midwest
architecture community
collaboration

Azure Security

Protecting data, applications, and resources in your cloud strategy

Tail Wind

Ross McNeely

Practice Manager, Ent Data Mgmt

www.rossmcneely.com

rmcneely@tailwindbi.com

@Ross_McNeely

Tail Wind Informatics

www.tailwindbi.com

952-544-2100

@TailWindBI

Microsoft Certified Professional
Microsoft
MCSA
SQL 2016 Business Intelligence Development
Earned 2019

Professional Graph Database
CERTIFIED
Neo4j Developer

snowflake
CERTIFIED
Associate

Microsoft Partner
Microsoft

Gold Data Platform
Gold Data Analytics

Abstract

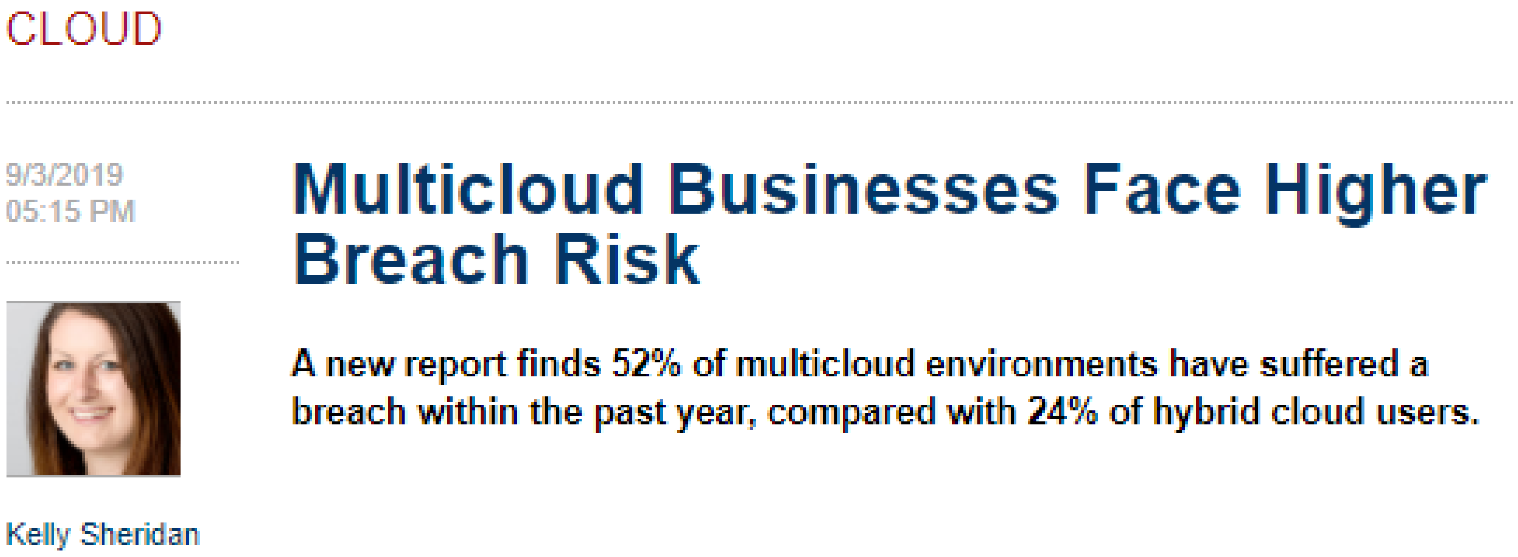
We now live in an identity-based security perimeter, and every XaaS has a variable depth of access and control. Security, and capabilities are the key questions for any cloud architecture. Nothing should be implemented today without a strong security surface that is able to meet the capability requirements. Join my session as I walk through key Azure security patterns for cloud infrastructure, data, and software. You will see how to manage identity and access. Know how platform protection is just the beginning for any capability rolled out. We will finish with how to secure your data and applications

Agenda

Topics

- Why more security architecture
- Security & Compliance
- Building Azure
- Protecting Azure
- Governance
- SIEM

Why are we talking about security?



CLOUD

9/3/2019
05:15 PM

Multicloud Businesses Face Higher Breach Risk

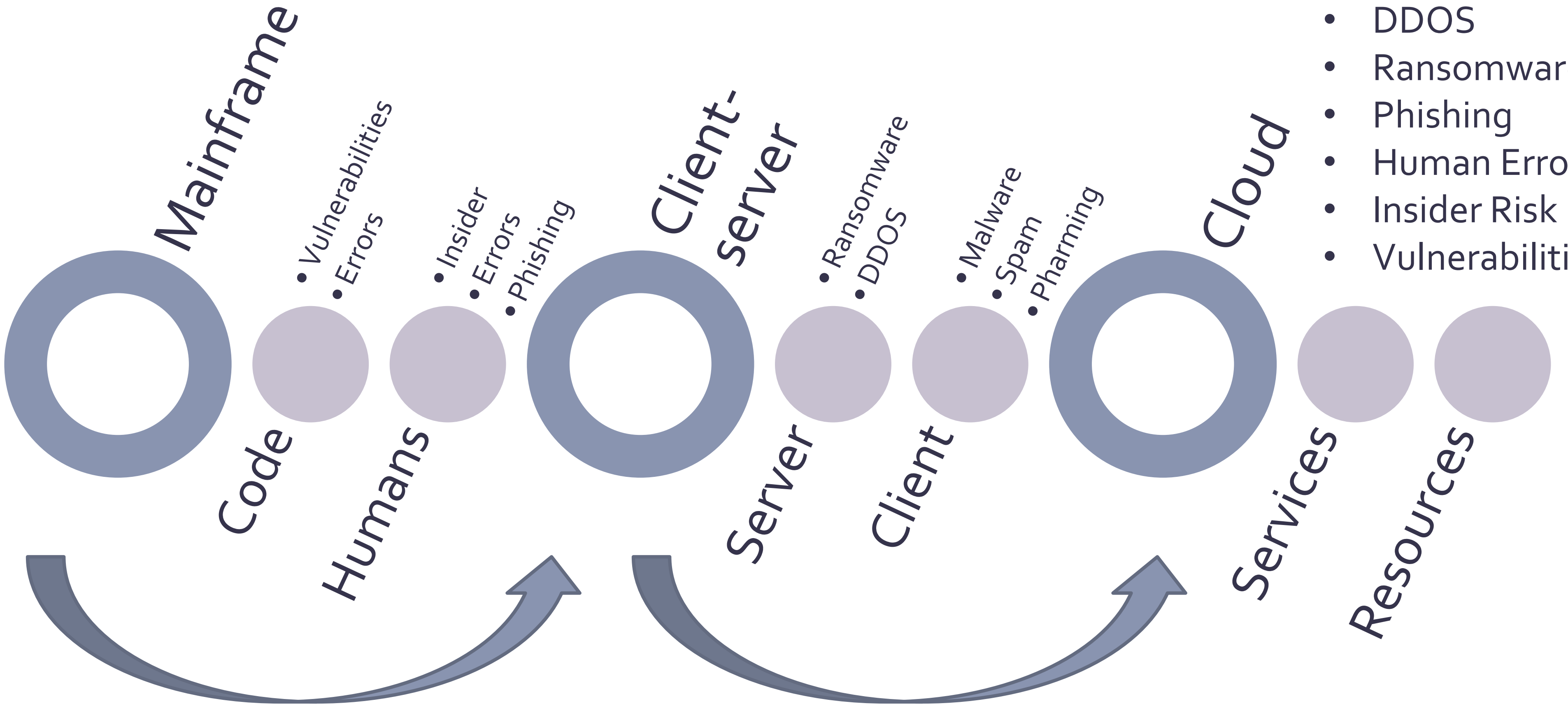
A new report finds 52% of multicloud environments have suffered a breach within the past year, compared with 24% of hybrid cloud users.

Kelly Sheridan

https://www.darkreading.com/author-bio.asp?author_id=837

HEADLINES

Attack Vectors



Mainframe

Code

- Vulnerabilities
- Errors

Humans

- Insider
- Errors
- Phishing

Client-server

Server

- Ransomware
- DDOS

Client

- Malware
- Spam
- Pharming

Cloud

Services

Resources

- Pharming
- Spam
- Malware
- DDOS
- Ransomware
- Phishing
- Human Error
- Insider Risk
- Vulnerabilities

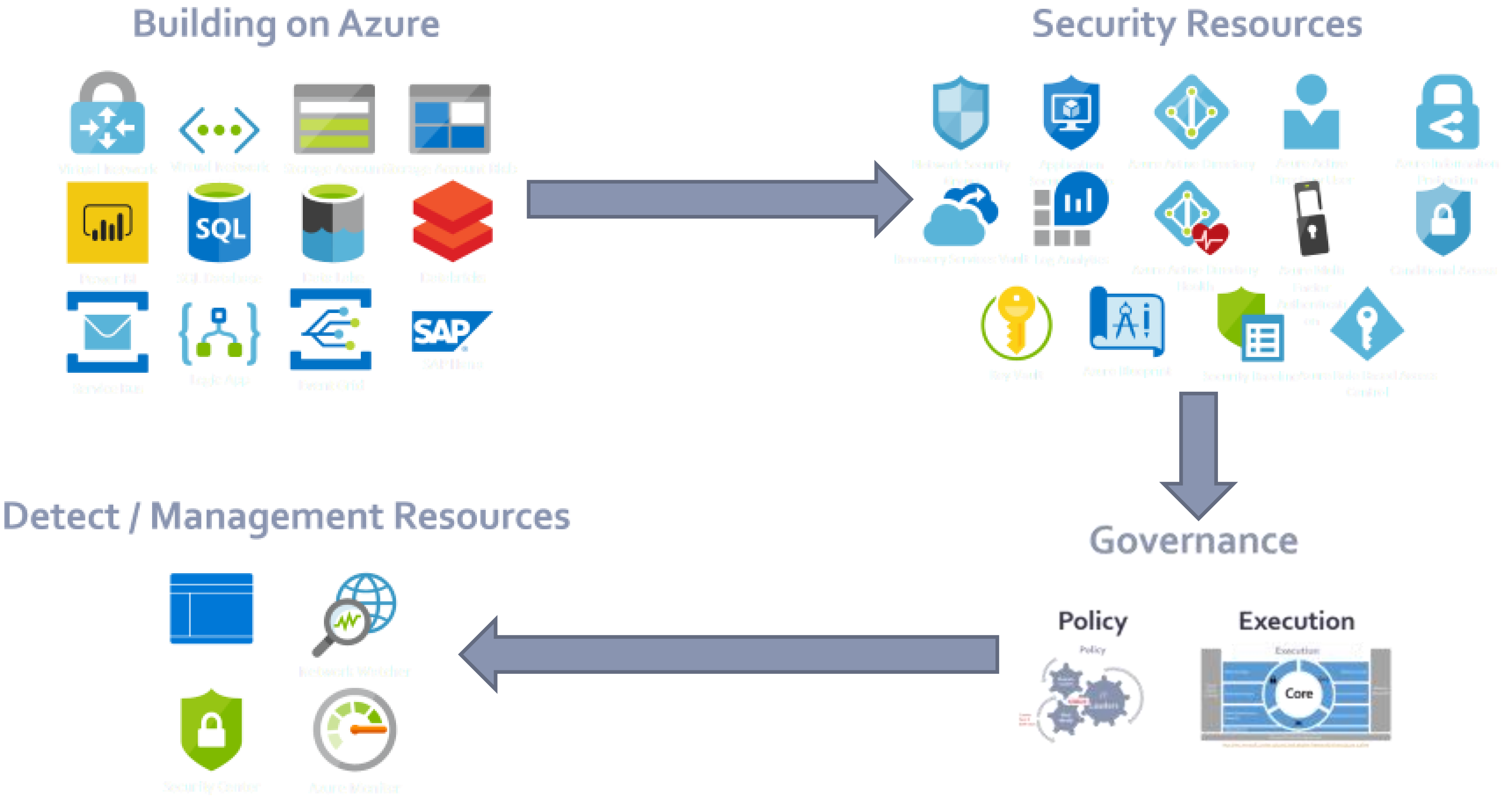
Why expand our attack landscape?

- Faster innovation in Azure.
- Quick data and app insights.
- Build and deploy anywhere.
- Cloud protection.

AZURE SECURITY

The Bigger Picture

Dev / Security / Compliance / Monitor



Building on Azure

Security Resources

Network Security Groups
Application Security Groups
Azure Active Directory
Azure Active Directory User
Azure Information Protection
Recovery Services Vault
Log Analytics
Azure Active Directory Health
Azure Multi Factor Authentication
Conditional Access
Key Vault
Azure Blueprint
Security Baseline
Azure Role Based Access Control

Governance

Policy

Execution

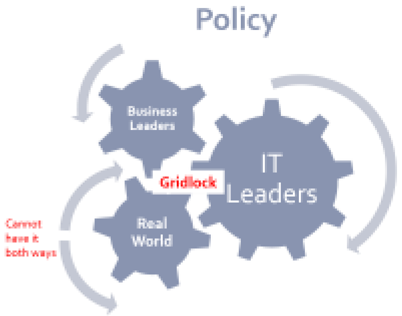
Detect / Management Resources

Building on Azure

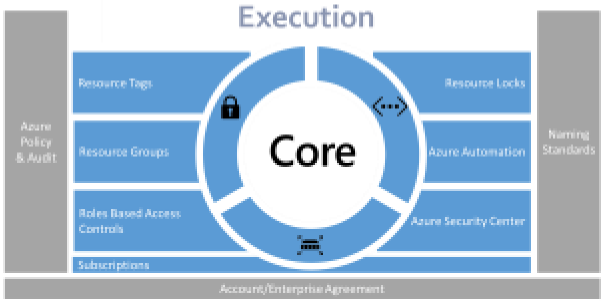
Security Resources

Governance

Policy

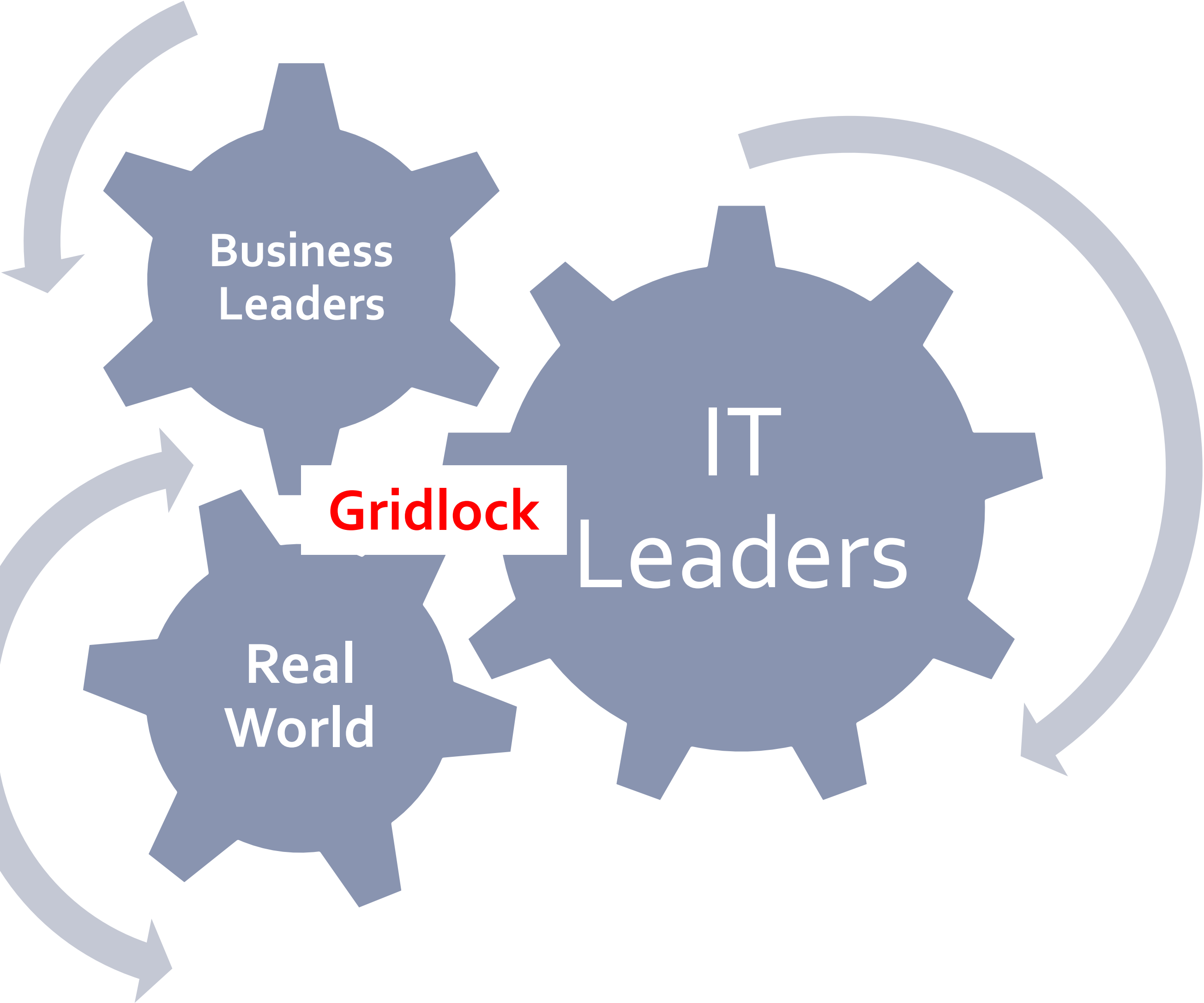


Execution



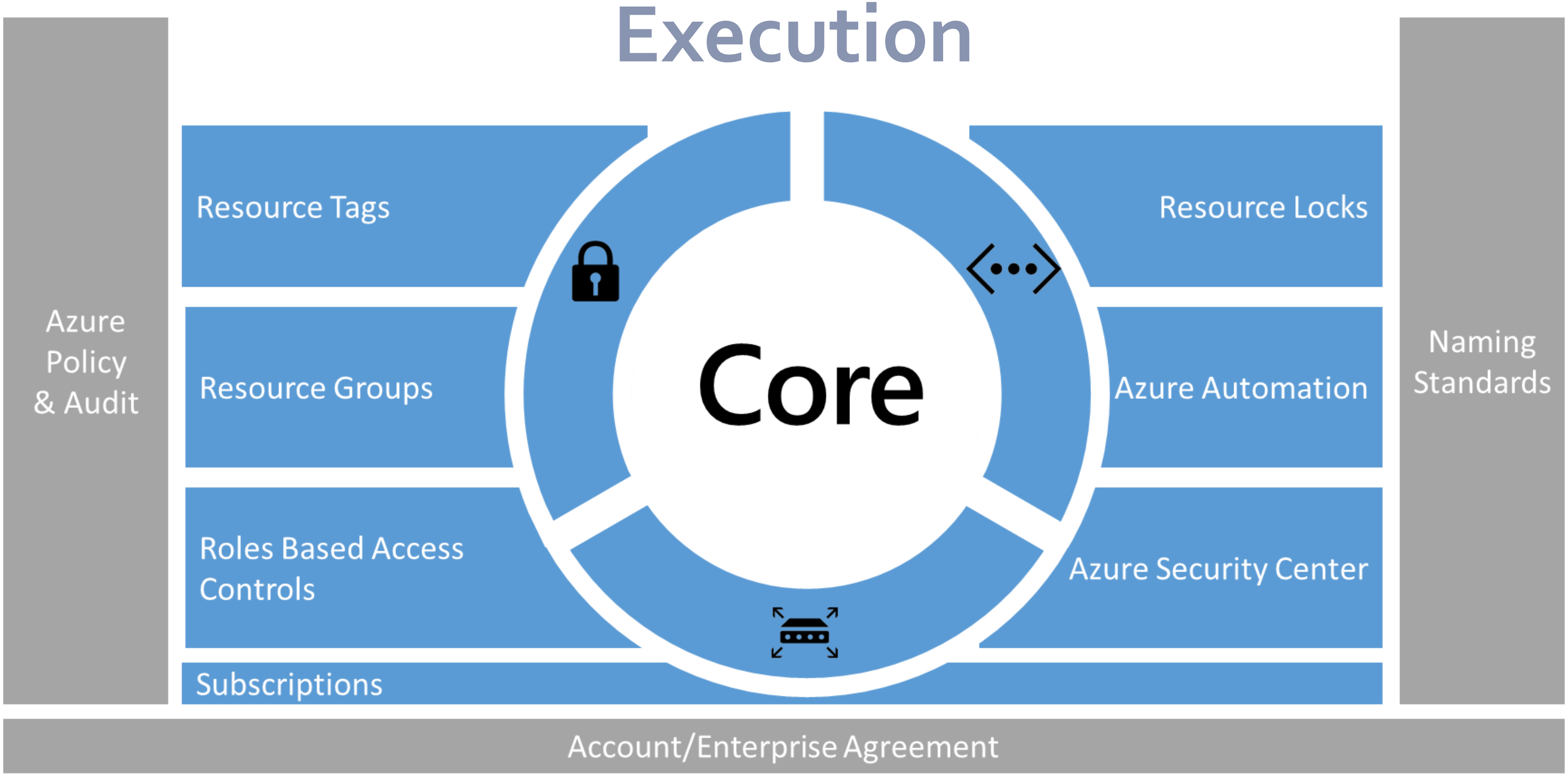
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/reference/azure-scaffold

Policy



Cannot have it both ways

Execution



Azure Policy & Audit

Resource Tags

Resource Groups

Roles Based Access Controls

Subscriptions

Core

Resource Locks

Azure Automation

Azure Security Center

Naming Standards

Account/Enterprise Agreement

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/reference/azure-scaffold

Detect / Management Resources

BUILDING ON AZURE

The missing ingredient

Building on Azure

Security
Development
Lifecycle

SDL

DevSecOps

OSA

Operational
Security
Assurance

DevOps

Security Development Lifecycle

- Provide Training
- Define Requirements
- Define Metrics and Compliance Reporting
- Use Software Composition Analysis (SCA) and Governance

SDL

Security Development Lifecycle

- Perform Threat Modeling
- Use Tools and Automation
- Keep Credentials Safe
- Use Continuous Learning and Monitoring

SDL

Operational Security Assurance

OSA

- Provide Training
- Use Multi-Factor Authentication
- Enforce Least Privilege
- Protect Secrets

Operational Security Assurance

OSA

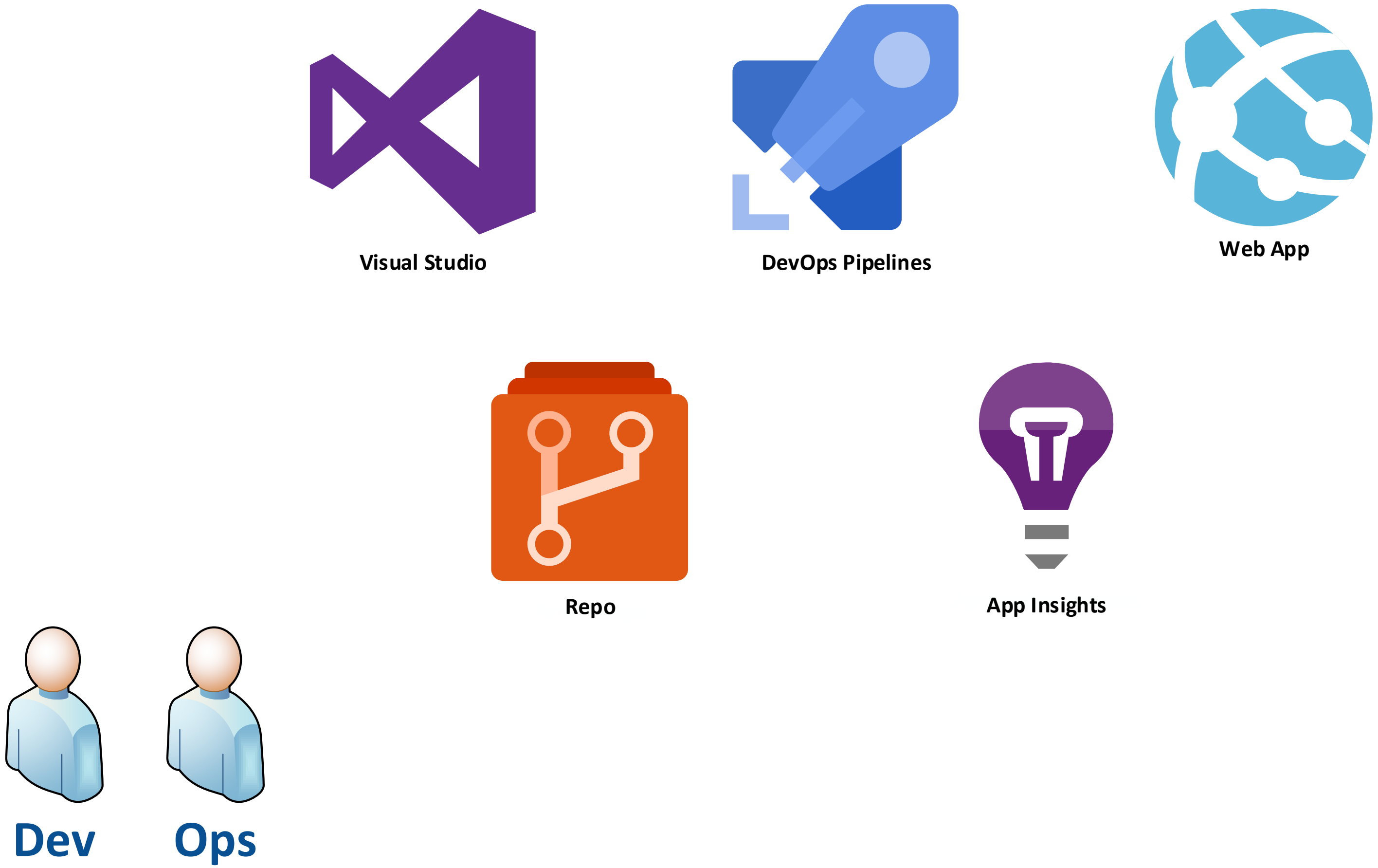
- Minimize Attach Surface
- Encrypt Data in Transit and at Rest
- Implement Security Monitoring
- Implement A Security Update Strategy

Operational Security Assurance

OSA

- Protect Against DDOS Attacks
- Validate the Configuration of Web Applications and Sites
- Perform Penetration Testing

Security with Serverless Architecture



Visual Studio

DevOps Pipelines

Web App

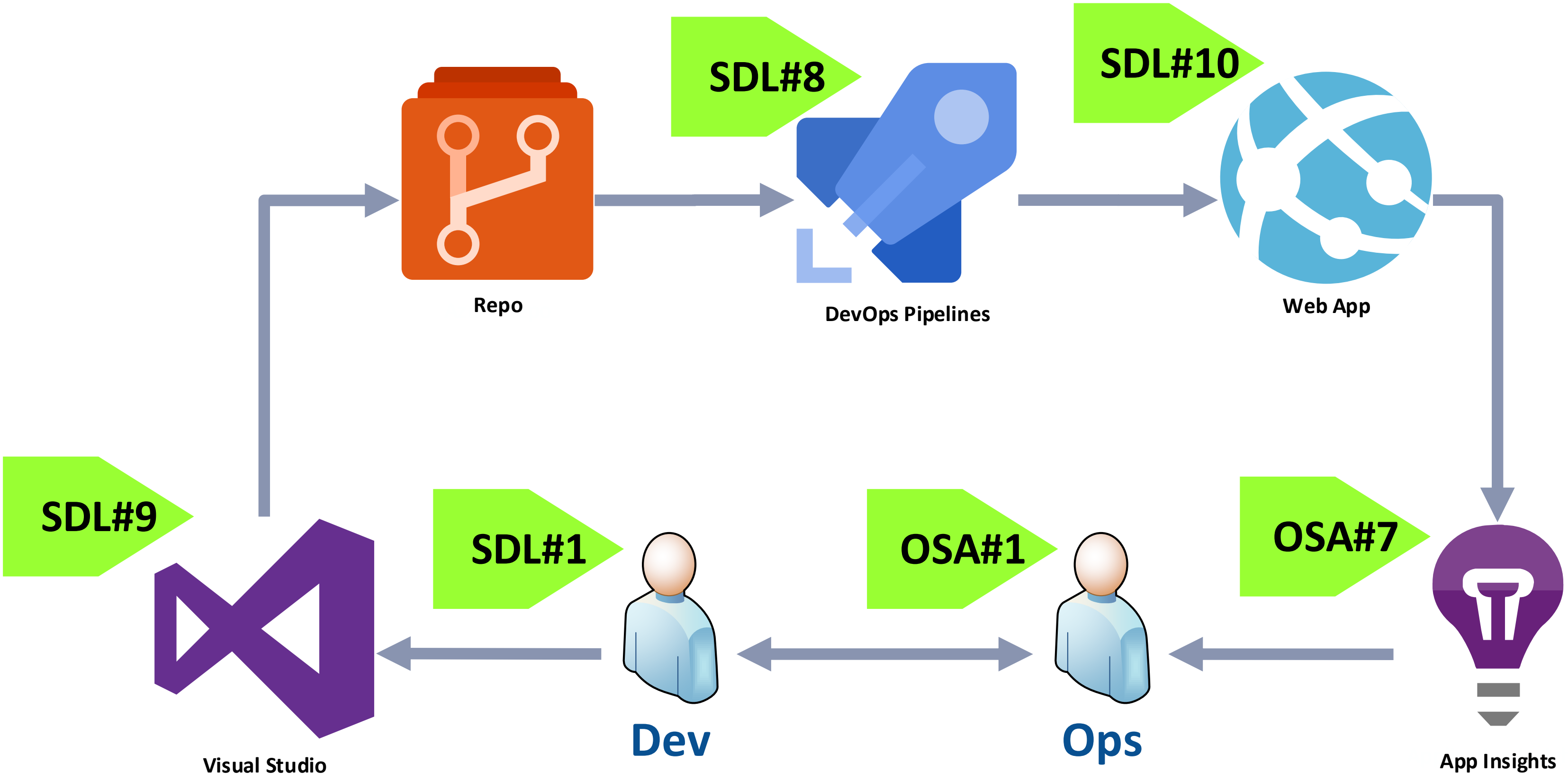
Repo

App Insights

Dev

Ops

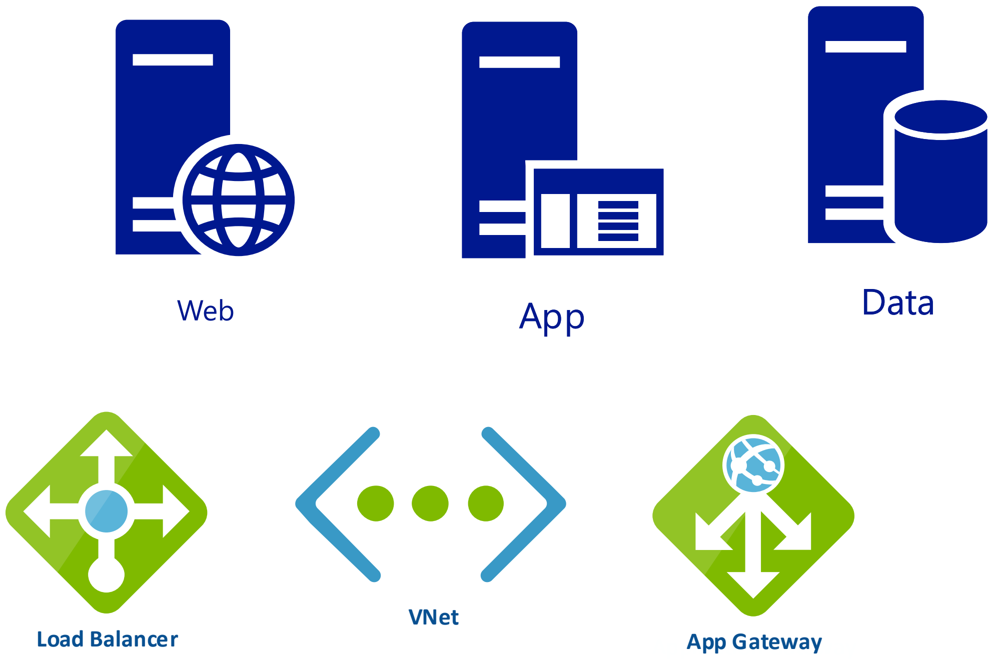
Security with Serverless Architecture



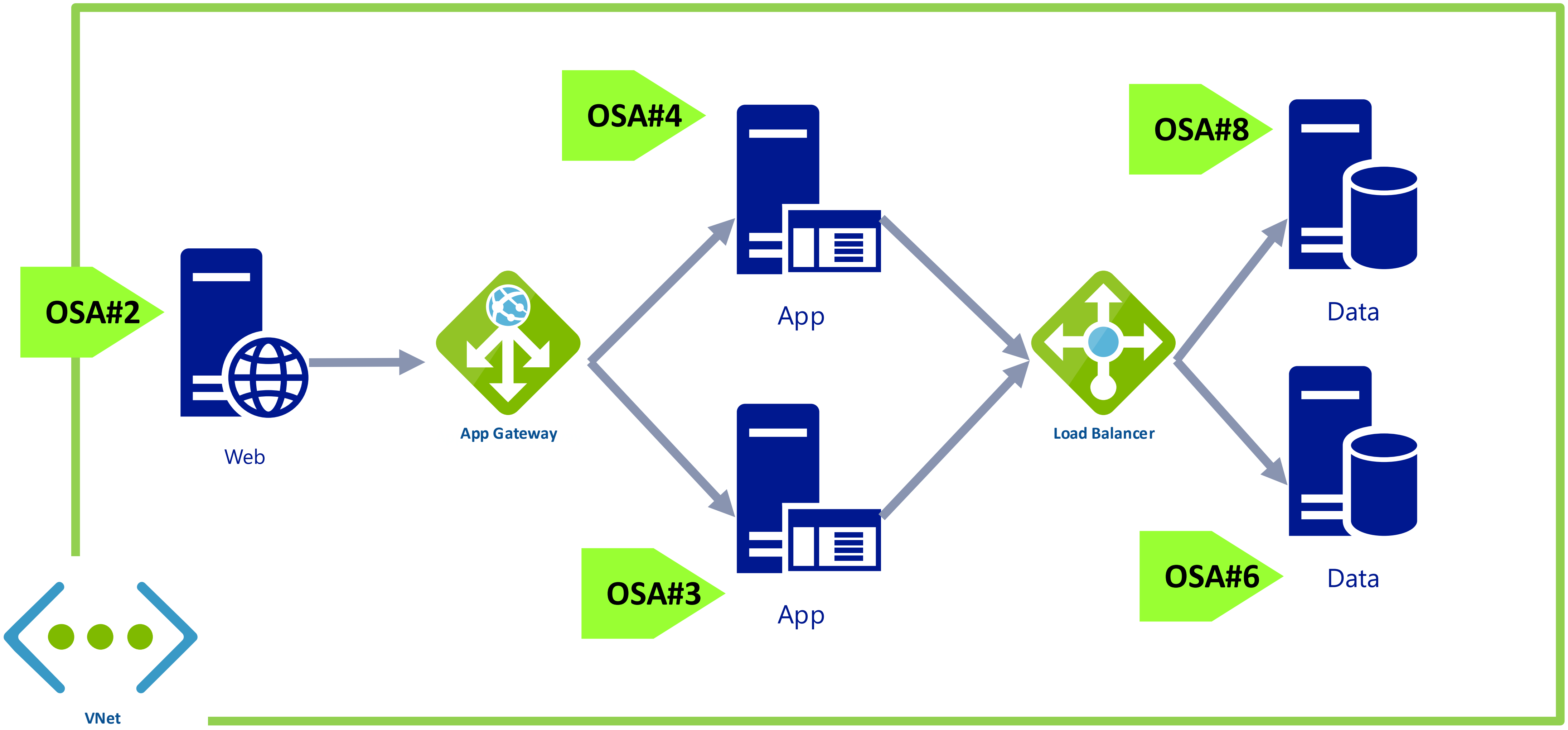
Security Development Lifecycle (SDL)

Operational Security Assurance (OSA)

Security with VM Architecture



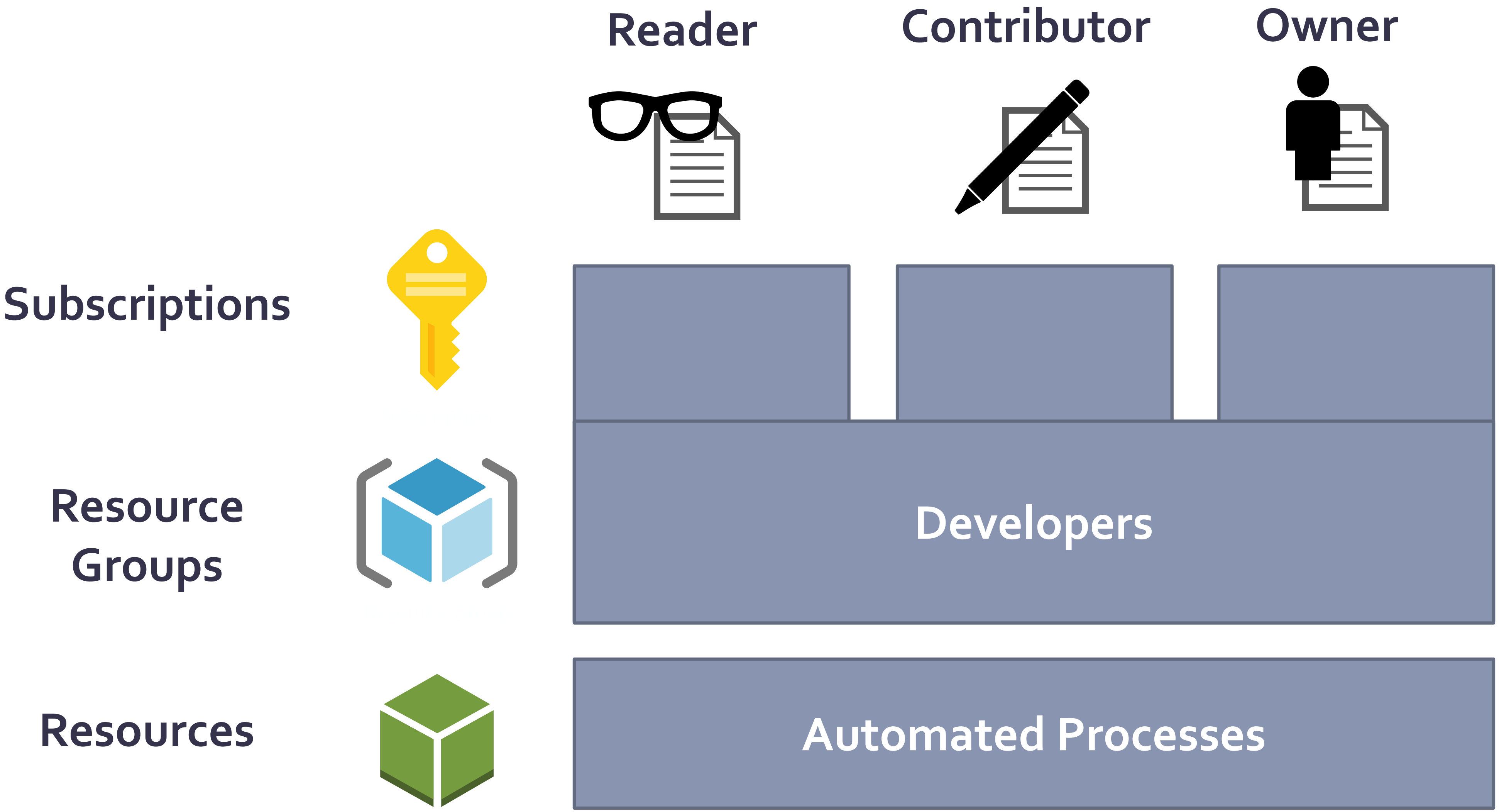
Security with VM Architecture



SECURITY & COMPLIANCE

2 big topics

Security and Compliance



Reader

Contributor

Owner

Subscriptions

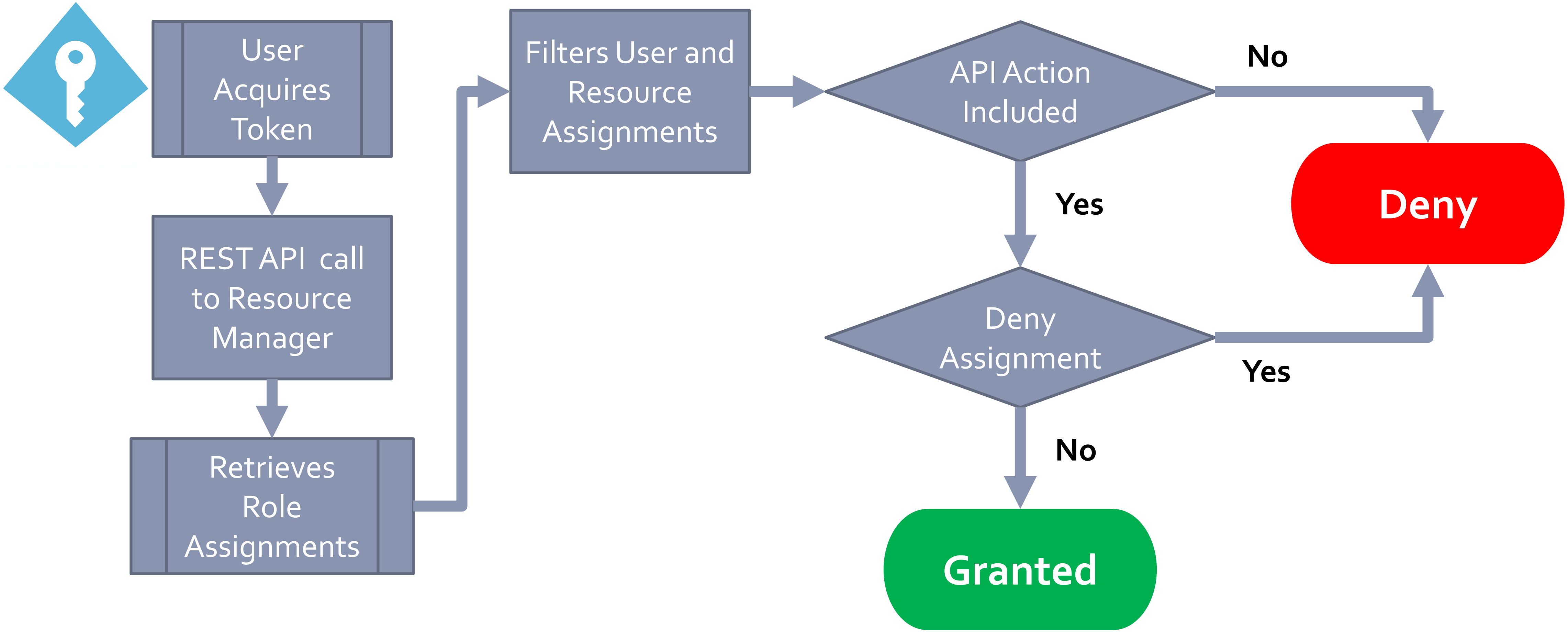
Resource Groups

Resources

Developers

Automated Processes

Security and Compliance - RBAC



User Acquires Token

REST API call to Resource Manager

Retrieves Role Assignments

Filters User and Resource Assignments

API Action Included

Deny Assignment

Deny

Granted

Security and Compliance

- Collection of security data
- Security status
- Detection and investigation
- Operational and Security management integration

PROTECTING AZURE

The 3 big ‘S’s

The big S3 + 1S

Data Security

At-Rest

- Server-side Encryption
  - Service Managed Keys
  - Azure Key Vault
  - On-premises Managed Keys
- Client Encryption

In-Transit

- SSL/TLS
- VPN
  - Site-to-site
  - Point-to-site
- ExpressRoute (bonus App-level encrypt)

Data Security

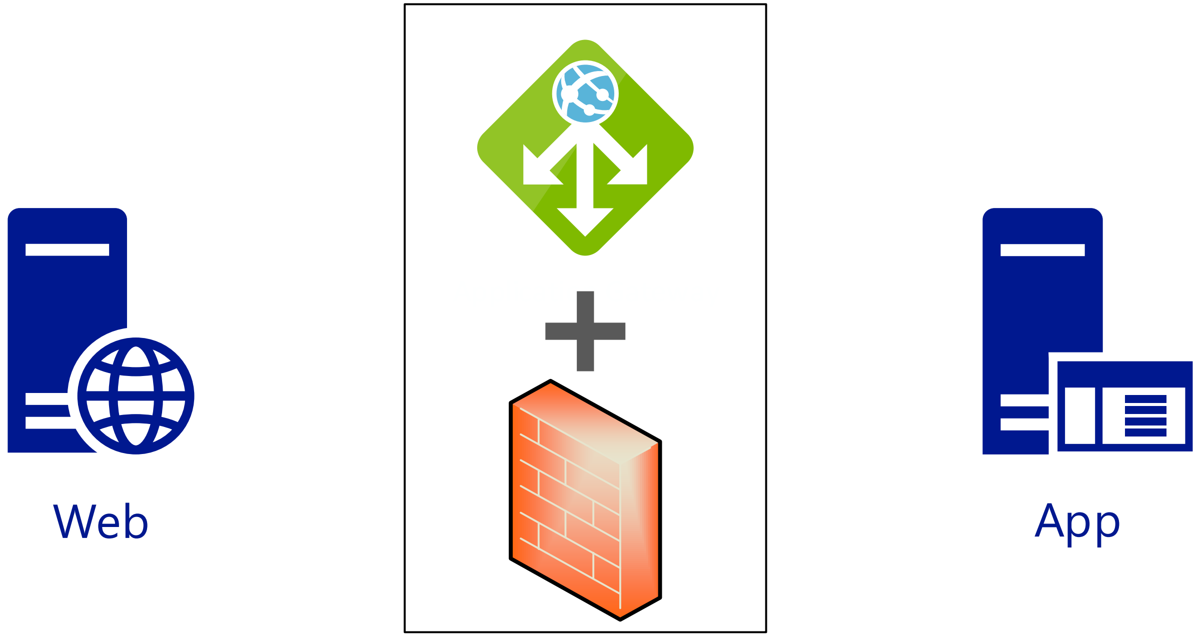
Left-the-Nest

- Azure Information Protection
  - Multiple file types
  - Files anywhere
  - Sharable
  - Monitoring (Auditable)
  - Multiple devices
  - Revoke access

Application Security

Application Gateway

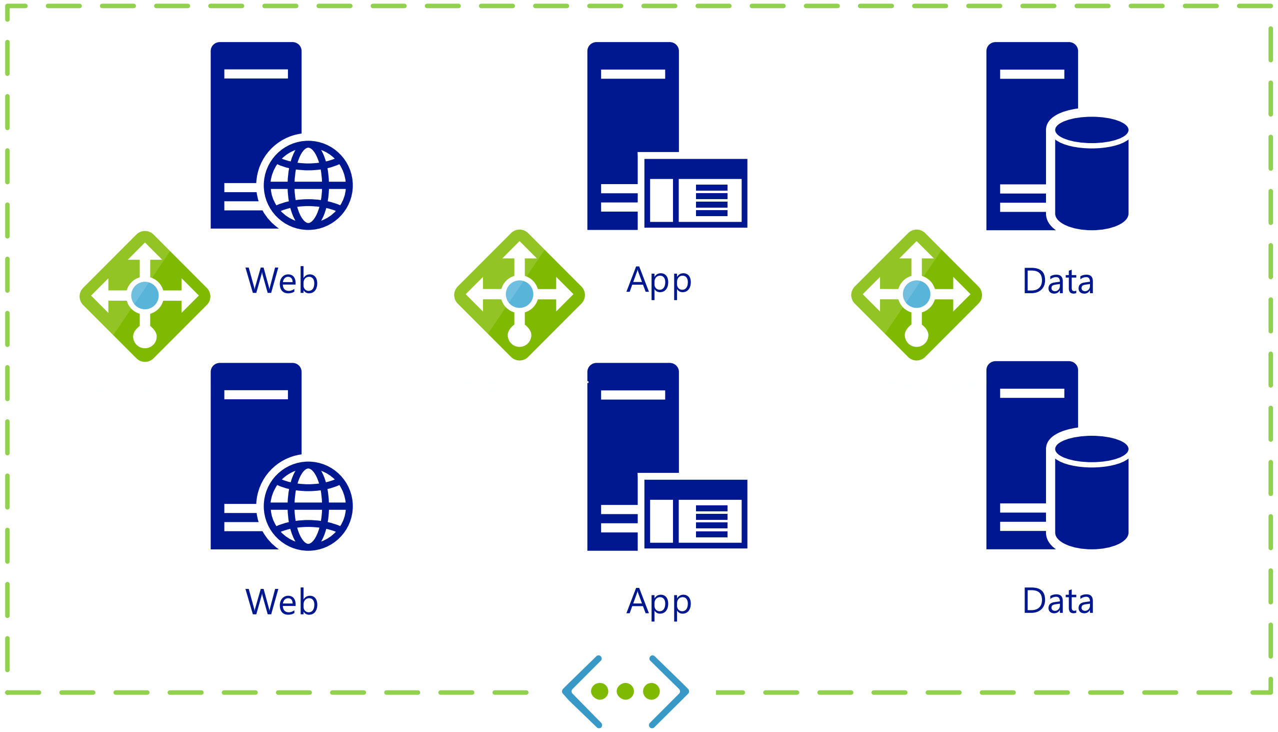
- SQL Injection protection
- Cross site scripting protection
- HTTP request smuggling
- HTTP response splitting
- Remote file inclusion attach
- HTTP protocol anomalies
- Bots, crawlers, scanners



Network Security

Azure network infrastructure

- VNets
- Network Security Groups
- Forced Tunneling



VM & AKS Security

Virtual Machine

- Any antimalware software
- Azure Backup
- Azure Site Recovery
  - Azure VM rep
  - On-premises VM rep
  - Data resilience
  - RTO and RPO targets

Azure Kubernetes Service

- Azure AD integration with AKS w/ RBAC
- Master Security maintained by MS
- *Node Security latest OS updates/configs
- Cluster upgrades
- Deploy into Vnets with Site-to-Site, or VPN and ingress controllers defined with private internal IP addresses

AZURE GOVERNANCE

Operations

Governance

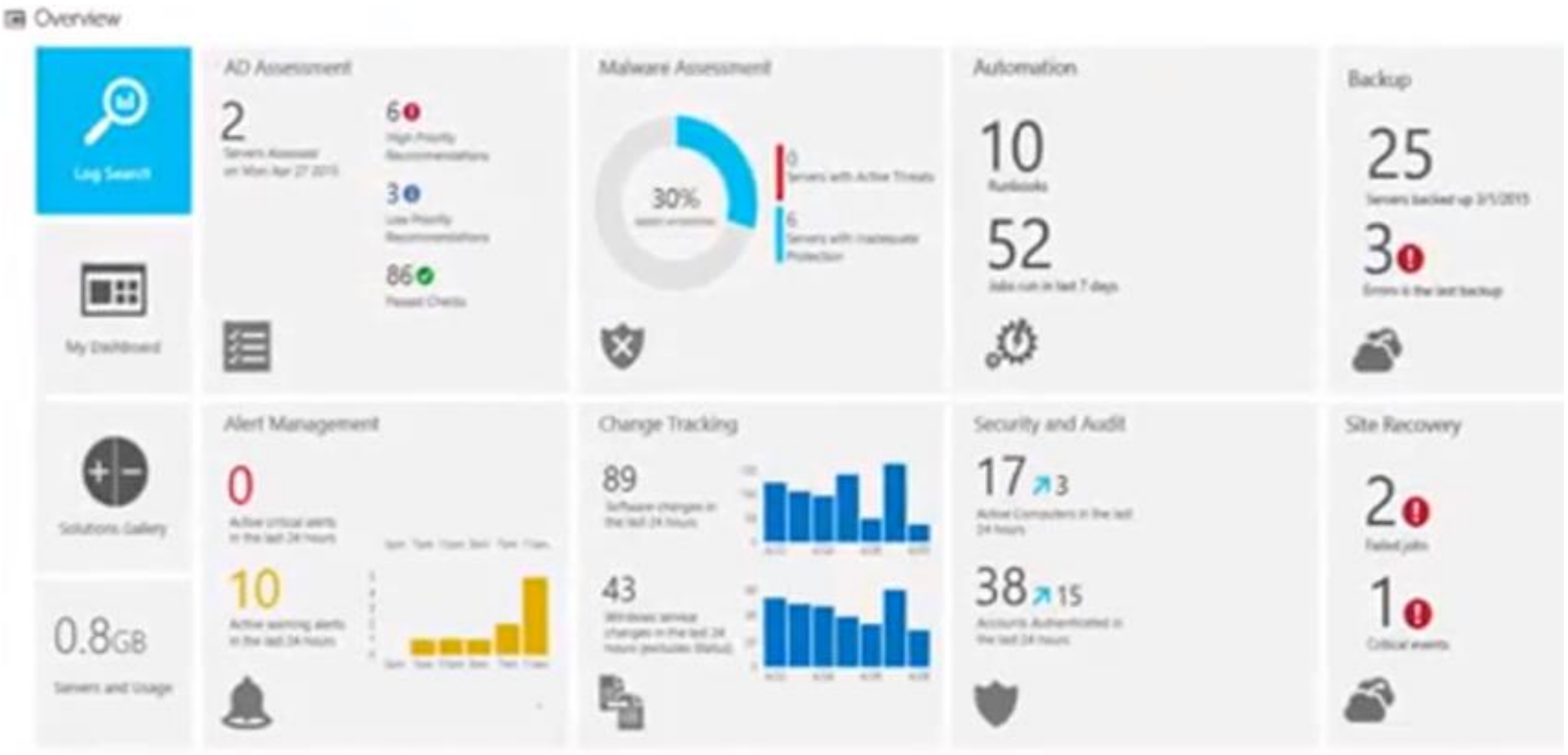
Operations Mgmt

Network Watcher

Azure Security Center

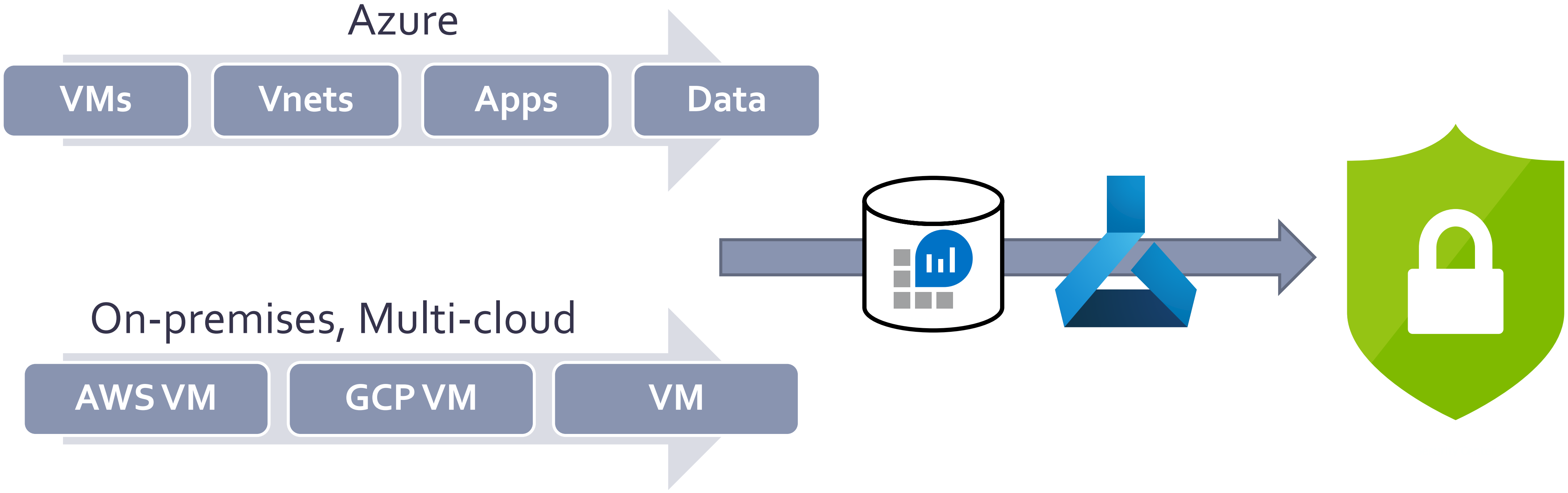
Azure Monitor

Azure Operations Management


Overview
Log Search
My Dashboard
Solutions Gallery
0.8GB
Servers and Usage
AD Assessment
2
Servers Assessed on Mon Apr 27 2015
6
High Priority Recommendations
3
Low Priority Recommendations
86
Passed Checks
Malware Assessment
30%
0
Servers with Active Threats
6
Servers with Inadequate Protection
Automation
10
Runbooks
52
Jobs run in last 7 days
Backup
25
Servers backed up 3/1/2015
3
Errors in the last backup
Alert Management
0
Active critical alerts in the last 24 hours
10
Active warning alerts in the last 24 hours
Change Tracking
89
Software changes in the last 24 hours
43
Windows service changes in the last 24 hours (excludes Status)
Security and Audit
17 ↗ 3
Active Computers in the last 24 hours
38 ↗ 15
Accounts Authenticated in the last 24 hours
Site Recovery
2
Failed jobs
1
Critical events

https://azure.microsoft.com/en-us/resources/videos/operations-management-suite-oms-overview/

Azure Security Center



Azure

VMs

Vnets

Apps

Data

On-premises, Multi-cloud

AWS VM

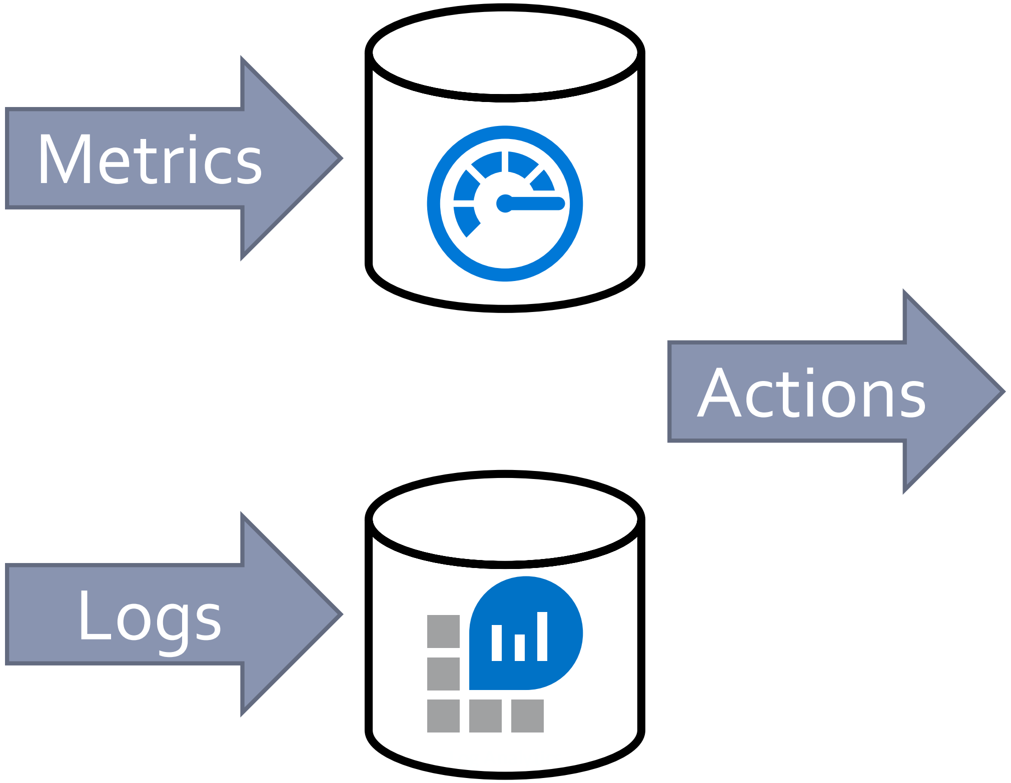
GCP VM

VM

Azure Monitor

Sources

- Applications
- Operating Systems
- Azure Resources
- Azure Subscription
- Azure Tenant
- Custom Sources



- Insights
- Visualize
- Analyze
- Respond
- Integrate

Network Watcher

Diagnostics

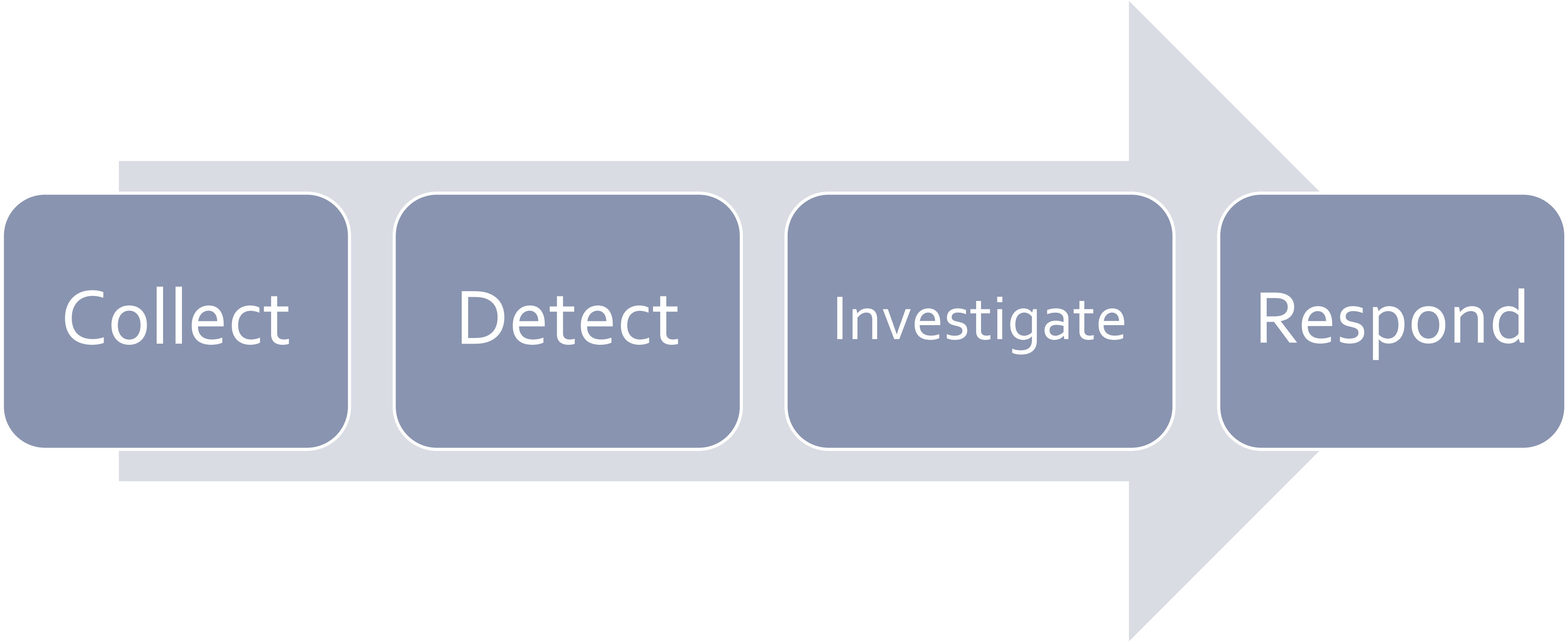
- Diagnose network traffic filtering problems to or from VMs
- Diagnose network routing problems from VMs
- Diagnose outbound connections from VMs
- Diagnose an Auzre Vnet gateway and connections

Network Watcher

Diagnostics

- Capture packets to and from VMs
- Determine latencies between Azure regions and ISVs
- View security rules for a network interface

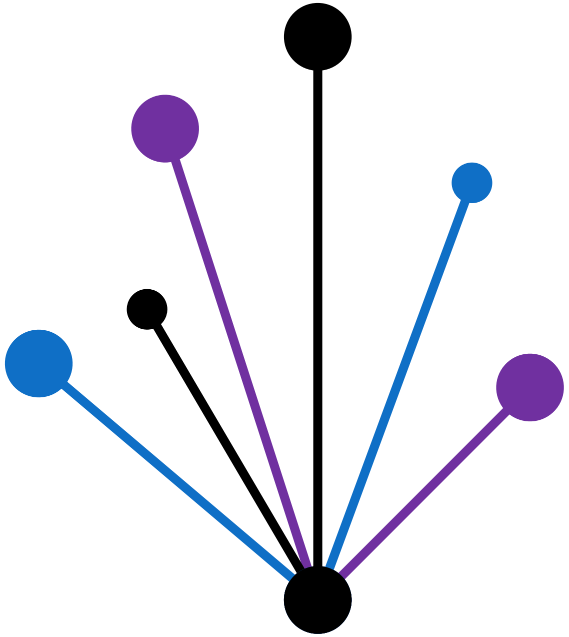
Security Information Event Management



Security Orchestration Automation Response

Azure Sentinel

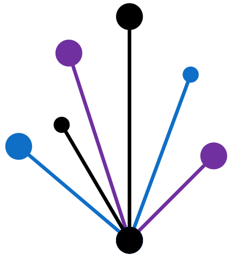
Collect data on all users, devices, applications, and infrastructure, both on-premises and multi-cloud.

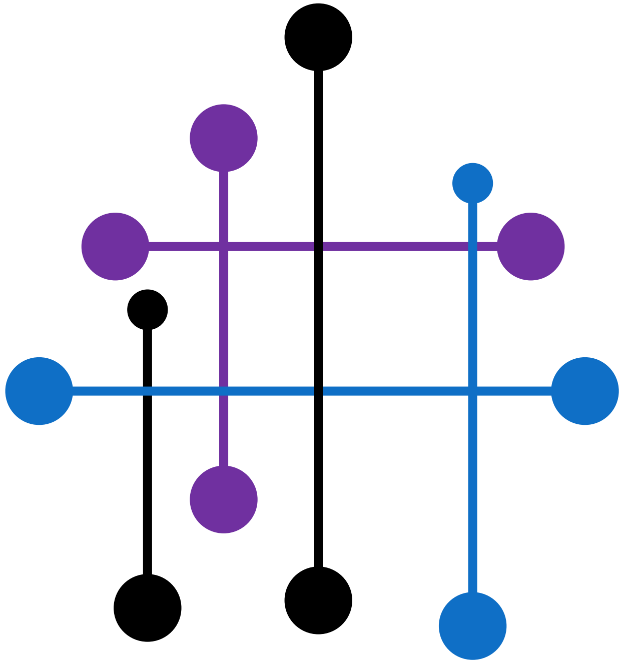


- Connect to security sources out of the box
- Non-Microsoft connectors included
- Standard event formats for REST-API

Azure Sentinel

Detect threats, and minimize false positives.

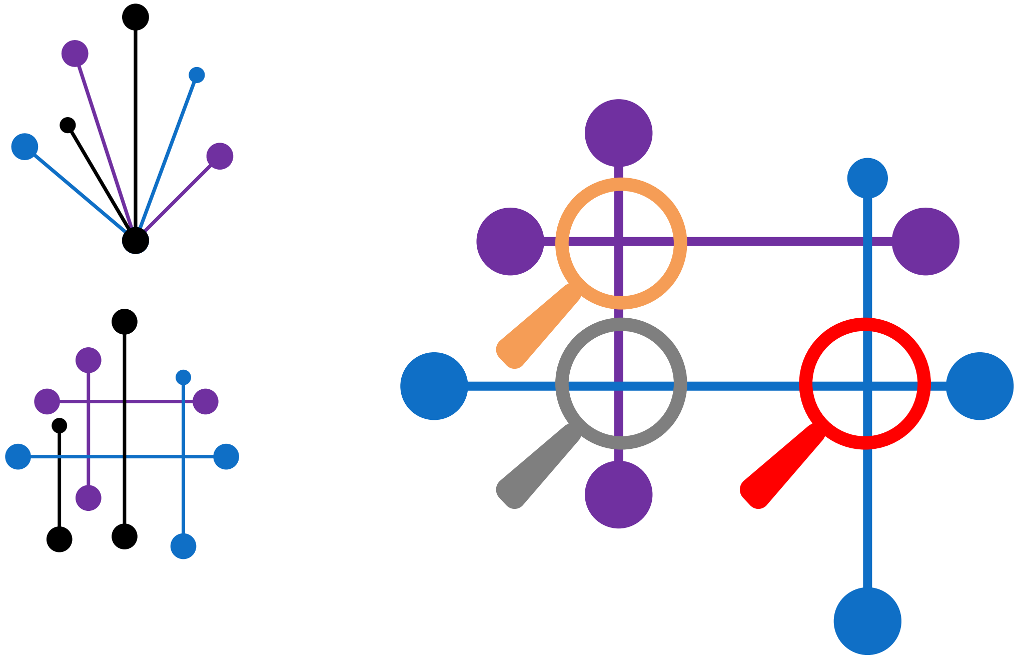




- Analytics to correlate alerts into incidents.
- Identifying incidents create an actionable possible-threat.

Azure Sentinel

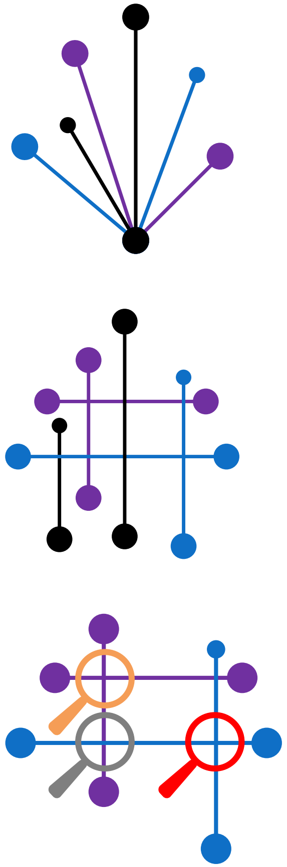
Hunt for suspicious activities across your systems.

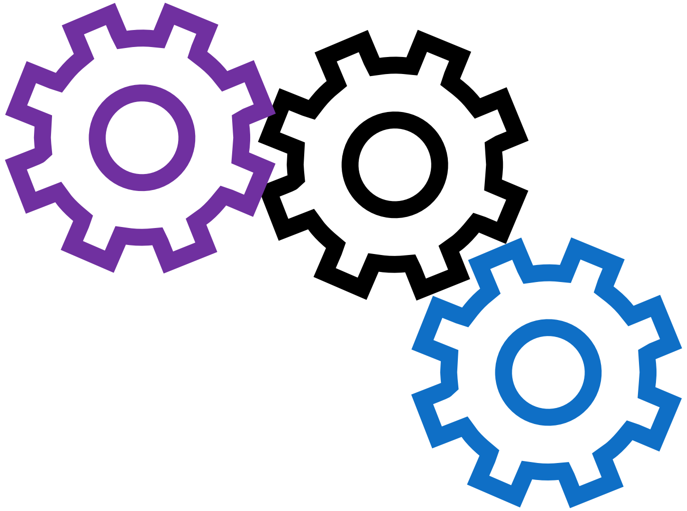


Reduce noise and hunt for security threats based on MITRE framework to proactivity discover attacks before an alert is triggered.

Azure Sentinel

Respond with built-in orchestration and automation of common tasks.

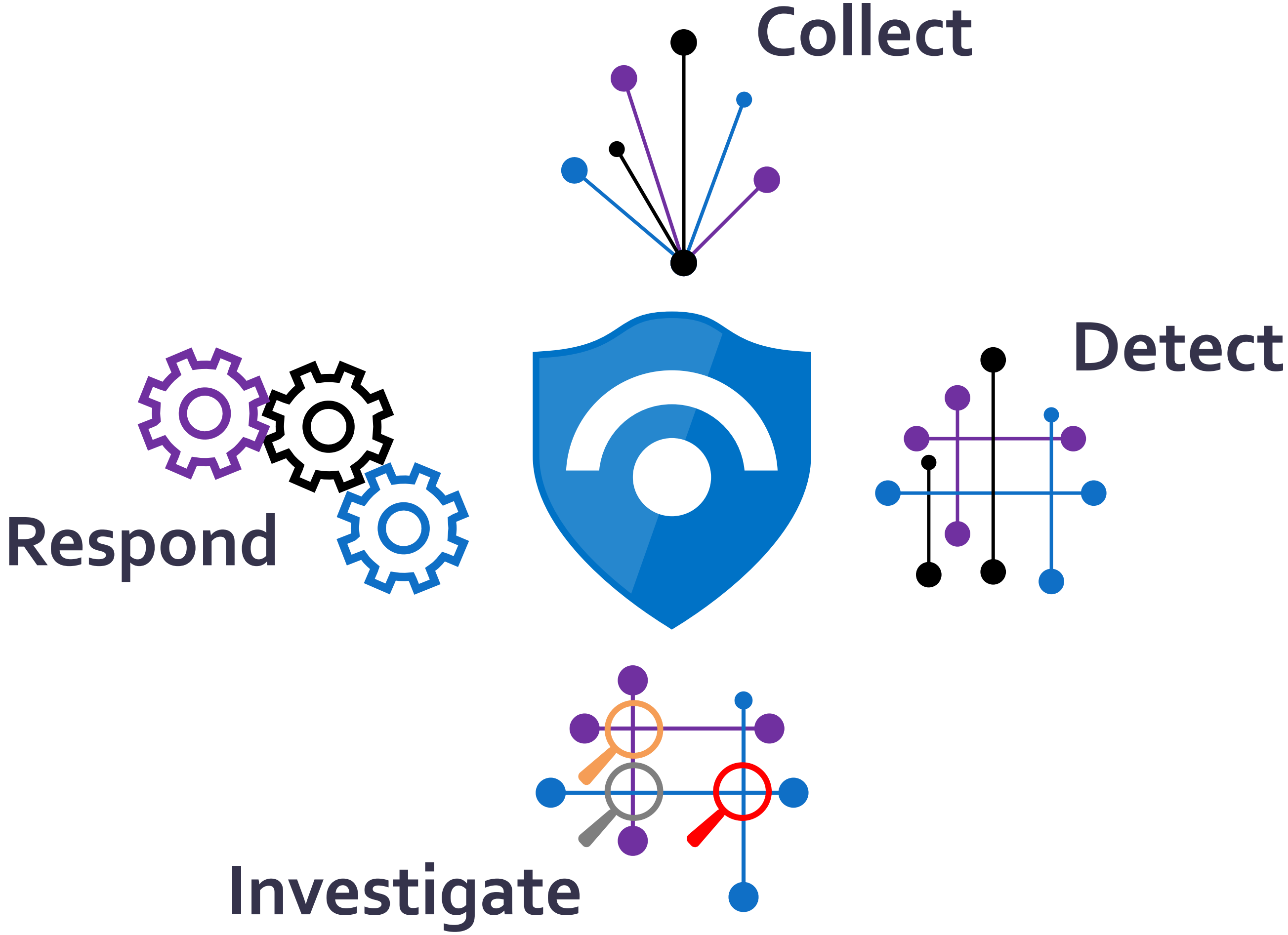




- Automate common tasks
- Create simplified security orchestration with playbooks.
- Create tickets in ServiceNow, Jira, etc. when an event occurs.

Azure Sentinel

Cloud-native SIEM + SOAR



Collect

Detect

Respond

Investigate