Microsoft

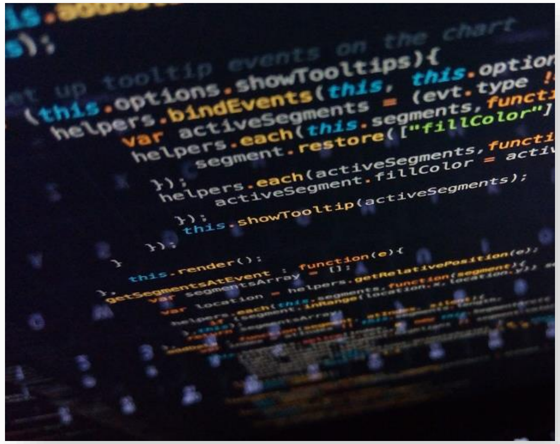
Protect your cloud workload from threats using Azure Security Center

Abbas Kudrati
Chief Cybersecurity Advisor
Microsoft Asia
https://aka.ms/abbas

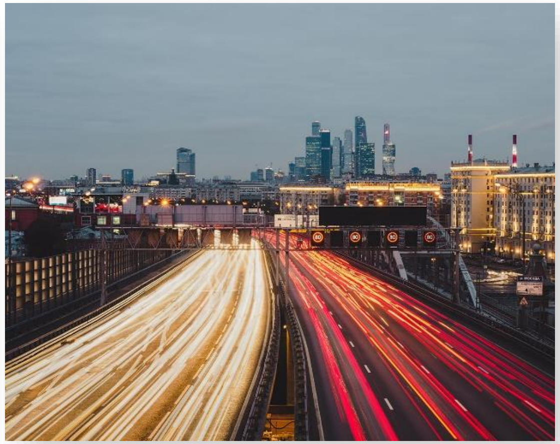
BRK3188

The era of flux and transformation

Everyone is now in the technology business



Conventional security tools have not kept pace



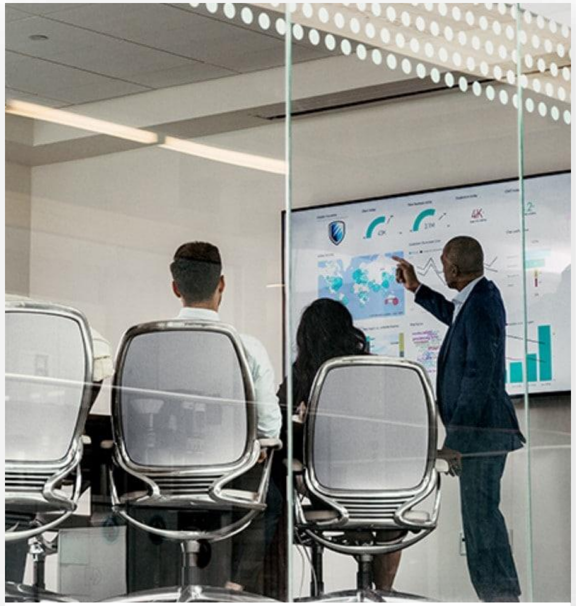
Security professionals alone can't fill the gap

Regulatory requirements and costs are increasing

Intelligent security

Identity and access management

Your universal platform to manage and secure identities



Threat protection

Stop attacks with integrated and automated security

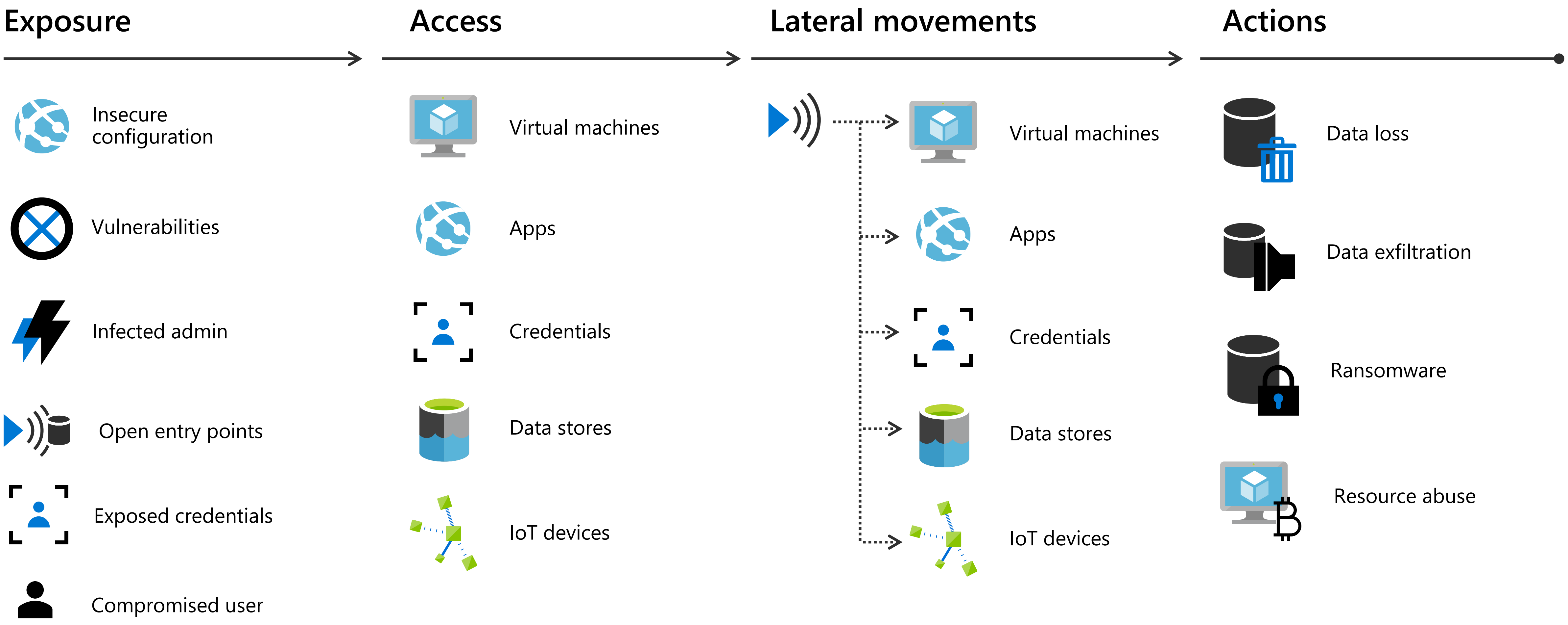
Information protection

Protect your sensitive data—wherever it lives or travels

Cloud security

Safeguard your cross-cloud resources

Threat actors leverage a variety of exposures to breach



Exposure

Insecure configuration

Vulnerabilities

Infected admin

Open entry points

Exposed credentials

Compromised user

Access

Virtual machines

Apps

Credentials

Data stores

IoT devices

Lateral movements

Virtual machines

Apps

Credentials

Data stores

IoT devices

Actions

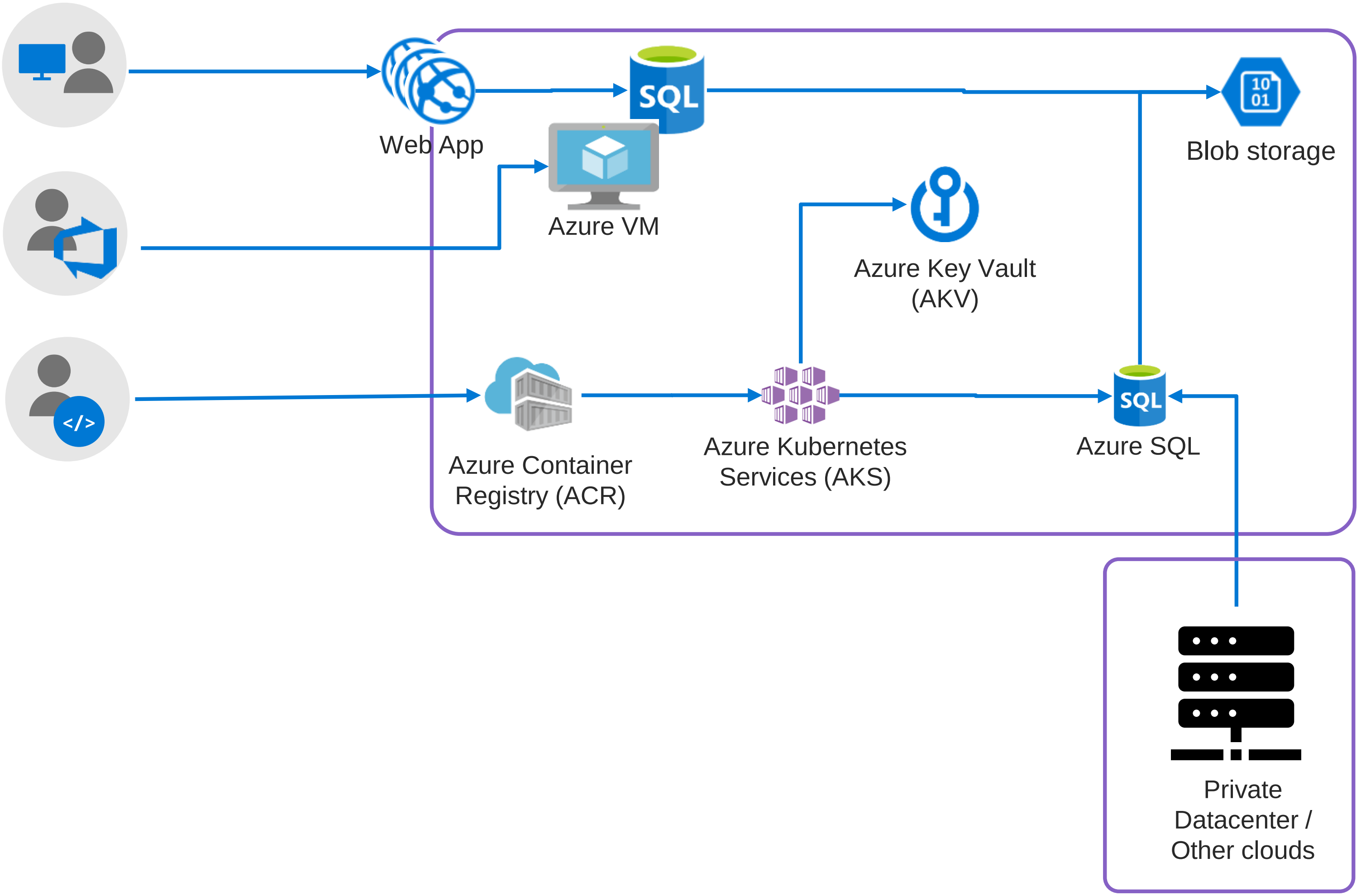
Data loss

Data exfiltration

Ransomware

Resource abuse

Workloads become heterogenous and hybrid


Web App
SQL
Blob storage
Azure VM
Azure Key Vault (AKV)
Azure Container Registry (ACR)
Azure Kubernetes Services (AKS)
Azure SQL
Private Datacenter / Other clouds

Common threats we see in the wild

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

Gain unmatched security with **Azure**

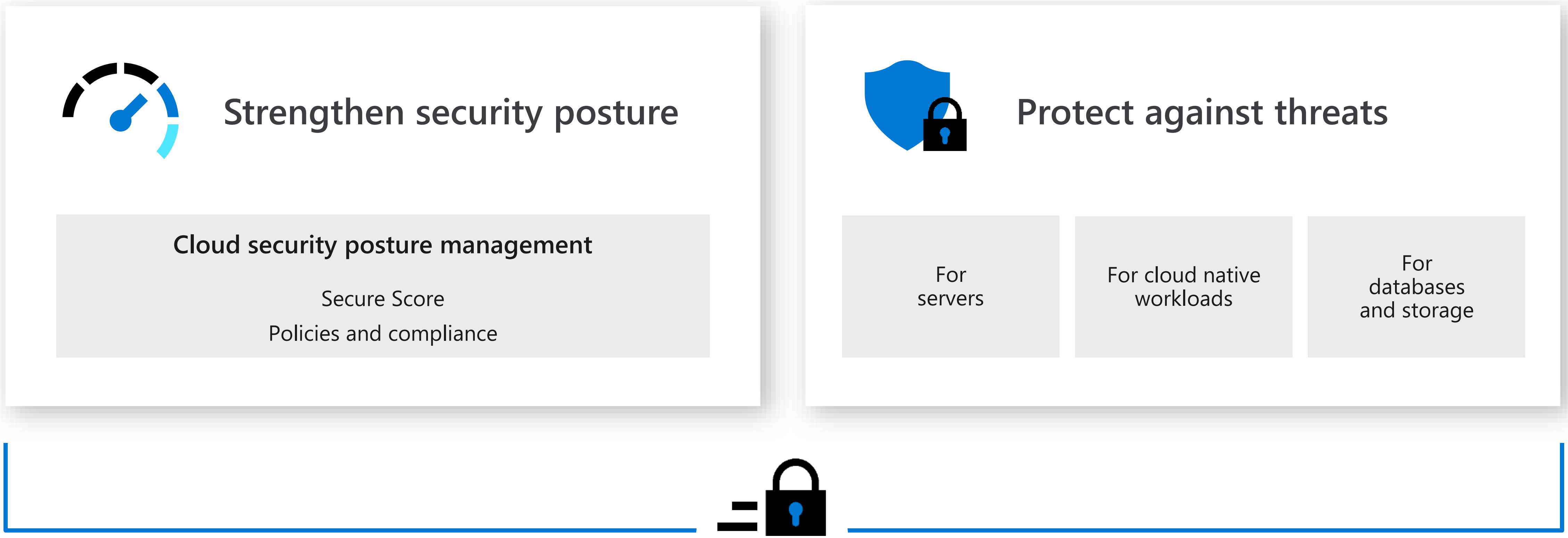
$1B annual investment in cybersecurity

3500+ global security experts

Trillions of diverse signals for unique intelligence

Microsoft Azure

Azure security center



Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

For servers

For cloud native workloads

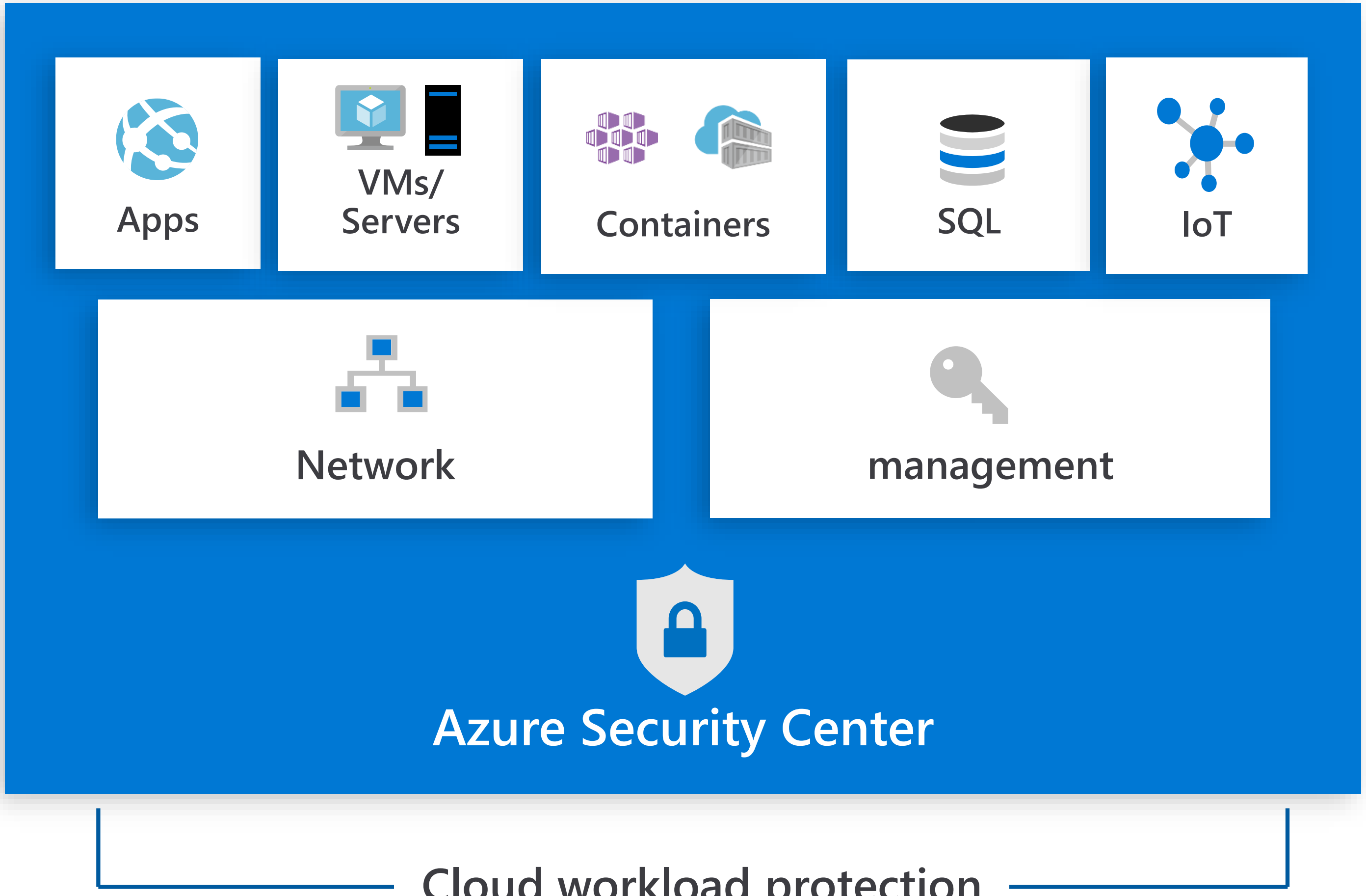
For databases and storage

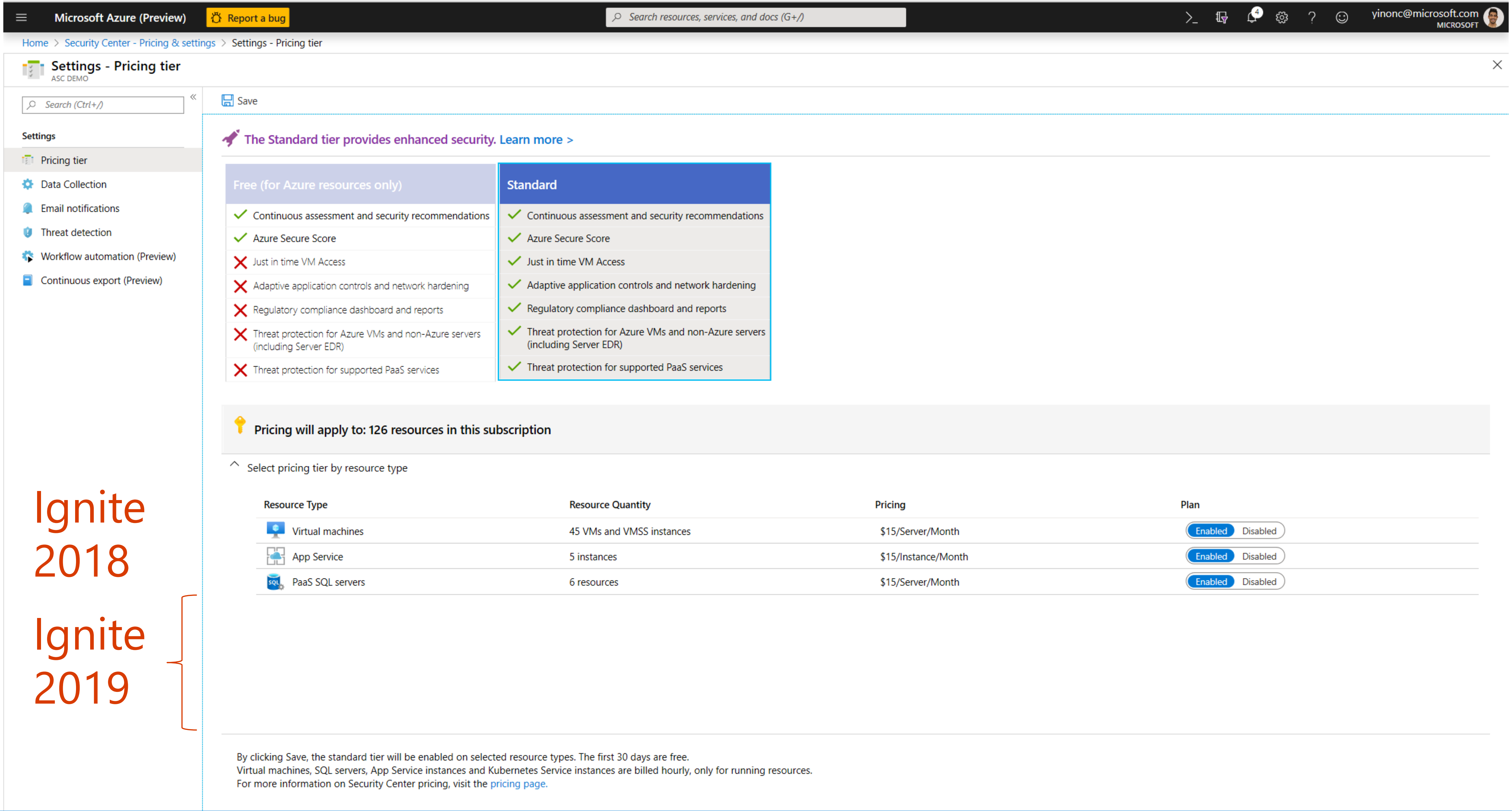
Get secure faster

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+/)
yinonc@microsoft.com
MICROSOFT

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

Settings - Pricing tier

ASC DEMO

Settings

- Pricing tier
- Data Collection
- Email notifications
- Threat detection
- Workflow automation (Preview)
- Continuous export (Preview)

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.

Ignite 2018

Ignite 2019

Get secure fast, just turn it ON

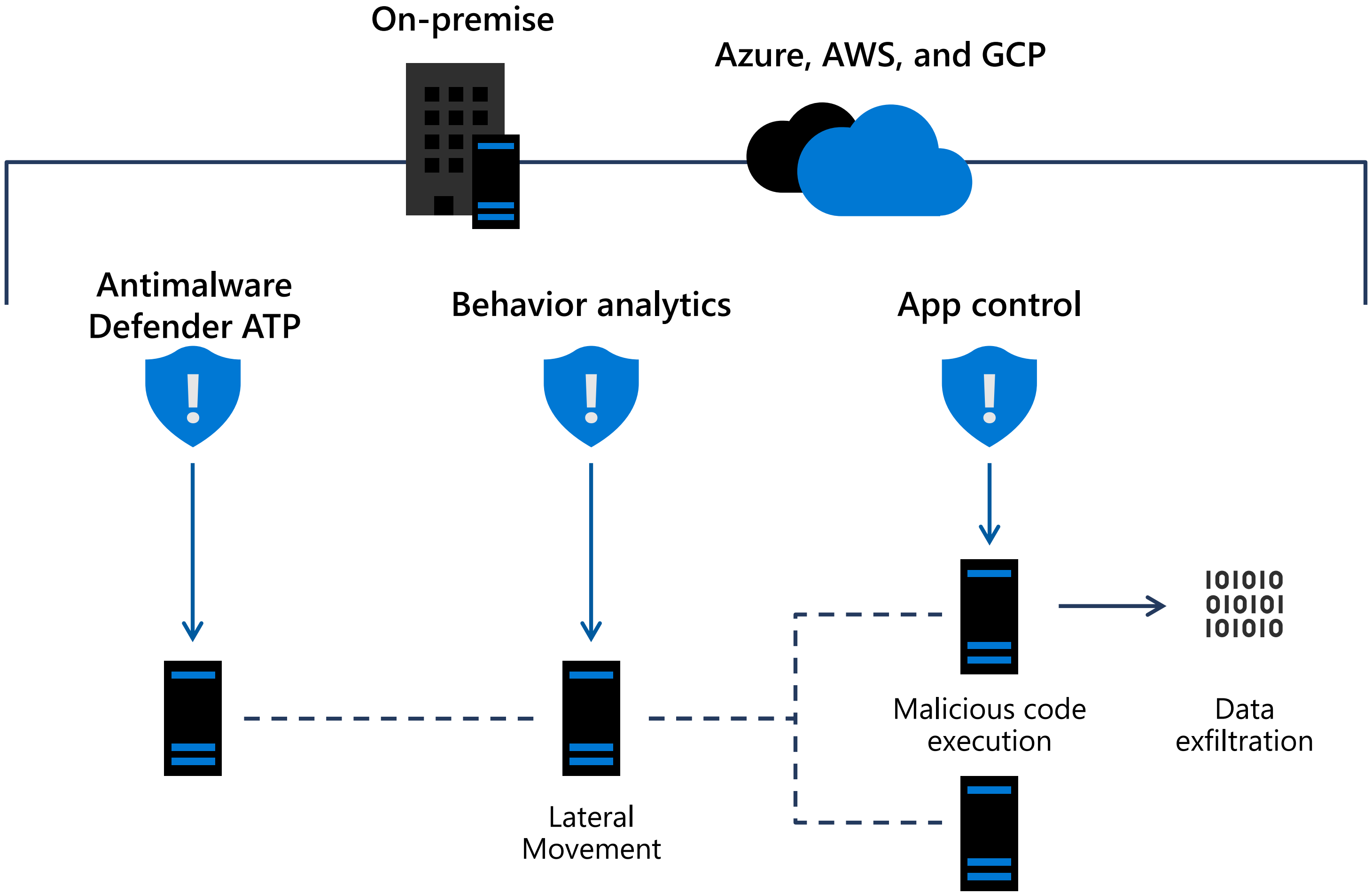
Protect Linux and Windows VMs from threats

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

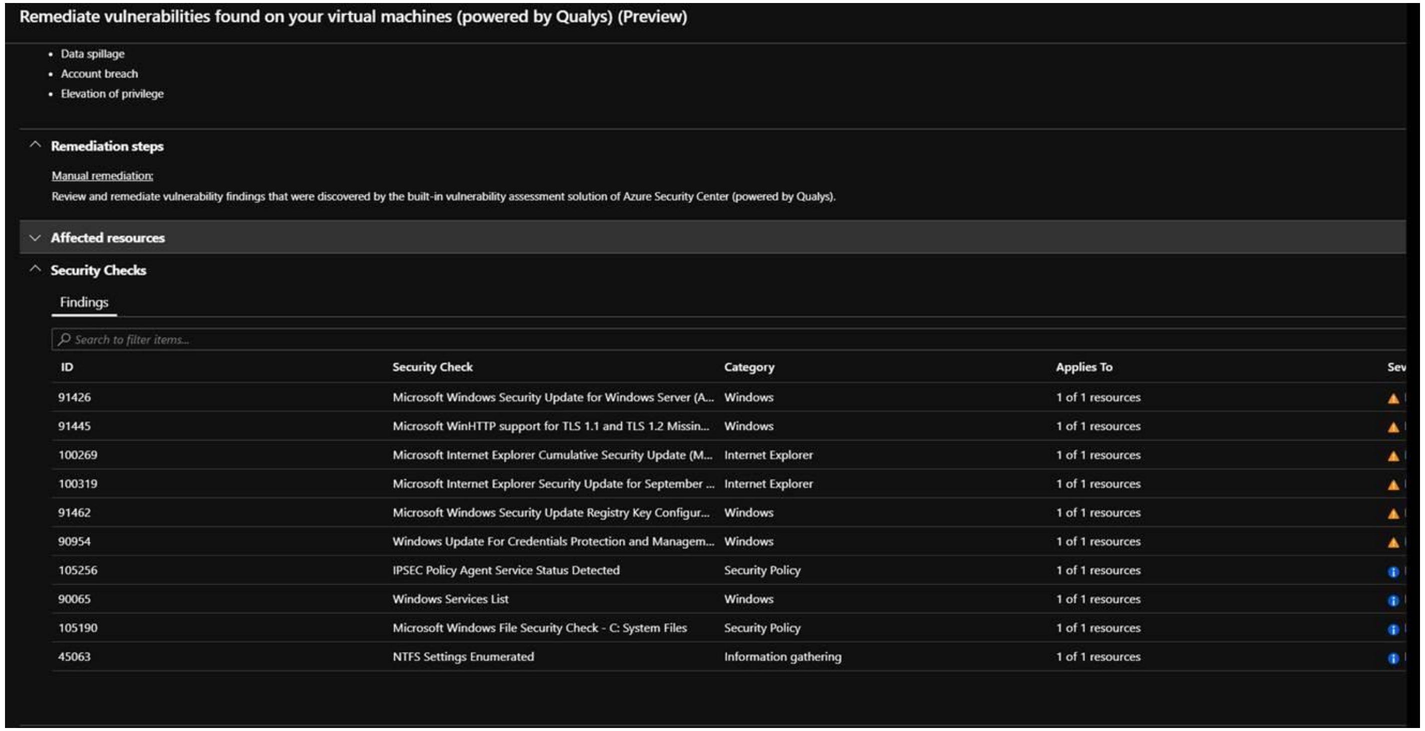


NEW

Announcing built-in vulnerability assessment for VMs

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

- Automated deployment of the 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 Managem...	Windows	1 of 1 resources	⚠
105256	IPSEC Policy Agent Service Status Detected	Security Policy	1 of 1 resources	ℹ
90065	Windows Services List	Windows	1 of 1 resources	ℹ
105190	Microsoft Windows File Security Check - C: System Files	Security Policy	1 of 1 resources	ℹ
45063	NTFS Settings Enumerated	Information gathering	1 of 1 resources	ℹ

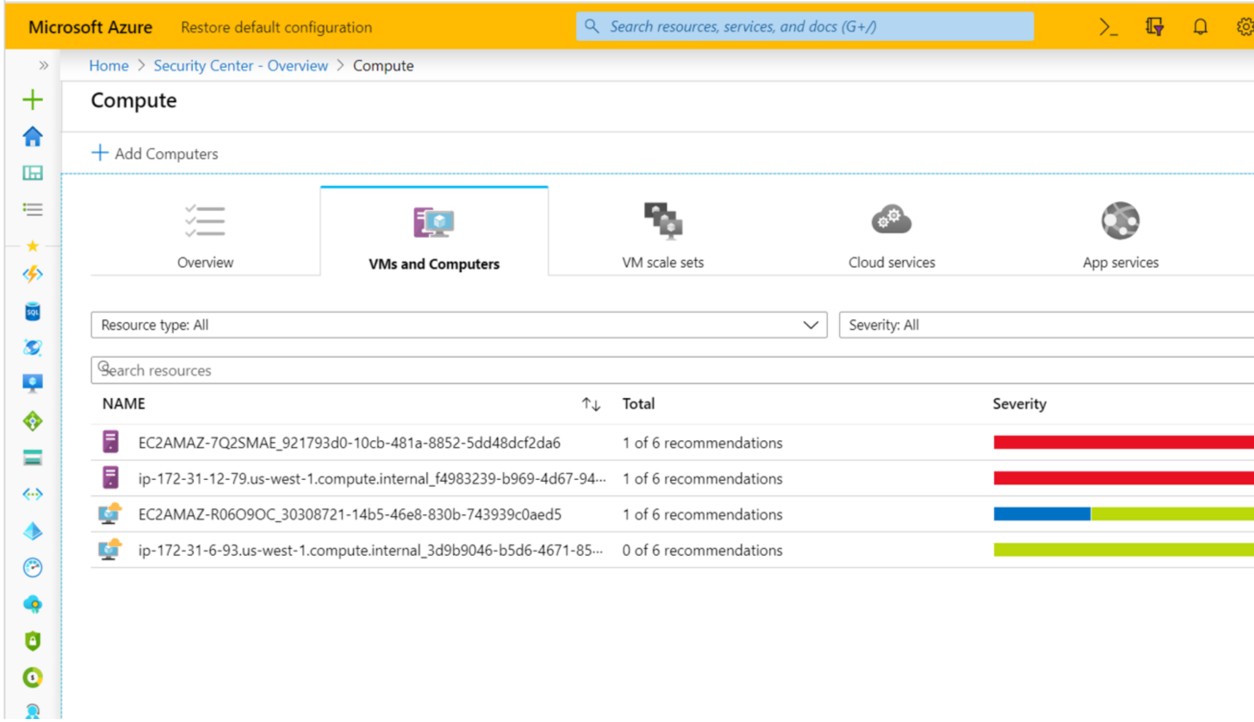
Protect hybrid datacenters and multi-cloud with Azure security center

NEW

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)


Microsoft Azure
Restore default configuration
Search resources, services, and docs (G+/)
Home > Security Center - Overview > Compute
+ Add Computers
Overview
VMs and Computers
VM scale sets
Cloud services
App services

Compute

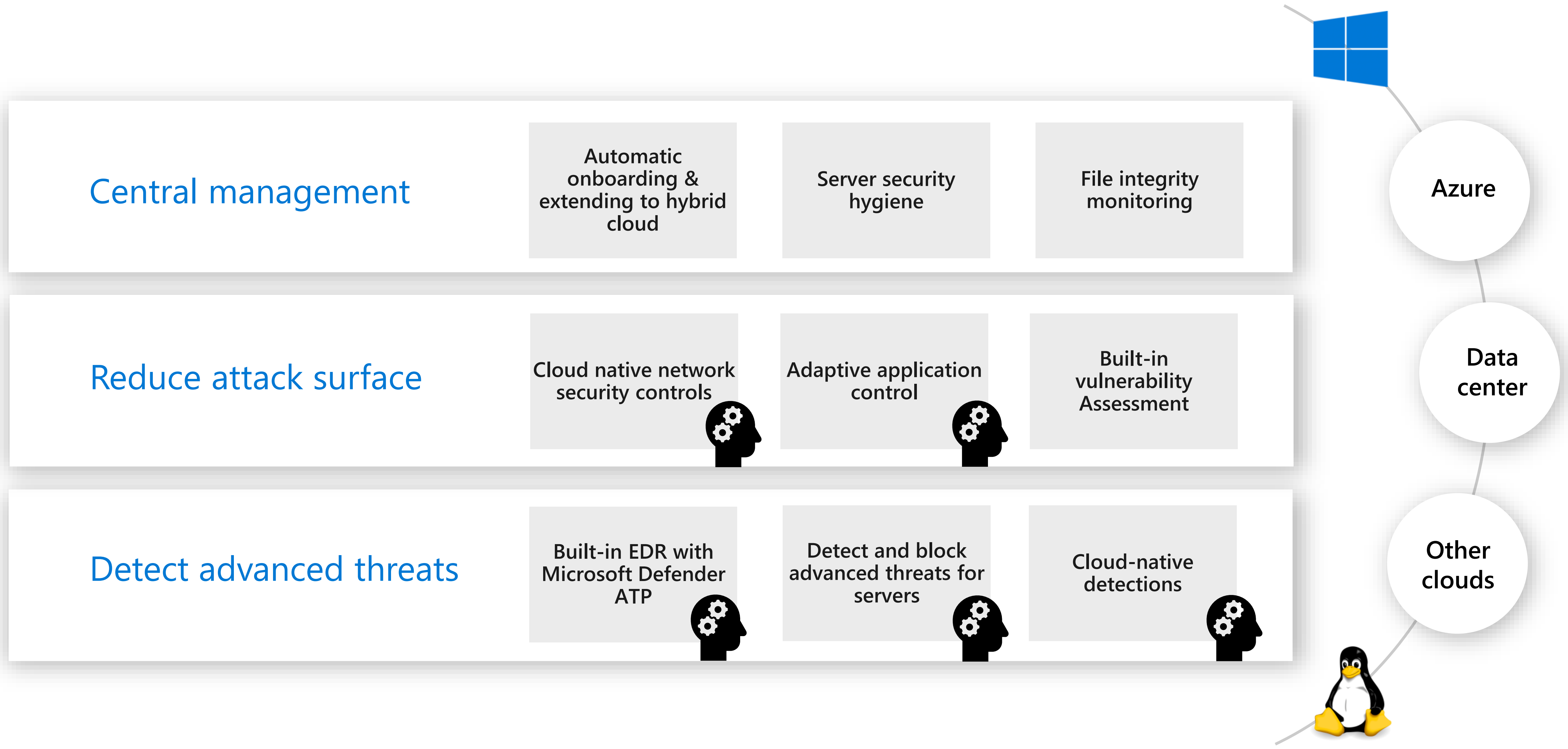
Resource type: All

Severity: All

Search resources

NAME	Total	Severity
EC2AMAZ-7Q2SMAE_921793d0-10cb-481a-8852-5dd48dcf2da6	1 of 6 recommendations	🟥
ip-172-31-12-79.us-west-1.compute.internal_f4983239-b969-4d67-94...	1 of 6 recommendations	🟥
EC2AMAZ-R06O9OC_30308721-14b5-46e8-830b-743939c0aed5	1 of 6 recommendations	🟦🟩
ip-172-31-6-93.us-west-1.compute.internal_3d9b9046-b5d6-4671-85...	0 of 6 recommendations	🟩

Cloud workload protection for hybrid VMs and servers



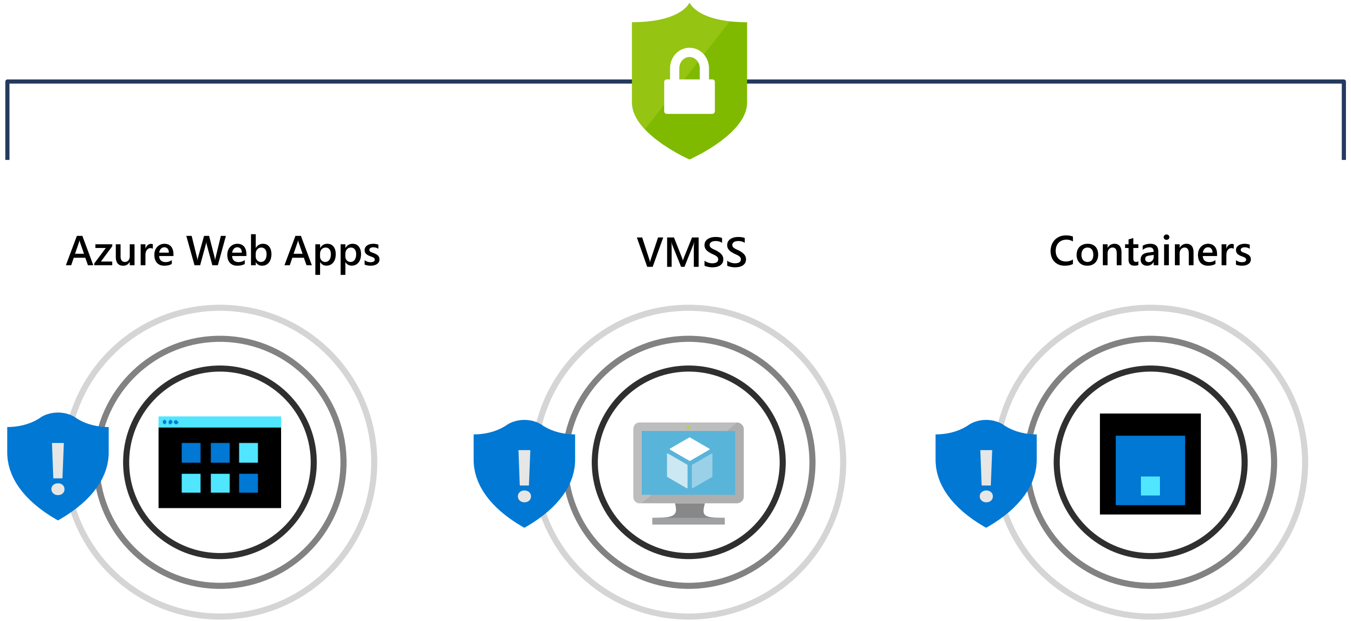
Central management	Automatic onboarding & extending to hybrid cloud	Server security hygiene	File integrity monitoring
Reduce attack surface	Cloud native network security controls	Adaptive application control	Built-in vulnerability Assessment
Detect advanced threats	Built-in EDR with Microsoft Defender ATP	Detect and block advanced threats for servers	Cloud-native detections

Server & VM threat protection with Azure Security Center

Demo

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



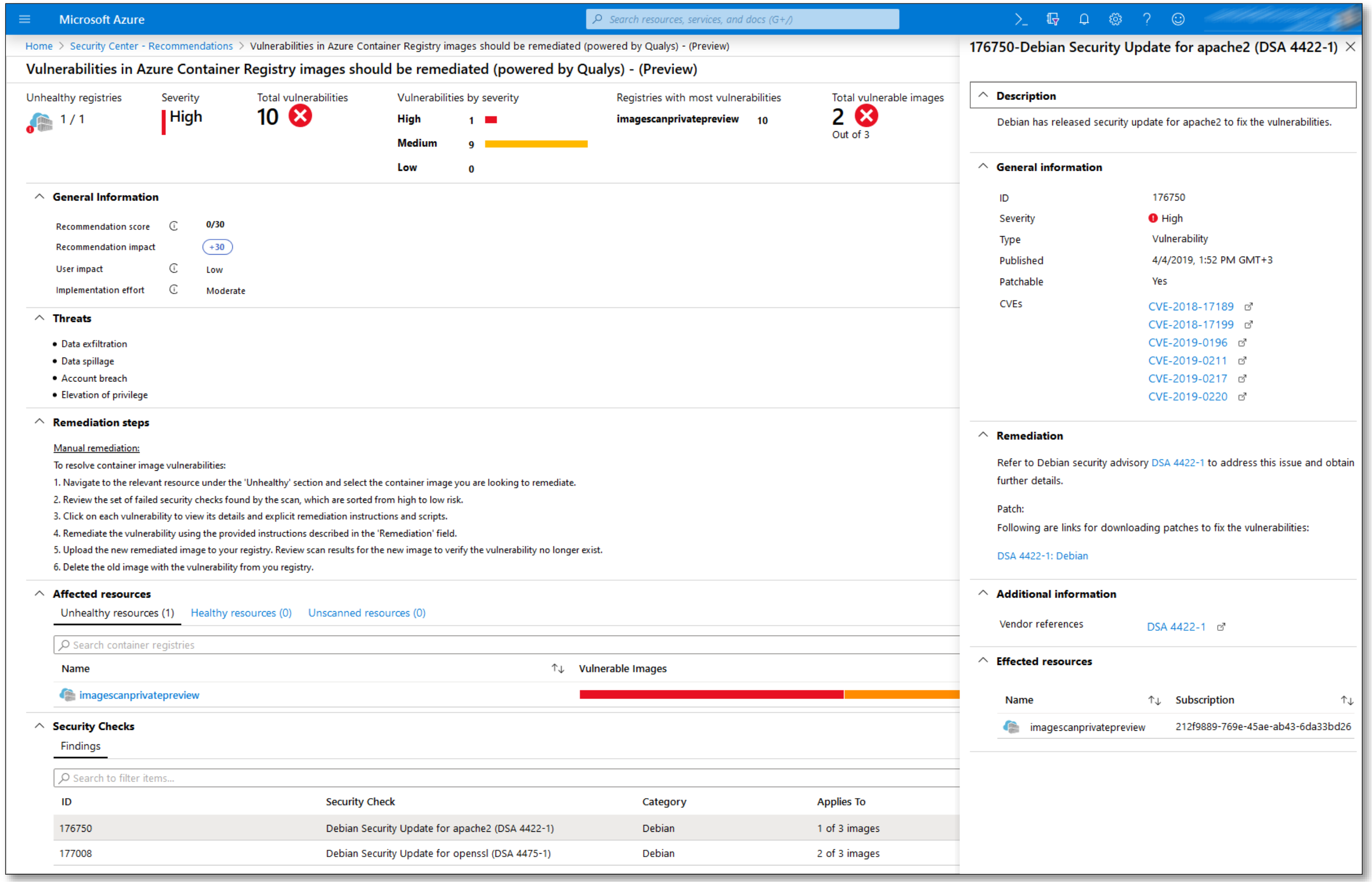
>75% of global organizations will be running containerized applications in production by 2022 (Gartner)

Built-in vulnerability assessment for container images

NEW

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



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Security Center - Recommendations > Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) - (Preview)

Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) - (Preview)

Unhealthy registries 1 / 1

Severity High

Total vulnerabilities 10

Vulnerabilities by severity

High	1
Medium	9
Low	0

Registries with most vulnerabilities: imagescanprivatepreview 10

Total vulnerable images 2 Out of 3

General Information

Recommendation score	0/30
Recommendation impact	+30
User impact	Low
Implementation effort	Moderate

Threats

- Data exfiltration
- Data spillage
- Account breach
- Elevation of privilege

Remediation steps

Manual remediation:

To resolve container image vulnerabilities:

1. Navigate to the relevant resource under the 'Unhealthy' section and select the container image you are looking to remediate.
2. Review the set of failed security checks found by the scan, which are sorted from high to low risk.
3. Click on each vulnerability to view its details and explicit remediation instructions and scripts.
4. Remediate the vulnerability using the provided instructions described in the 'Remediation' field.
5. Upload the new remediated image to your registry. Review scan results for the new image to verify the vulnerability no longer exist.
6. Delete the old image with the vulnerability from you registry.

Affected resources

Unhealthy resources (1) Healthy resources (0) Unscanned resources (0)

Name	Vulnerable Images
imagescanprivatepreview	

Security Checks

Findings

ID	Security Check	Category	Applies To
176750	Debian Security Update for apache2 (DSA 4422-1)	Debian	1 of 3 images
177008	Debian Security Update for openssl (DSA 4475-1)	Debian	2 of 3 images

176750-Debian Security Update for apache2 (DSA 4422-1)

Description

Debian has released security update for apache2 to fix the vulnerabilities.

General information

ID	176750
Severity	High
Type	Vulnerability
Published	4/4/2019, 1:52 PM GMT+3
Patchable	Yes
CVEs	CVE-2018-17189 CVE-2018-17199 CVE-2019-0196 CVE-2019-0211 CVE-2019-0217 CVE-2019-0220

Remediation

Refer to Debian security advisory DSA 4422-1 to address this issue and obtain further details.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

DSA 4422-1: Debian

Additional information

Vendor references DSA 4422-1

Effected resources

Name	Subscription
imagescanprivatepreview	212f9889-769e-45ae-ab43-6da33bd26

Cloud workload protection for containers

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

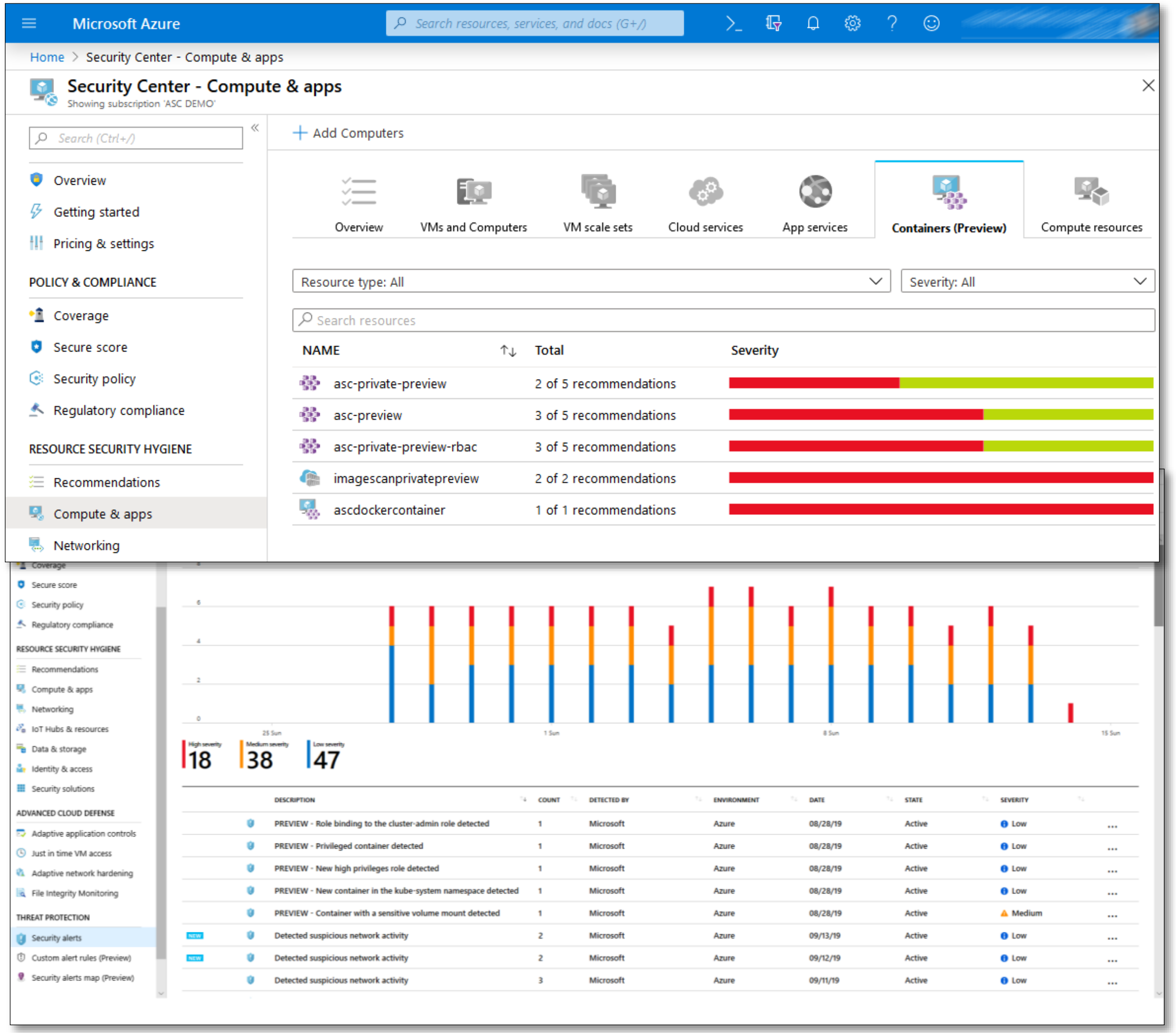
NEW

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



NAME	Total	Severity
asc-private-preview	2 of 5 recommendations	
asc-preview	3 of 5 recommendations	
asc-private-preview-rbac	3 of 5 recommendations	
imagescanprivatepreview	2 of 2 recommendations	
ascdockercontainer	1 of 1 recommendations	

	DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	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	...
	PREVIEW - Container with a sensitive volume mount detected	1	Microsoft	Azure	08/28/19	Active	Medium	...
NEW	Detected suspicious network activity	2	Microsoft	Azure	09/13/19	Active	Low	...
NEW	Detected suspicious network activity	2	Microsoft	Azure	09/12/19	Active	Low	...
	Detected suspicious network activity	3	Microsoft	Azure	09/11/19	Active	Low	...

Protecting against advanced cloud threats

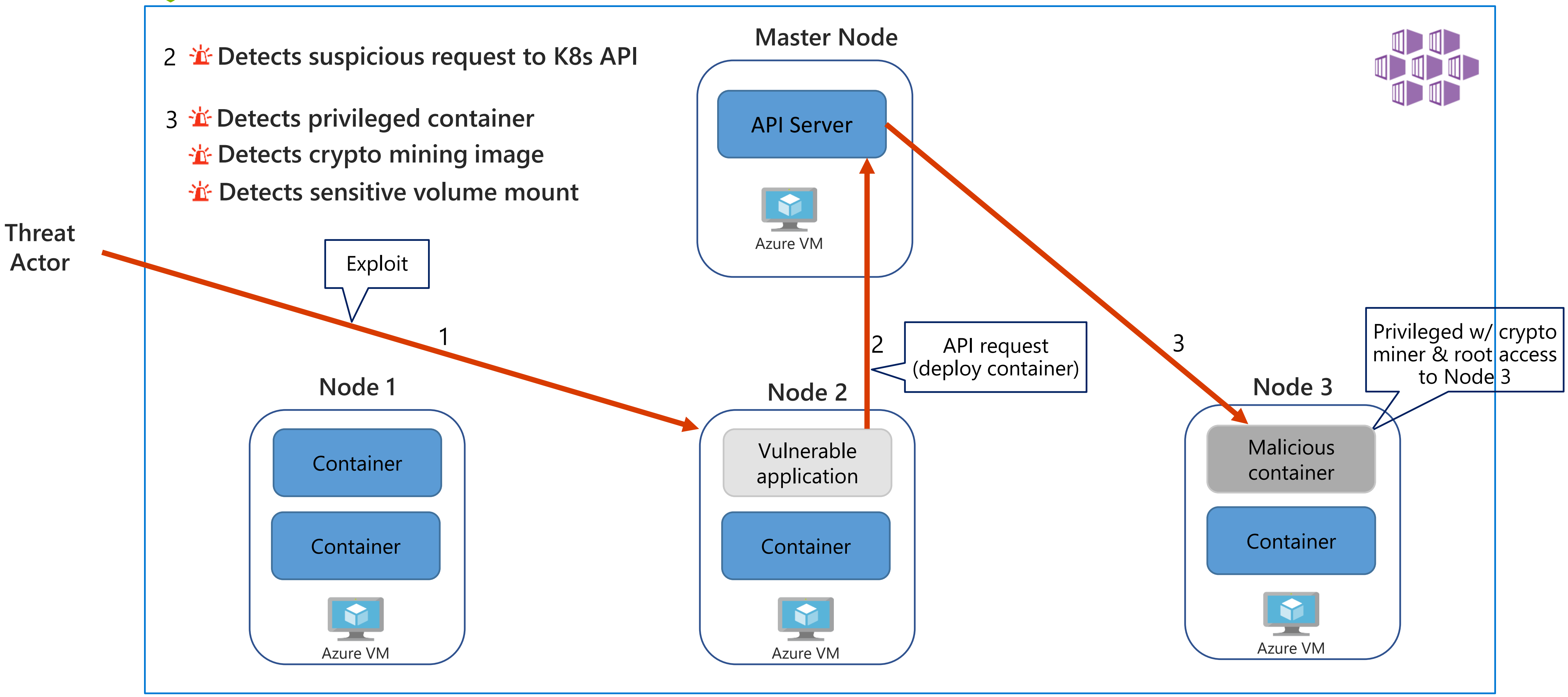
🔒 Recommending to use RBAC on K8s

2 🚨 Detects suspicious request to K8s API

3 🚨 Detects privileged container

🚨 Detects crypto mining image

🚨 Detects sensitive volume mount



Threat Actor

Exploit

1

Master Node

API Server

Azure VM

2

API request (deploy container)

3

Privileged w/ crypto miner & root access to Node 3

Node 1

Container

Container

Azure VM

Node 2

Vulnerable application

Container

Azure VM

Node 3

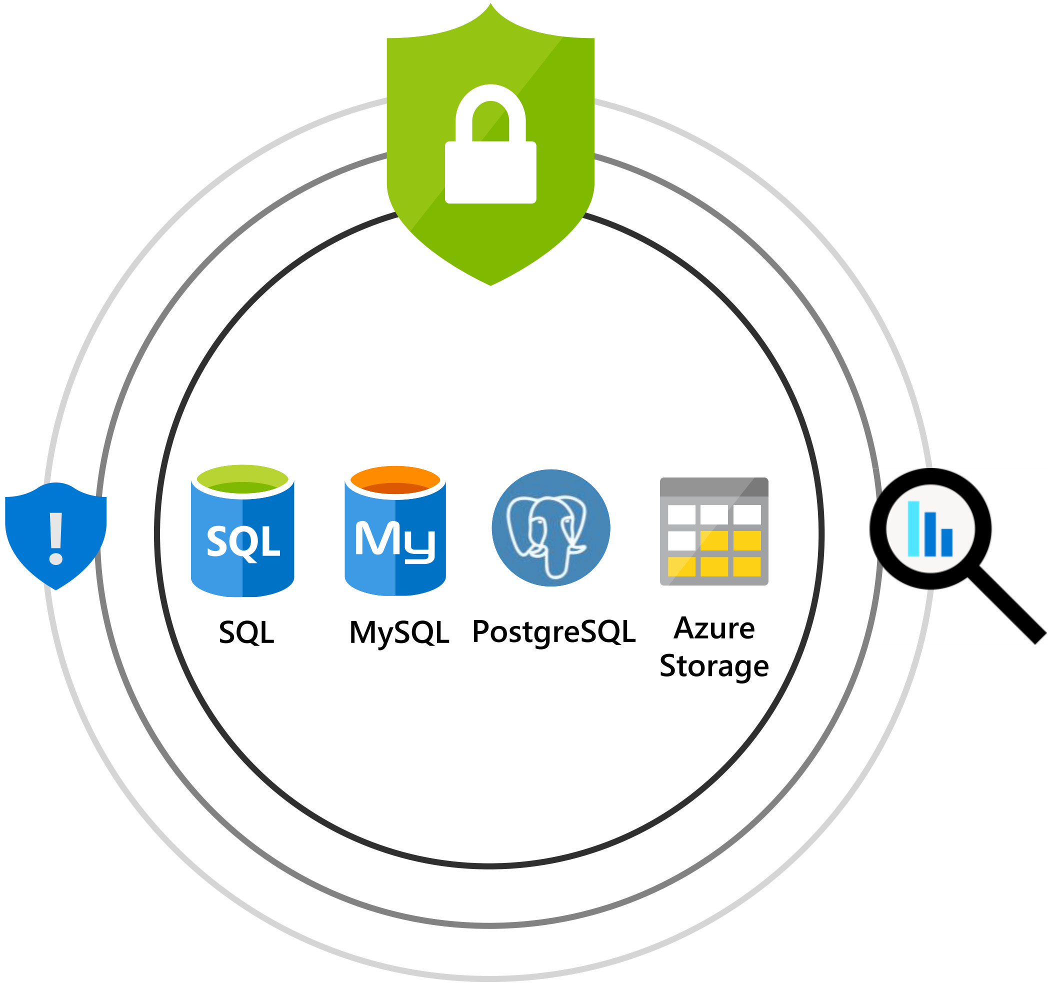
Malicious container

Container

Azure VM

Protect data services from threats

- Prevent & detect threats targeting your Azure SQL databases, My SQL, 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

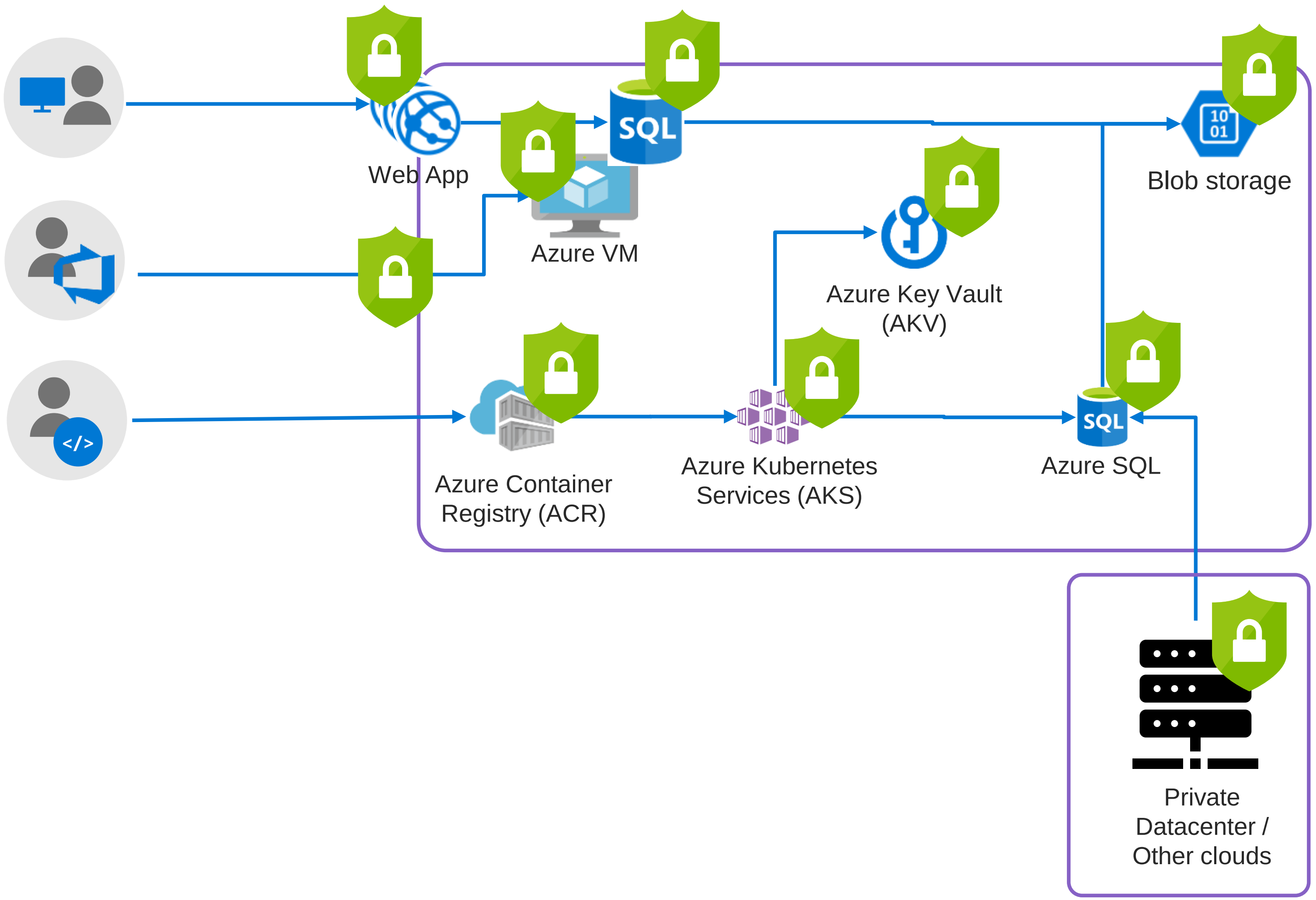
- ➢ Malware reputation screening or suspicious files (.cspkg)
- ➢ Access anomalies by location, principal, or application
- ➢ Permission change anomalies, anonymous access detection
- ➢ And more…

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…

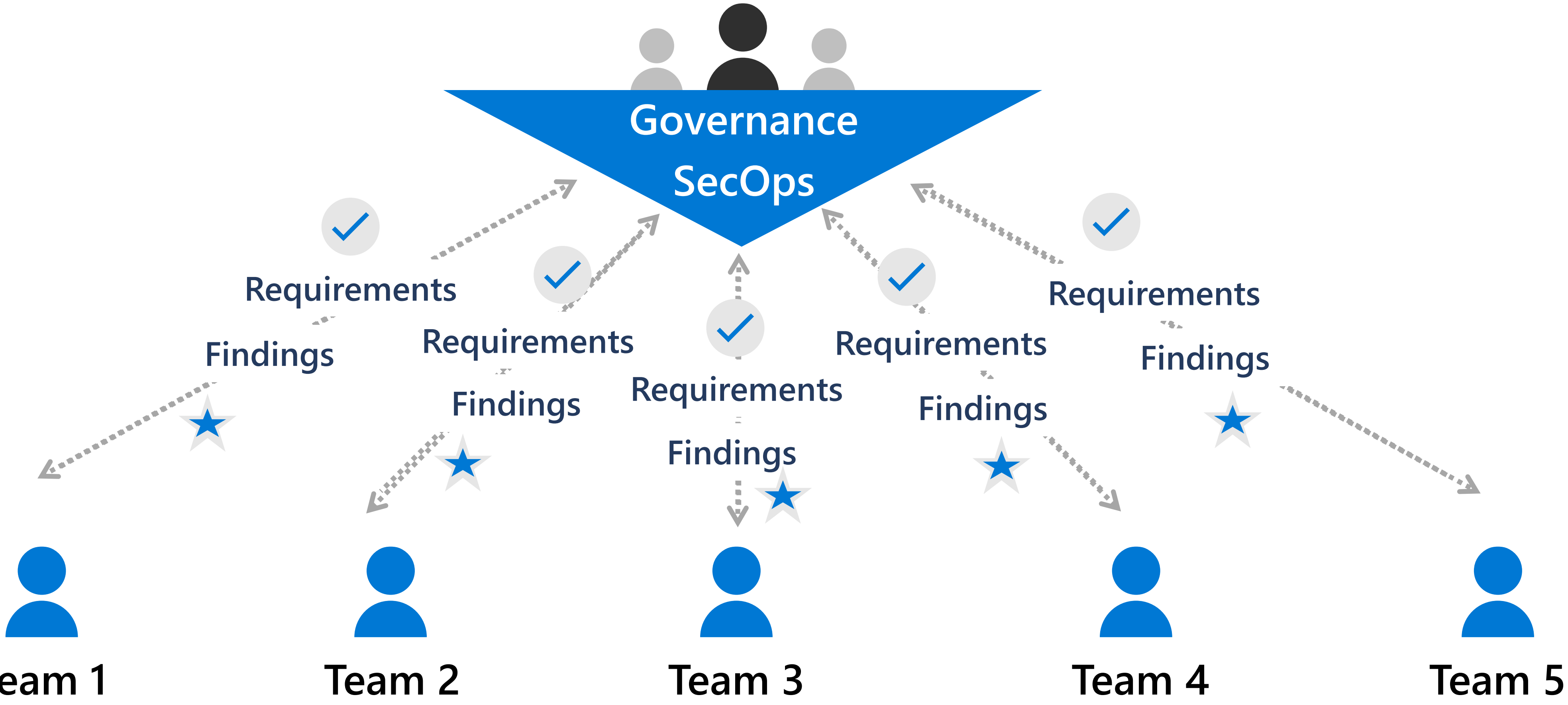
Example solution architecture on Azure


Web App
SQL
Azure VM
Blob storage
Azure Key Vault (AKV)
Azure Container Registry (ACR)
Azure Kubernetes Services (AKS)
SQL
Azure SQL
Private Datacenter / Other clouds

Azure security center enterprise integrations

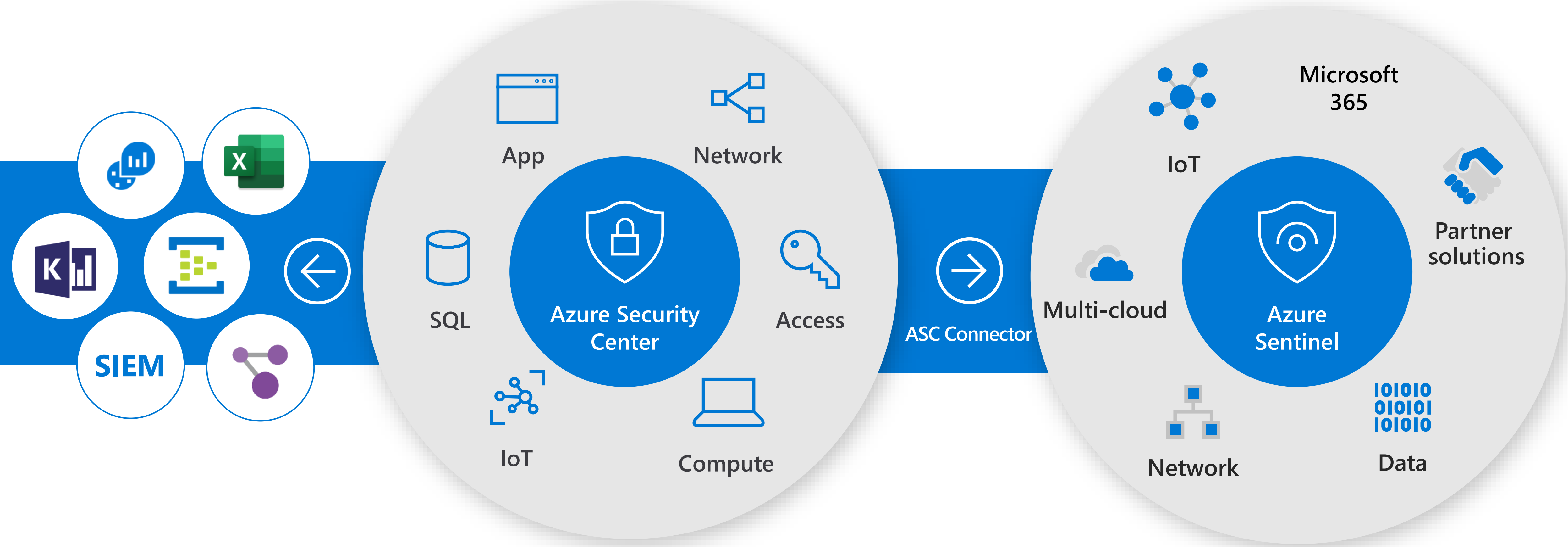
Driving threat protection through the organization

Through a central SecOps & cloud governance role



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

NEW



Azure Security Center
Cloud Workload Protection

Azure Sentinel
Cloud Native SIEM

Automate workflows with ASC

NEW

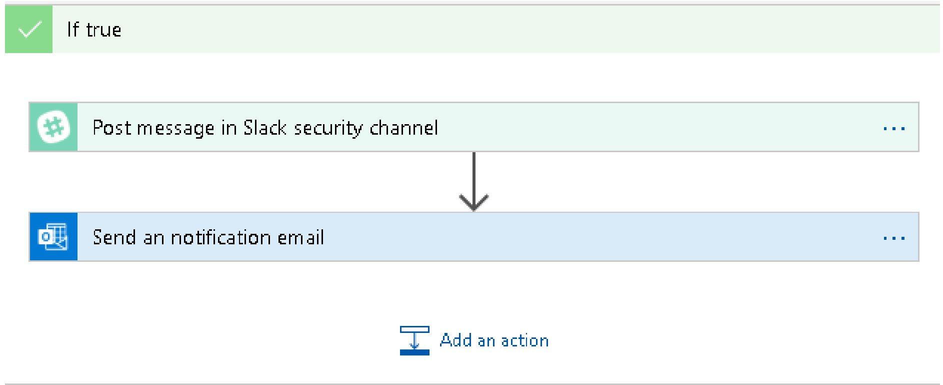
Automate workflows with ASC

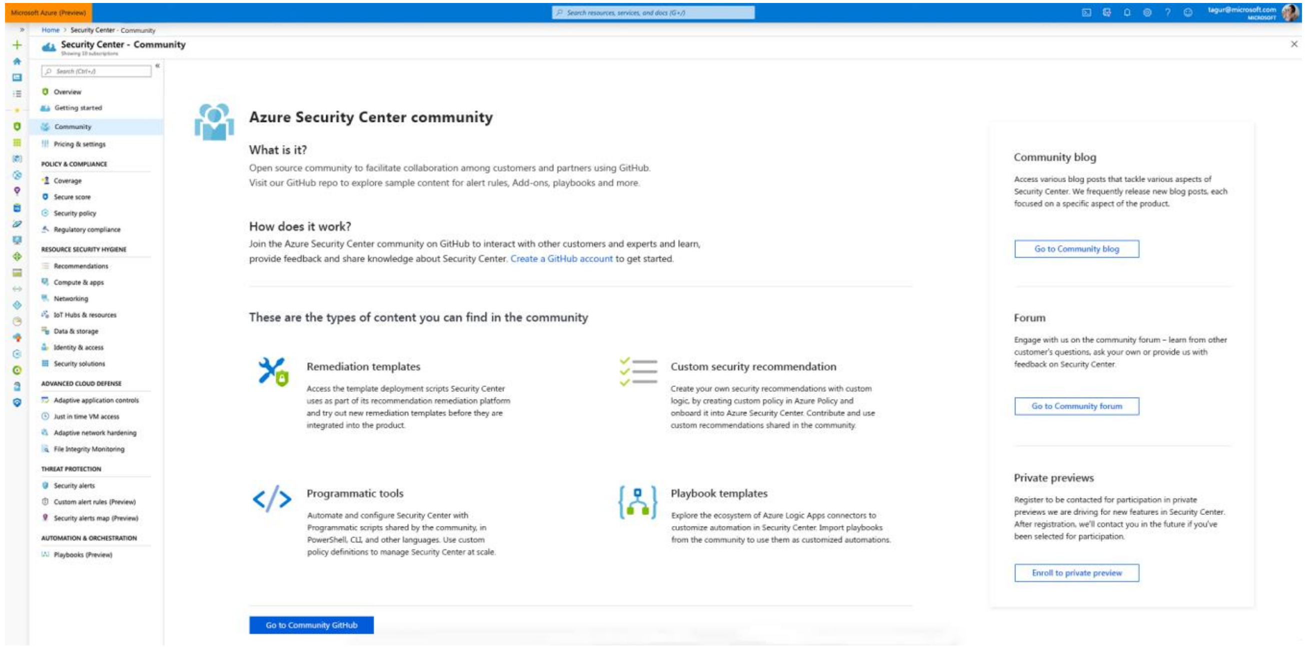
- Trigger playbooks based on ASC recommendations and alerts
- Built-in playbooks, build your own with Azure Logic apps

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

Automate and script through API and PowerShell


If true
Post message in Slack security channel
...
Send an notification email
...
Add an action



Azure Security Center community

What is it?

Open source community to facilitate collaboration among customers and partners using GitHub.
Visit our GitHub repo to explore sample content for alert rules, Add-ons, playbooks and more.

How does it work?

Join the Azure Security Center community on GitHub to interact with other customers and experts and learn, provide feedback and share knowledge about Security Center. Create a GitHub account to get started.

These are the types of content you can find in the community

Remediation templates

Access 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.

Custom security recommendation

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.

Programmatic tools

Automate and configure Security Center with Programmatic scripts shared by the community, in PowerShell, CLI, and other languages. Use custom policy definitions to manage Security Center at scale.

Playbook templates

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.

Community blog

Access various blog posts that tackle various aspects of Security Center. We frequently release new blog posts, each focused on a specific aspect of the product.

Forum

Engage with us on the community forum – learn from other customer's questions, ask your own or provide us with feedback on Security Center.

Private previews

Register to be contacted for participation in private previews we are driving for new features in Security Center. After registration, we'll contact you in the future if you've been selected for participation.

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 Ignite 2019 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**

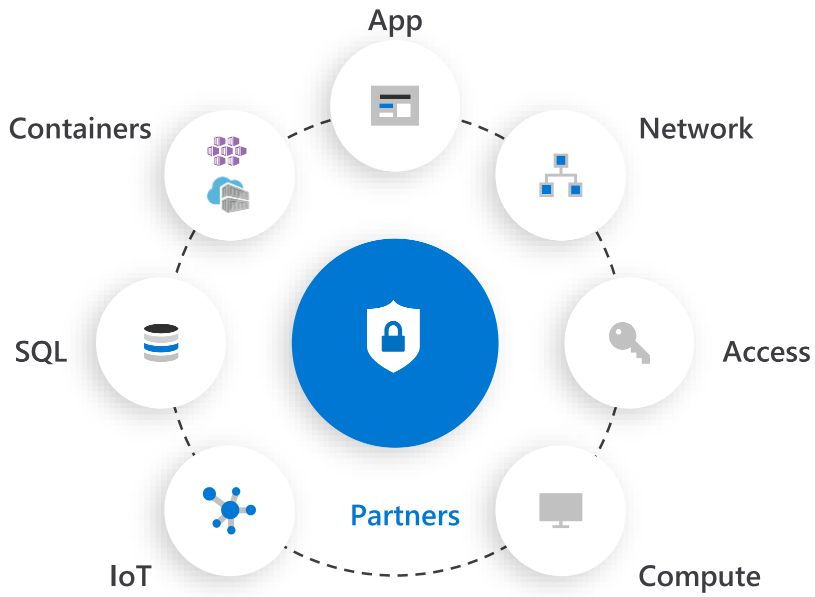
Built-in vulnerability assessment with Security Center Standard

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**

Microsoft

Microsoft Ignite The Tour: Free Certification Exam Offer

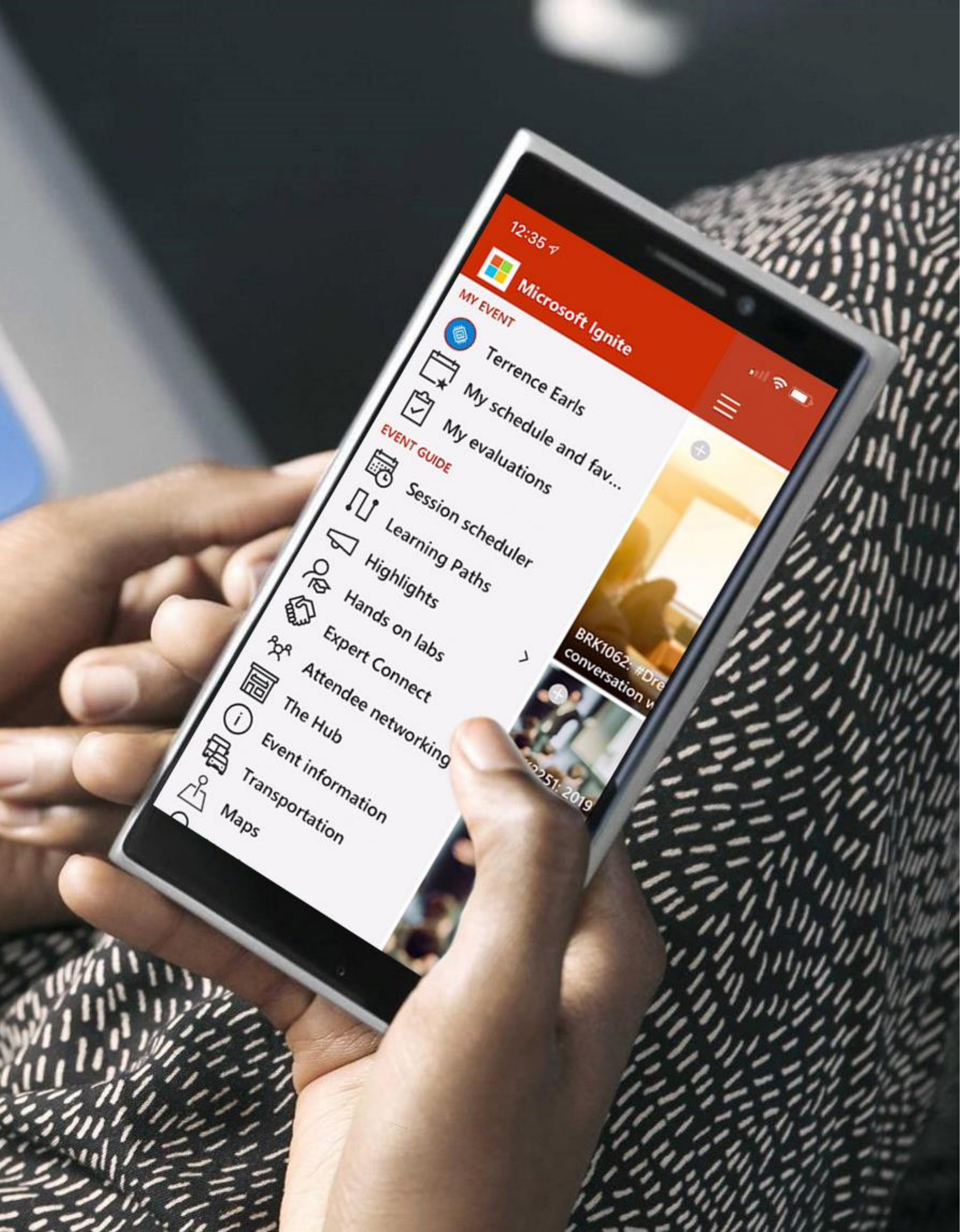
https://aka.ms/Freeexam

Microsoft

Thank you!

To learn more, visit
azure.microsoft.com/en-us/services/security-center/

[ASC Tech Community Page]



Please evaluate this session

Your feedback is important to us!

Please evaluate this session through MyEvaluations on the mobile app or website.

Download the app:
https://aka.ms/ignite.mobileapp

Go to the website:
https://myignite.techcommunity.microsoft.com/evaluations

Find this session in Microsoft Tech Community

Visit aka.ms/MicrosoftIgnite2019/BRK3188

- ✓ Download slides and resources
- ✓ Access session recordings in 48 hours
- ✓ Ask questions & continue the conversation

Microsoft