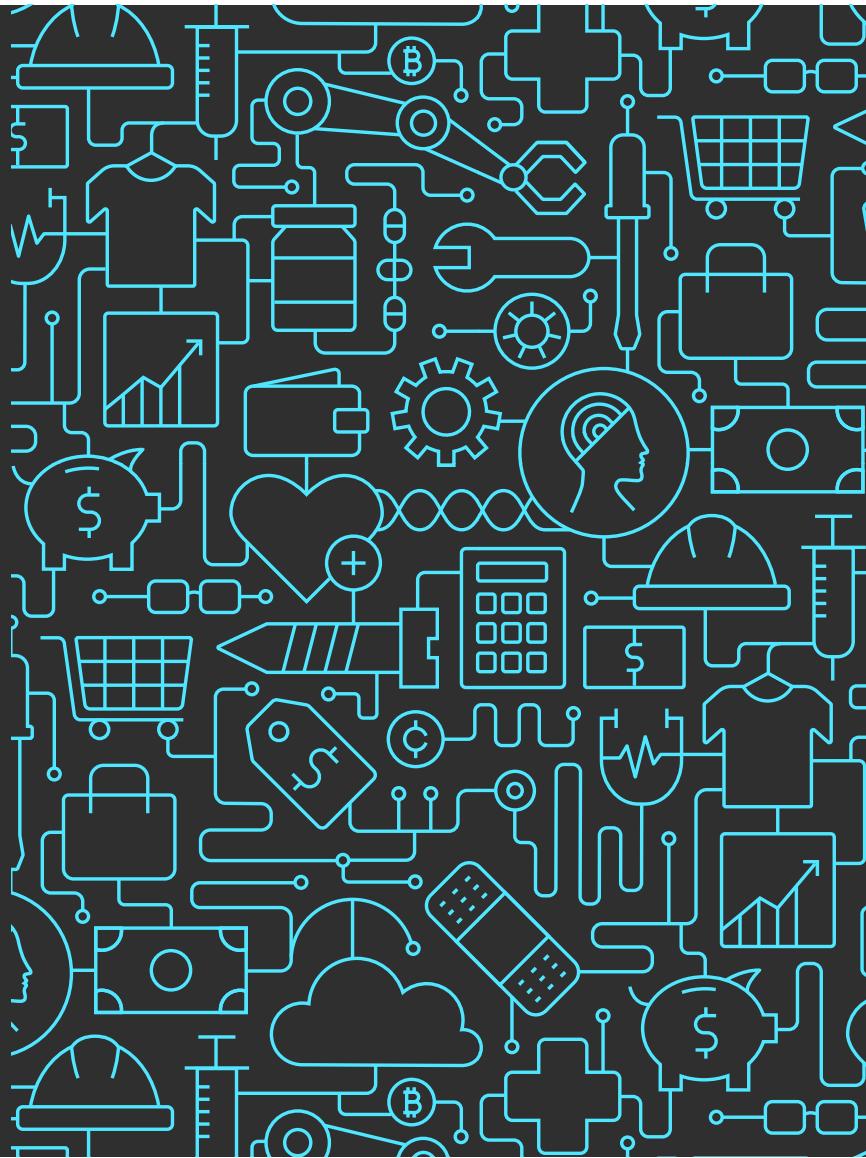




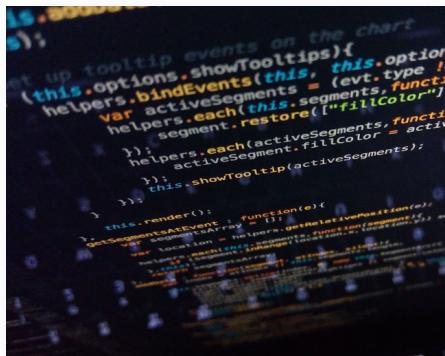
# Building Security into Azure

Ramesh Chinta  
Group PM, Azure security



# The era of flux and transformation

Everyone is now in  
the technology business



Conventional security  
tools have not kept pace



Security professionals  
alone can't fill the gap



Regulatory requirements  
and costs are increasing





# Endless complexity

## Zero Trust is a mindset

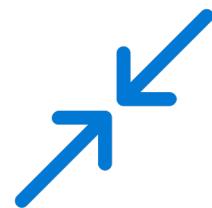
- Assumes pervasive risk
- Every access attempt as if it's originating from an untrusted network

[Zero Trust model](#)

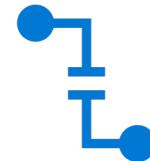
# Principles of Zero Trust



Verify explicitly



Use least privilege access



Assume breach

**PROTECT**

**DETECT**

**Security  
Intelligence**

**RESPOND**



# Intelligent security



## Identity and access management

Your universal platform to manage and secure identities



## Threat protection

Stop attacks with integrated and automated security



## Information protection

Protect your sensitive data—wherever it lives or travels



## Cloud security

Safeguard your cross-cloud resources

## Gain unmatched security with Azure

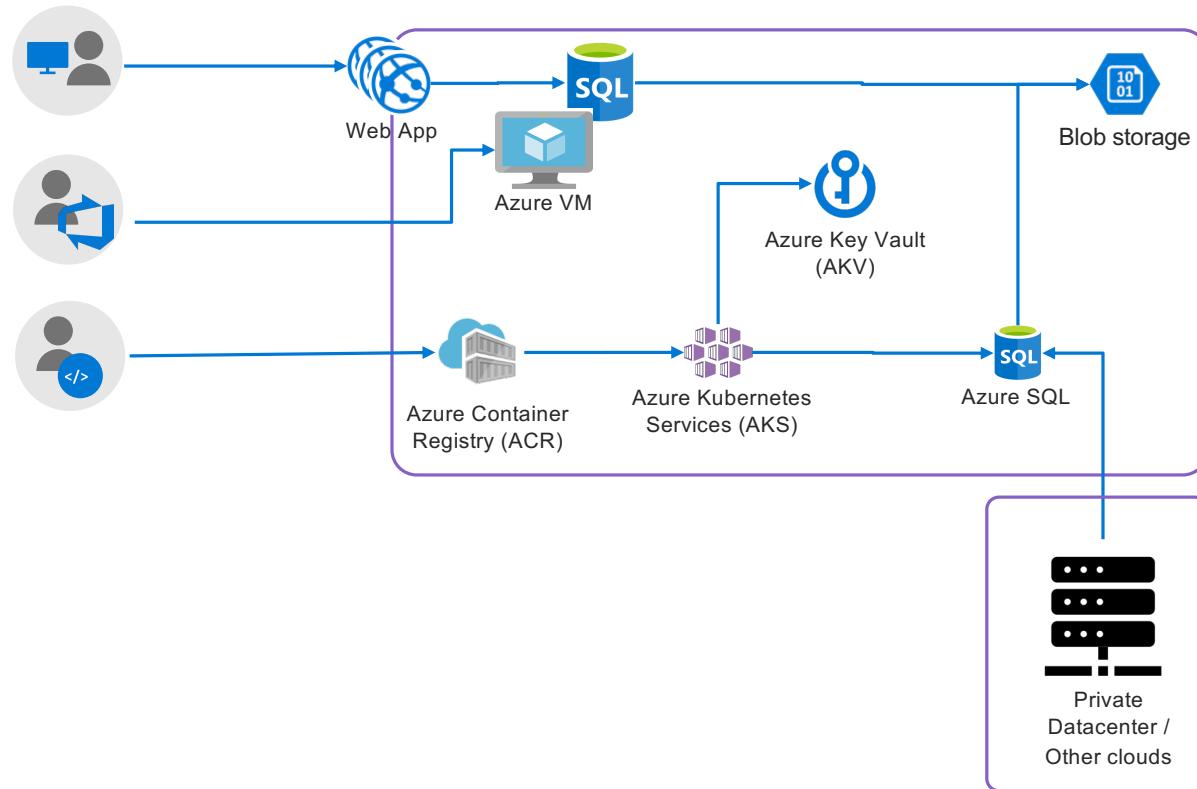
\$1B annual investment  
in cybersecurity

3500+ global security experts

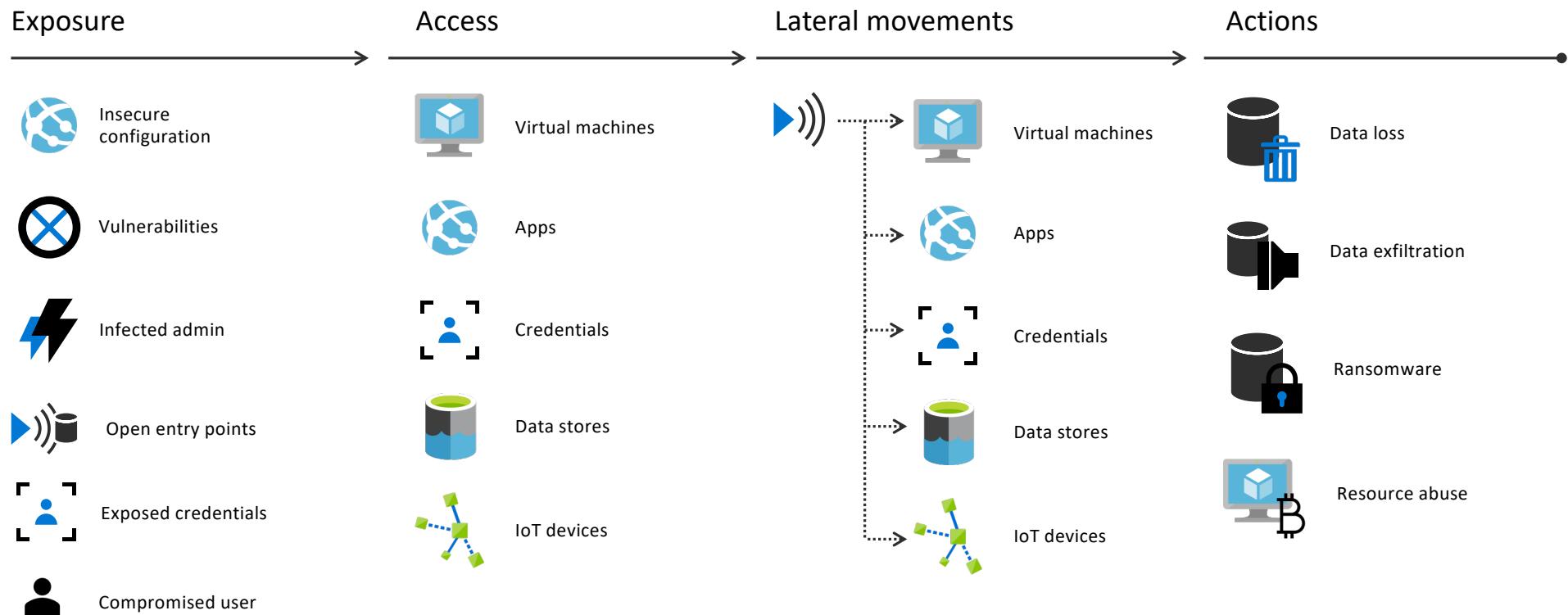
Trillions of diverse signals for  
unique intelligence



# Workloads become heterogenous and hybrid



# Threat actors leverage a variety of exposures to breach



# Common threats

## VMs

- Brute force of open management ports
- Exploit through an unpatched vulnerability
- Run bitcoin mining on a compromised VM

## Containers

- Exposed Kubernetes dashboards
- RBAC not configured in the cluster
- Insecure container/host configuration

## App services

- Web shell deployment
- server-side request forgery (SSRF)
- Reconnaissance attempts

## SQL Database

- SQL injection vulnerabilities and attacks
- Access by a remote threat actor
- Brute-force against SQL credentials

## Storage account

- Use to propagate malware or load malicious images/packages
- Access by a remote threat actor
- Public access to storage accounts
- Harvest for reconnaissance or exfiltration of data

## Key Vault

- Permissive policies grant access to unneeded resources
- Harvest for secrets

# Azure security center



Strengthen security posture

Cloud security posture management

Secure Score and Policies & compliance



Protect against threats

servers

cloud native

Data & Storage

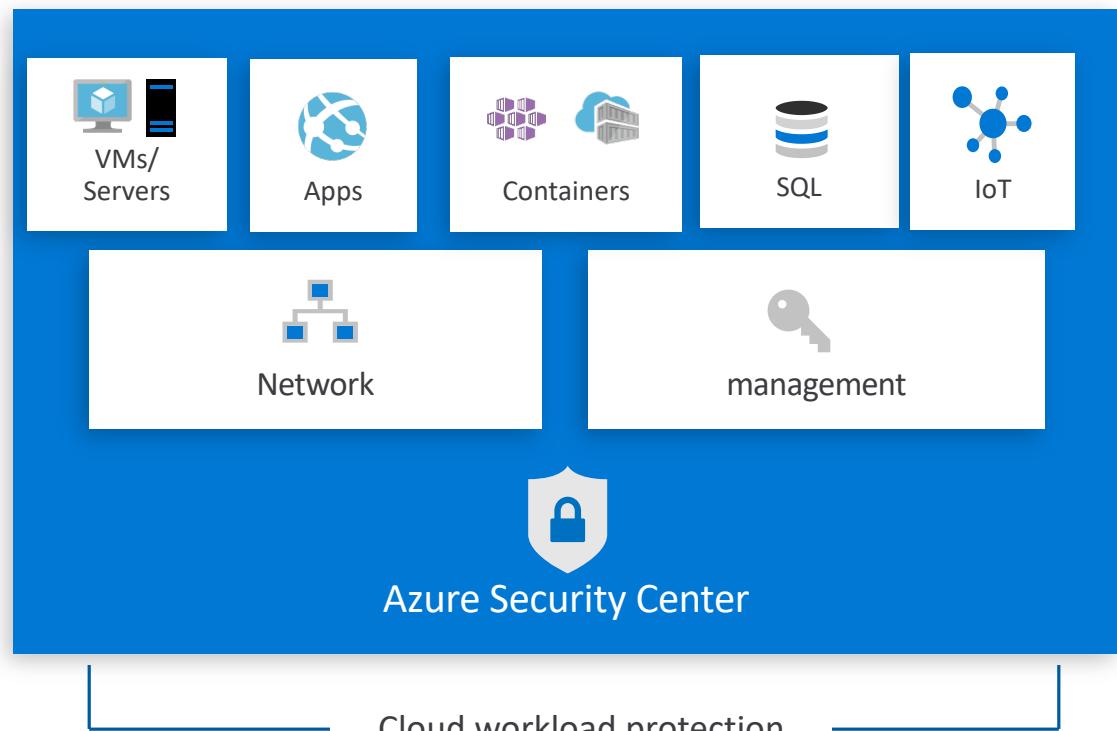


Get secure faster

## Protect your workloads from threats

Use industry's most extensive threat intelligence to gain deep insights

- Detect & block advanced malware and threats for Linux and Windows Servers on any cloud
- Protect cloud-native services from threats
- Protect data services against malicious attacks
- Protect your Azure IoT solutions with near real time monitoring
- Service layer detections: Azure network layer and Azure management layer (ARM)



Microsoft Azure (Preview) Report a bug Search resources, services, and docs (G+) yinon@microsoft.com MICROSOFT

Home > Security Center - Pricing & settings > Settings - Pricing tier

### Settings - Pricing tier ASC DEMO

Save

The Standard tier provides enhanced security. Learn more >

Free (for Azure resources only)	Standard
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Azure Secure Score	✓ Azure Secure Score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Pricing will apply to: 126 resources in this subscription

Select pricing tier by resource type

Resource Type	Resource Quantity	Pricing	Plan
Virtual machines	45 VMs and VMSS instances	\$15/Server/Month	Enabled Disabled
App Service	5 instances	\$15/Instance/Month	Enabled Disabled
PaaS SQL servers	6 resources	\$15/Server/Month	Enabled Disabled

By clicking Save, the standard tier will be enabled on selected resource types. The first 30 days are free. Virtual machines, SQL servers, App Service instances and Kubernetes Service instances are billed hourly, only for running resources. For more information on Security Center pricing, visit the [pricing page](#).

2018

2019

Get secure fast, just turn it ON

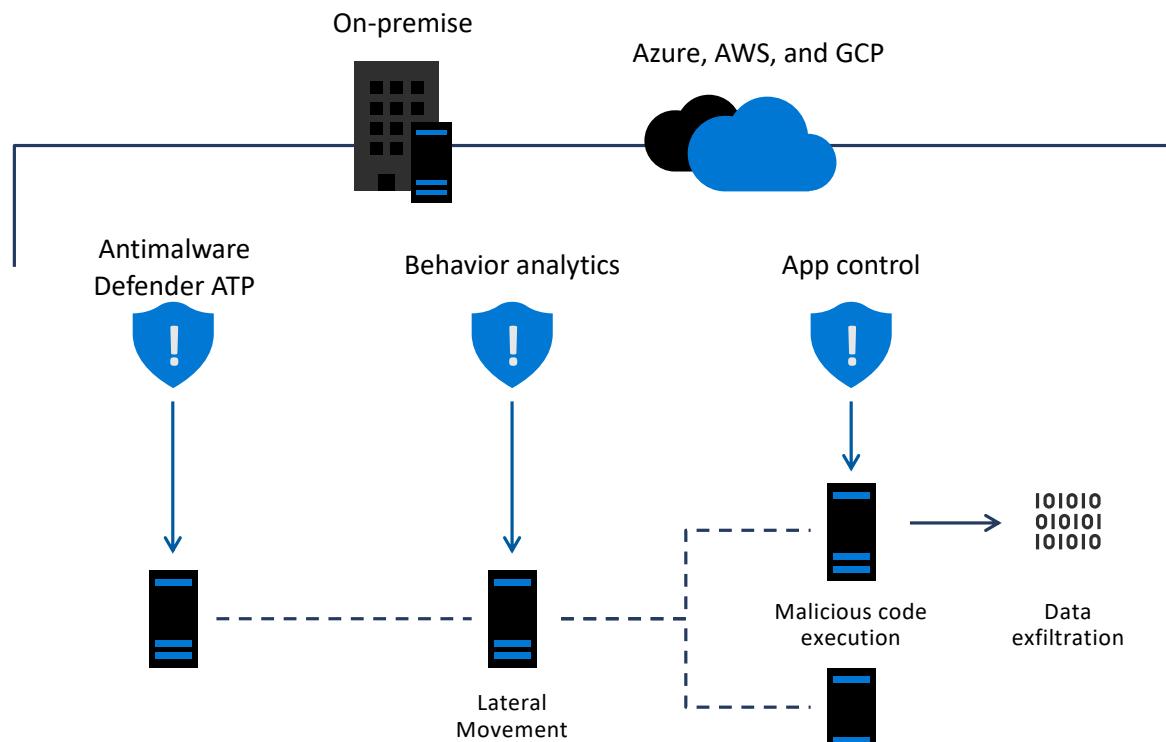
# Protect Linux and Windows VMs from threats

## Reduce open network ports:

- Use Just-in-Time to avoid exposure of management ports
- Limit open ports with adaptive network hardening

## Protect against malware:

- Block malware with adaptive application controls
- Built-in Microsoft Defender ATP EDR
- Crash dump analysis and fileless attack detections



NEW

## Announcing built-in vulnerability assessment for VMs

Available as part of *standard* ASC for VM pricing, no extra charge

- Automated deployment of vulnerability scanner
- Continuously scans installed applications to find vulnerabilities
- Visibility to the vulnerability findings in Security Center portal and APIs

Remediate vulnerabilities found on your virtual machines (powered by Qualys) (Preview)

- Data spillage
- Account breach
- Elevation of privilege

Remediation steps

Manual remediation

Review and remediate vulnerability findings that were discovered by the built-in vulnerability assessment solution of Azure Security Center (powered by Qualys).

Affected resources

Security Checks

Findings

Search to filter items...

ID	Security Check	Category	Applies To	Sev
91426	Microsoft Windows Security Update for Windows Server (A... Windows		1 of 1 resources	▲
91445	Microsoft WinHTTP support for TLS 1.1 and TLS 1.2 Missin...	Windows	1 of 1 resources	▲
100269	Microsoft Internet Explorer Cumulative Security Update (M...	Internet Explorer	1 of 1 resources	▲
100319	Microsoft Internet Explorer Security Update for September ... Internet Explorer		1 of 1 resources	▲
91462	Microsoft Windows Security Update Registry Key Configur...	Windows	1 of 1 resources	▲
90954	Windows Update For Credentials Protection and Managemen...	Windows	1 of 1 resources	▲
105256	IPSEC Policy Agent Service Status Detected	Security Policy	1 of 1 resources	●
90065	Windows Services List	Windows	1 of 1 resources	●
105190	Microsoft Windows File Security Check - C System Files	Security Policy	1 of 1 resources	●
45063	NTFS Settings: Enumerated	Information gathering	1 of 1 resources	●

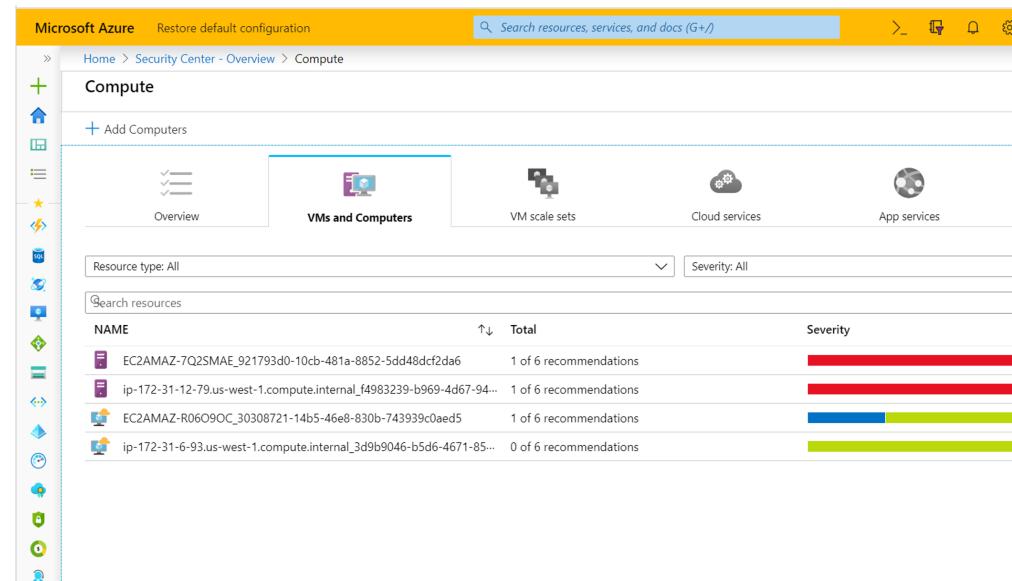
# Protect hybrid datacenters and multi-cloud with Azure security center



 Hybrid Server protection for Datacenters and other clouds

Onboard on-prem servers to Security Center from Windows Admin Center

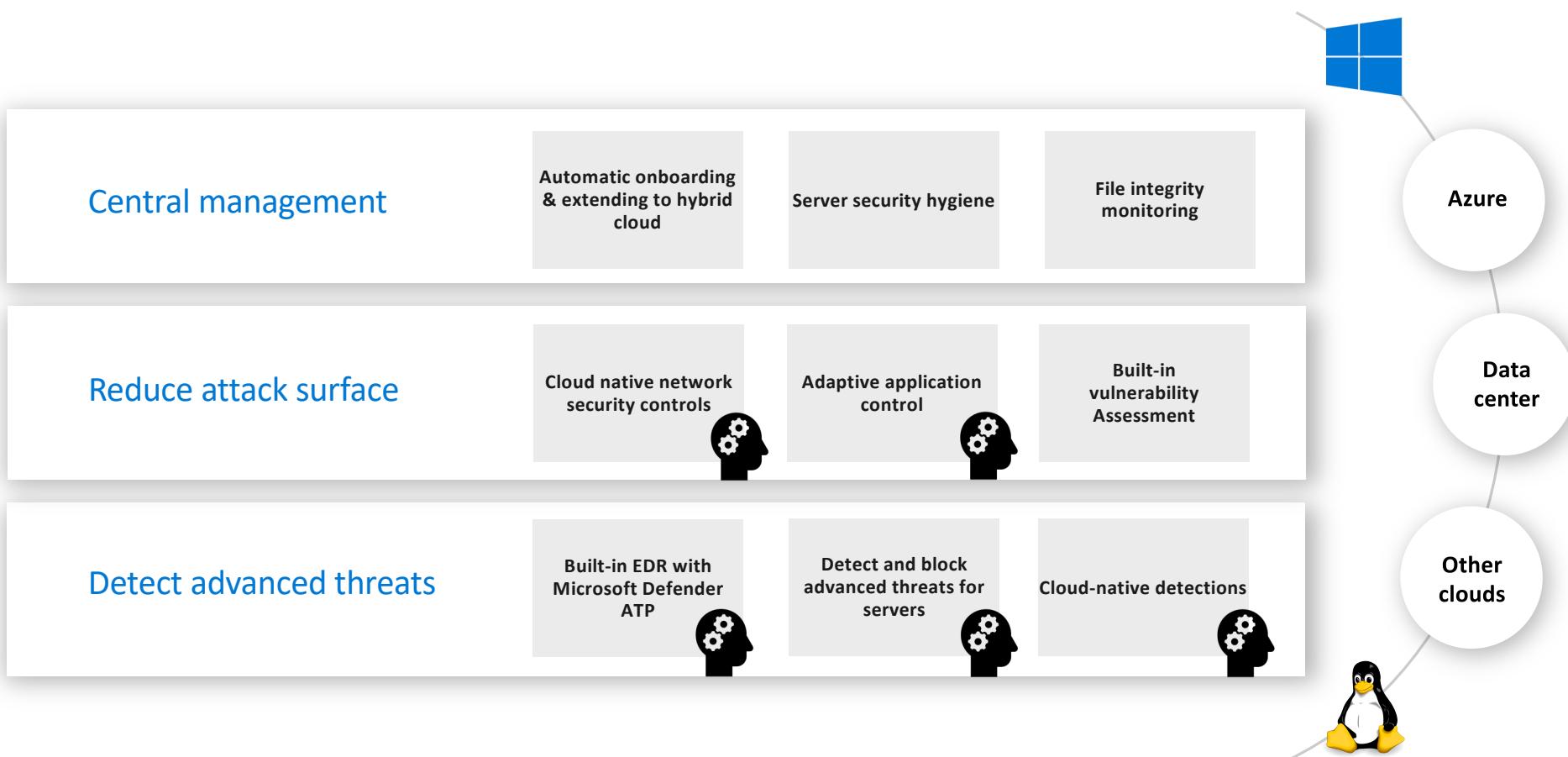
 Auto-onboard AWS EC2 instances using a new API connector (preview)



The screenshot shows the Microsoft Azure Security Center interface for the Compute blade. The top navigation bar includes 'Microsoft Azure' and 'Restore default configuration'. Below it, the breadcrumb path is 'Home > Security Center - Overview > Compute'. A search bar at the top right says 'Search resources, services, and docs (G+/-)'. On the left, there's a sidebar with icons for '+ Add Computers', 'Overview', 'VMs and Computers' (which is selected), 'VM scale sets', 'Cloud services', and 'App services'. The main area has tabs for 'Resource type: All' and 'Severity: All'. A search bar labeled '@search resources' is present. Below is a table of recommendations:

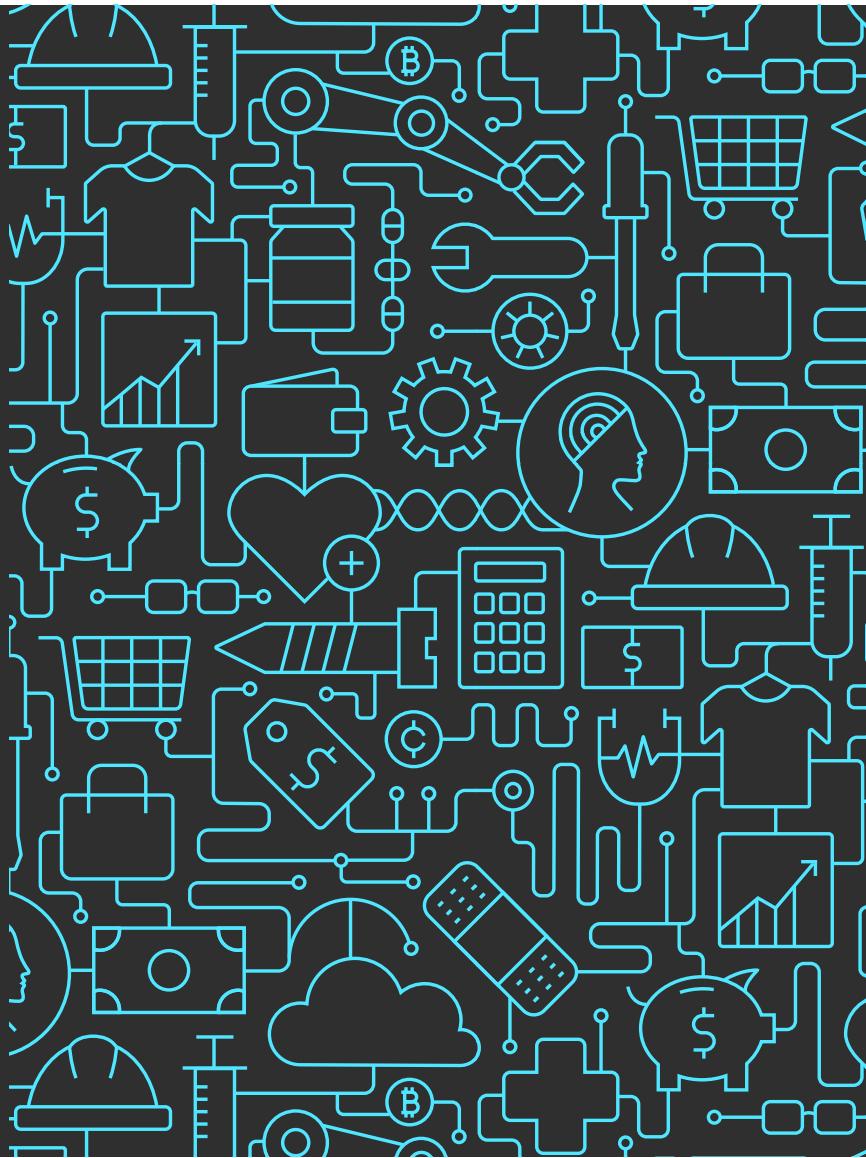
NAME	Total	Severity
EC2AMAZ-7Q2SMAE_921793d0-10cb-481a-8852-5dd48dcf2da6	1 of 6 recommendations	Red
ip-172-31-12-79.us-west-1.compute.internal_f4983239-b969-4d67-94...	1 of 6 recommendations	Red
EC2AMAZ-R0609OC_30308721-14b5-46e8-830b-743939c0aed5	1 of 6 recommendations	Blue
ip-172-31-6-93.us-west-1.compute.internal_3d9b9046-b5d6-4671-85...	0 of 6 recommendations	Green

# Cloud workload protection for hybrid VMs and servers



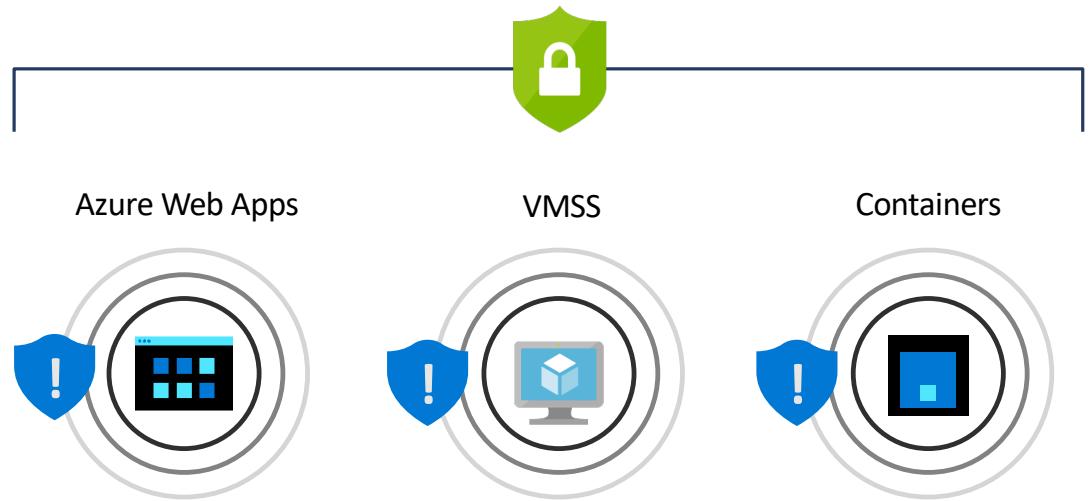


## Server & VM threat protection with Azure Security Center



## Protect cloud-native workloads from threats

- Detect and alert on abnormal admin behavior or compromised web applications
- Protects VMSS and containers from malicious attacks
- CIS benchmark for Dockers on Linux IaaS & vulnerability scanning on ACR images



>75% of global organizations will be [running containerized applications](#) in production by 2022 (Gartner)

**NEW**

## Built-in vulnerability assessment for container images

Public preview available in *standard* ASC with a new container registries add-on

- Seamless deployment and configuration of the vulnerability scanner
- Scan container images for vulnerabilities upon push to an ACR
- Visibility to vulnerable ACR container images including vulnerabilities details, severity classification and guidance to remediation

The screenshot displays the Microsoft Azure Security Center interface, specifically the 'Recommendations' section. The main header reads 'Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) - (Preview)'. Below this, key statistics are shown: 1 Unhealthy registry, Severity High, Total vulnerabilities 10 (with 1 critical), Vulnerabilities by severity (High 1, Medium 9, Low 0), Registries with most vulnerabilities (imagescanprivatepreview 10), and Total vulnerable images 2 (Out of 3).

The interface is divided into several sections:

- General Information:** Includes recommendation score (0/30), impact (+30), user impact (Low), and implementation effort (Moderate).
- Threats:** Lists Data exfiltration, Data spillage, Account breach, and Elevation of privilege.
- Remediation steps:** Provides instructions for manual remediation, including steps to resolve container image vulnerabilities.
- Affected resources:** Shows 1 Unhealthy resource (imagescanprivatepreview) and 0 Healthy resources.
- Security Checks:** Displays findings for two security checks: 176750 (Debian Security Update for apache2 (DSA 4422-1)) and 177008 (Debian Security Update for openssl (DSA 4475-1)).
- Description:** Details the Debian security update for apache2 (DSA 4422-1), stating it has released a security update for apache2 to fix the vulnerabilities.
- General information:** Lists the ID (176750), Severity (High), Type (Vulnerability), Published (4/4/2019, 1:52 PM GMT+3), Patchable (Yes), and CVEs (CVE-2018-7189, CVE-2018-7199, CVE-2019-0196, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220).
- Remediation:** Provides links to the Debian security advisory (DSA 4422-1) and download patches for the vulnerabilities.
- Additional information:** References the vendor reference (DSA 4422-1).
- Effected resources:** Lists the affected resource (imagescanprivatepreview) and its subscription information.

**NEW**

# Cloud workload protection for containers

Now available in standard Azure security center with the new container service add-on

The screenshot shows the Azure Security Center interface for Compute & apps. On the left, a navigation pane includes links for Overview, Getting started, Pricing & settings, POLICY & COMPLIANCE (Coverage, Secure score, Security policy, Regulatory compliance), RESOURCE SECURITY HYGIENE (Recommendations, Compute & apps, Networking), ADVANCED CLOUD DEFENSE (Secure score, Security policy, Regulatory compliance), and THREAT PROTECTION (Security alerts, Custom alert rules (Preview), Security alerts map (Preview)).

The main area displays a list of recommendations for various resources:

NAME	Total	Severity
asc-private-preview	2 of 5 recommendations	Red
asc-preview	3 of 5 recommendations	Red
asc-private-preview-rbac	3 of 5 recommendations	Red
image scan private preview	2 of 2 recommendations	Red
ascdockerccontainer	1 of 1 recommendations	Red

Below the recommendations is a bar chart showing the distribution of severity levels:

Severity	Count
High severity	18
Medium severity	38
Low severity	47

At the bottom, a table lists detected threats:

DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	START	END	SEVERITY
PREVIEW - Role binding to the cluster-admin role detected	1	Microsoft	Azure	08/28/19	Active		Low
PREVIEW - Privileged container detected	1	Microsoft	Azure	08/28/19	Active		Low
PREVIEW - New high privileges role detected	1	Microsoft	Azure	08/28/19	Active		Low
PREVIEW - New container in the kube-system namespace detected	1	Microsoft	Azure	08/28/19	Active		Low
Detected suspicious network activity	2	Microsoft	Azure	09/19/19	Active		Low
Detected suspicious network activity	2	Microsoft	Azure	09/17/19	Active		Low
Detected suspicious network activity	3	Microsoft	Azure	09/11/19	Active		Low

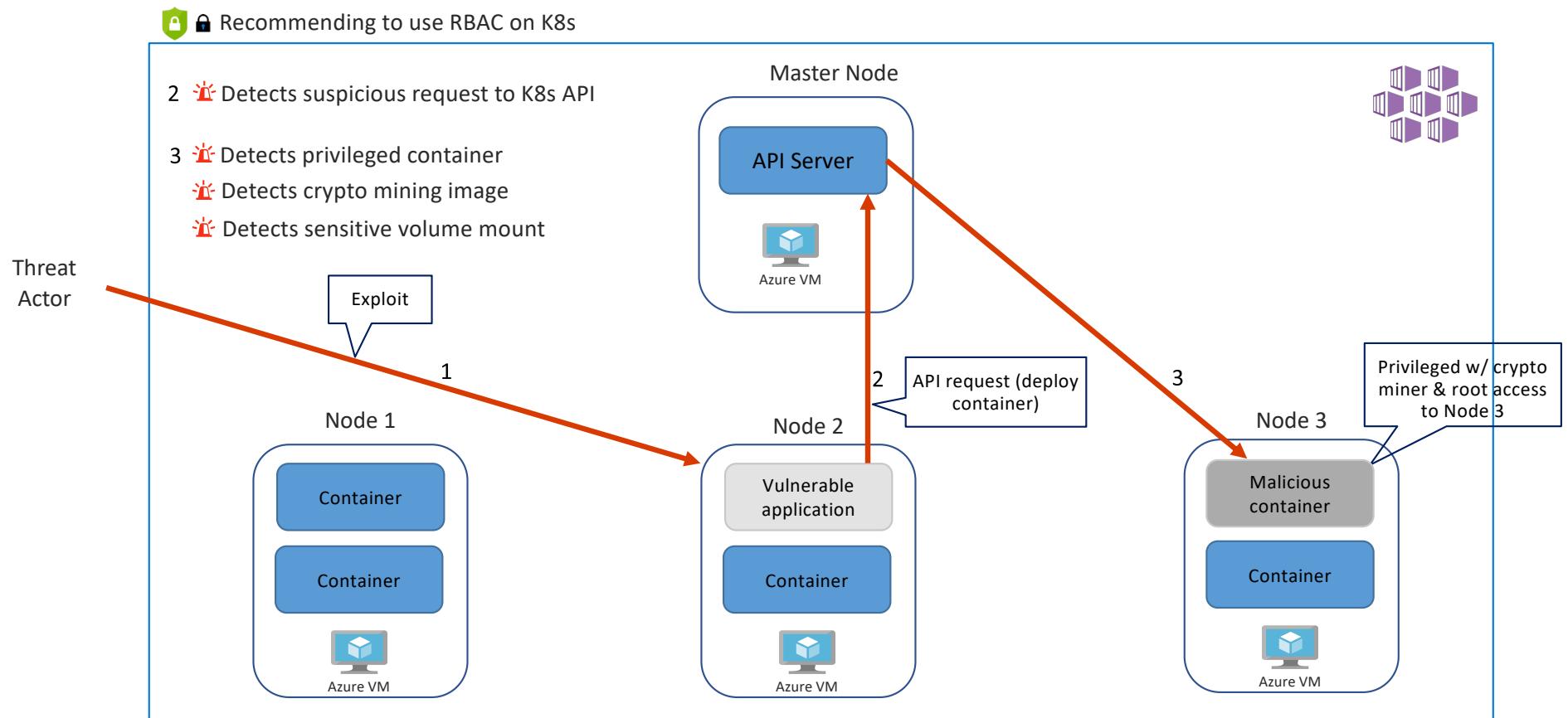
## Protecting Container hosts (IaaS)

- CIS Docker Benchmark assessment
- Node Threat Protection

## Protecting AKS

- Actionable recommendations based on AKS best practices
- Cluster and Node Threat detection based on AKS audit log and Node Auditd

# Protecting against advanced cloud threats



## Protect data services from threats

- Prevent & detect threats targeting your Azure SQL databases, MySQL, PostgreSQL
- Discover and remediate security misconfigurations in Azure SQL databases
- Storage account protection to detect threats and misuse
- Discover, classify, label and protect sensitive data in your Azure SQL databases



NEW

## New advanced protection capabilities for data services

Now in preview



### [Protect SQL servers on Azure VMs](#)

Vulnerability assessment and Advanced Threat Protection to prevent and detect threats across SQL estate in Azure



### [Malware reputation screening for Azure Storage](#)

Detect advanced threats in Azure Storage with hash reputation analysis upon upload



### [Advanced Threat Protection for Azure Key Vault](#)

Detect unusual and potentially harmful attempts to exploit Azure Key Vault

## Detections of the common cloud threats

### SQL Database detections

Now available for SQL on IaaS

- SQL injection vulnerabilities and attacks
- Access anomalies by location, principal, or application
- Brute-force against SQL credentials
- And more...

### Storage account detections

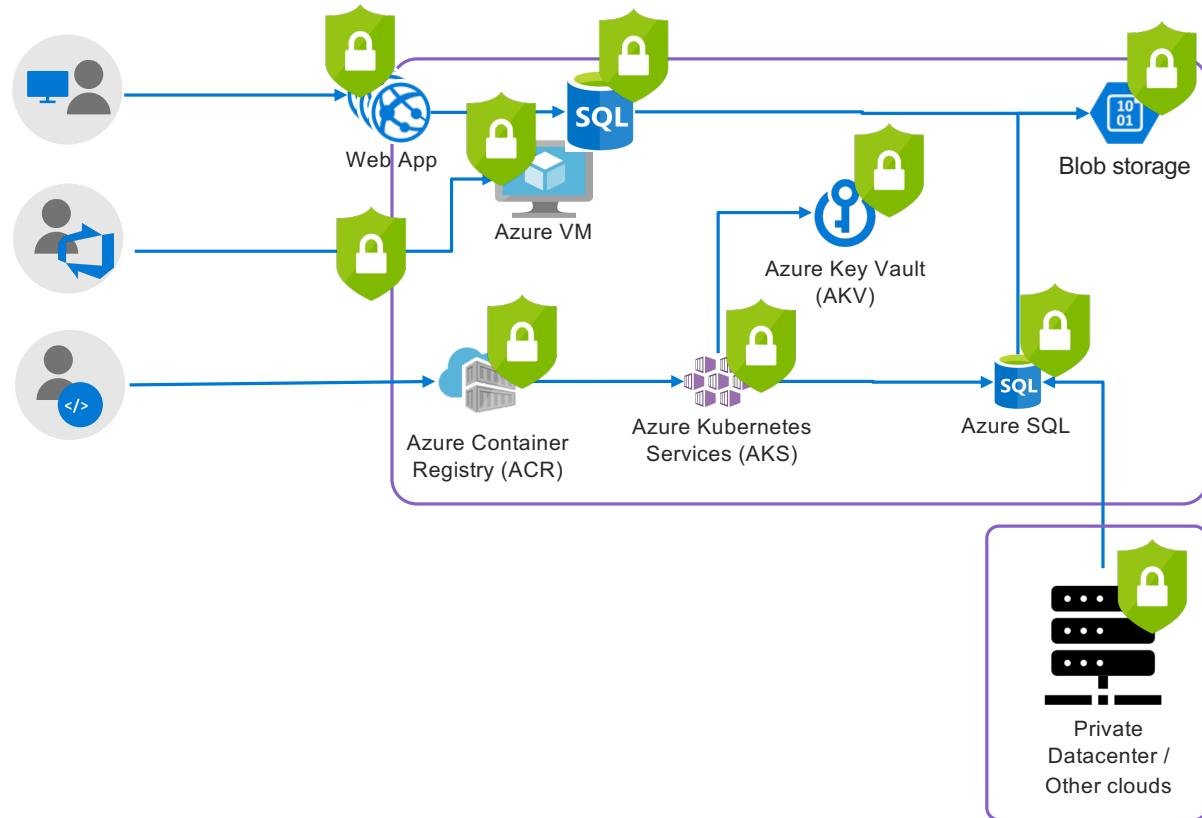
- Malware reputation screening or suspicious files (.cspkg)
- Access anomalies by location, principal, or application
- Permission change anomalies, anonymous access detection
- And more...

### Key vault detections

Now available in NA regions

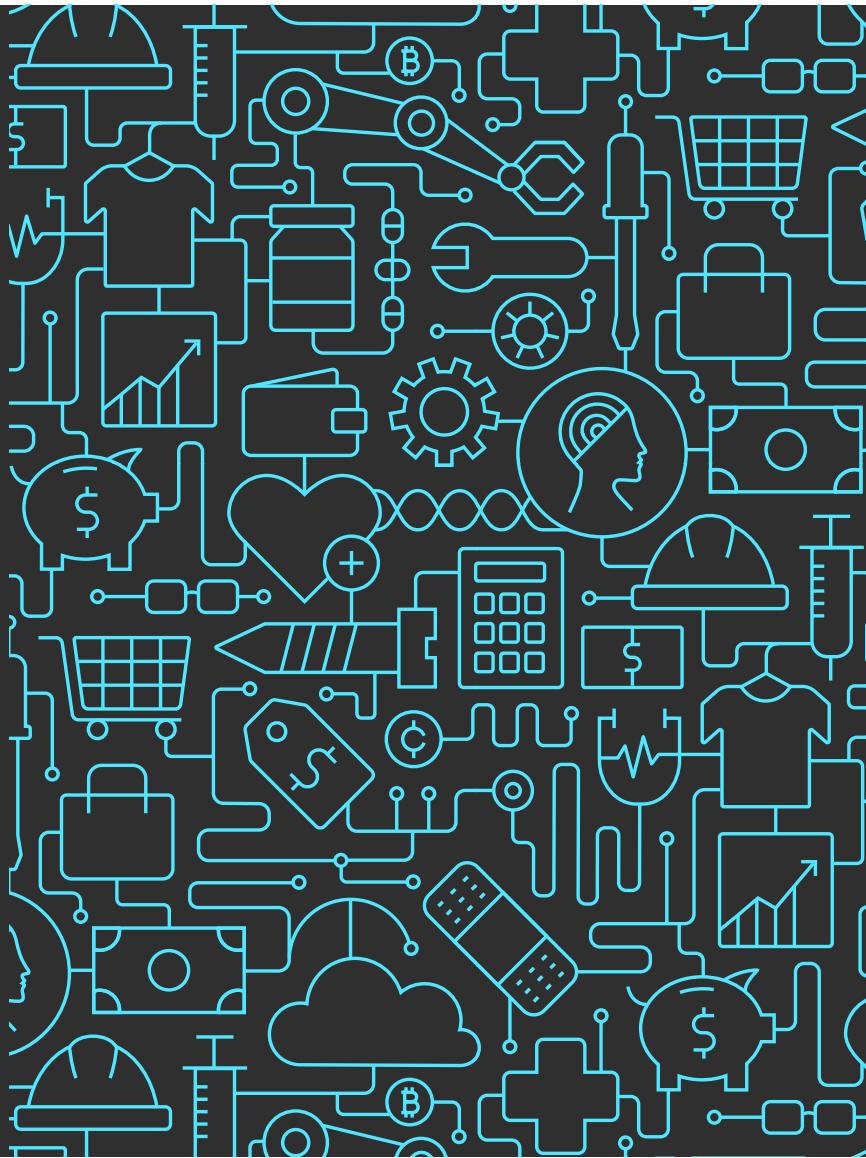
- Access from a suspicious location, Tor network
- Unusual policy change or listing and secret get
- Unusual volume or pattern of Key Vault operations
- And more...

## Example solution architecture on Azure



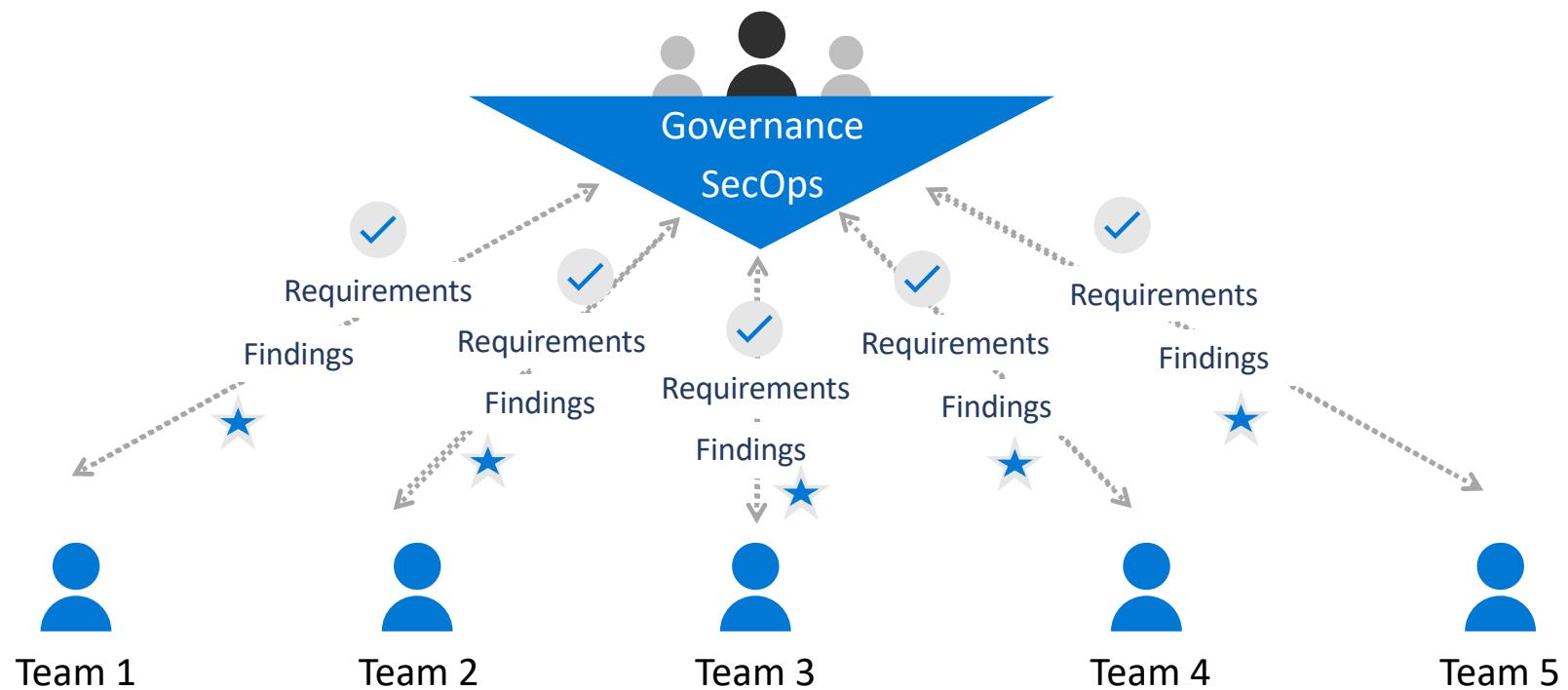


## Azure security center enterprise integrations

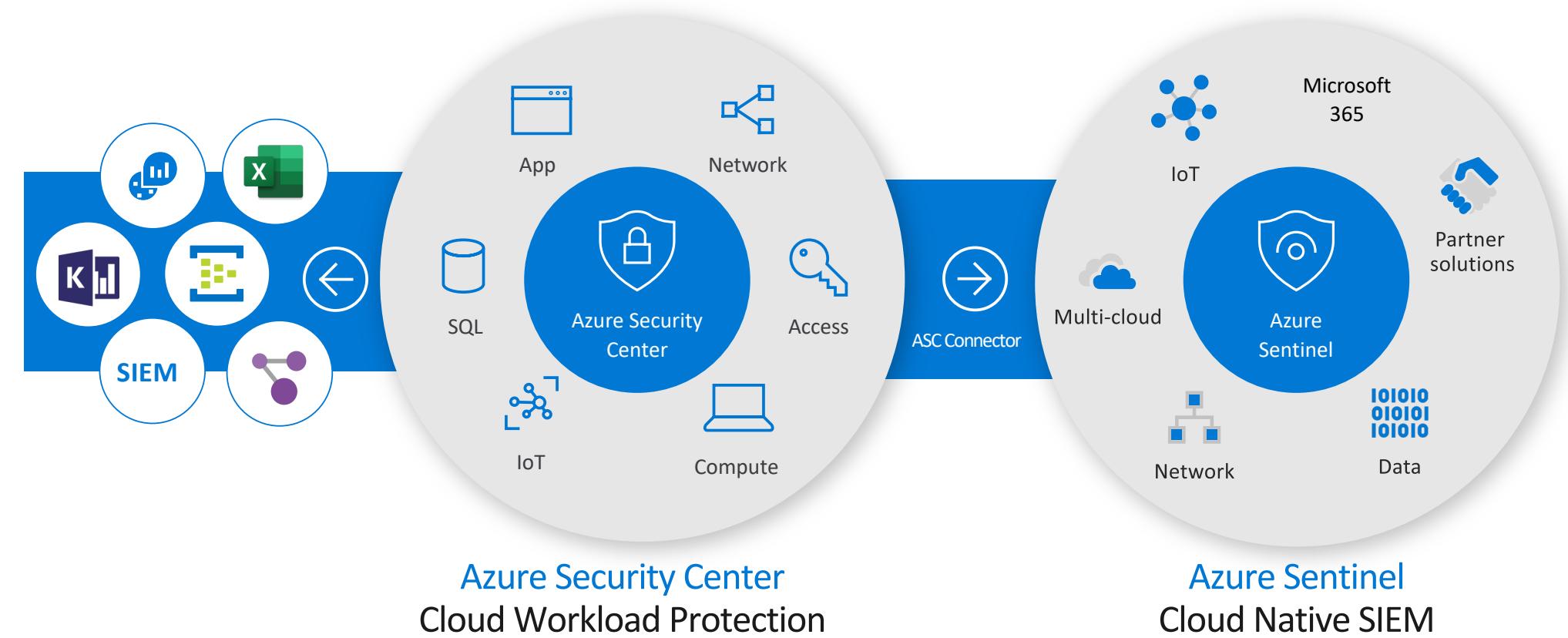


# Driving threat protection through the organization

Through a central SecOps & cloud governance role



Threat protection for cloud at scale:  
Export assessments and alerts for security roles

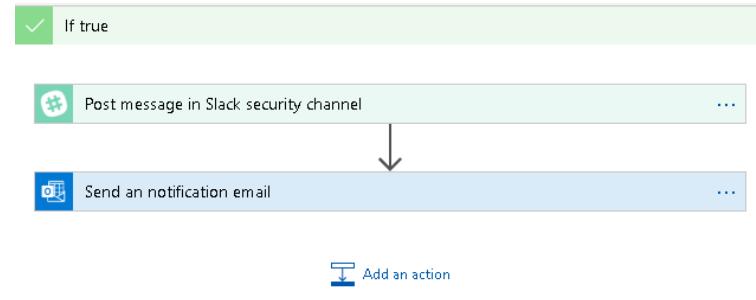


# Automate workflows with ASC



## Automate workflows with ASC

- Trigger playbooks based on ASC recommendations and alerts
- Built-in playbooks, build your own with Azure Logic apps



## New community hub

- Share workflows and remediation policies with the community the things that you've built
- Learn what others did and deploy directly to Azure

A screenshot of the Azure Security Center Community page. The left sidebar shows a navigation menu with categories like Overview, Pricing &amp; settings, Policies &amp; compliance, Security policy, Adaptive compliance, Resource security request, Recommendations, Compute &amp; apps, Networking, IoT hubs &amp; resources, Data &amp; storage, Identity &amp; access, and Security solutions. The main content area has a heading "Azure Security Center community". It includes sections for "What is it?", "How does it work?", and "These are the types of content you can find in the community". Under "Remediation templates", it says "Across the template deployment scripts Security Center uses as part of its recommendation remediation platform and try out new remediation templates before they are integrated into the product.". Under "Custom security recommendation", it says "Create your own security recommendations with custom logic, by creating custom policy in Azure Policy and onboard it into Azure Security Center. Contribute and use custom recommendations shared in the community.". Under "Programmatic tools", it says "Automate and configure Security Center with Programmable scripts shared by the community in PowerShell, C# and other languages. Use custom Policy definitions to manage Security Center at scale.". Under "Playbook templates", it says "Explore the ecosystem of Azure Logic Apps connectors to customize automation in Security Center. Import playbooks from the community to use them as customized automations.". There are also sections for "Community blog", "Forum", and "Private previews".

## Automate and script through API and PowerShell

# Protect your workloads against threats: a go-do list

01

---

**Good hygiene comes first,**  
strengthen your cloud  
security posture

02

---

**Turn on threat protection** for all  
cloud resources

03

---

**Reduce attack surface** for VMs  
with JIT, Network and app controls

04

---

**Integrate alerts into your**  
SIEM & notify app owners

05

---

**Identify root cause** and  
drive new security hygiene  
up

# Azure security center announcements

Enhanced threat protection for your cloud resources with security center

Support for threat protection & vulnerability assessment for **SQL DBs running on Azure IaaS VM**

**Built-in vulnerability assessment** with Security Center Standard

**Container security** for Azure Kubernetes Services with Azure Security Center

**Threat Protection for Azure key vault** in Public Preview in North America Regions

**Malware reputation screening** as part of ATP for Azure Storage

Extending Security Center's coverage with platform for community & partners



Enhanced cloud security posture management

**Secure score simplified**

Support for **customer created assessments**

**Quick remediation** for bulk resources

**Automatic assessment** of NIST SP 800-53 R4, SWIFT CSP CSCF v2020, Canada Federal PBMM and UK Official together with UK NHS

**Implement security faster with Security Center**

**Workflow automation** with logic apps

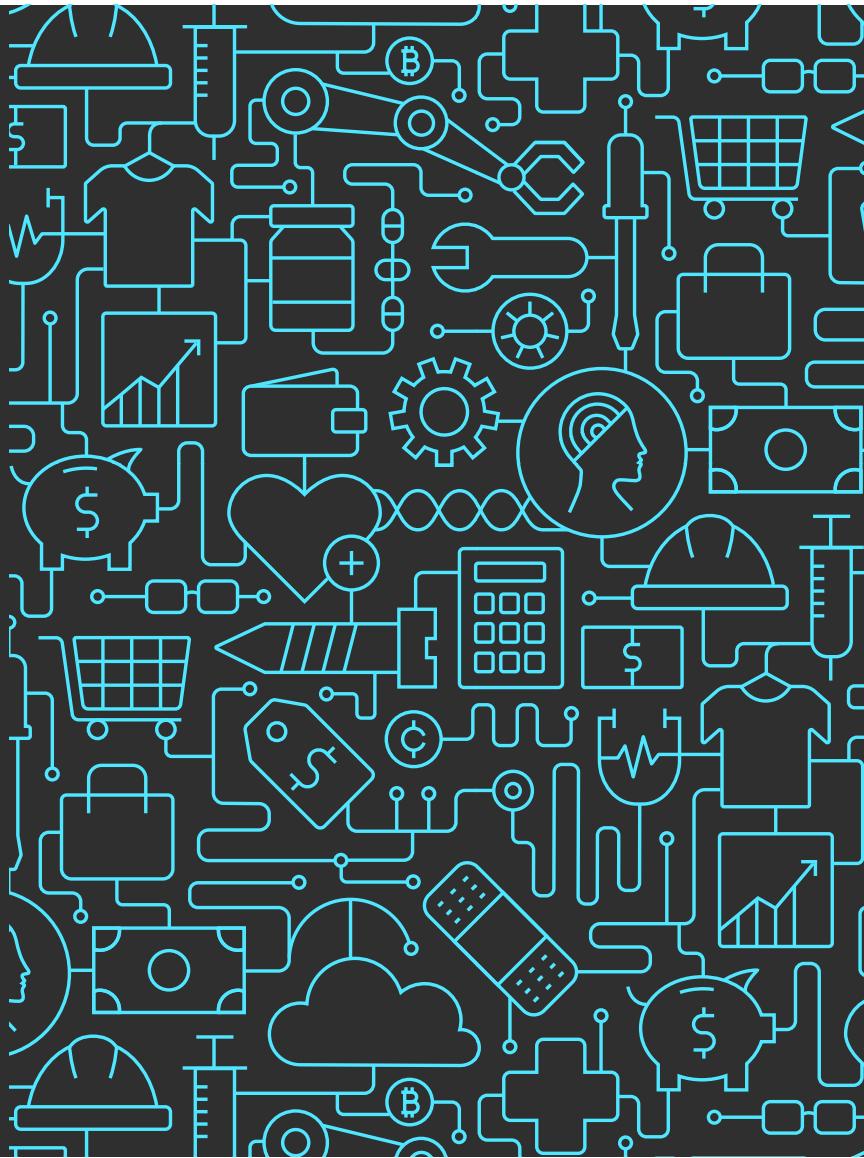
**Improved reporting** and export for Security Center alerts and recommendations

Auto-discover, onboard and **protect your AWS EC2 instances** with Azure security center

Onboard on-prem servers to security center from **Windows Admin Center**

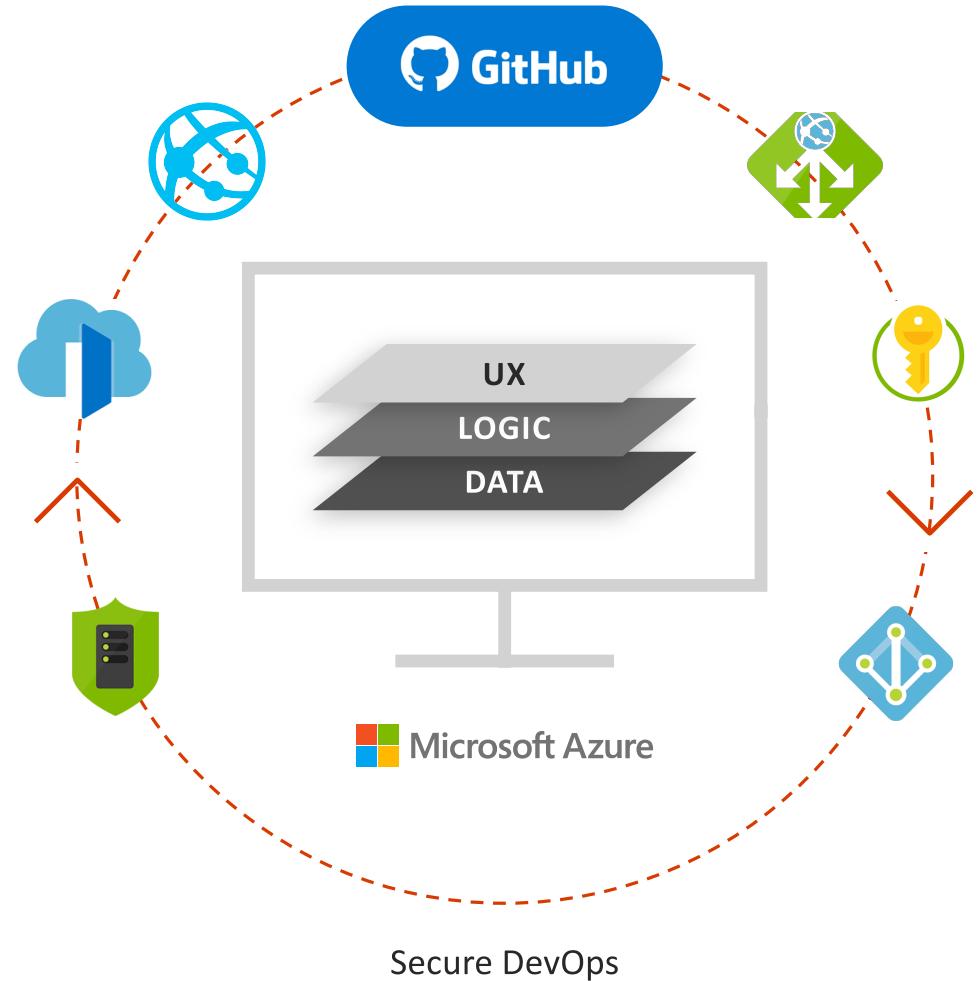


# Develop and operate secure apps in the cloud

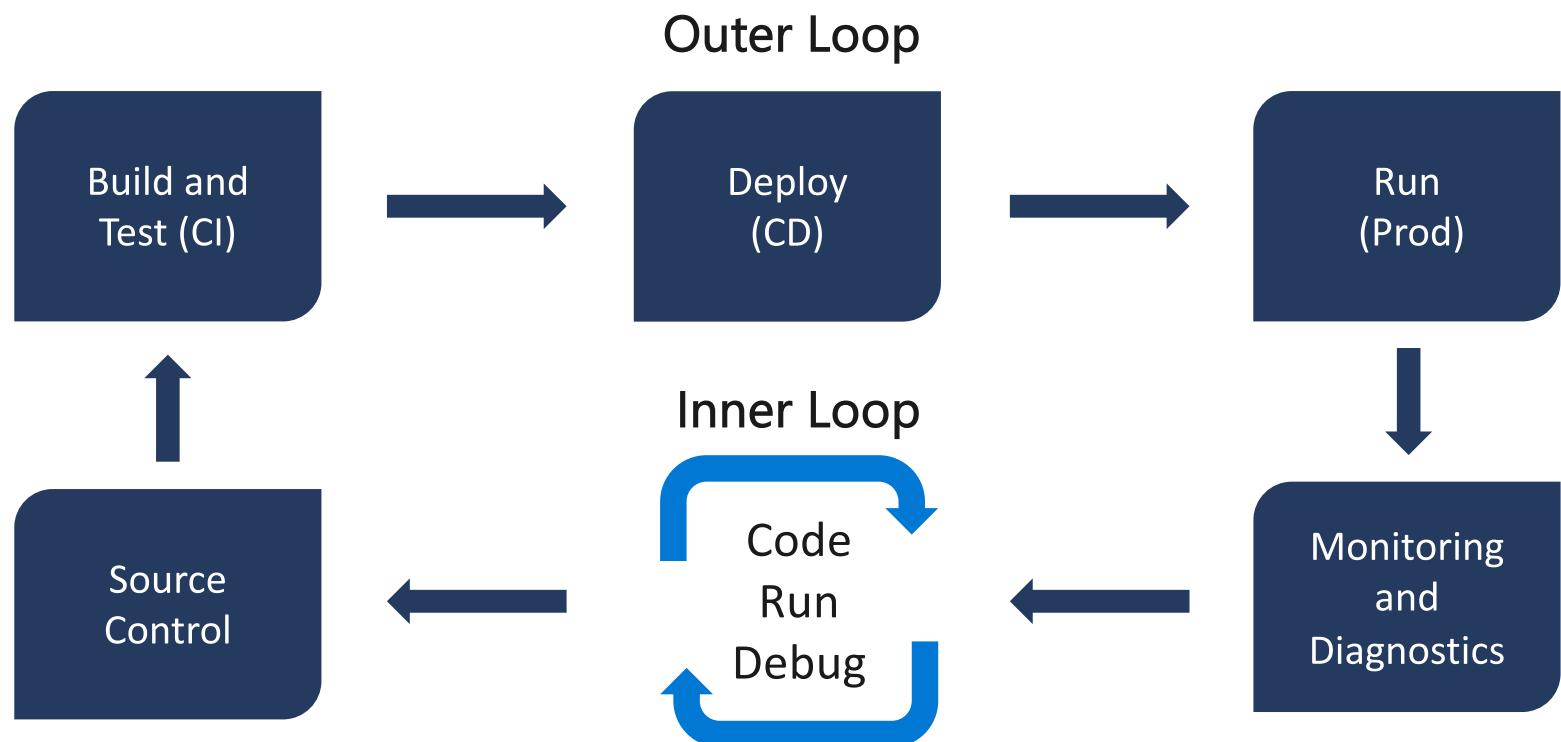


# Shipping secure applications

- Build secure applications faster
  - Threat modeling, vulnerability scanning, unit testing, token scanning, directly inside your release pipeline
- Protect every layer of your application
  - Azure provides you with security tools at the data, network, identity and runtime
    - Encryption at rest, in transit, and in use
- Guidance to help you succeed
  - Best practices documentation
  - Secure Devops toolkit



# Inner and Outer Loop Development

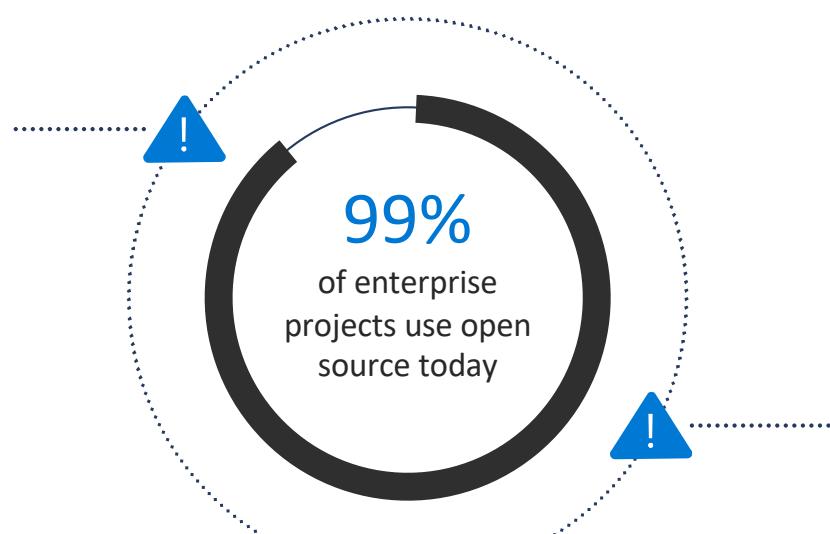


# Securing your codebase with GitHub

## Understand and secure your software supply chain

View and track all your dependencies with **Dependency Insights** and **Dependabot**

Get automated security alerts and version patches



## Integrate security into your code-to-cloud workflows

- Scan for thousands of vulnerabilities with **Semmle**
- Protect leakage of secrets with **GitHub Token Scanning**

# Outer loop

## Microsoft Security Code Analysis

Embrace Secure DevOps by infusing secret scanning, security tools & analysis into Azure DevOps CI/CD pipelines as recommended by Microsoft's Secure Development Lifecycle (SDL) experts.



### Security Simplified

Protect code and enable security analysis in your Azure DevOps pipelines by simply adding easily configurable build tasks



### Clean Builds

Address issues and keep your code clean by configuring build breaks to get notified when regressions are introduced



### Set it & Forget it

The extension can ensure the tools stay up-to-date and you never have to worry about managing updates

Available today  
(via Support)

A 1<sup>st</sup> Step

# Outer loop

## Microsoft Security Code Analysis – Developer Experience

Enable application security testing and Secure DevOps in CI/CD pipelines



### Credential Scanning

Prevent breaches due to leaked secrets

- Easily scan for secret in your Azure DevOps CI/CD pipeline
- Includes 25 searchers supporting 70+ file types out of the box
- Supports custom patterns for your business needs



### Security Code Analysis

Analyze code for common security vulnerabilities

- Simple and consistent UI/UX abstracts the complexities of running various code analysis tools
- Tool set includes BinSkim (compiler flags), Roslyn Analyzers (C#), Anti-Malware Scanner, TSLint (TS & JS) & Security Risk Detection (Fuzzing)



### Stay Clean

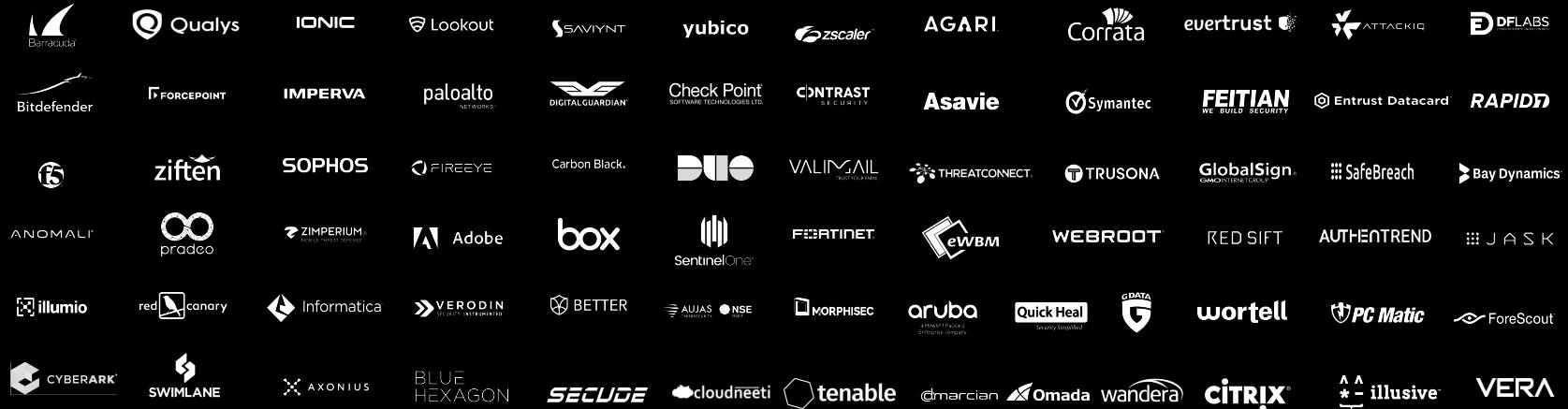
Identify bugs as they're introduced into the codebase.

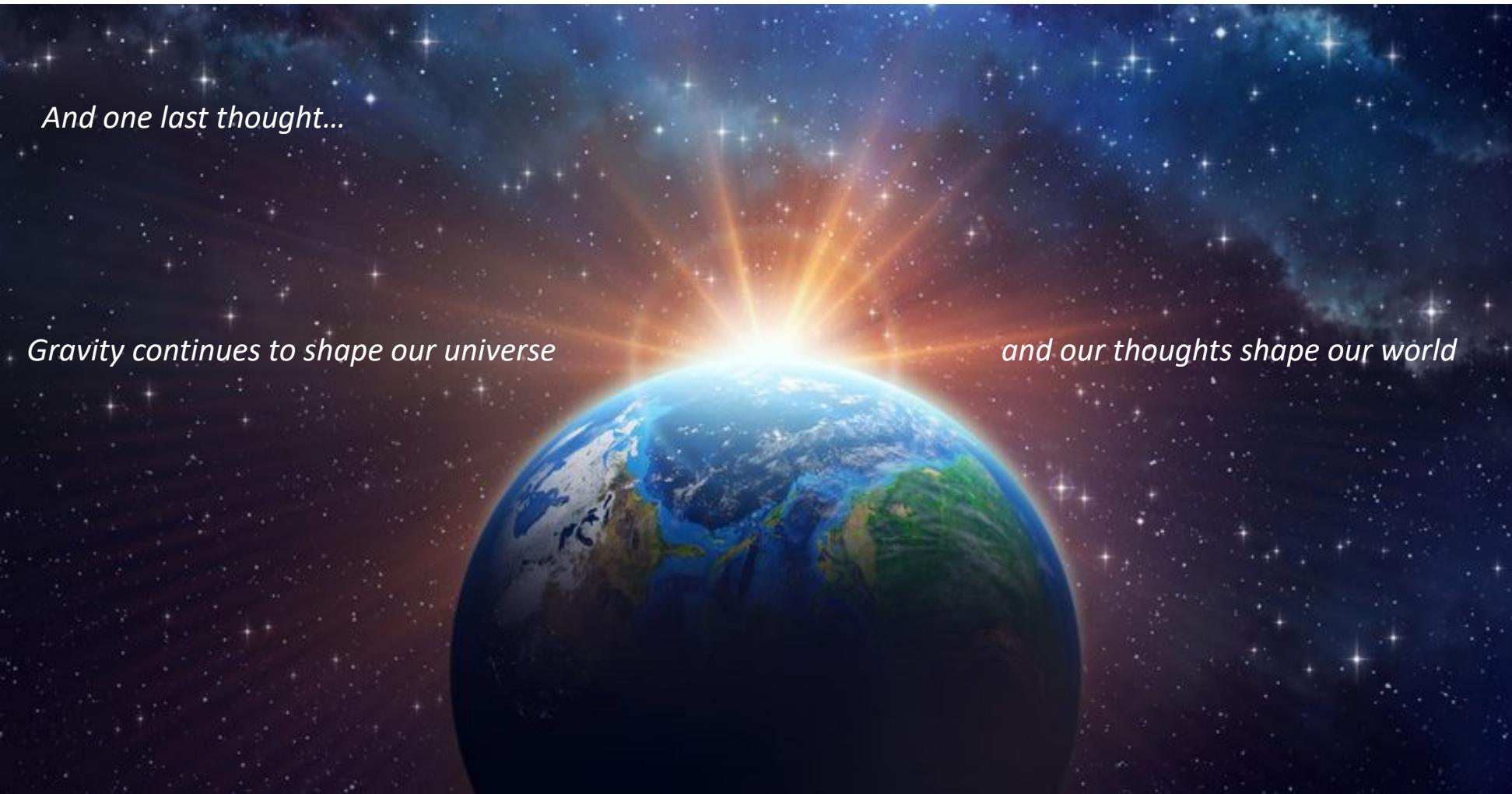
- Easily integrate each tool into your existing CI/CD pipeline as build tasks
- Break the build & block PR completion when any tool finds a vulnerability
- Produce a summary for each build with all results in 1 report

Available today  
(via Support)

A 1<sup>st</sup> Step

# Partners





*And one last thought...*

*Gravity continues to shape our universe*

*and our thoughts shape our world*



*Together, we can shape the security of our digital world... !*



# Thank you!

To learn more, visit  
[azure.microsoft.com/en-us/services/security-center/](https://azure.microsoft.com/en-us/services/security-center/)  
ASC Tech Community Page

