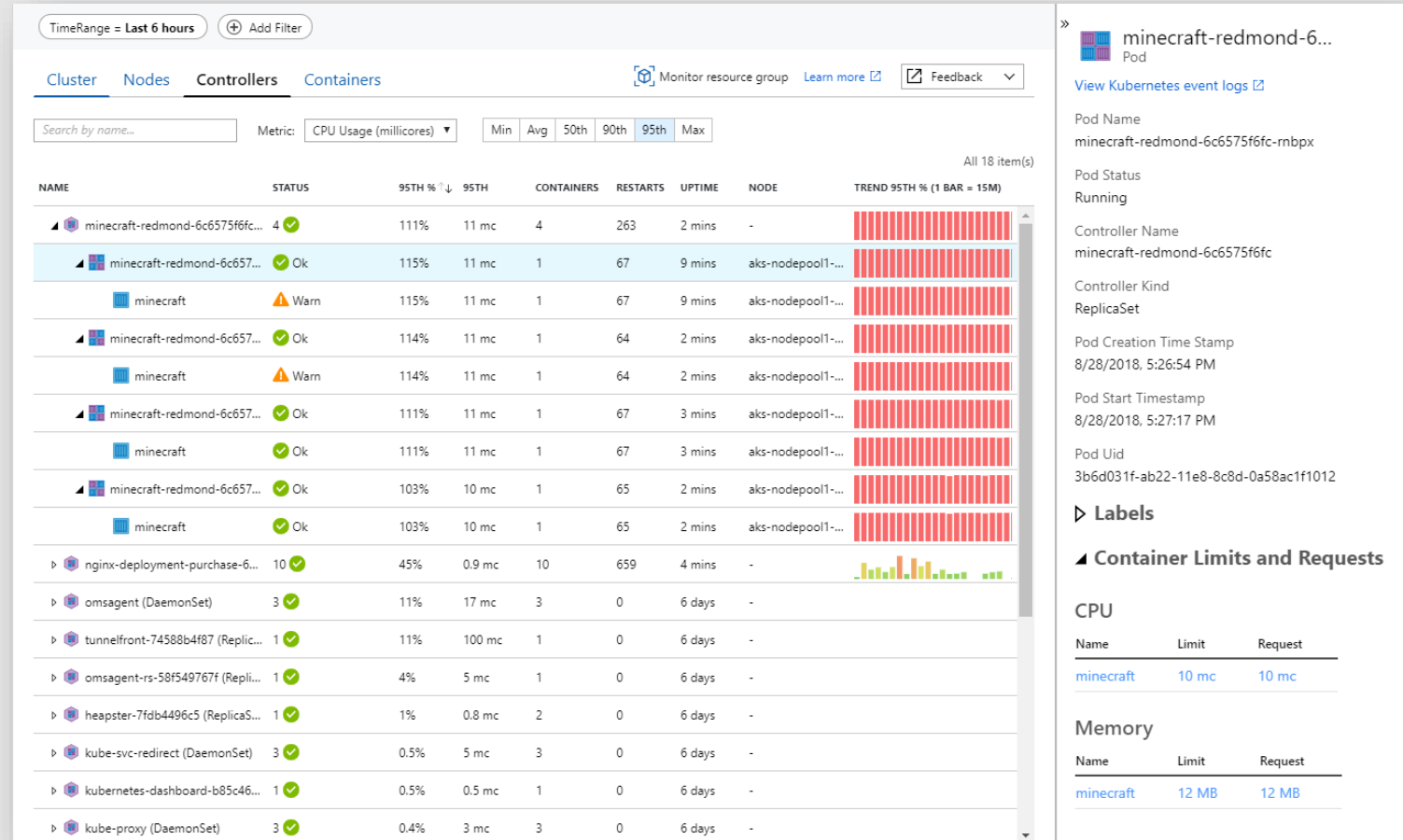
- ➔ Monitor single VMs or at scale
- ➔ Identify & isolate host-level or guest-level health problems
- ➔ Troubleshoot perf issues like CPU, memory, disk, and network
- ➔ Visualize service dependencies & connection failures in Maps
- ➔ Onboard at scale using PowerShell or Azure Policy



Drill down into AKS Containers



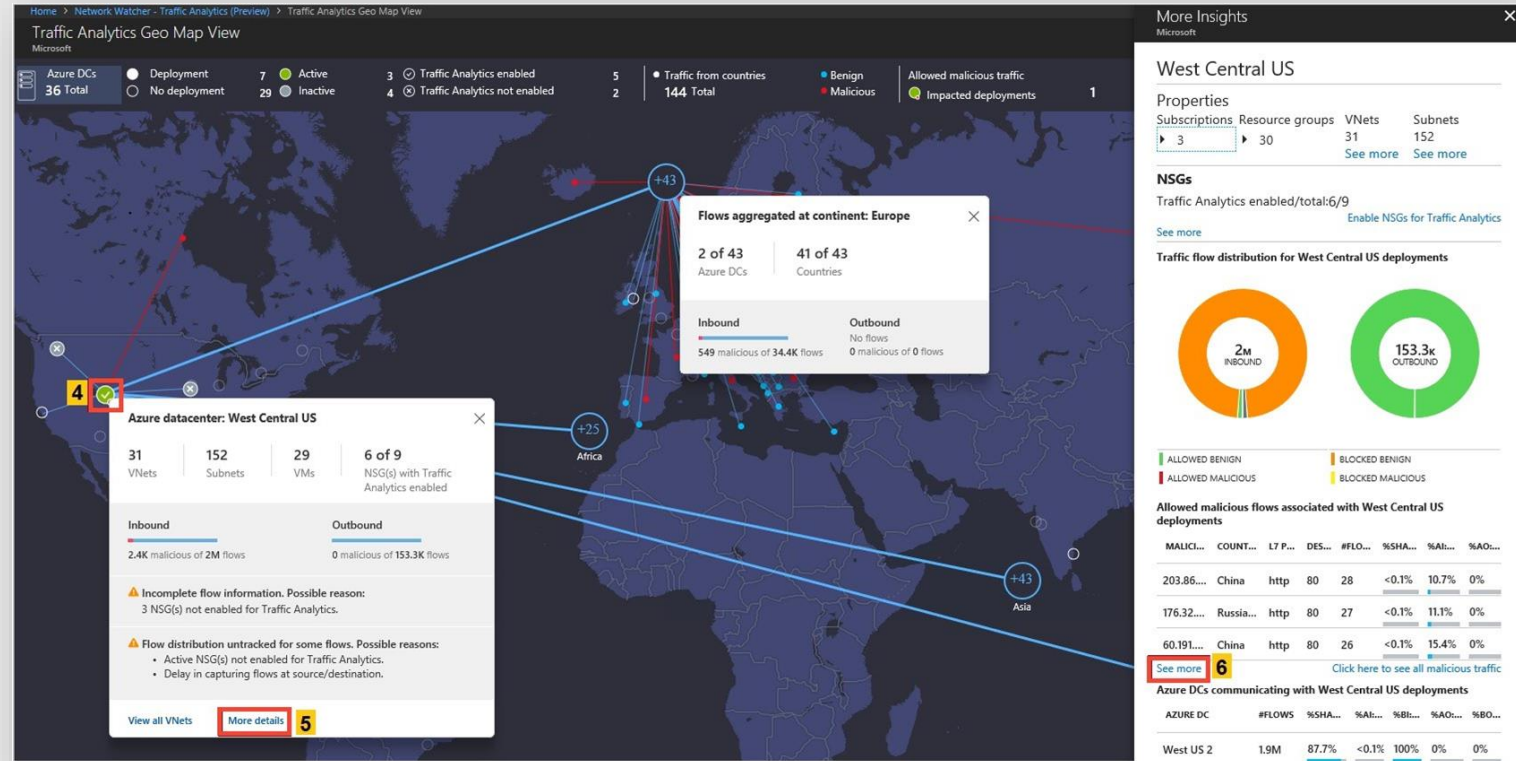
- ➔ Monitor multi-cluster health & node/pod status
- ➔ View overall perf across nodes, controllers and containers
- ➔ Analyze Kubernetes event & container logs for troubleshooting
- ➔ Understand cluster capacity needs under average or heaviest loads
- ➔ Monitor containers on demand in AKS with virtual nodes



Monitor Network Health & Traffic



- ➔ Secure and audit your network with Network Watcher Traffic Analytics
- ➔ Discover and monitor ExpressRoute circuits, across subscriptions
- ➔ Monitor ExpressRoute connectivity to virtual networks and O365
- ➔ Monitor connectivity to LoB apps with Service Connectivity Monitor



[Learn more](#): BRK3298 (Monitoring your networks in Azure)

Advanced Queries with Log Analytics



- ➔ Log Analytics advanced query experience now in Azure Portal
- ➔ Central Analytics Platform across Monitoring, Management, Security
- ➔ Run queries for investigations, statistics & root cause/trend analyses
- ➔ Utilize ML algorithms for clustering and anomaly detection



Recap: What's New



Unified Monitoring

One Metrics. One Logs. One Alerts.

Log Analytics query experience integrated into Azure Portal

Integration into native Azure resource blades

Configure Azure AD to send audit & sign-up logs to Azure Monitor

Ability to send Custom Metrics

Data Driven Insights

Azure Monitor for resource groups

Azure Monitor for VMs (health, performance, and maps)

Multi-cluster health rollup view for AKS

Distributed Tracing for Python/Go in addition to .NET, Java & Node.js apps

Java Local Forwarder, Micrometer & Spring Boot support

Scale & Security

Onboard VMs at scale via Azure Policy

Secured monitoring inside Virtual Networks

Store logs in firewall restricted secured storage accounts

Monitor ER and store NSG flow logs across subscriptions

Workflow Integrations



Unified Monitoring



Azure Monitor

Application

Operating System

Azure Resources

Azure Subscription

Azure Tenant

Custom Sources



Insights



Application



Container



VM



Monitoring Solutions

Visualize



Dashboards



Views



Power BI



Workbooks

Analyze



Metrics Explorer



Log Analytics

Respond



Alerts



Autoscale

Integrate



Event Hubs



Logic Apps



Ingest & Export APIs

Continuous Monitoring for DevOps & IT Ops



- ➔ Native IDE integrations in VS (.NET) and VS Code (Node.js)
- ➔ Onboard with Azure Pipelines Release Management & DevOps Projects
- ➔ Configure Pre- or Post-Deployment Quality Gates in Azure Pipelines
- ➔ Run Load Test or Multi-Step Web Test for Synthetic Perf Monitoring
- ➔ Work Item Management with Azure Boards for filing bugs and tracking
- ➔ Alerts & Notifications with automated actions & ITSM integrations

The screenshot displays the Azure DevOps web interface for a release pipeline named 'Greenlighting Demo'. The pipeline is in the 'Release' state, showing a 'Manually triggered' release by user 'msft 3' at 11/13/2017 5:32 PM. The pipeline consists of three stages: 'Dev' (Succeeded), 'Canary' (Succeeded with 2 warnings), and 'Rollback_Canary' (Succeeded). The 'Canary' stage is currently active, showing a 'Canary' deployment with '2 warnings' at 11/13/2017 7:45 PM. The 'Canary' deployment is successful, with 'Post-deployment conditions' marked as 'Succeeded'. A 'Gates' section on the right shows a table of deployment gates with their status across different samples.

Deployment gates \ samples	07:30 PM	07:35 PM	07:40 PM	07:45 PM
Check Health - Azure Monitor Observe the configured Azure mo...	✗	✗	✗	✓
Check Active Customer Tickets Executes a work item query and ch...	✓	✓	✓	✓

Partner Integration



Integration themes

Export data to existing cloud management tools

Security & Incident management

Dashboarding/Reporting

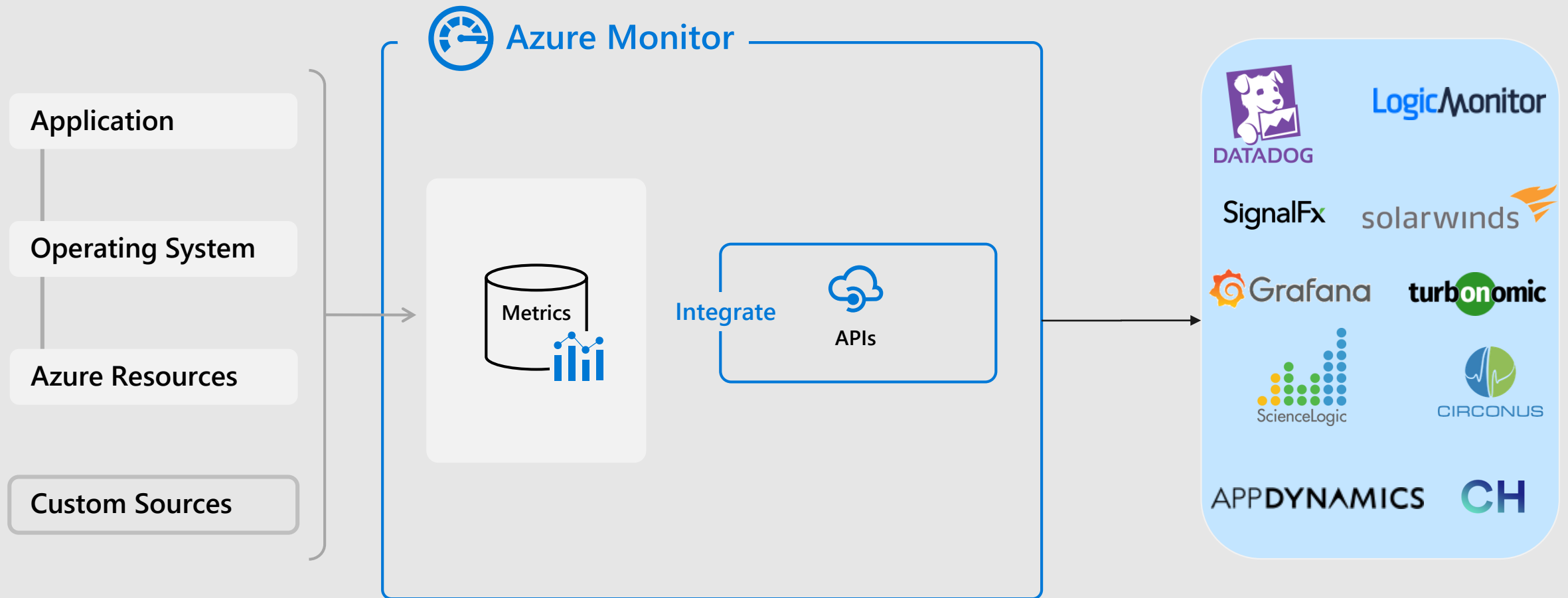
Analytics tools, Cost Management

Ingest custom data to Azure Monitor

OSS Integrations

Monitor Proprietary Workloads

Integrate metric data into a partner system



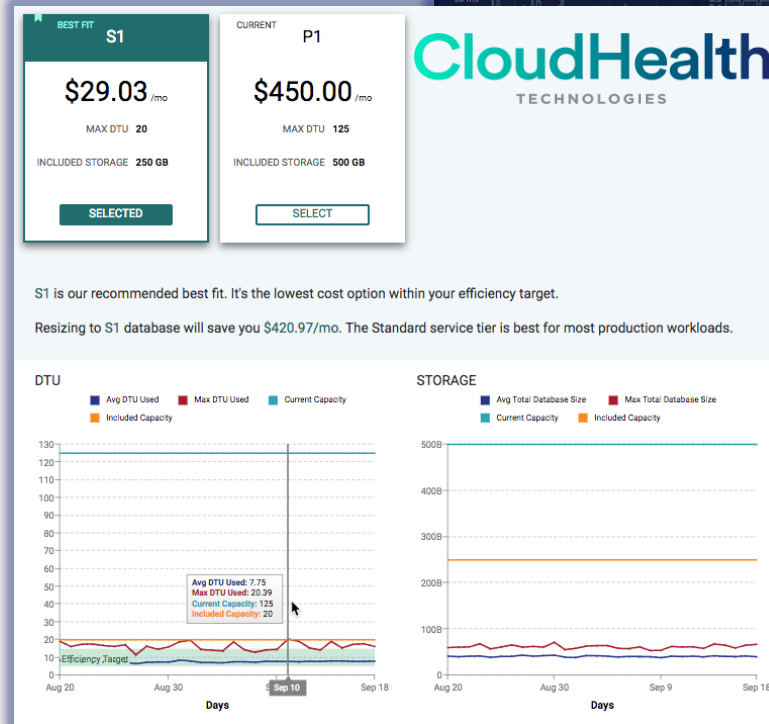
Metric data – use cases



➔ Ops Center Dashboards & Reporting



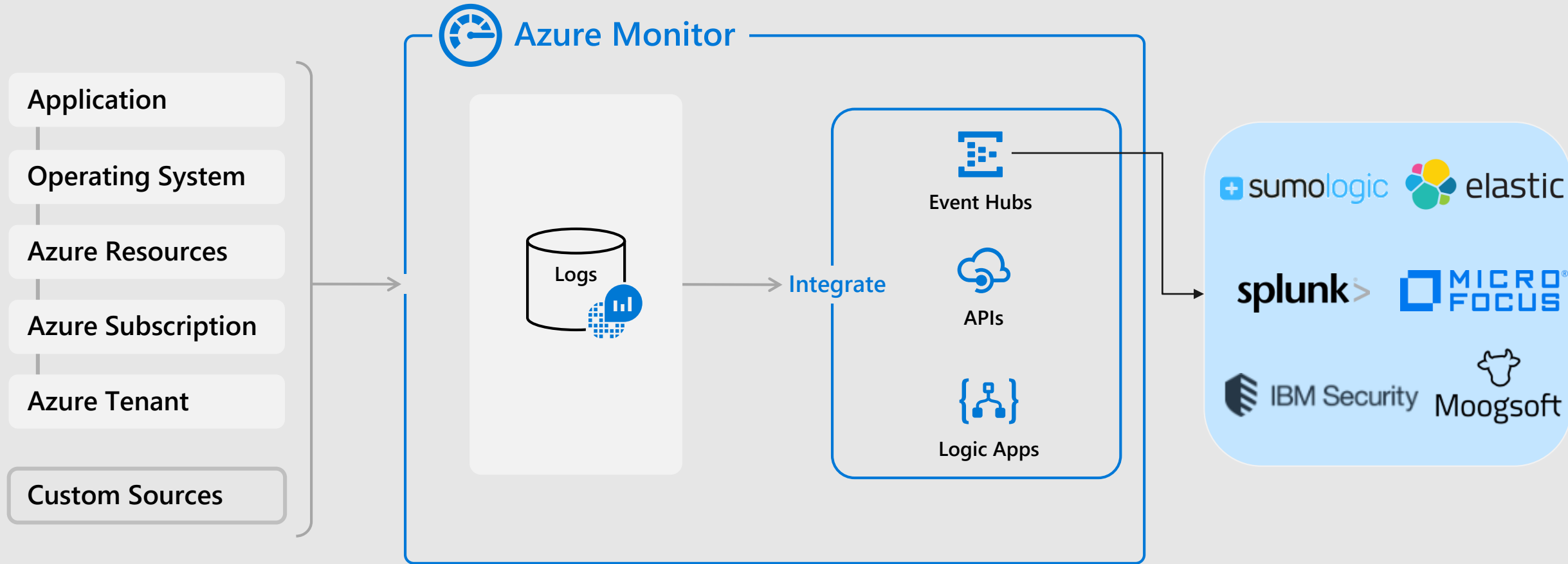
➔ Cost Management & Recommendations



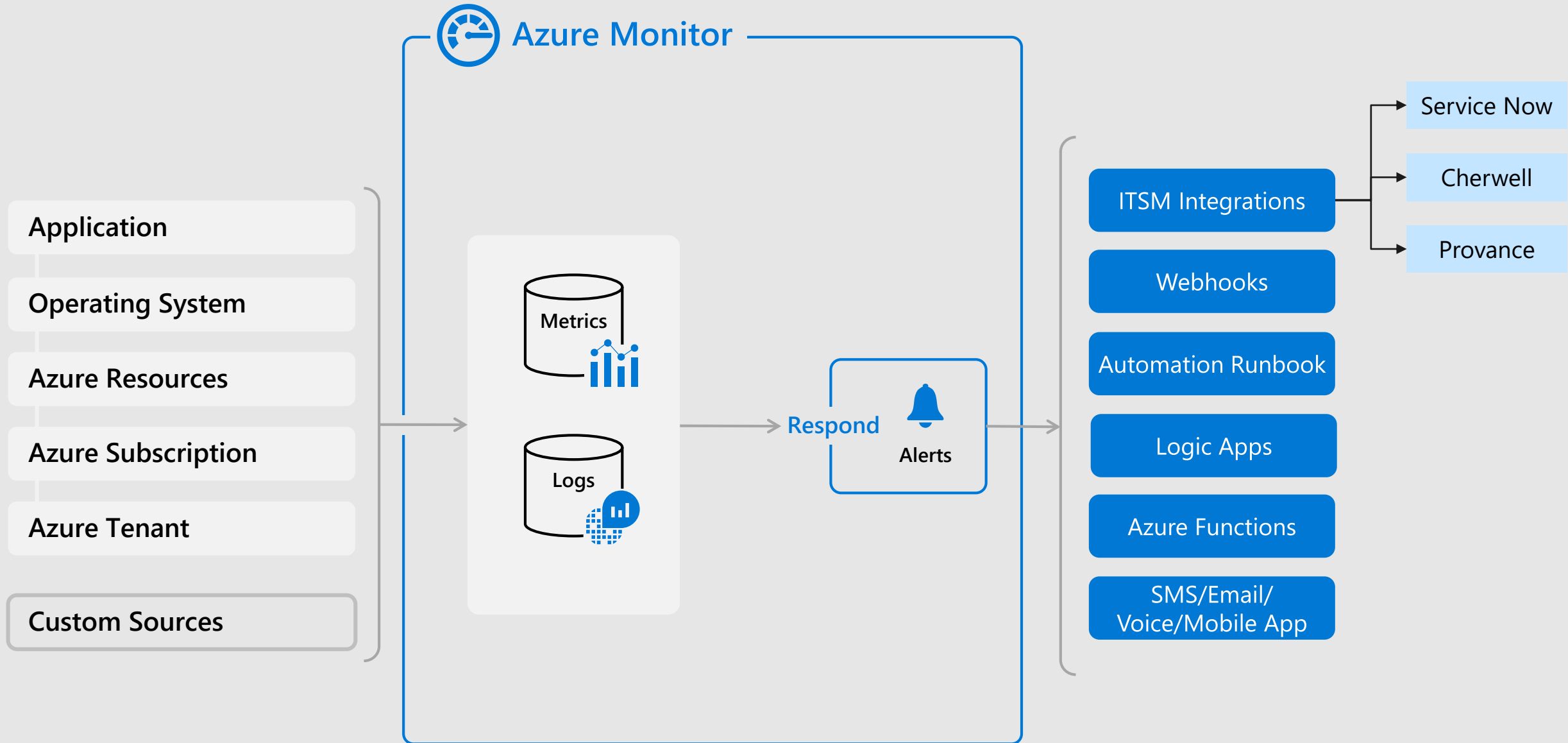
➔ Full Suite of Monitoring & Analytics



Integrate logs with a Log Analysis tool



Integrate your alerts into a partner system



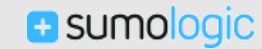
Key Takeaways



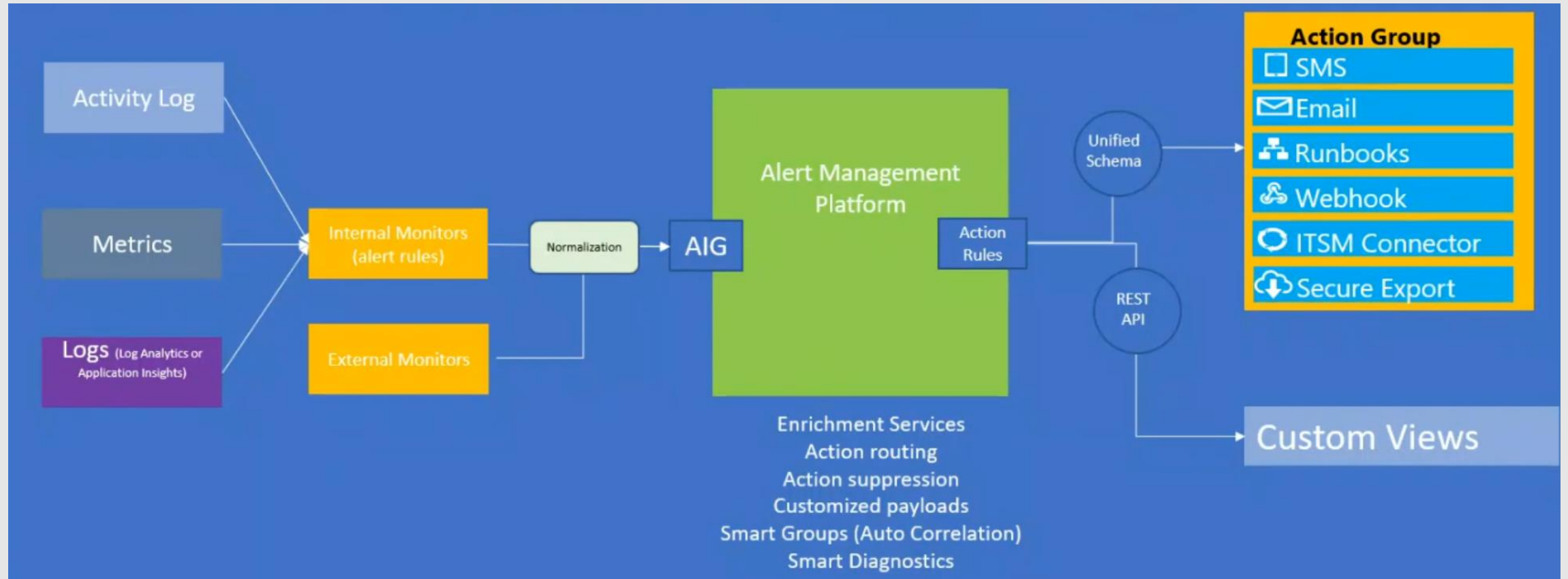
- Azure Monitor is best for Azure, and provides both APM & SIEM capabilities
- Open and extensible to continue using your favorite tools & solutions
- Integrate your existing APM/Monitoring solutions with Azure Monitor
- Route telemetry to your SIEM solutions for analytics & security management
- Extend & build on top of Azure Monitor for specific scenarios & workloads



APPDYNAMICS





Alert Management Platform





Azure Monitor - Alerts

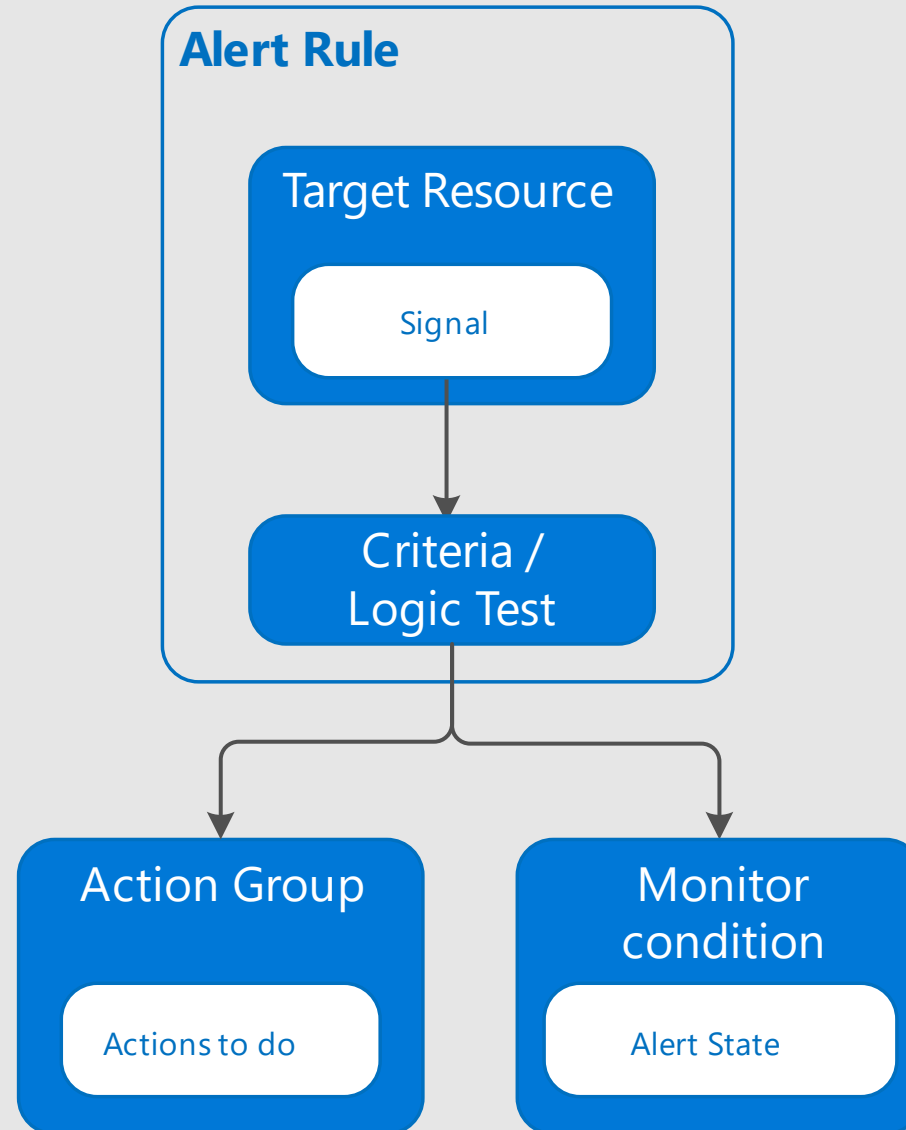
Alert on your **Azure services**:

Metric values	 Metric	Triggers when value of a specified metric crosses threshold
Activity log events	 Activity Log	Trigger on every event or only when certain events occurs

Alert on your **Azure Log Analytics Search**:

Custom Search	 Log	Triggers when value of a specified metric crosses threshold
Saved Search Query	 Log(Saved Query)	Trigger on every event or only when certain events occurs

Alert Rule Overview



Alerts – General

Alert rule is in three parts:

- **Alert condition:**
 - Alert target – let you select the Azure resource that will be monitored by the alert rule (example – your Log Analytics Workspace)
 - Alert criteria – specific condition or logic that should trigger the action
- **Alert Details:**
 - Alert configuration – name, description and severity
- **Action Group:**
 - Specific call sent to a receiver of a notification – email, SMS, webhook, etc. k etc.

Creating an alert rule

1. Define alert condition

- Alert Target (Log Analytics WS)
- Target Criteria

2. Define alert details

- Alert rule name
- Description
- Severity

3. Define action group

- Action Group
- Customize Actions


Hearbeat alerts on all Windows computers in a workspace [Log to Metric]

Rules management

Save Discard Disable Delete




1. Define alert condition


Alert condition configuration requires 1) Target selection and 2) Alert criteria definition where signal(s) and alert logic is configured. Start by selecting a Target.



* Alert target


Target Hierarchy

 contosoaretail-IT  Contoso IT - demo >  ContosoAzureHQ




* Alert criteria

Monthly cost in USD (Estimated) ⓘ


 Whenever the Heartbeat is Less than 5 count

Variable



TotalVariable

+ Add criteria



We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met

2. Define alert details

* Alert rule name ⓘ

Hearbeat alerts on all Windows computers in a workspace [Log to Metric]

* Description

This rule will trigger when any of the windows computers connected to the workspace report less than 5 heartbeats in 5 mins.

* Severity ⓘ

Sev 3

3. Define action group

Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	SUBSCRIPTION	ACTION GROUP TYPE	REMOVE
Create Ticket	Contoso IT - demo	1 ITSM	