



Cloud Security Posture Management with Azure Security Center

Tom Janetscheck
Senior Program Manager
CxE Security | Azure Security Center

Why security hygiene should be your number one priority?

"The biggest threat in 2020 is the continued need for basic fundamental data-center/cloud hygiene," warns [Dave Klein, Senior Director Engineering & Architecture at Guardicore](#).

While cloud-based systems provide better data storage options and collaboration opportunities, they pose a higher risk of data breaches, hacked accounts and other security issues. Taking steps to secure your cloud helps prevent your company's data, as well as customer and client data you hold, from falling into the wrong hands.

In order to mitigate cybersecurity risks to your cloud (and possible financial and reputation damage), Klein suggests organizations:

- Add two-factor authentication
- Update patch and certification management processes
- Improve segmentation
- Use (or improve) vulnerability testing
- Implement (or improve) incident response planning and practice

Source: <https://i-sight.com/resources/11-cybersecurity-threats-for-2020-plus-5-solutions/>

The truth is that the vast majority of data breaches can be prevented with basic actions, such as vulnerability assessments, patching and proper configurations. An [Online Trust Alliance](#) study estimated that 93 percent of reported incidents could have been avoided with basic cyber hygiene best practices, a figure that remains largely unchanged in the past decade. While advanced threats are growing in volume and sophistication, organizations are still getting breached due to poor key management, unpatched applications and misconfigured cloud databases.

Source: <https://securityintelligence.com/your-security-strategy-is-only-as-strong-as-your-cyber-hygiene/>

37% Of Organisations Have Suffered A Cyberattack On Cloud Environments Due To The Lack Of Basic Cloud Security Hygiene

By [Outpost24](#) August 22, 2019

4721 0



New study reveals 42 percent of organisations are concerned about cloud security but many fail to carry out any security testing on the environment

With the recent exposure of a huge data breach affecting US bank Capital One, cloud security has once again been put under the spotlight. However, a recent survey from Outpost24 has revealed that many companies today would be unable to detect abnormalities in their cloud environment, while 37 percent have already experienced a cyberattack on their cloud systems. As more organisations embrace digital transformation and migrate to the cloud – the results of the survey highlight the lack of security hygiene when it comes to cloud environments.

Source: <https://www.informationsecuritybuzz.com/study-research/37-of-organisations-have-suffered-a-cyberattack-on-cloud-environments-due-to-the-lack-of-basic-cloud-security-hygiene/>

Why security hygiene should be your number one priority?

Palo Alto Networks Report Finds Poor Security Hygiene Leads to Escalating Cloud Vulnerabilities

☆ 0 saves 👁 857 views 🔗

Palo Alto Networks Santa Clara, CA Feb 05, 2020 at 03:00 AM

Unit 42 Cloud Threat Report uncovers 199,000 insecure cloud templates, finds 43% of cloud databases unencrypted

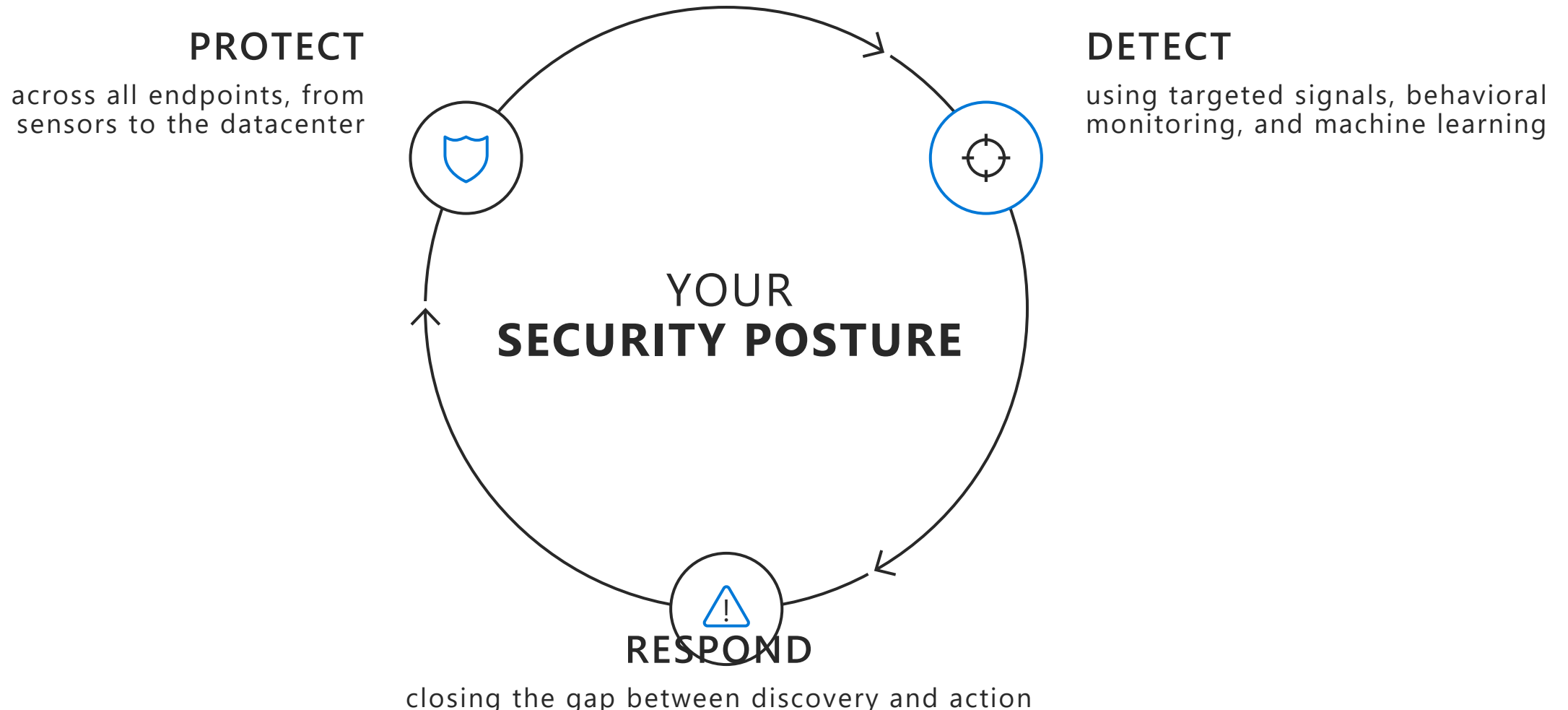
SANTA CLARA, Calif., Feb. 5, 2020 /PRNewswire/ -- Palo Alto Networks (NYSE: PANW), the global cybersecurity leader, today released research showing how vulnerabilities in the development of cloud infrastructure are creating significant security risks.

The [Unit 42 Cloud Threat Report: Spring 2020](#) investigates why cloud misconfigurations happen so frequently. It finds that as organizations move to automate more of their cloud infrastructure build processes, they are adopting and creating new infrastructure as code (IaC) templates. Without the help of the right security tools and processes, these infrastructure building blocks are being crafted with rampant vulnerabilities.

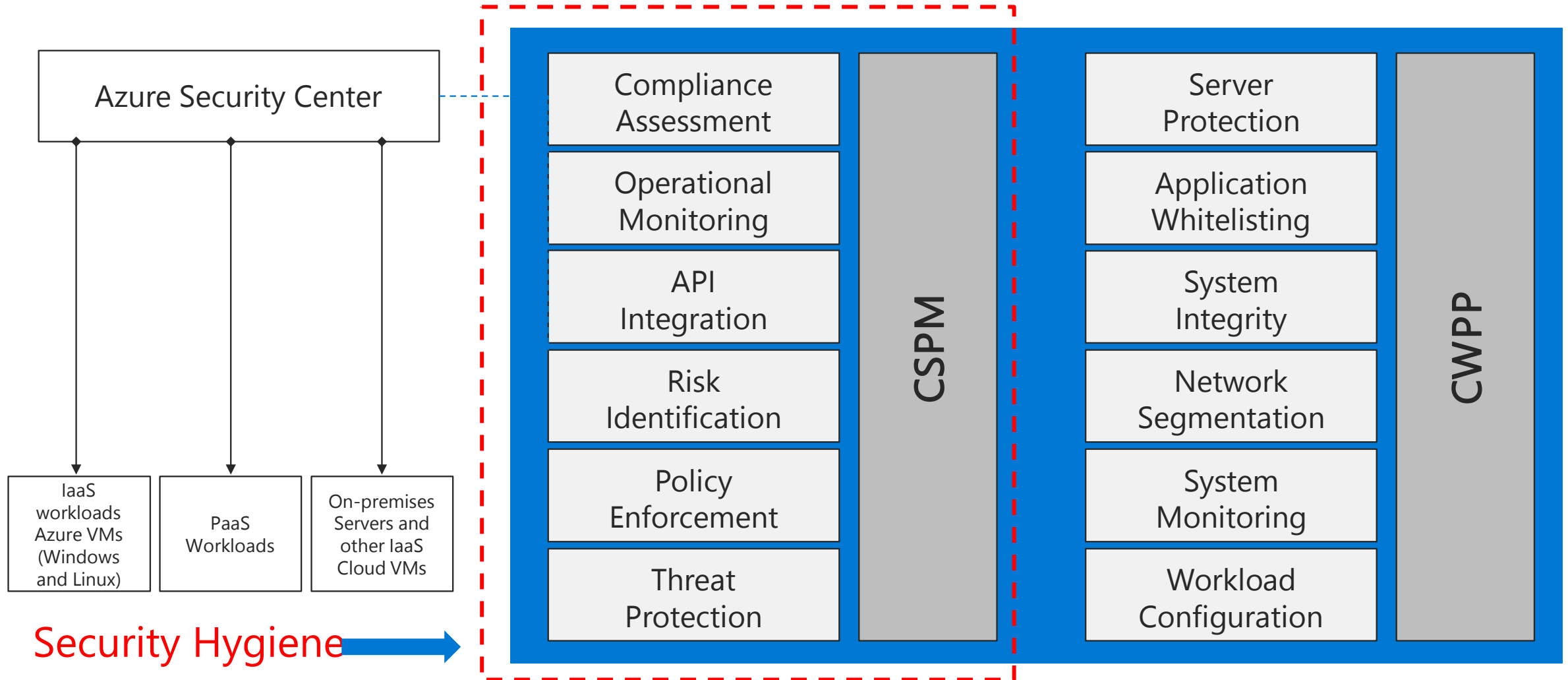
Key findings include:

- **199,000+ insecure templates in use:** Unit 42 researchers identified high- and medium-severity vulnerabilities throughout their investigation. [Previous research](#) by Unit 42 shows 65% of cloud incidents were due to simple misconfigurations. These new report findings shed light on why cloud misconfigurations are so common.
- **43% of cloud databases not encrypted:** Keeping data encrypted not only prevents attackers from reading stored information, it is a requirement of compliance standards, such as HIPAA.
- **60% of cloud storage services have logging disabled:** Storage logging is critical when attempting to determine the scale of the damage in cloud incidents, such as the U.S. voter records leak in 2017 or the National Credit Federation data leak that same year.
- **Cybercrime groups are using the cloud for cryptojacking:** Adversary groups likely associated with China, including Rocke, 8220 Mining Group and Pacha, are stealing cloud resources. They are mining for Monero, likely through public mining pools or their own pools.

Improve your defense against threats by enhancing your security posture



Cloud Security Posture Management (CSPM) + Cloud Workload Protection Platform (CWPP)



Azure Security Center



Strengthen security posture

Cloud security posture management

Secure Score
Policies and compliance



Protect against threats

For
servers

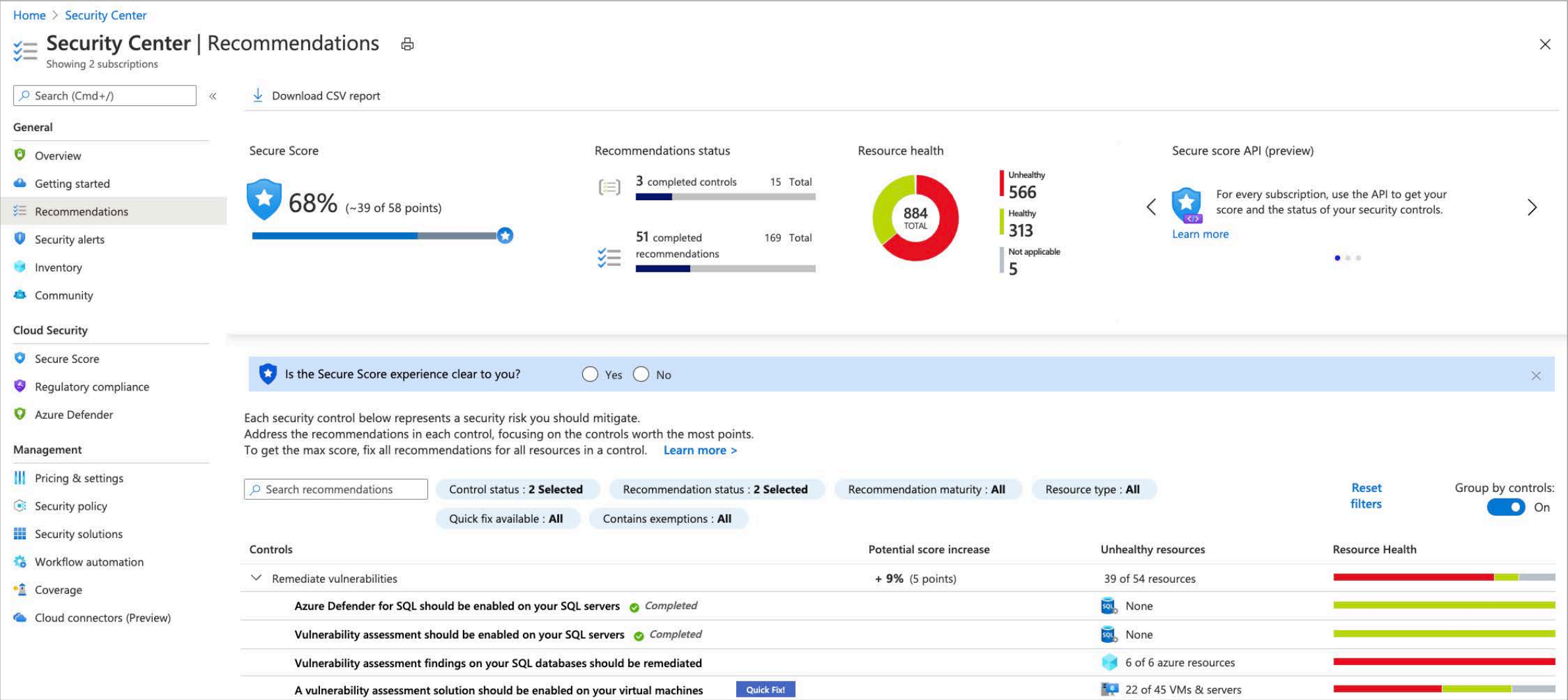
For cloud native
workloads

For
databases
and storage



Get secure faster

Secure Score and recommendations

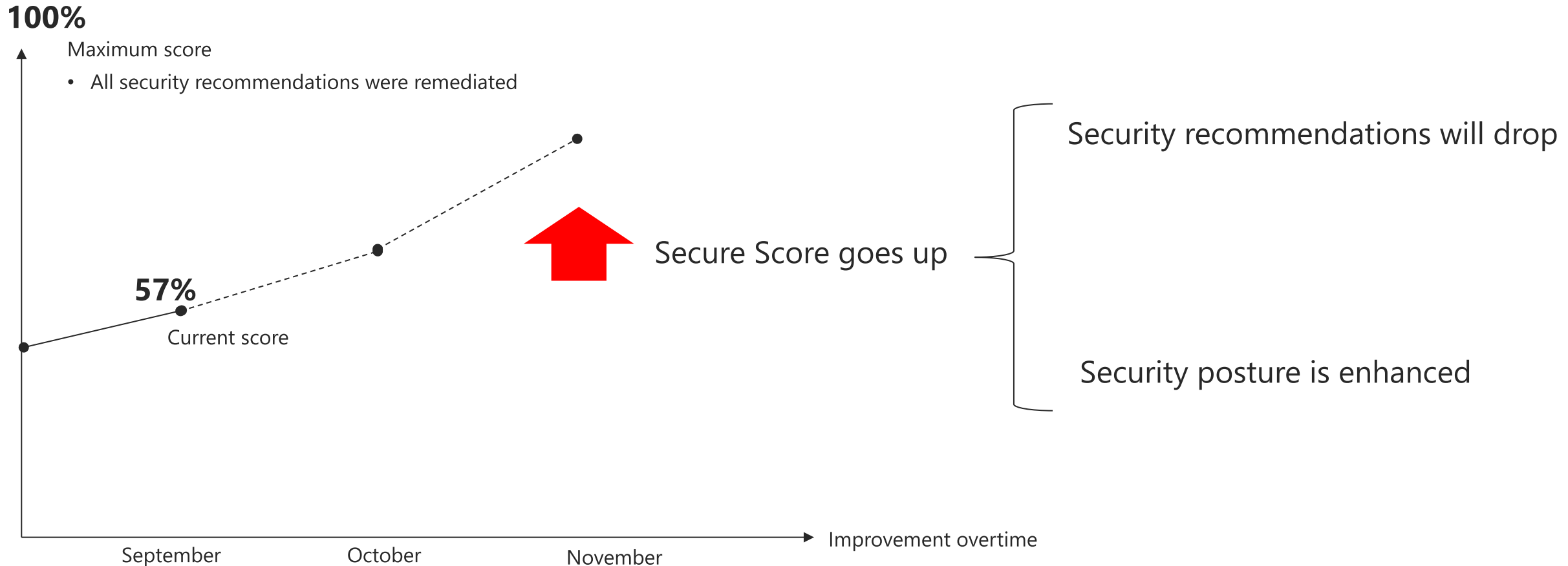


Secure Score controls

Control	Max Score
Enable MFA	10
Secure management ports	8
Apply system updates	6
Remediate vulnerabilities	6
Enable encryption at rest	4
Encrypt data in transit	4
Manage access and permissions	4
Remediate security configurations	4
Restrict unauthorized network access	4
Adaptive application control	3
Apply data classification	2
Enable DDoS protection on Vnet	2
Enable endpoint protection	2
Enable auditing and logging	1
Additional best practices	0

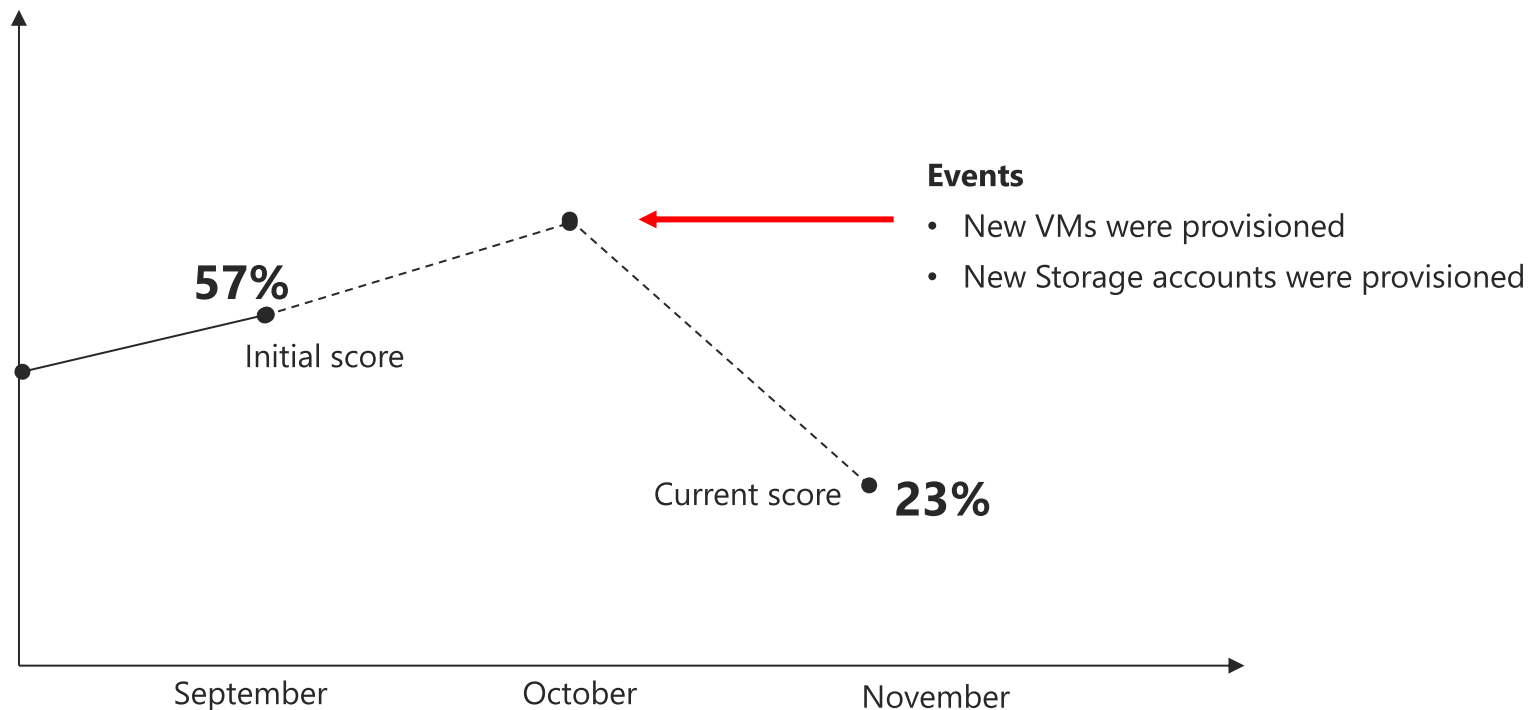
- The max score reflects the importance to solve the misconfiguration
- The overall max score is 60 points, if you have 60 points -> 100% score *
- The more you remediate, the higher your score -> your environment is more secure
- * The max score of 60 points might not appear in all environments

Use Secure Score as your Security KPI

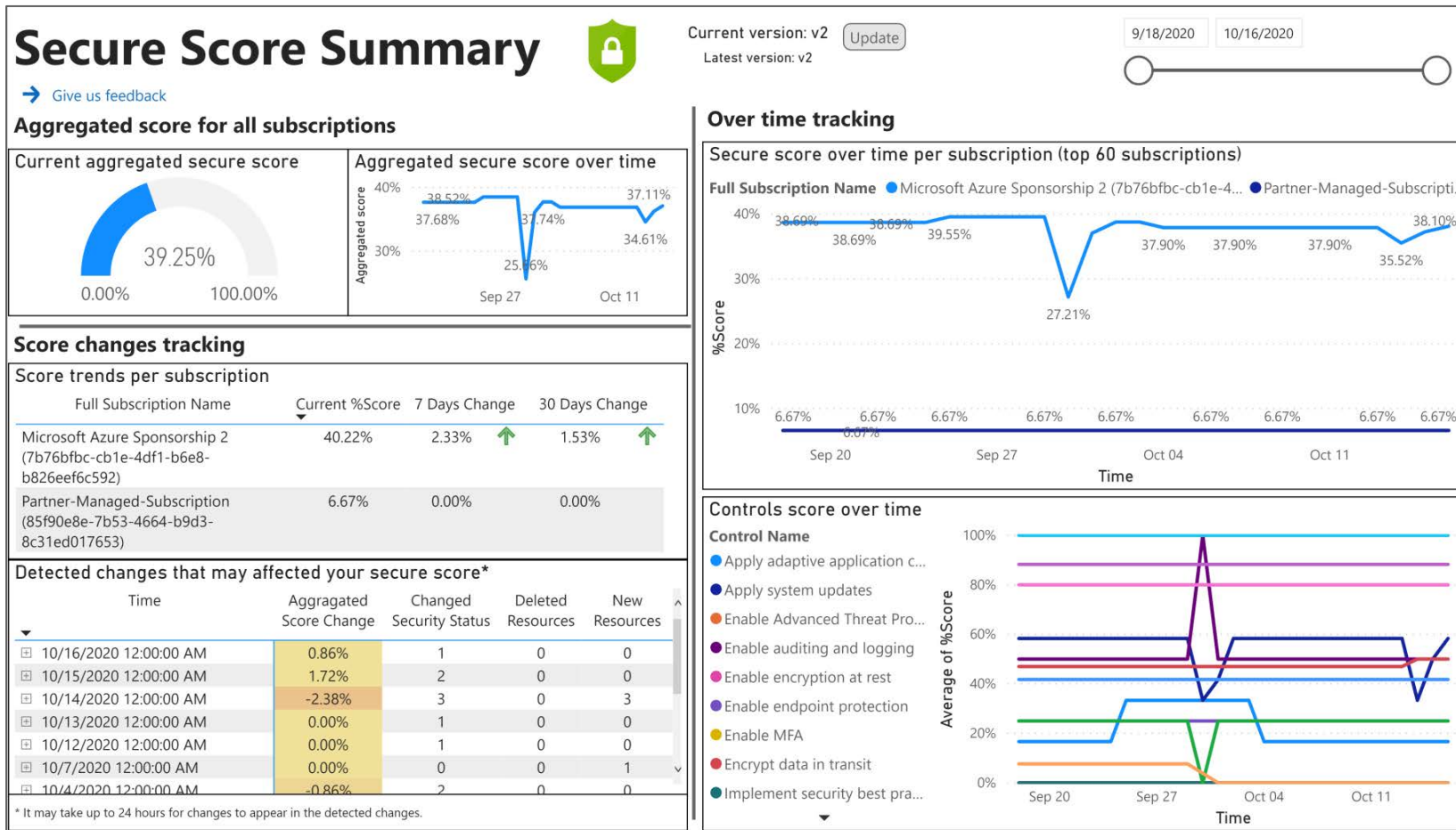


The importance of Azure governance

- Without governance your secure score will drop once you provision new resources that are not secure by default



Secure Score over time



<https://github.com/Azure/Azure-Security-Center/tree/master/Secure%20Score/PowerBI-SecureScoreReport>

Policy Enforcement



1

Ensure compliance

2

Empower DevOps

Code

Build/Test

Policy as Code

Pre-flight

Validation

Authoring

Deploy

Operate



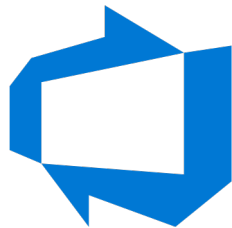
Policy



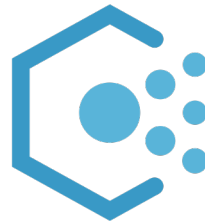
Security



Monitoring



Azure DevOps



Azure Policy

The new security dashboard New!

Updated user experience

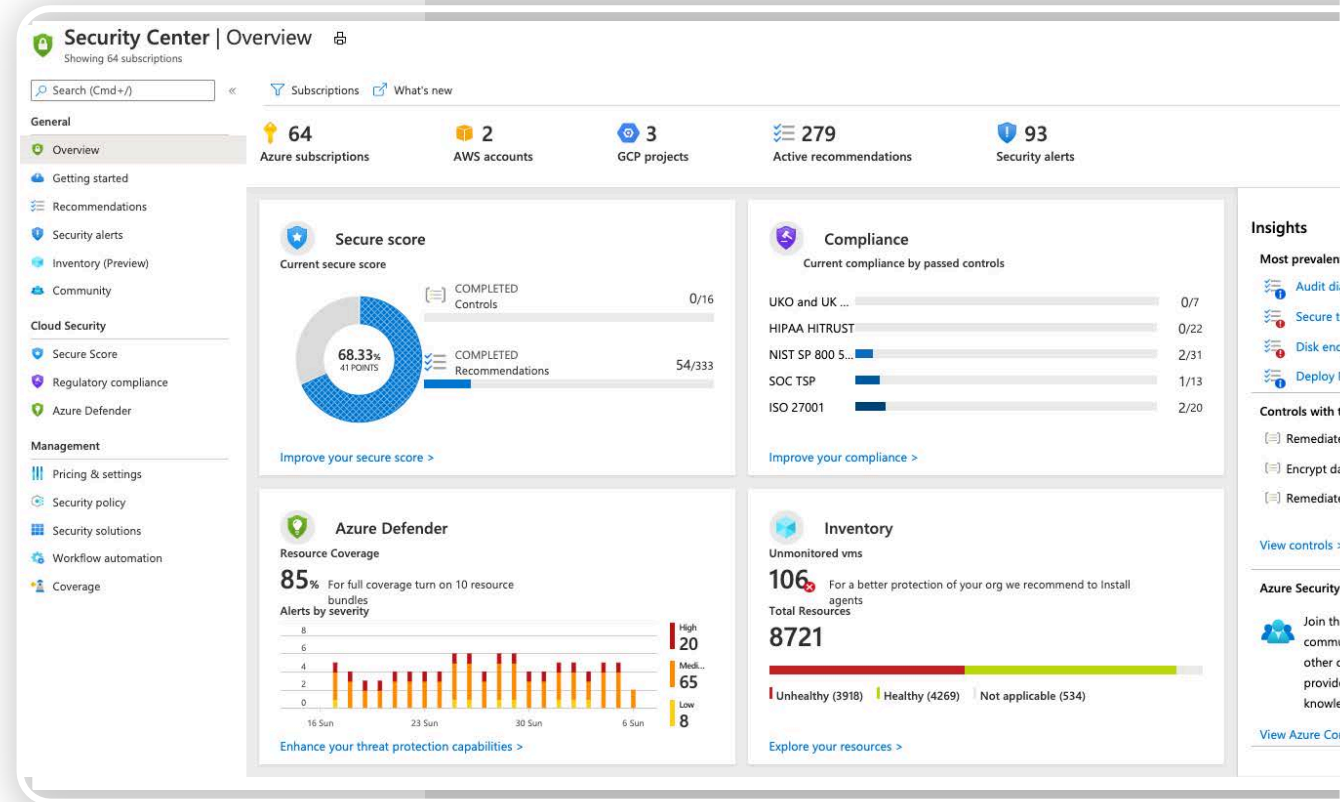
Unified view of all your cloud resources: in Azure, on premises and in other clouds

Focused views for security posture, compliance and Azure Defender

Clear & simple view

Identify all your security related stats at a glance

Emphasis on visibility & clear KPIs



CSPM enhancements

Asset Management - Improved visibility across the entire estate

New!

Now Generally Available

Single view of all monitored resources

- Resource centric view

Easy filtering, sorting and cross-referencing experience

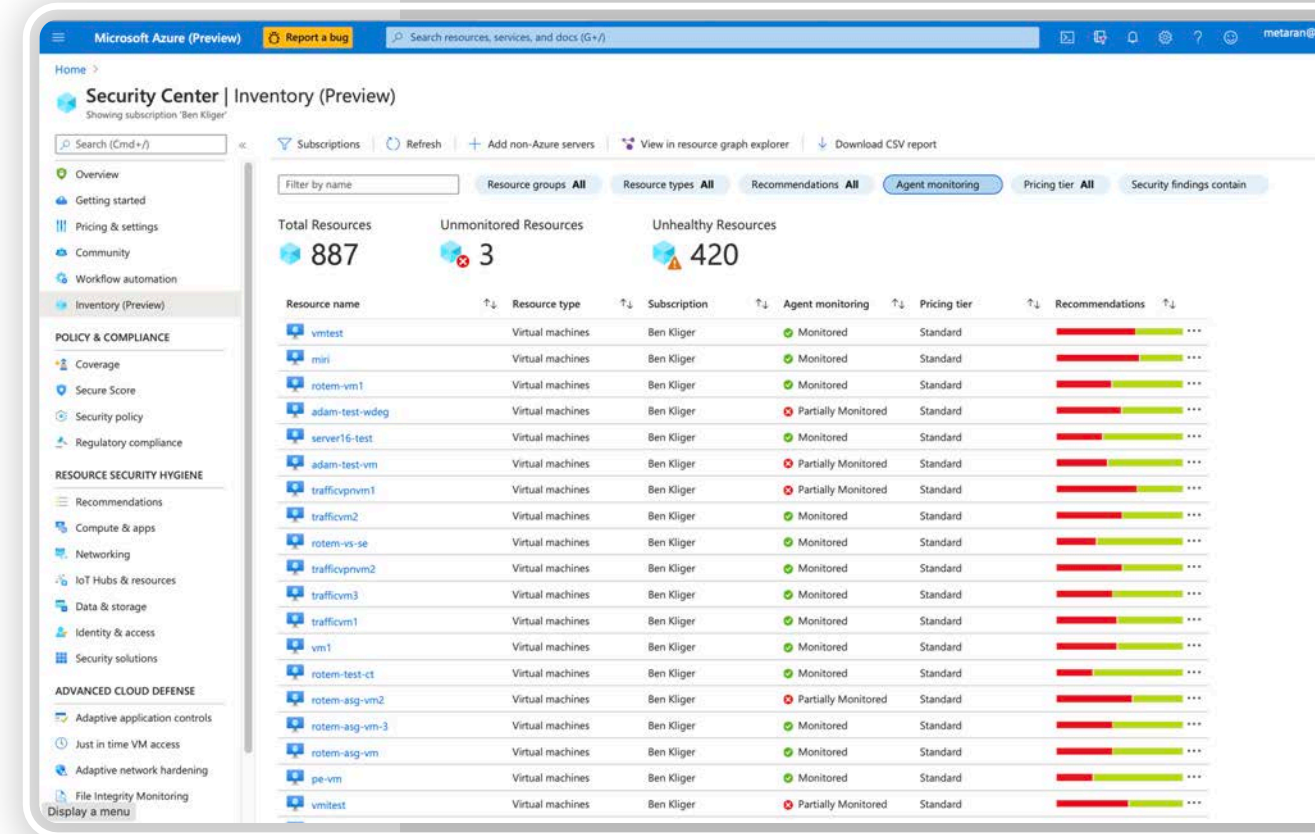
- Filter by resource properties (tags, RG)
- Filter by security posture (recommendations, specific vulnerabilities)
- Filter by status & coverage (pricing, agent status)

Continue exploration & export

- Export to CSV
- Continue exploration in Azure Resource Graph
- Build reports, Azure workbooks, etc.

Management

- Assign tags



Refined security posture management

Now in Public Preview

New!

Greater granularity for policy management and Secure Score

- **Exempt resources** from recommendation & Secure Score
- Exempt resources from regulatory compliance
- Keep track of exempted resources and exemption reason
- **Disable security findings** by ID or by different categories
- Built in governance capabilities for control

Find automation examples at

- <https://aka.ms/ASC-RequestResourceExemption>
- <https://aka.ms/ASC-NotifyResourceExemption>

Create Exemption (Preview)

1 resource

You can exempt a resource so that it doesn't affect your secure score. The resource's status will change to not applicable.

Exemption scope

Name

centralus-local-sec

Exemption details

Name *

ASC-centralus-local-sec-diagnosticsLoginRedisCacheMoni

Edited By

metaran@microsoft.com

Justification category * ⓘ

☒ Mitigated

☐ Waiver

Justification details (optional) ⓘ

mitigated by a 3rd party solution approved by the admin

Save

Cancel

Cloud security management at scale

ASC CSPM platform is extensible with standard operational tools and interfaces

Create custom policies or import from GitHub

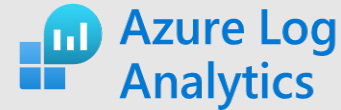
Adjust Secure Score with custom policies

Automate remediation with built in remediation scripts and ARM templates

Deploy LogicApp templates to automation scenarios (remediation, connect to ITSM solutions, notify owner)

Build reports for overtime tracking using API samples and OOTB logic apps.

Query your security posture directly from Azure Resource Graph

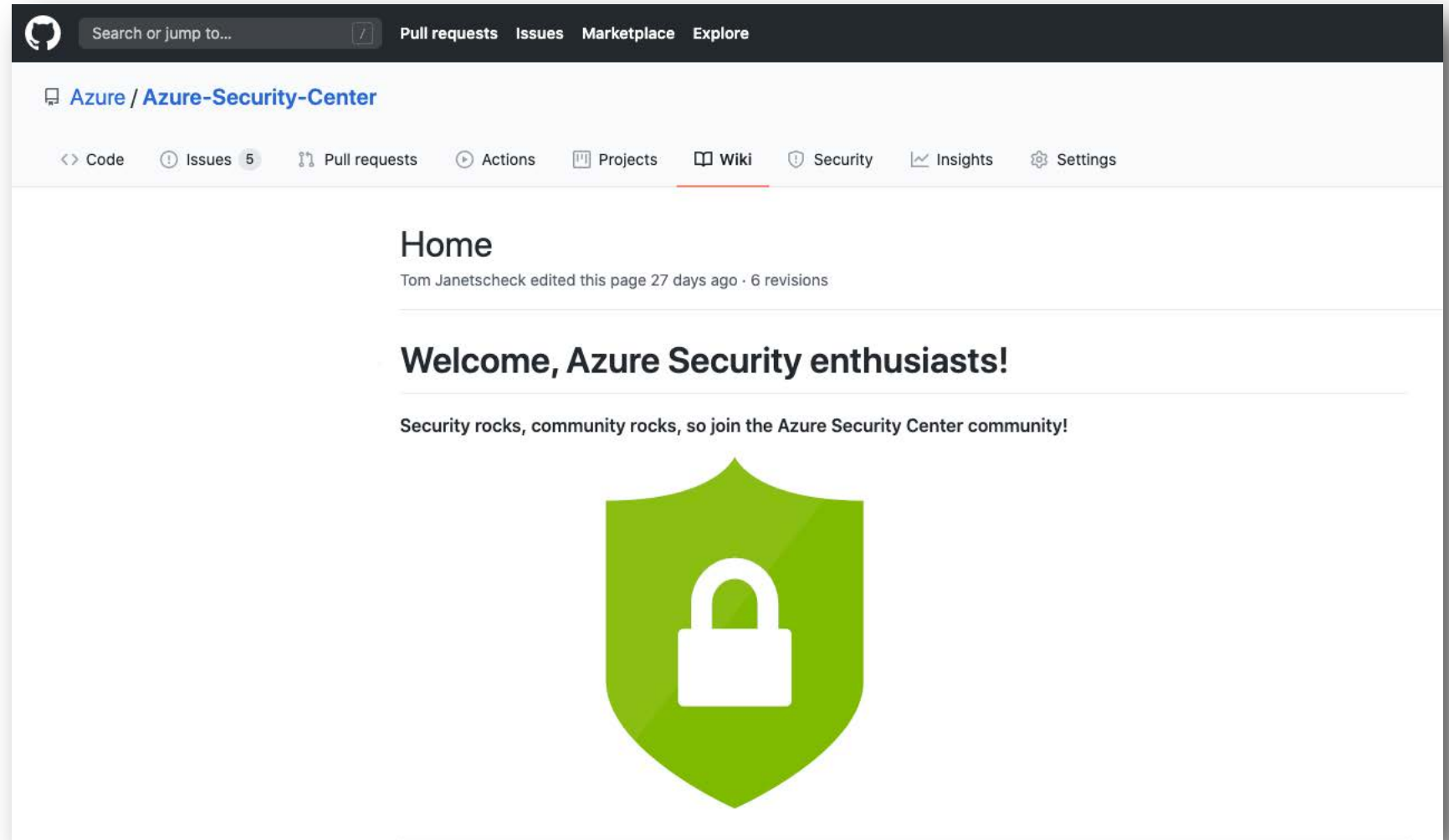


Join the ASC GitHub community

Our [GitHub repo](#) is deeply integrated with ASC portal

Place for publishing tools and automation artifacts, such as Policy Templates, LogicApps, PowerShell scripts, that enable governance and remediation at scale

Visit <https://aka.ms/ASC-Github> for more details.





Demo

Azure Security Center



Strengthen security posture

Cloud security posture management

Secure Score
Policies and compliance



Protect against threats

For
servers

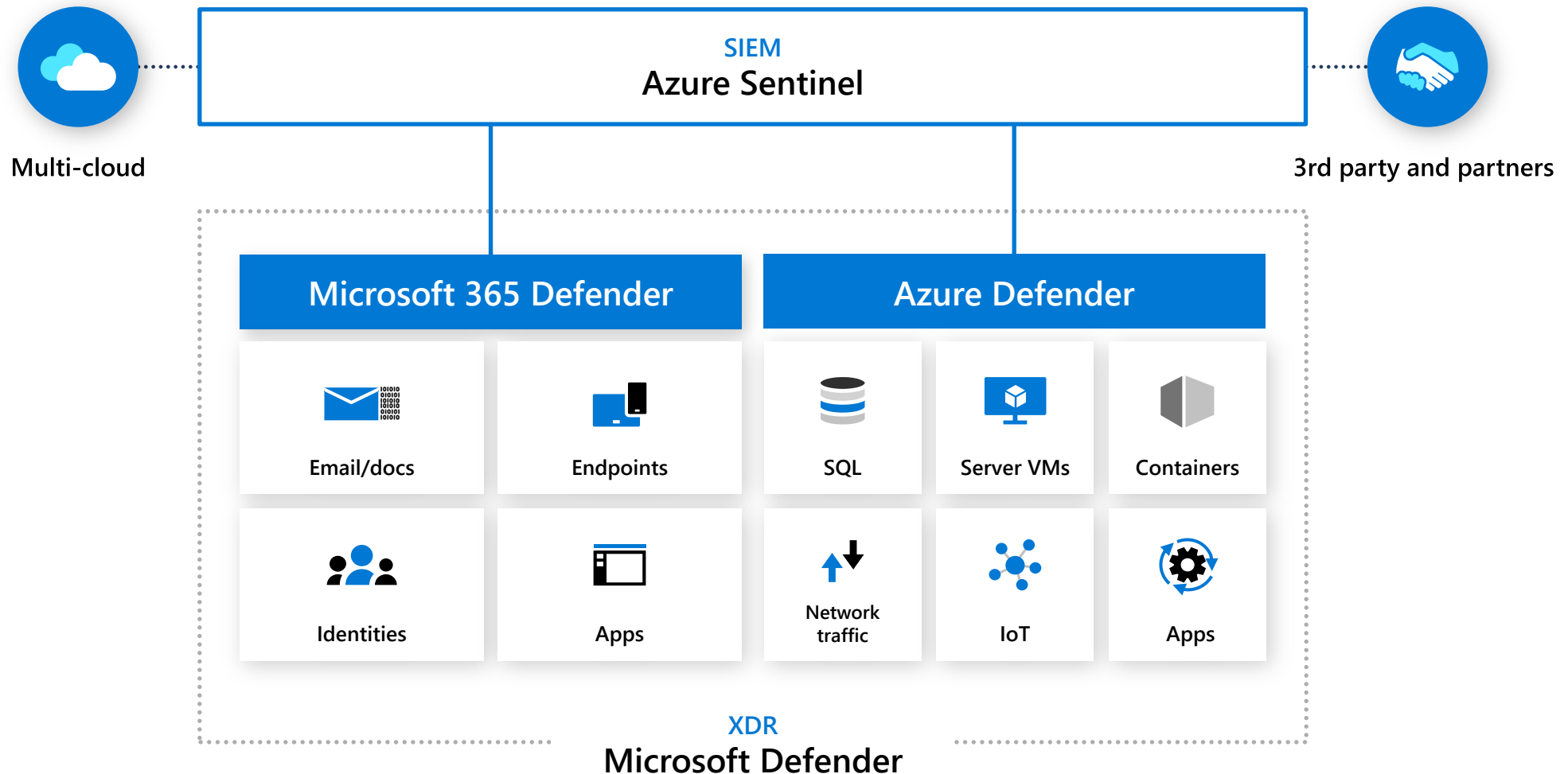
For cloud native
workloads

For
databases
and storage



Get secure faster

Integrated threat protection for your enterprise



Azure Defender new dashboard

New!

Protects hybrid workloads

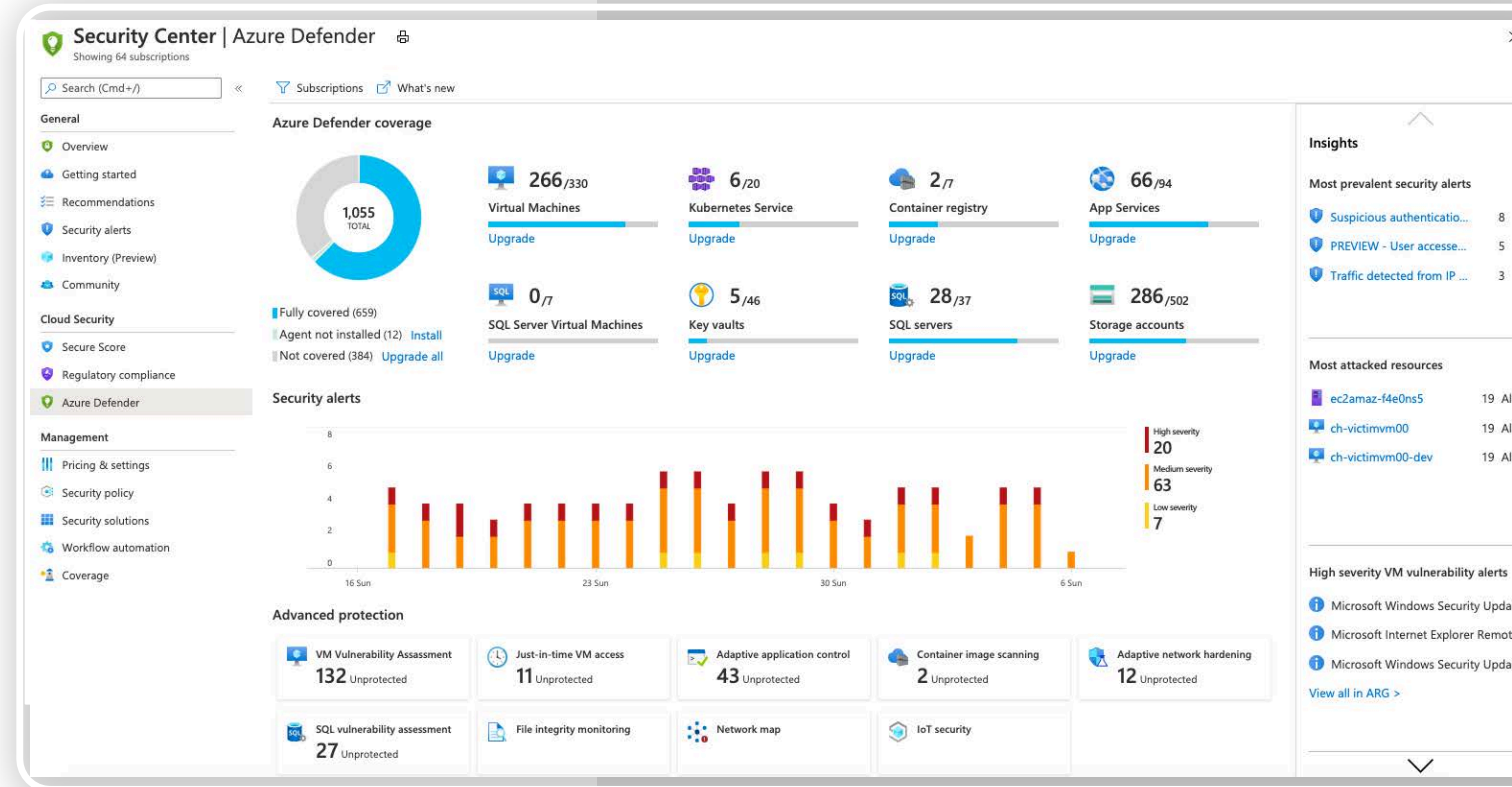
Server and container protection

Seamless integration for Azure Arc

Protects Azure services

Data services protection

App services and key vaults



Introducing Multi-cloud in Azure Security Center

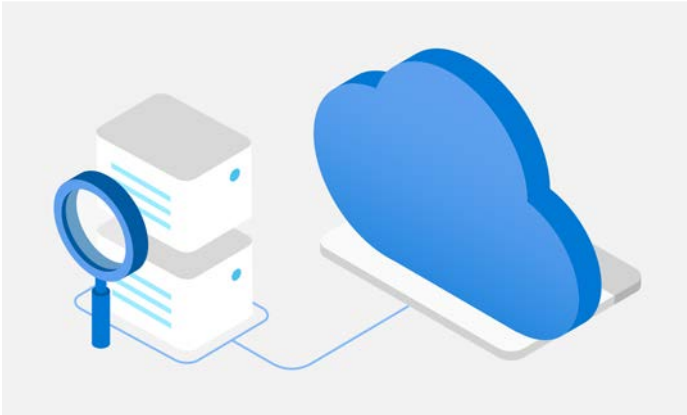


Azure Arc

Azure services & management capabilities on any infrastructure, anywhere

1

Azure Arc for servers



Organize and govern servers across environments

Azure Arc extends Azure's management to physical and virtual servers anywhere. Govern and manage servers from a single, scalable management pane.

2

Azure Arc for Kubernetes

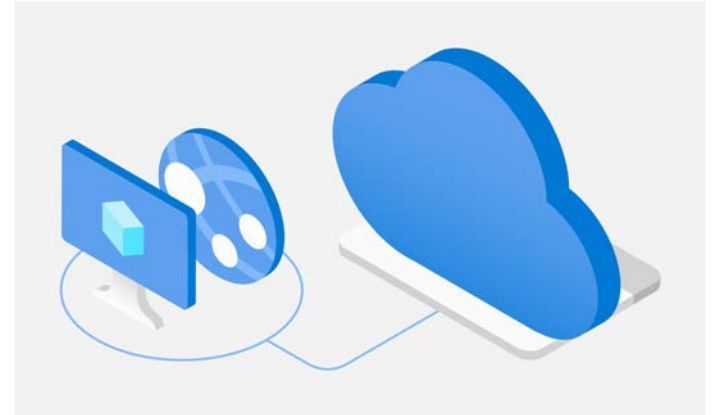


Manage Kubernetes applications at-scale

Deploy and configure Kubernetes applications consistently across all your environments with modern DevOps techniques.

3

Azure data services on Azure Arc



Run data services anywhere

Deploy Azure data services in moments anywhere you need them. Get simpler compliance, faster response times, and better security for your data.

Deploy Azure Defender anywhere with Azure Arc

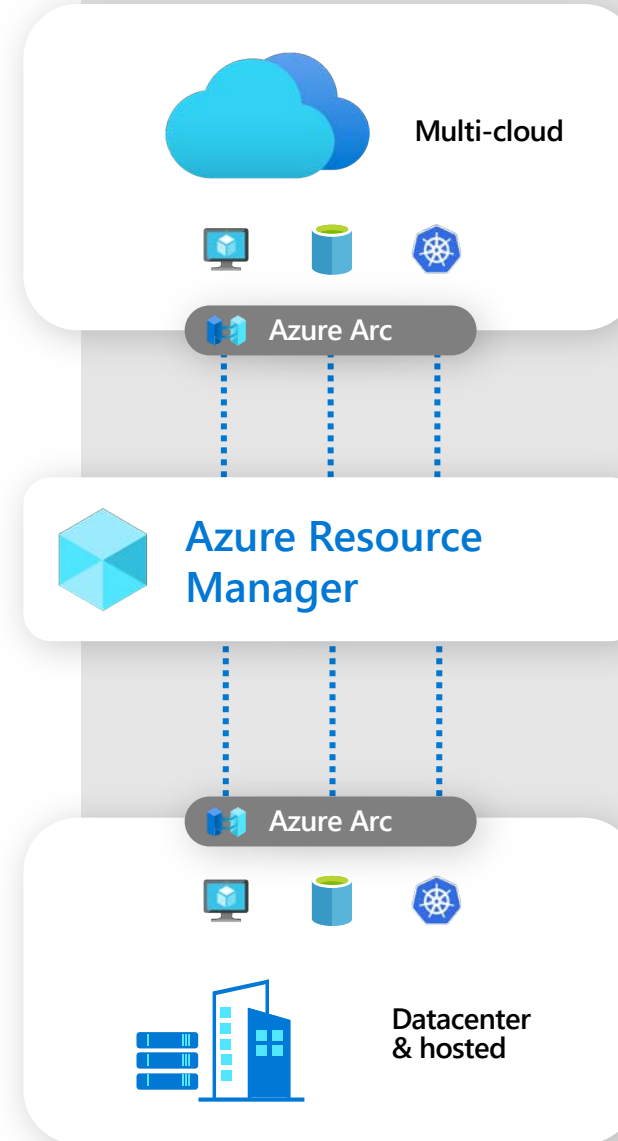
Extension installation, e.g. Log Analytics agent, Qualys

Enforce compliance and simplify audit reporting

Identified as an Azure resource

Asset organization and inventory with a unified view in the Azure Portal – Azure Tags

Server owners can view and remediate to meet their compliance – RBAC in Azure






Azure Arc enables cloud management and security protections

Single Control Plane for any resource, anywhere

Multi-cloud & hybrid protection in ASC



 Security posture & compliance	Secure score	Asset management	Policy
 Server protection (Azure Defender for VMs)	Threat detection	VA (powered by Qualys)	Application control
 Automation & management at scale	Automation	SIEM integration	Export

Summary

Azure Security Center



Cloud security posture management
ASC free tier



ASC free tier



Cloud workload protection
ASC standard tier (paid)



Azure Defender (paid)

Azure Security Center



Strengthen multi cloud security posture

Secure Score

Policies and compliance

Improved automation



Leveraging
Azure Arc



Protect your hybrid cloud with Azure Defender

For servers

For cloud native workloads

For databases and storage

For Azure service layers

For IoT devices



Streamline security management

Take actions today

Get started with the preview



Enable Security Center
to assess your secure score across the
entire organization



Act upon your top
5 recommendations today



Enable Azure Defender to maximize
security value

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

