

# Azure Security Center

Rising costs



Increasing complexity



The security landscape



Evolving threats

By 2021, 25% of the world's personal data will be compromised and housed in a Data Lake analyzed and utilized by consortiums of Threat Actors\*

Nine in ten have real concerns about security risks due to misconfiguration, and less than a third continuously monitor for them. \*\*



Intelligent Edge



Talent gap

\*Source: [IDC FutureScape: Worldwide Security Products and Services](#)

\*\* Source: [IDC FutureScape: Worldwide Security Products and Services](#)

Unmatched security across operations, technology, and partnerships

---

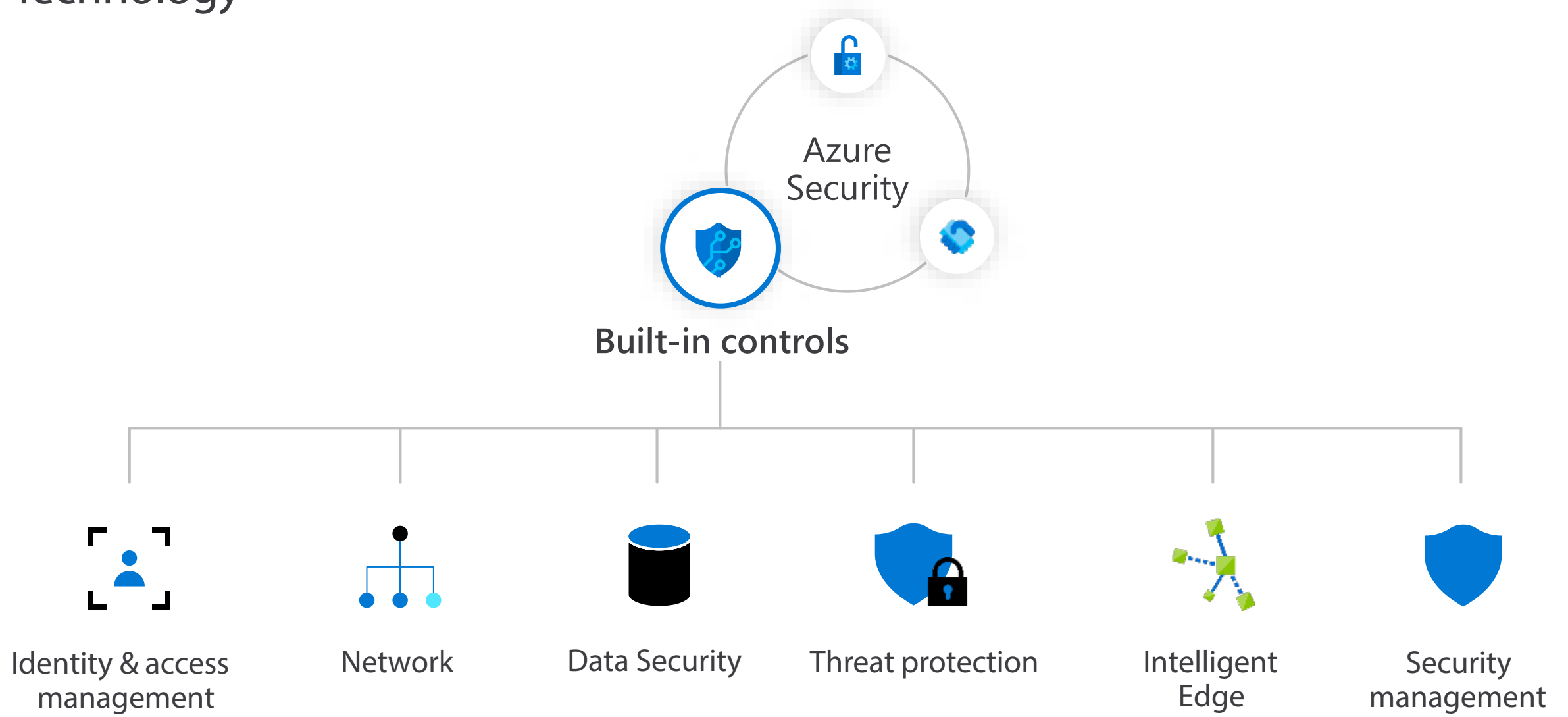
\$1B annual investment in cybersecurity

3500+ global security experts

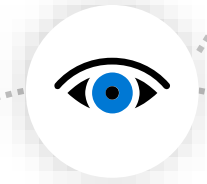
Trillions of diverse signals for unique intelligence



# Technology



Visibility into security and compliance



Without security controls in place, **68%** of breaches take months or longer to discover.

## Cloud security challenges



Insecure configurations



Increase in number and sophistication of attacks



With cyber attacks on the rise, successful breaches per company each year has risen more than **27%**, from an average of 102 to 130.\*\*

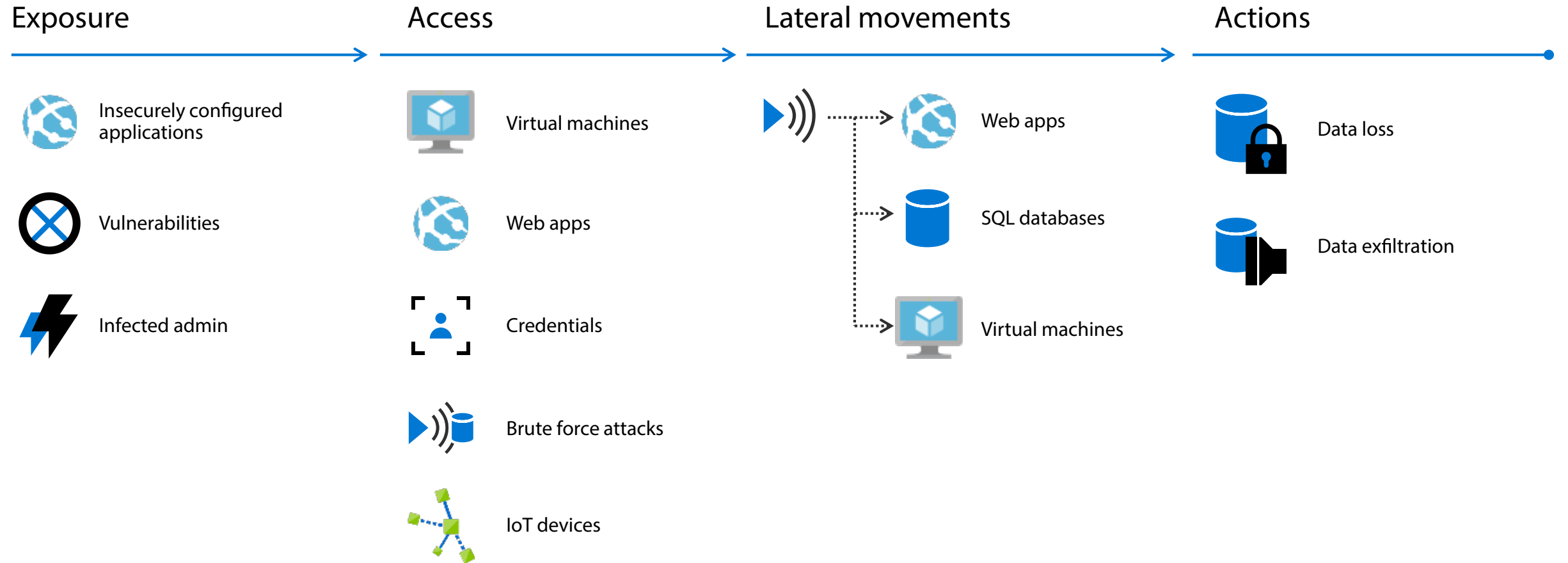
Forbes  
.COM

“Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities”\*

\*Source: [The One Cloud Security Metric Every CISO Should Know](#), Forbes

\*\*Source: Ponemon: 2017 Cost of Cybercrime Study

# The cloud kill chain model



# Azure Security Center



## Strengthen security posture

Cloud security posture management  
Secure Score | Policies and compliance



## Protect against threats

For servers

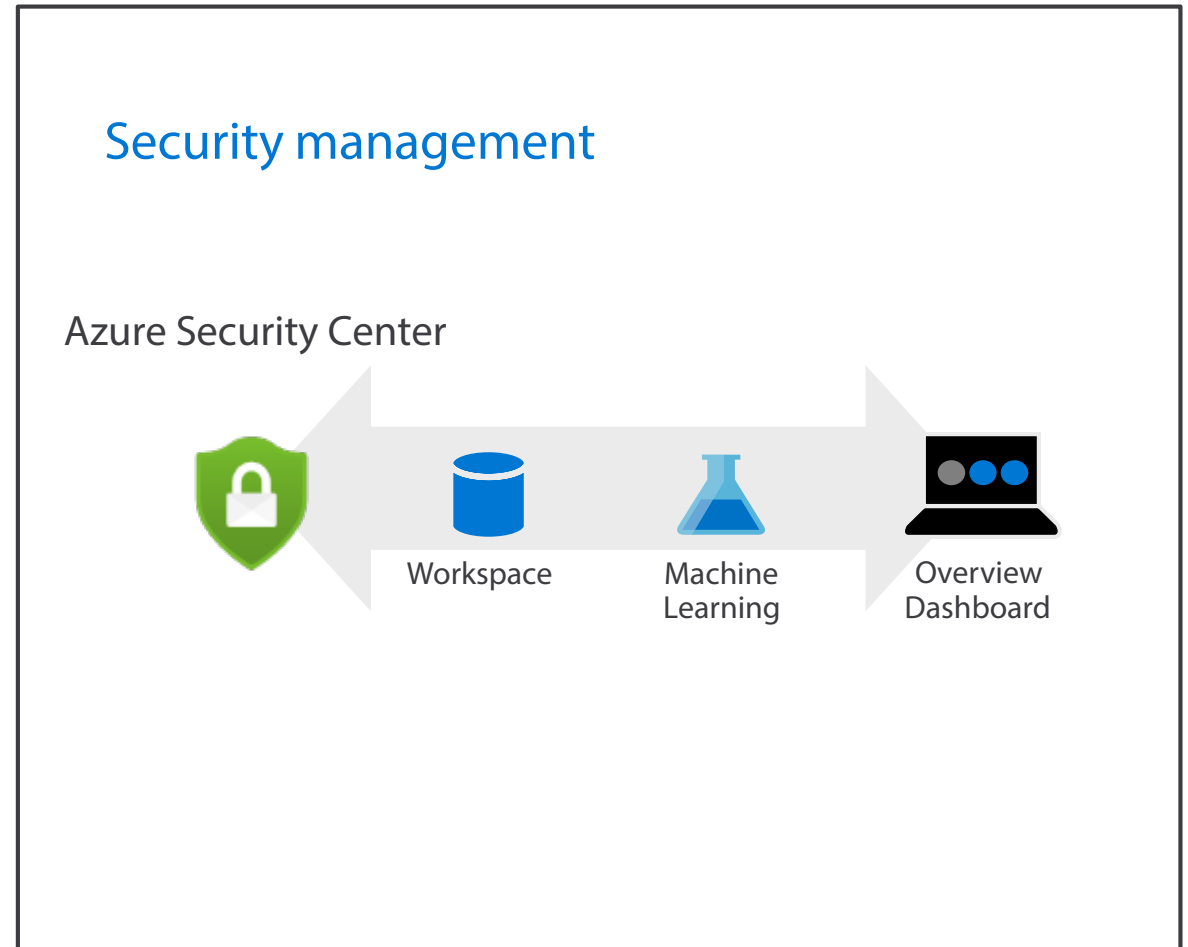
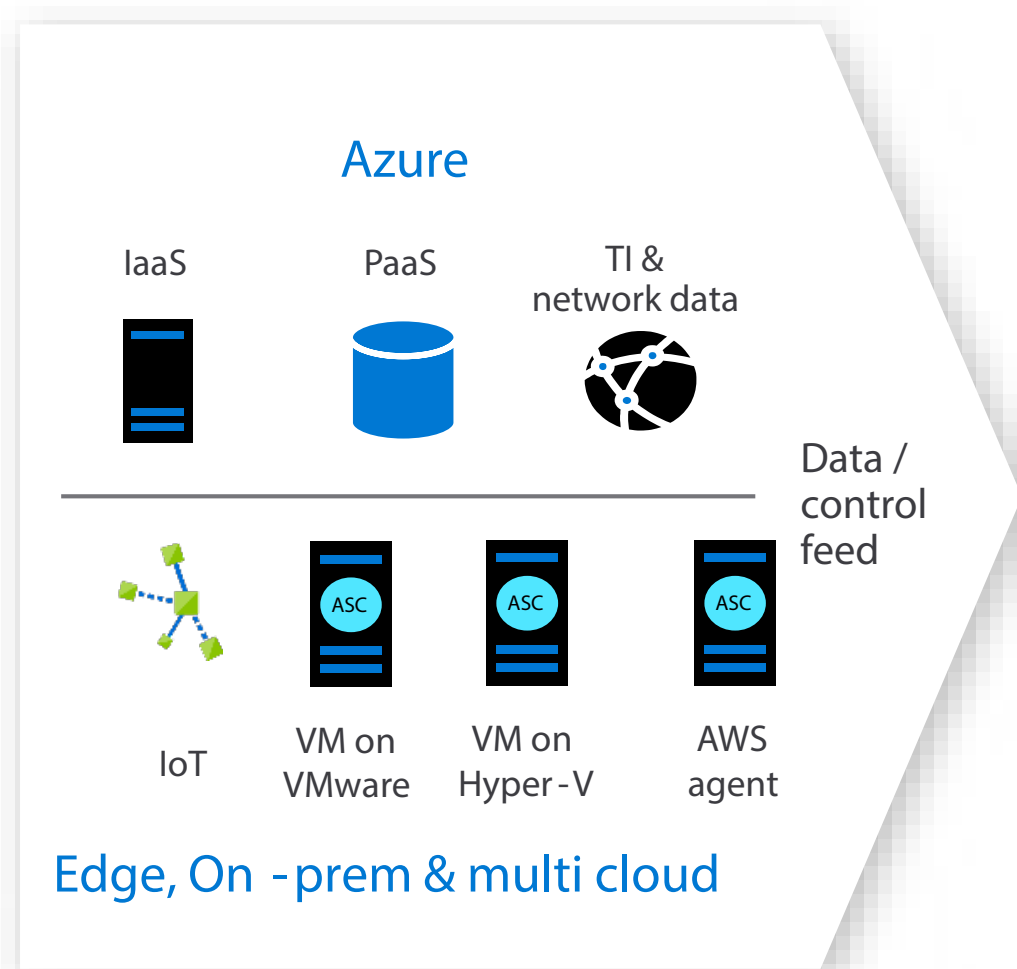
For cloud native workloads

For databases and storage



Get secure faster

# Azure Security Center Architecture





# Azure Security Center



## Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Improved Automation



## Protect against threats

For servers

For cloud native workloads

For databases & storage

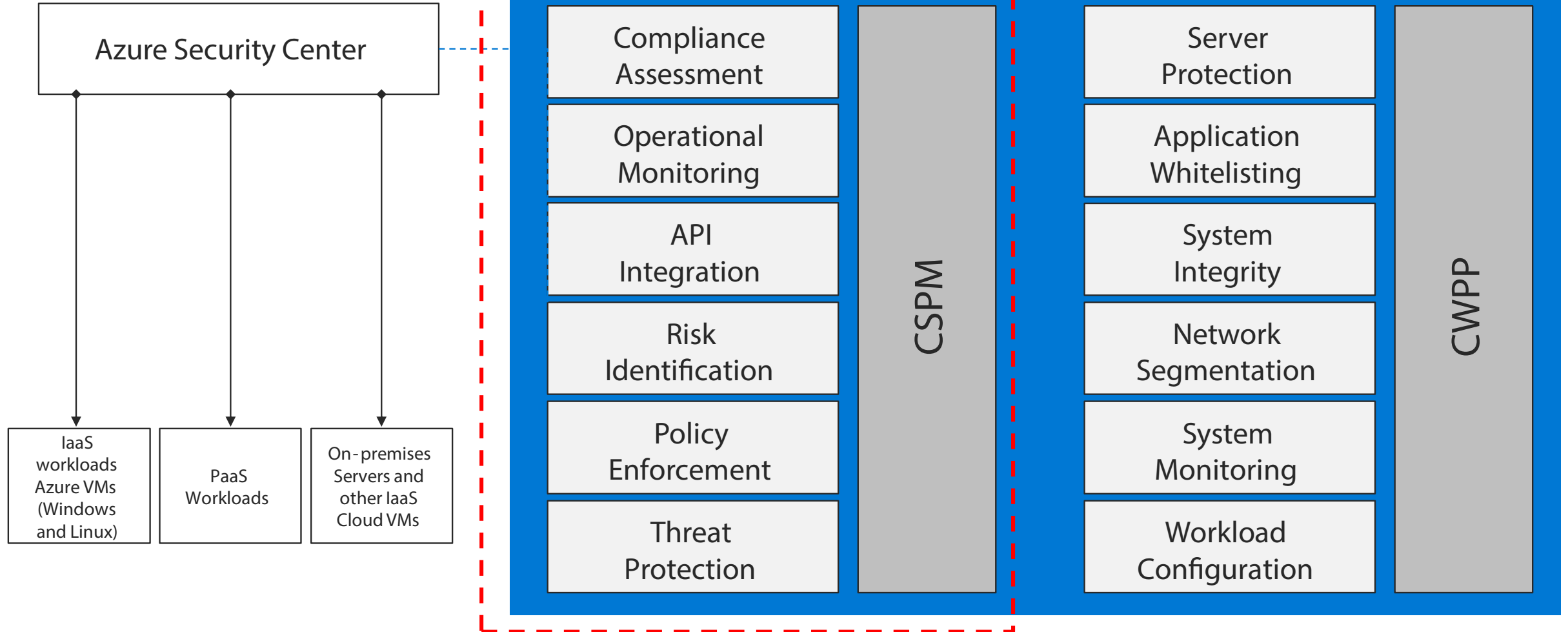
For IoT devices



Get secure faster

# CSPM + CWPP

Security Hygiene



# Security posture management with Secure Score

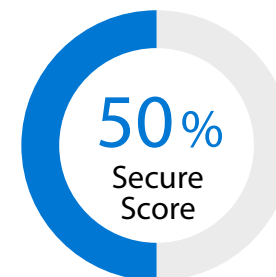
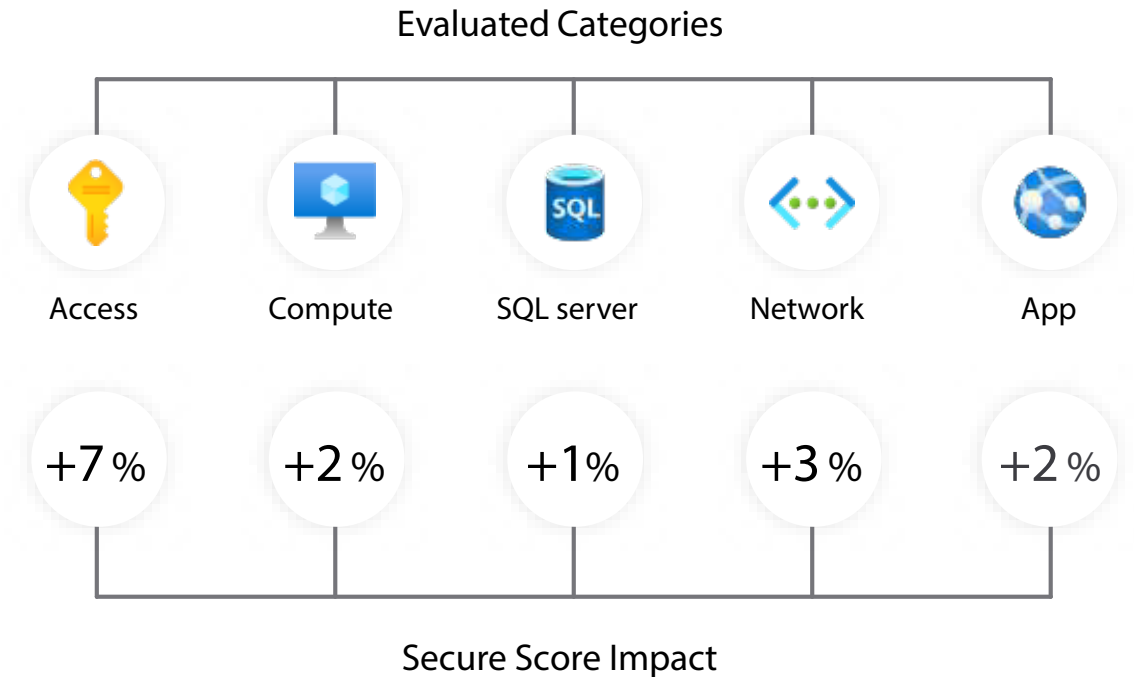


Gain instant insight into the security state of your cloud workloads

Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

Speed up regulatory compliance





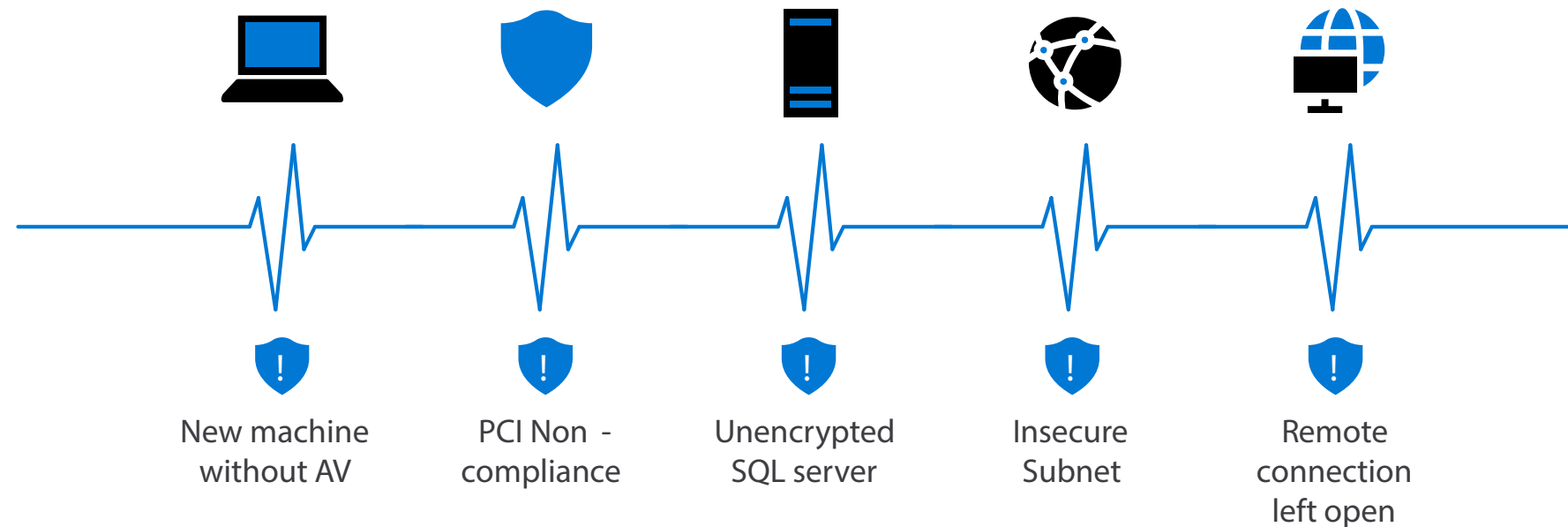
# Manage organizational security policies and assess compliance in minutes

Manage security policies at an organizational level

Easily set security policies for subscriptions or management groups

Instantly understand your current policy compliance and review compliance overtime

## Highly Dynamic Environment



# Improved Automation

Apply Quick Fixes to recommendations

Automate responses with LogicApps

Continuously export to Event Hub and Log Analytics

Export to CSV



# Extend, customize, and share your organizational policy



Create your own  
organizational policy

Pick and choose from  
built-in standards

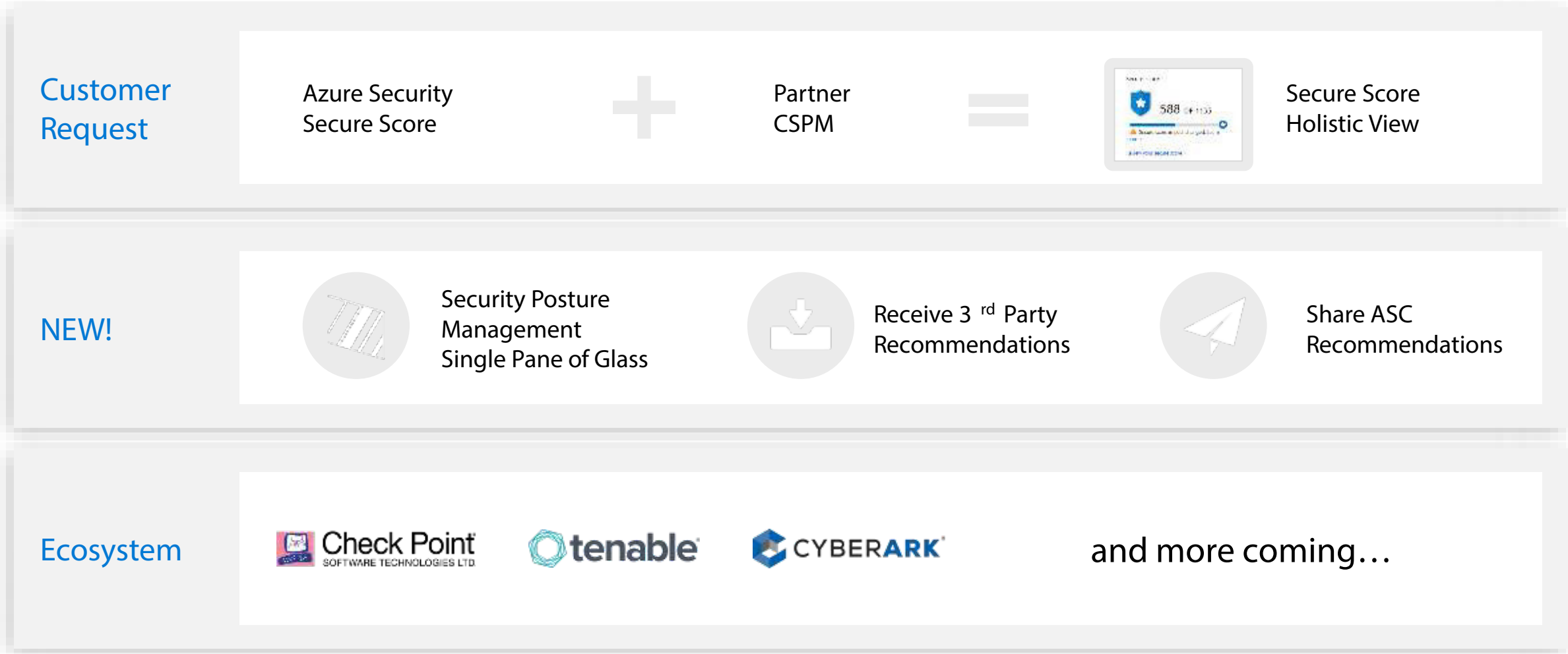


Write your own  
recommendations + apply  
custom score  
to it



Share with the  
ASC Community

# Growing ASC Ecosystem with Microsoft Intelligent Security Association





# Strengthen your cross -cloud cloud security posture

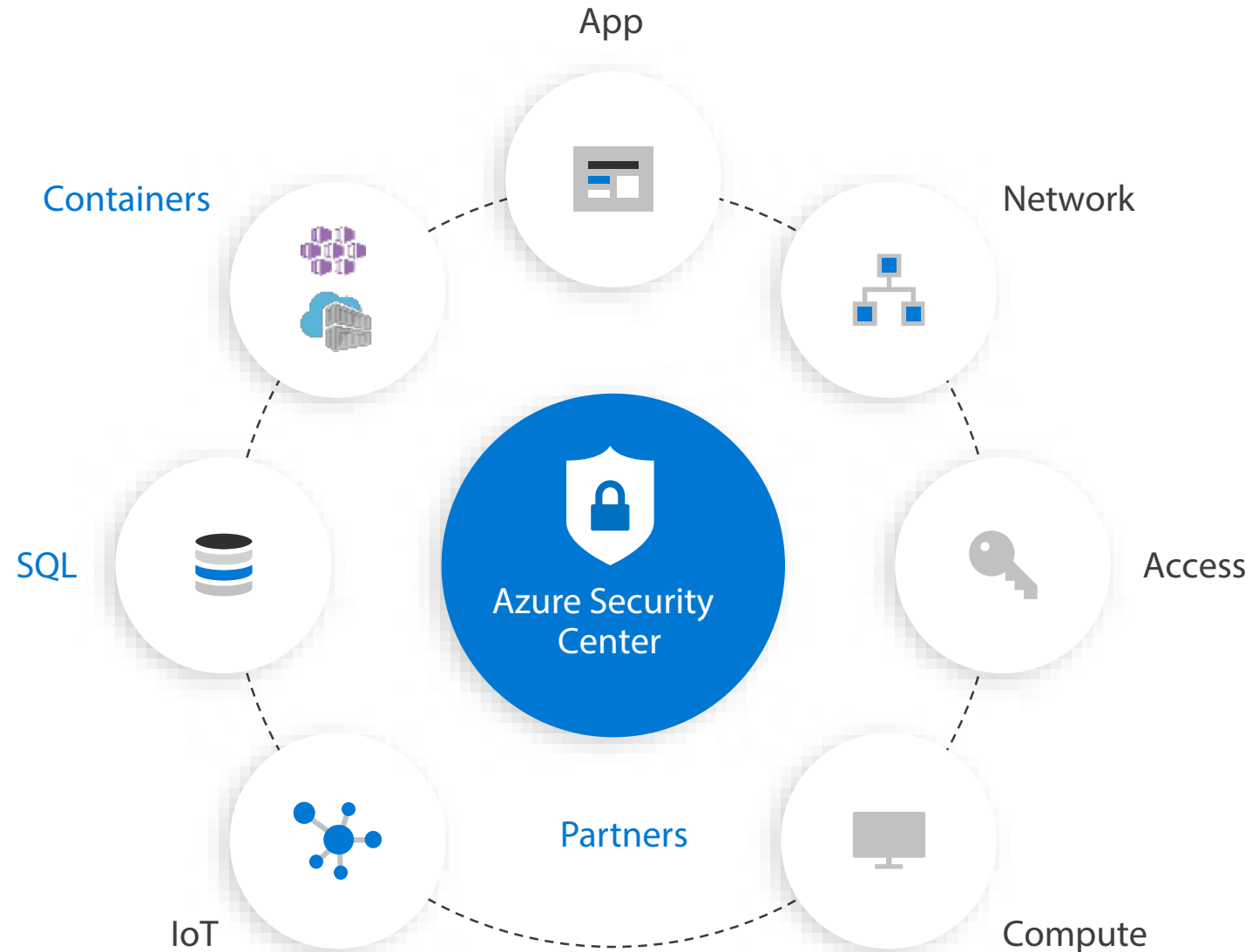
## Industry leading coverage

Get a bird's eye security posture view

Continuously monitor and protect all your cross -cloud resources

Follow best practice recommendations

Get visibility into the compliance state of your Azure environment





# Azure Security Center



## Strengthen security posture

Cloud security posture management and Azure IoT

Secure Score

Security policies and compliance



## Protect against threats

For servers

For cloud native workloads

For databases & storage

For IoT devices



Get secure faster

# Protect Linux and Windows servers from threats

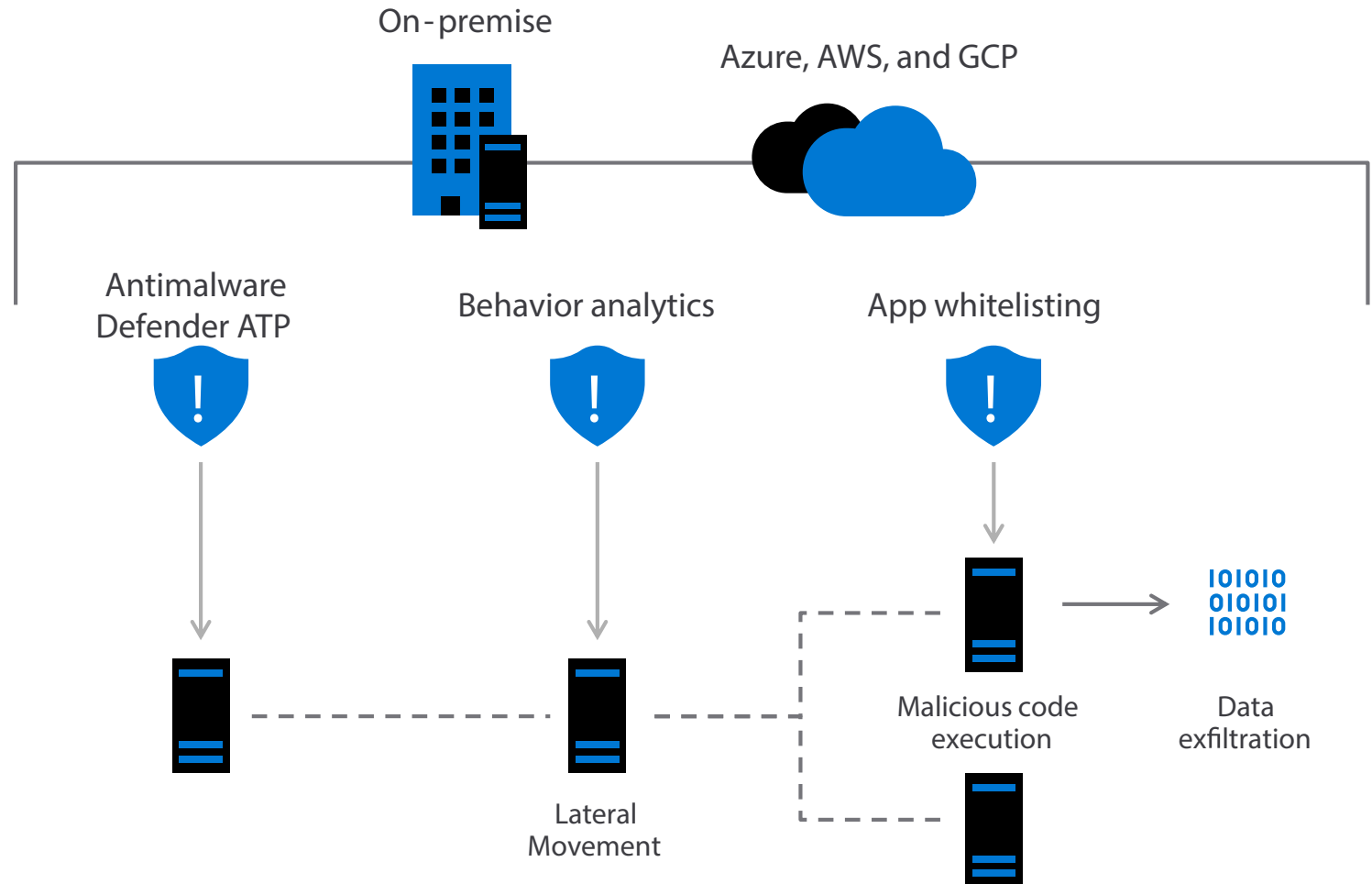


## Reduce open network ports

- Use Just-in-Time VM to control access to commonly attacked management ports
- Limit open ports with adaptive network hardening

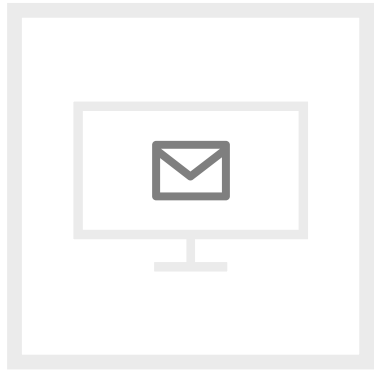
## Block malware with adaptive application controls

Protect Windows servers and clients with the integration of Microsoft Defender ATP and Linux servers



# Example of built-in analytics and machine learning

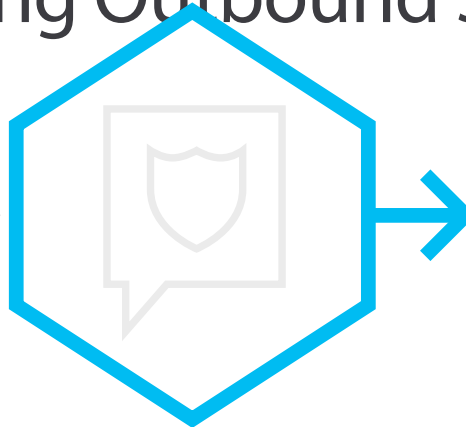
## Azure Security Center detecting Outbound SPAM



An attacker gains access to a VM and begins to send spam emails.



Security Center machine learning detects a spike in SMTP traffic.



Traffic is correlated with O365 SPAM database to determine if the traffic is likely legitimate or not.

Possible outgoing spam activity detected  
VM1LIN1

DESCRIPTION	Network traffic analysis detected suspicious outgoing traffic from VM1LIN1. This traffic may be a result of a spam activity. If this behavior is intentional, please note that sending spam is against Azure Terms of service. If this behavior is unintentional, it may mean your machine has been compromised.
DETECTION TIME	Saturday, July 9, 2016 7:27:15 AM
SEVERITY	<span>Low</span>
STATE	Active
ATTACKED RESOURCE	VM1LIN1
DETECTED BY	<span>Microsoft</span>
ACTION TAKEN	Detected
COMPROMISED HOST	VM1LIN1

Azure Security Center triggers an alert.



# Turn on built-in vulnerability assessment for VMs

Available as part of Azure Security Center Standard VM pricing, no extra charge

Automated deployment of the vulnerability scanner

Continuously scans installed applications to find vulnerabilities for Linux & Windows VMs

Visibility to the vulnerability findings in Security Center portal and APIs

Powered by Qualys

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

- Data spillage
- Account breach
- Escalation 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 or filter items...

ID	Security Check	Category	Applies To	See
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 Configu...	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	■
90965	Windows Services List	Windows	1 of 1 resources	■
105190	Microsoft Windows File Security Check - C: System Files	Security Policy	1 of 1 resources	■
45063	NTPS Settings Enumerated	Information gathering	1 of 1 resources	■



# Cloud Workload Protection for Containers

## Protecting ACR

- Discovery of scanned ACR registries in a customer subscription within Azure Security Center
- Vulnerability scanning for all pushed images to ACR registries in a customer subscription
- Visibility into security vulnerabilities: description, details and severity classification

## Protecting AKS

- Continuous discovery of managed AKS instances within Azure Security Center
- Actionable recommendations for best practices and threat remediation
- Intelligent analytics for threat detection

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



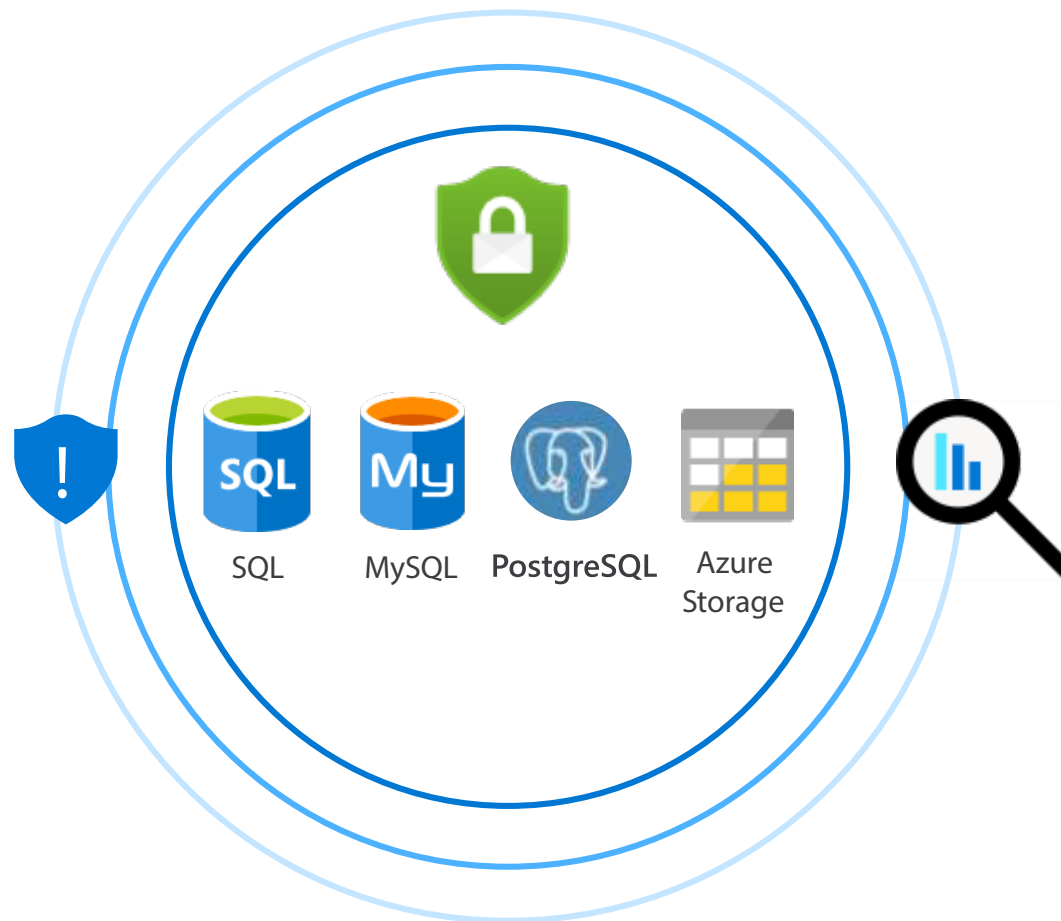
# Protect data services from threats

Detect attacks targeting your SQL databases, My SQL, PostgreSQL, and storage accounts

Mitigate threats targeting your Azure SQL databases and configure security best practices

Storage account protection to detect threats and misuse

Discover, classify, label and protect sensitive data in your Azure SQL databases





# 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



# Protect your IoT Solution from Threats

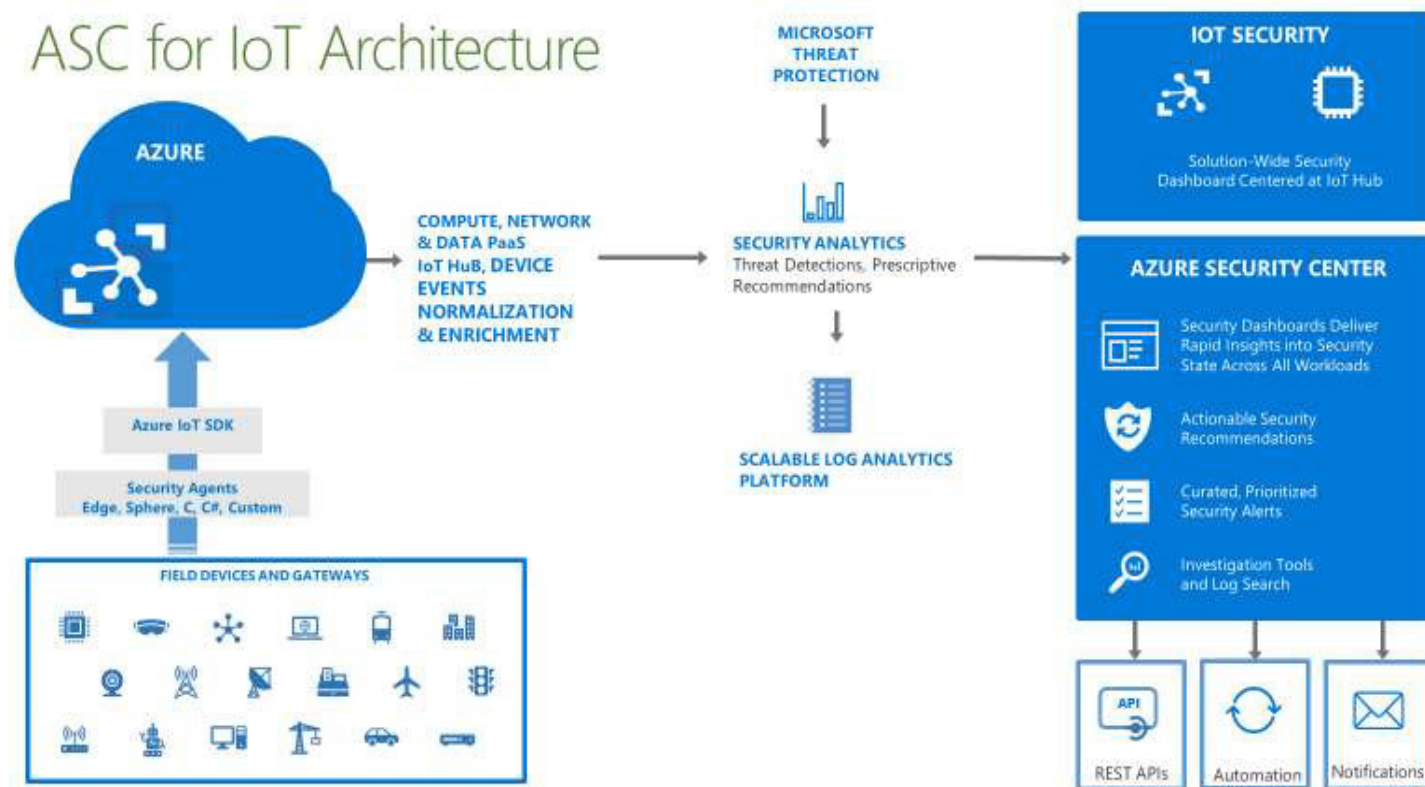
End to end security for your IoT infrastructure (from devices to applications)

Implement security best practices and mitigate threats for IoT devices, hubs, compute and data

Define alerts based on advanced queries across all IoT data as well as relevant ASC data in Azure Log Analytics

Azure Sentinel protects the entire enterprise from threats including those affecting IoT devices

## ASC for IoT Architecture





# Protect your workloads from threats

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

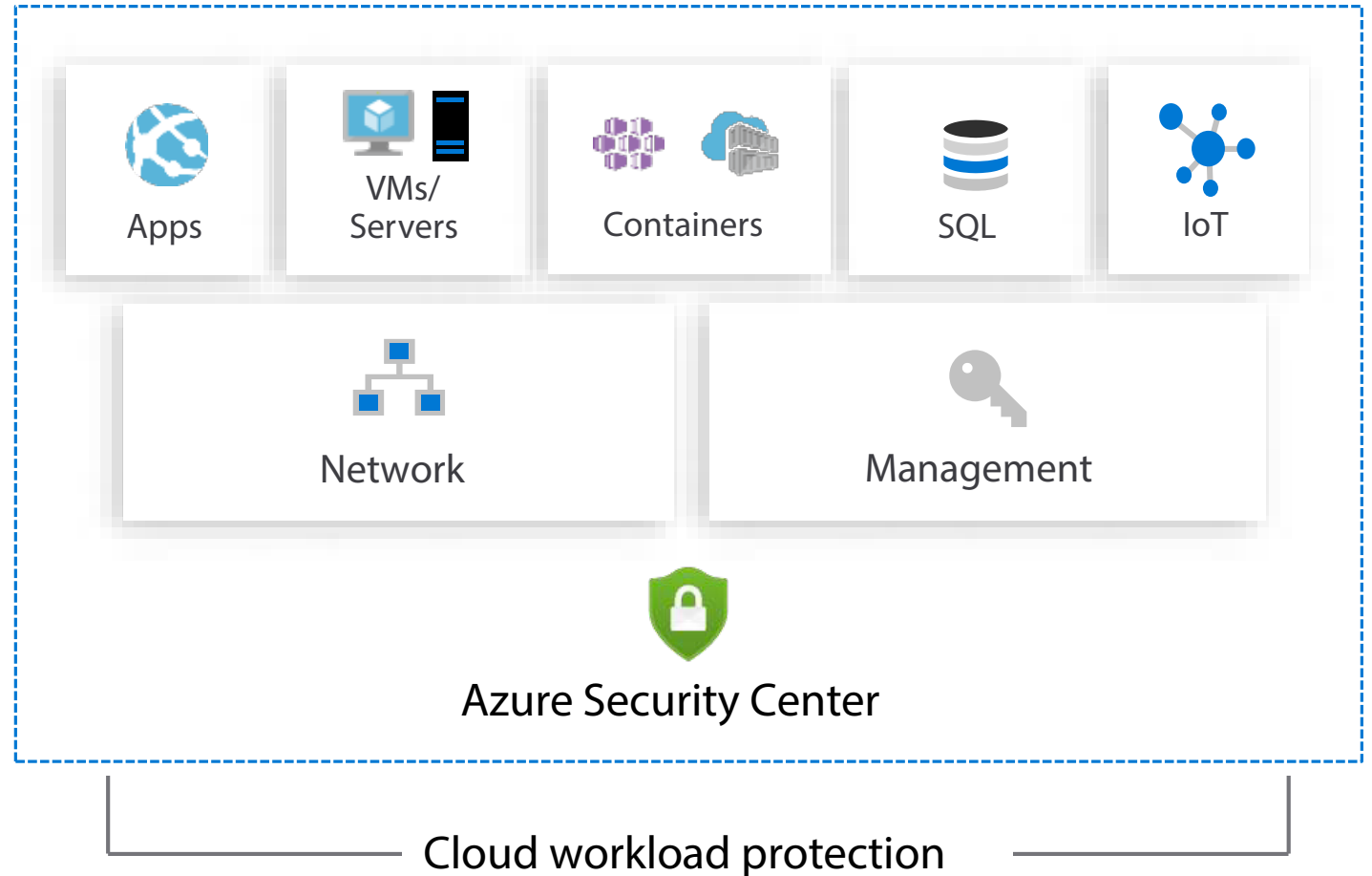
Detect & block advanced malware and threats for Linux and Windows Servers on any cloud

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)



# Azure Security Center



## Strengthen security posture

Cloud and Azure IoT security posture management

Secure Score

Security policies and compliance



## Protect against threats

For servers

For cloud native workloads

For databases & storage

For IoT devices



Get secure faster

# Get secure faster

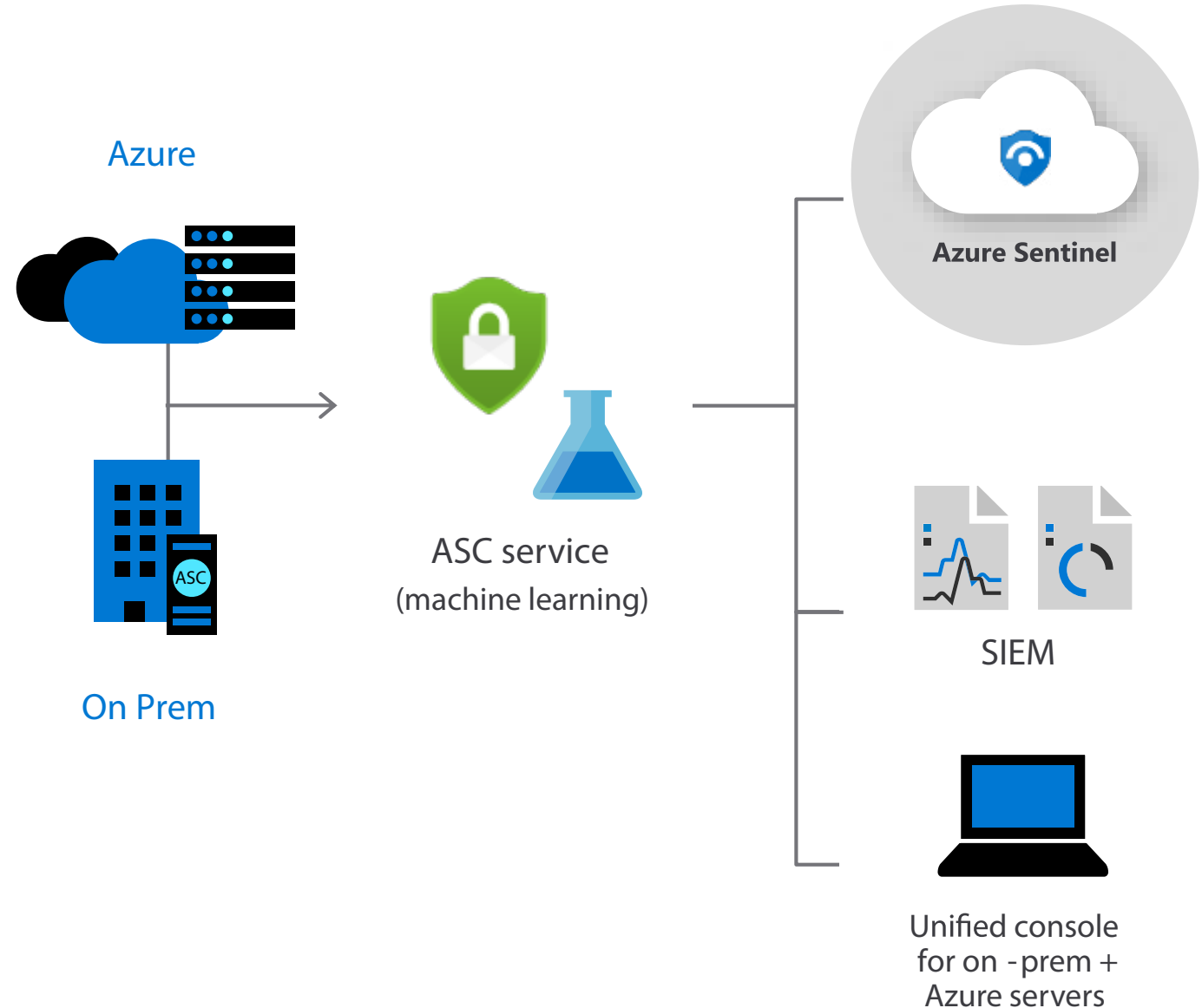


Automatically discover and onboard Azure resources

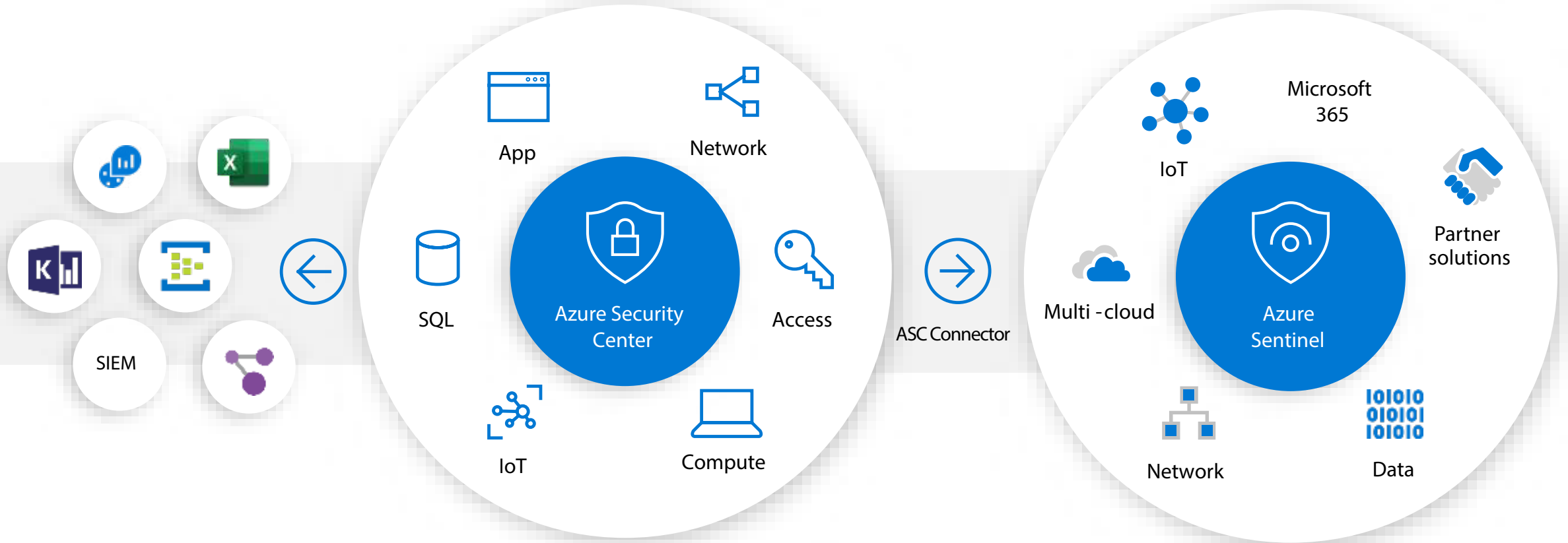
Gain a unified view of security across your hybrid cloud workloads

Integrate with Azure Sentinel or existing SIEM or partner solutions to streamline threat mitigation

Assess compliance in a click



# Threat protection for cloud at scale



**Azure Security Center**  
Cloud Workload Protection

**Azure Sentinel**  
Cloud Native SIEM

# Azure Security Center Pricing

FEATURES	FREE TIER	STANDARD TIER
Continuous assessment and security recommendations	✓	✓
Azure secure score	✓	✓
Just in time VM Access	--	✓
Adaptive application controls and network hardening	--	✓
Regulatory compliance dashboard and reports	--	✓
Threat protection for Azure VMs and non-Azure servers (including Server EDR)	--	✓
Threat protection for PaaS services	--	✓

<https://azure.microsoft.com/en-us/pricing/details/security-center/>

## Why Korcomptenz

Korcomptenz is a technology transformation provider that partners with clients to improve their digital experience and insight. With more than 18 years of experience, our strong team across India and the US helps companies build their digital capabilities. We help our clients achieve more and remain competitive with a connected, secured, and scalable environment that has minimum complexities, zero security compromises, is disaster proof, high availability, and low downtime. We have empowered our clients to attain a multi-layered grasp of their day-to-day operations turning your IT cost-center into a powerful tool to accelerate business model change, optimize ROI, and lower TCO by 40%.

## Thank you



35 Waterview Boulevard, Suite 207  
Parsippany, NJ 07054

## Get in touch with us:

Ph. +1 (973) 601 8770 | [sales@korcomptenz.com](mailto:sales@korcomptenz.com)  
[www.korcomptenz.com](http://www.korcomptenz.com) | Fax. 1-973-272-1140