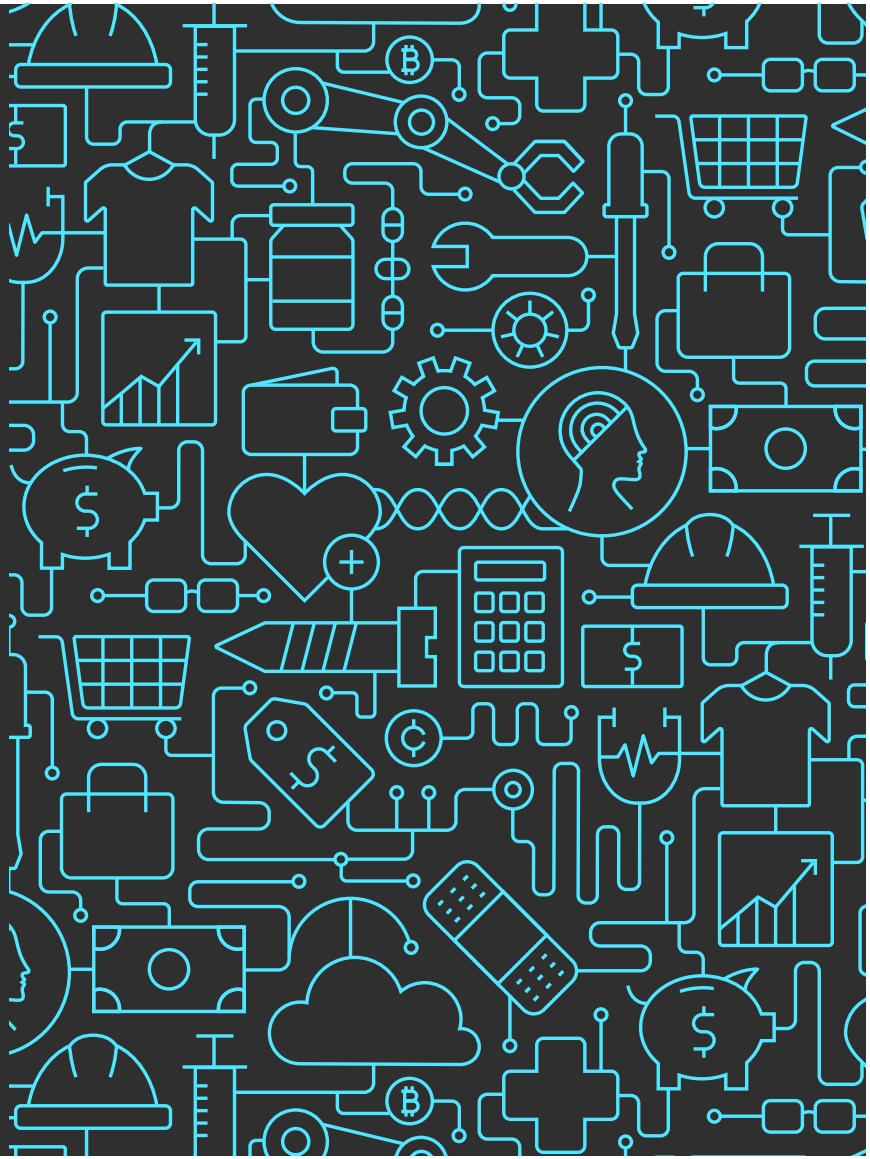
Microsoft

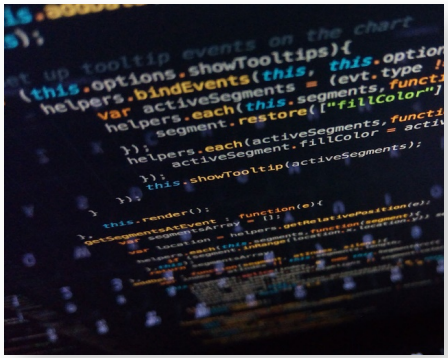
Building Security into Azure

Ramesh Chinta
Group PM, Azure security

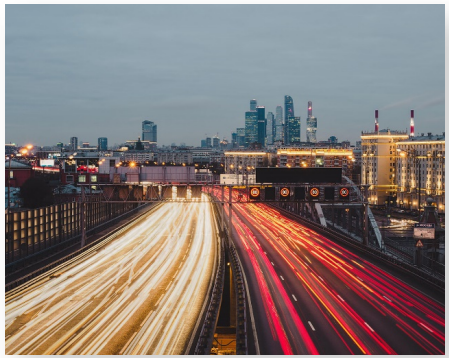


The era of flux and transformation

Everyone is now in the technology business

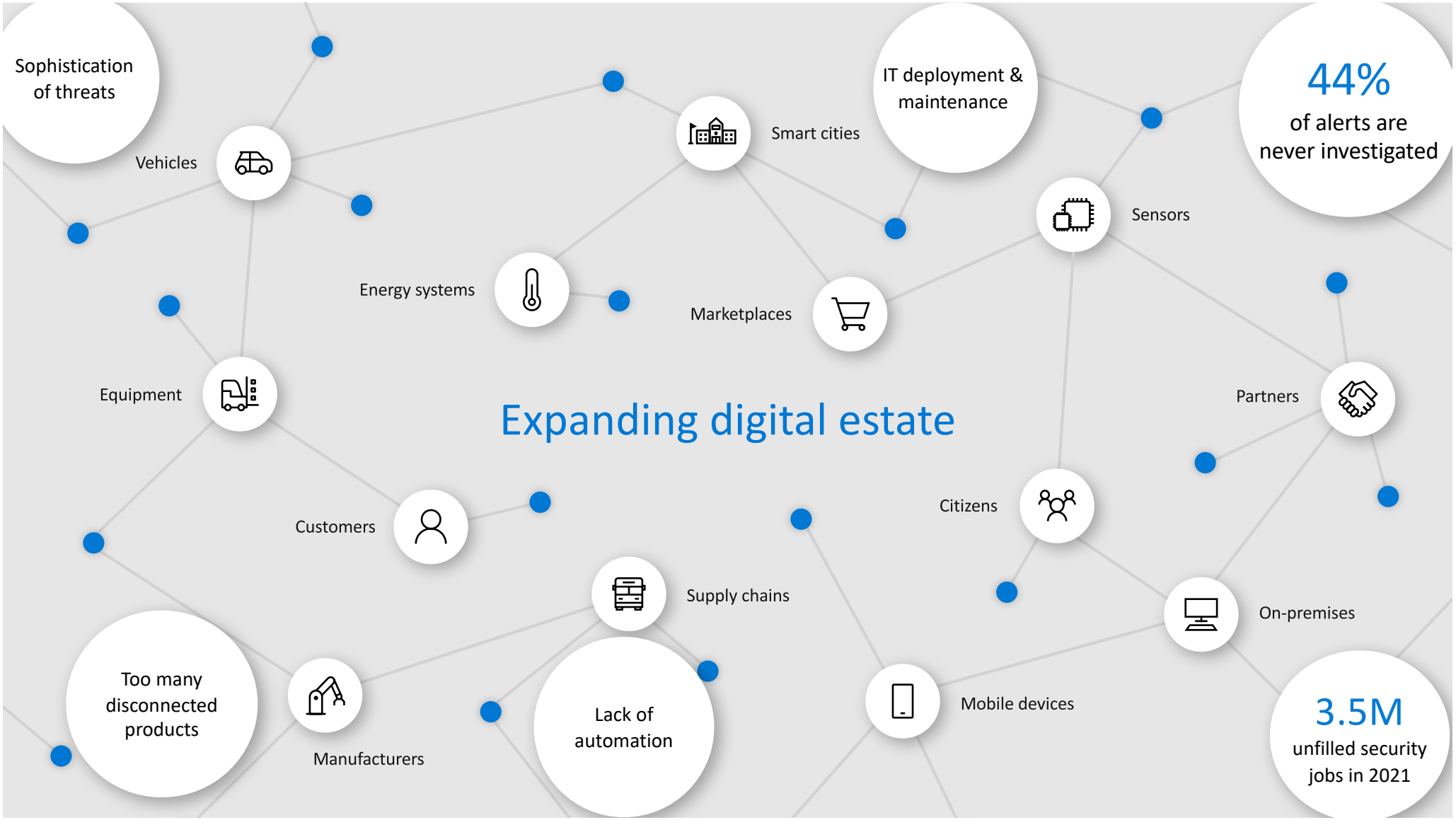


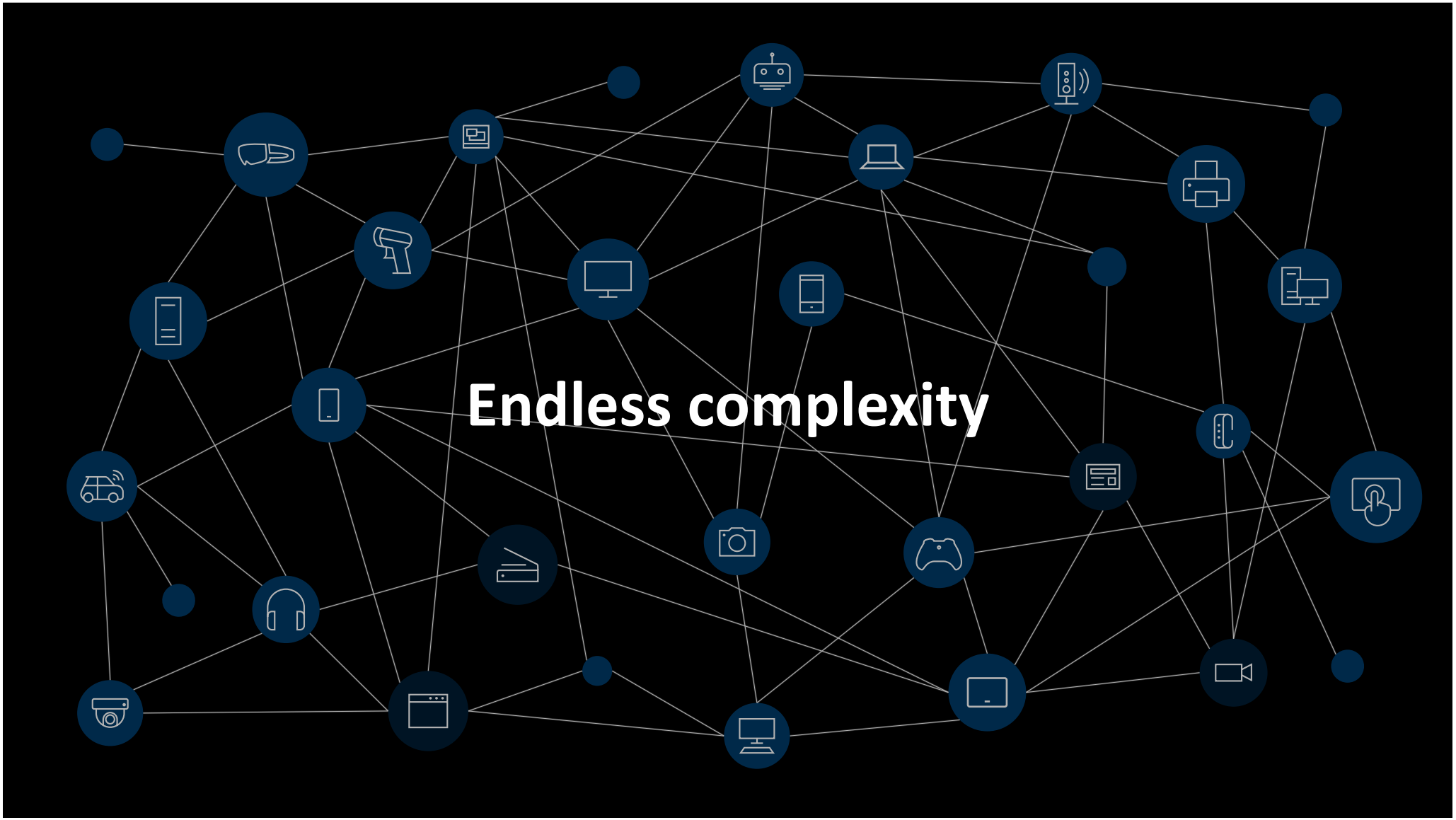
Conventional security tools have not kept pace



Security professionals alone can't fill the gap

Regulatory requirements and costs are increasing


Sophistication of threats
Vehicles
Smart cities
IT deployment & maintenance
44%
of alerts are never investigated
Sensors
Energy systems
Marketplaces
Equipment
Partners
Expanding digital estate
Customers
Citizens
Supply chains
On-premises
Too many disconnected products
Manufacturers
Lack of automation
Mobile devices
3.5M
unfilled security jobs in 2021


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

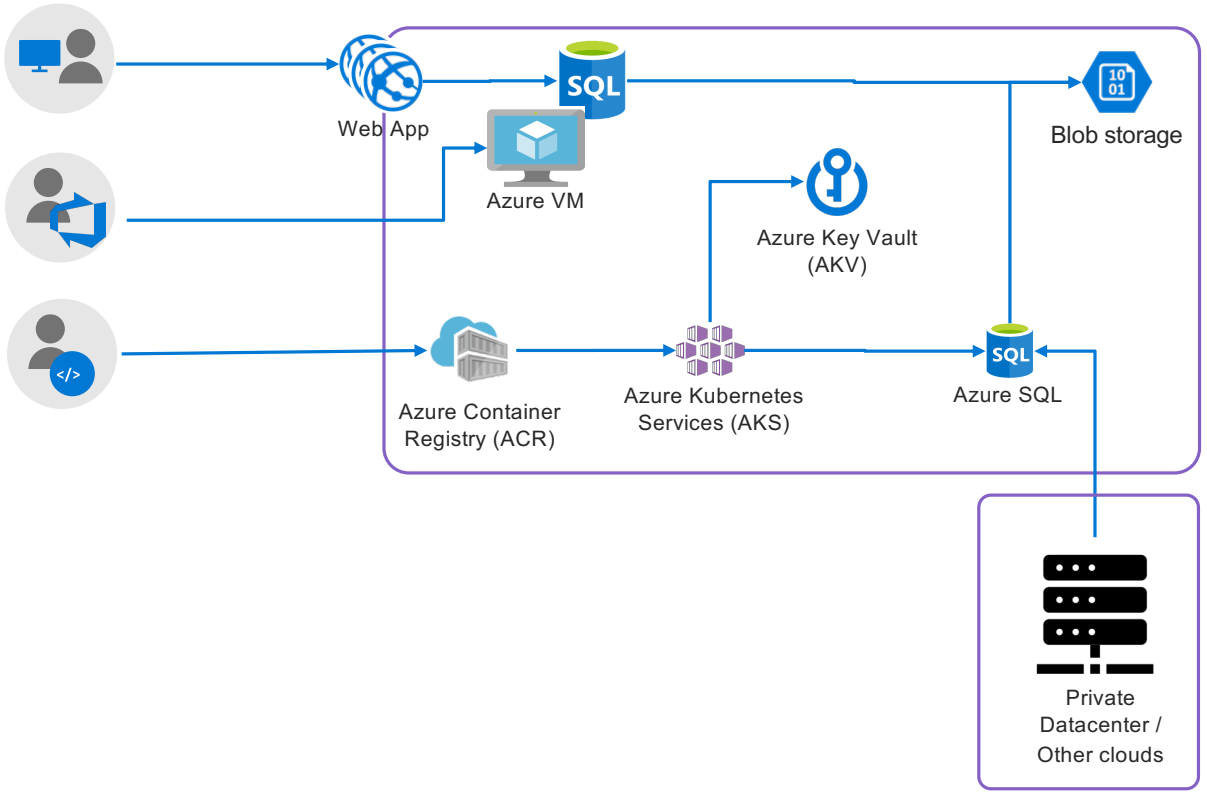
Gain unmatched security with Azure

$1B annual investment in cybersecurity

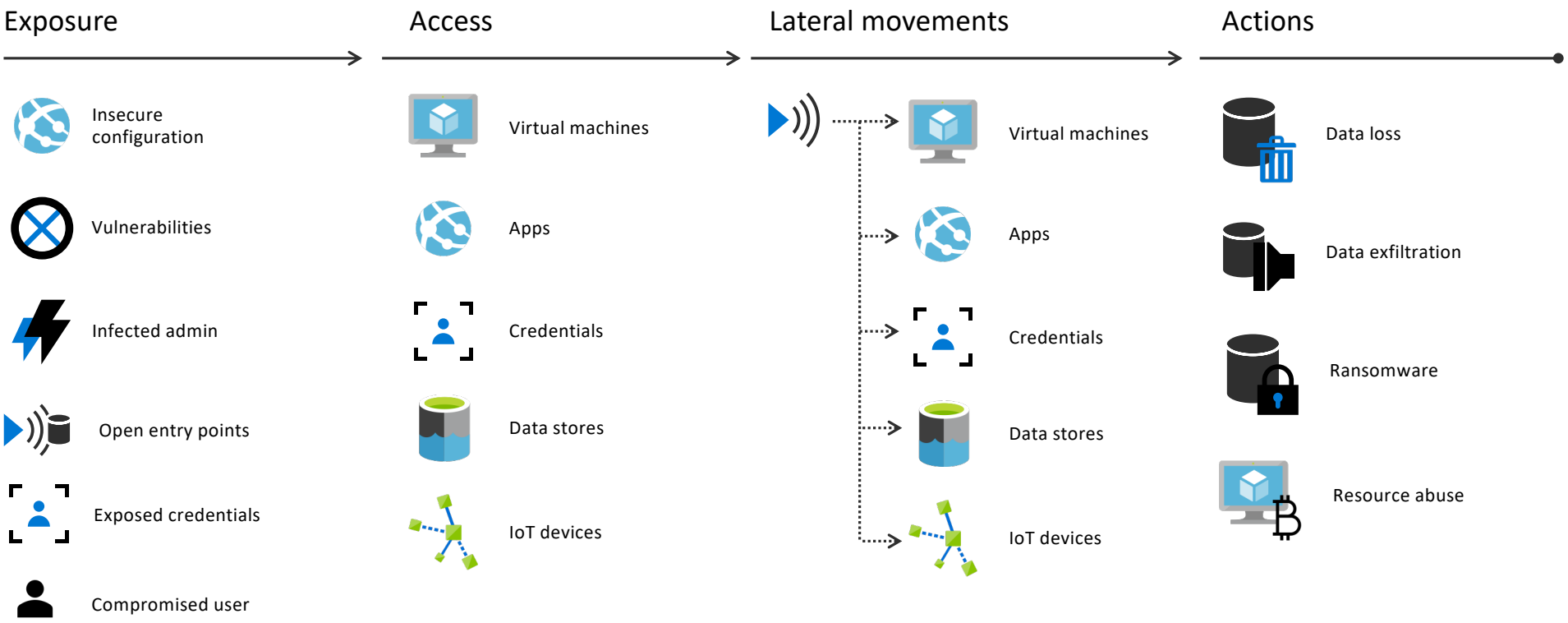
3500+ global security experts

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

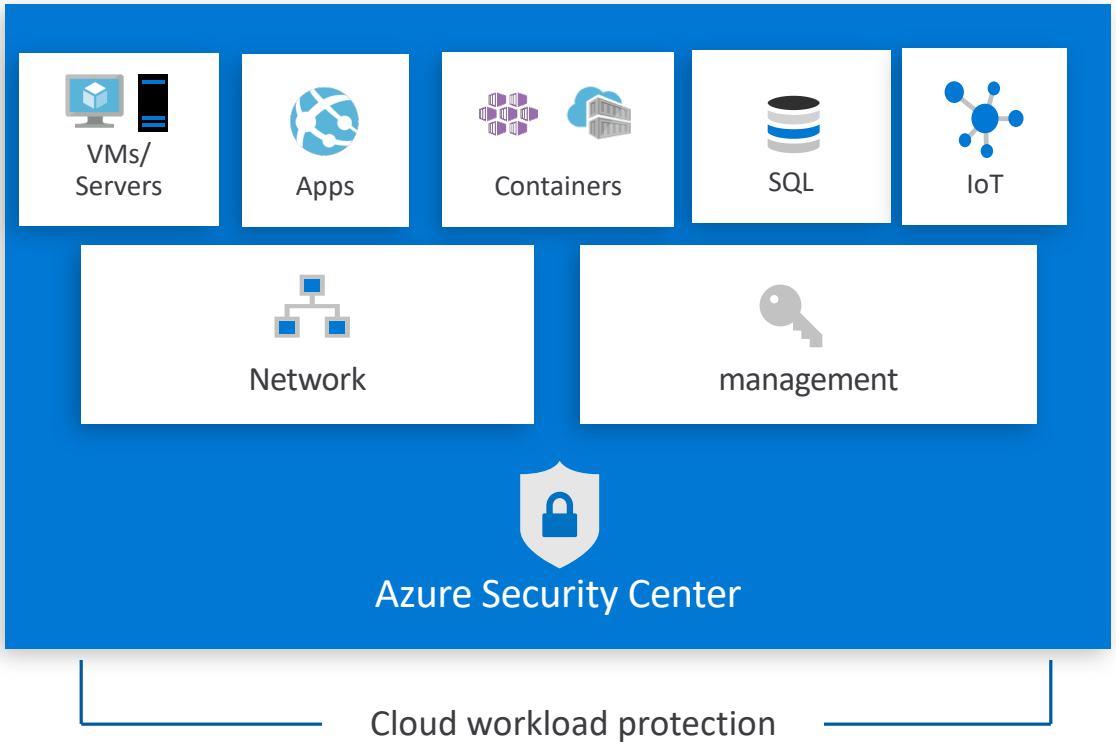
Data & Storage

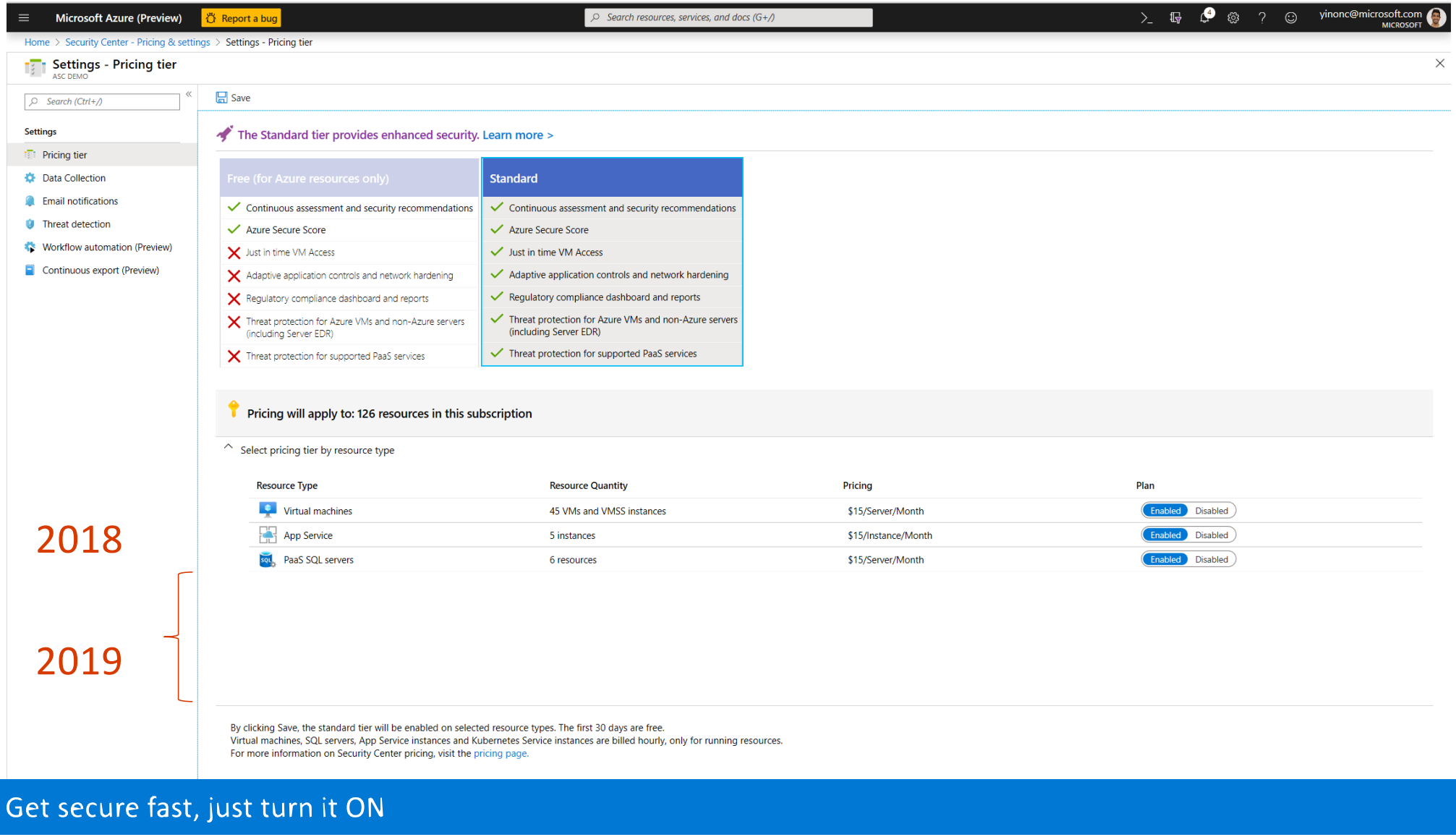
Get secure faster

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)





2018

2019

Get secure fast, just turn it ON

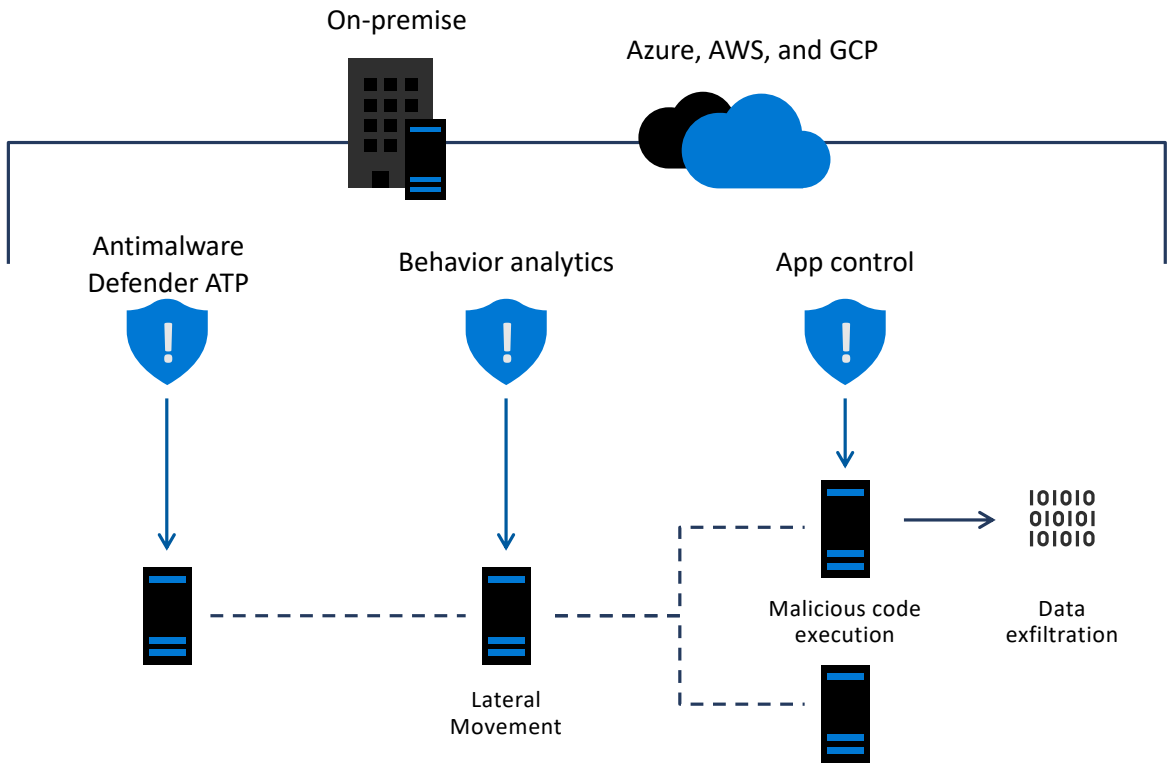
Protect Linux and Windows VMs from threats

Reduce open network ports:

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

Protect against malware:

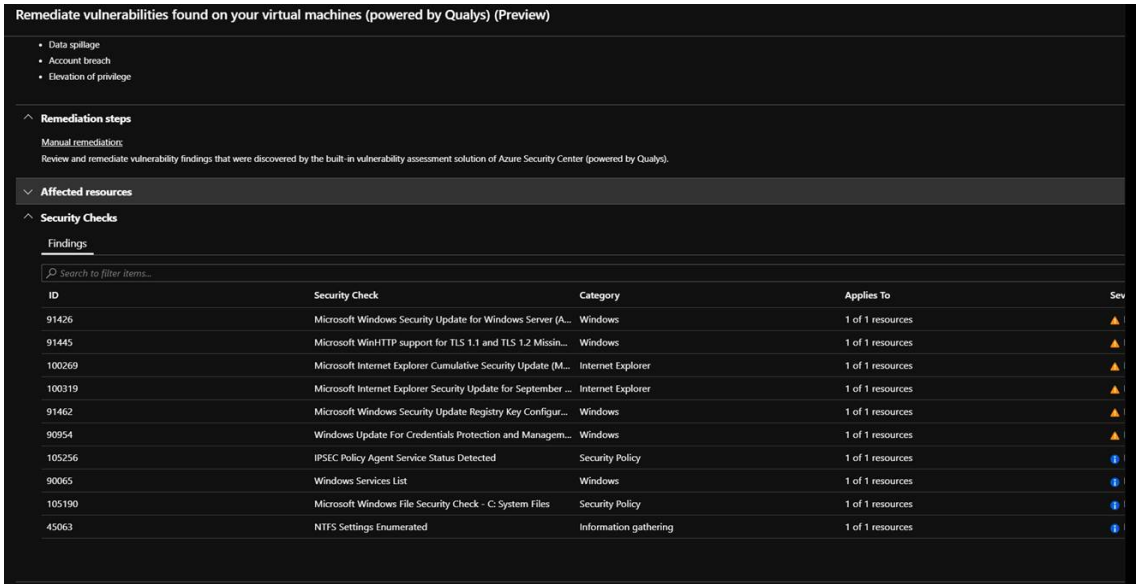
- Block malware with adaptive application controls
- Built-in Microsoft Defender ATP EDR
- Crash dump analysis and fileless attack detections



Announcing built-in vulnerability assessment for VMs

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

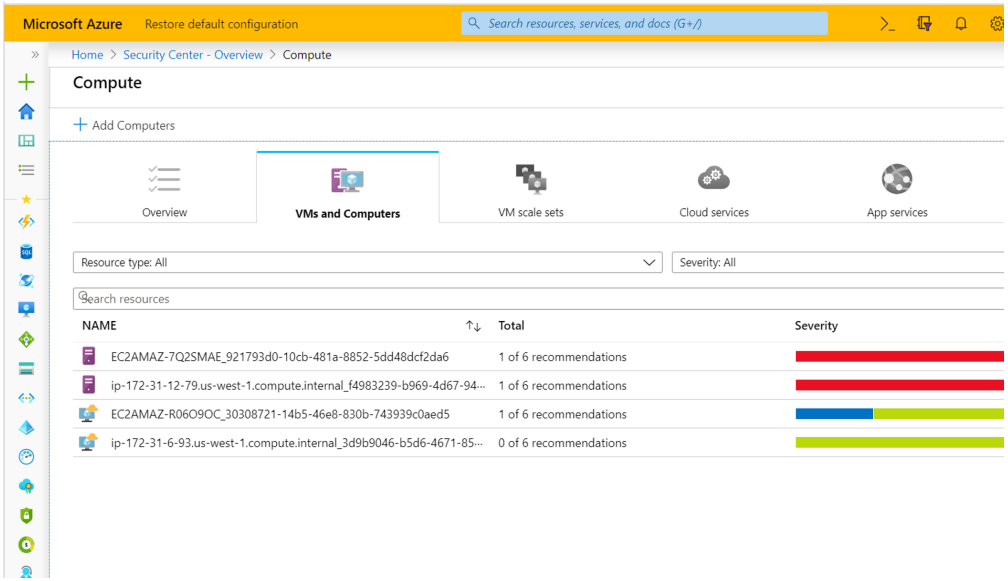
- Automated deployment of vulnerability scanner
- Continuously scans installed applications to find vulnerabilities
- Visibility to the vulnerability findings in Security Center portal and APIs



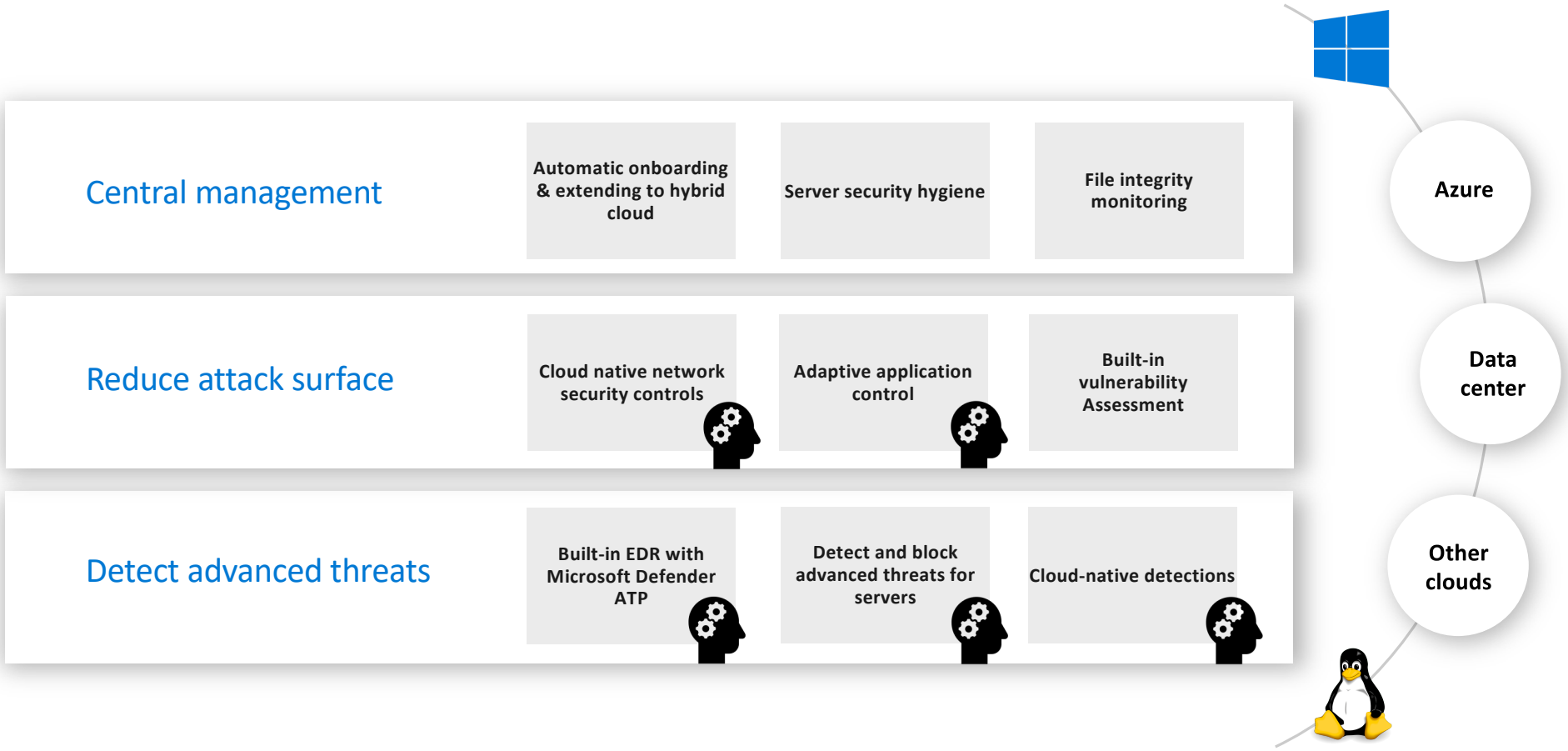
Protect hybrid datacenters and multi-cloud with Azure security center

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)

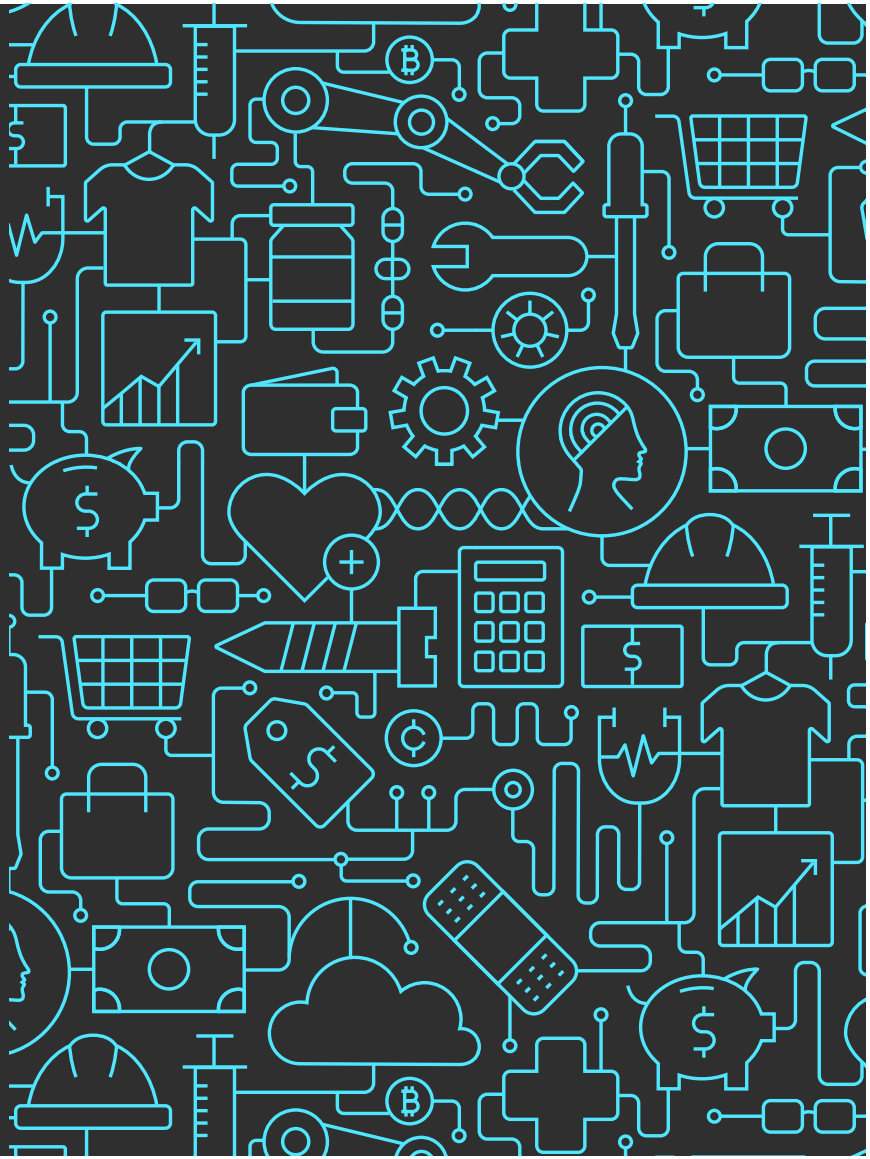


Cloud workload protection for hybrid VMs and servers



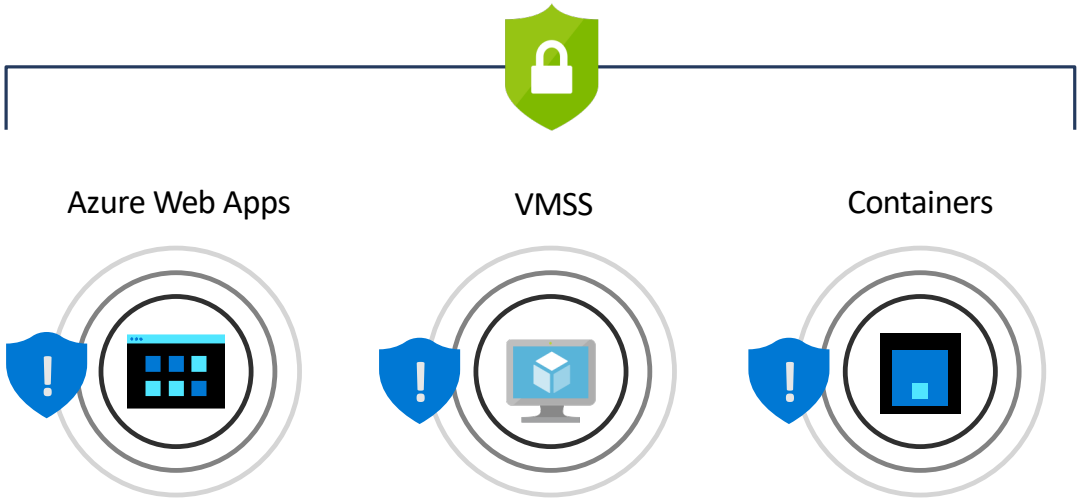
Microsoft

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

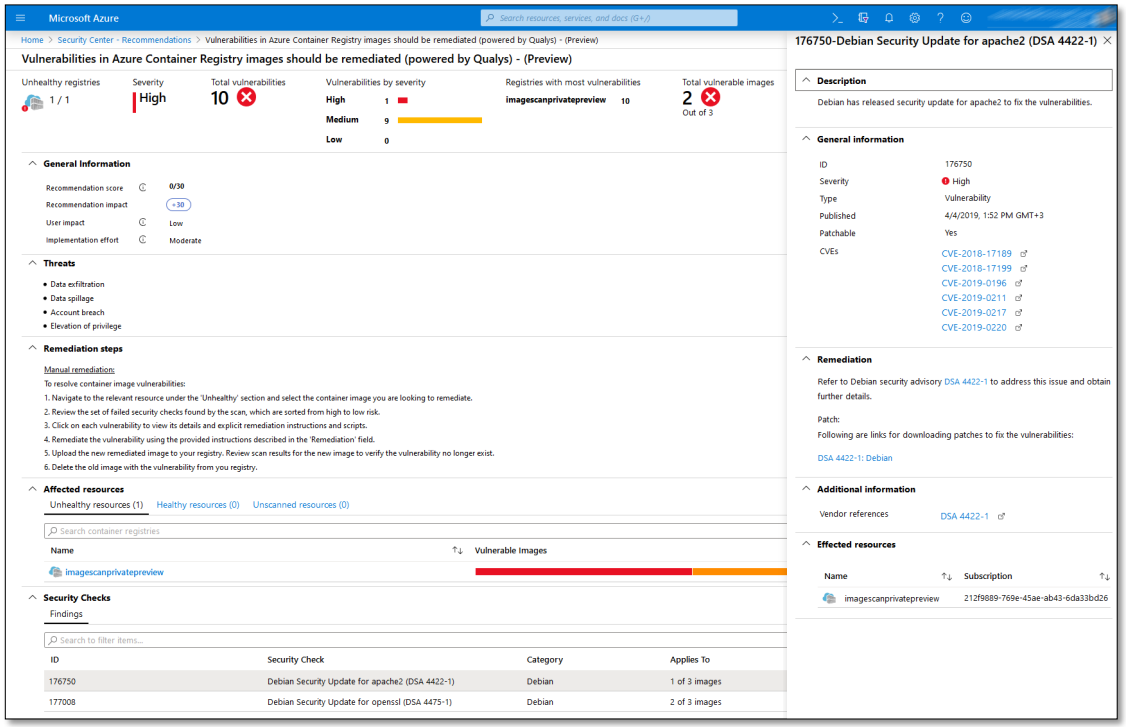


>75% of global organizations will be running containerized applications in production by 2022 (Gartner)

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



Cloud workload protection for containers

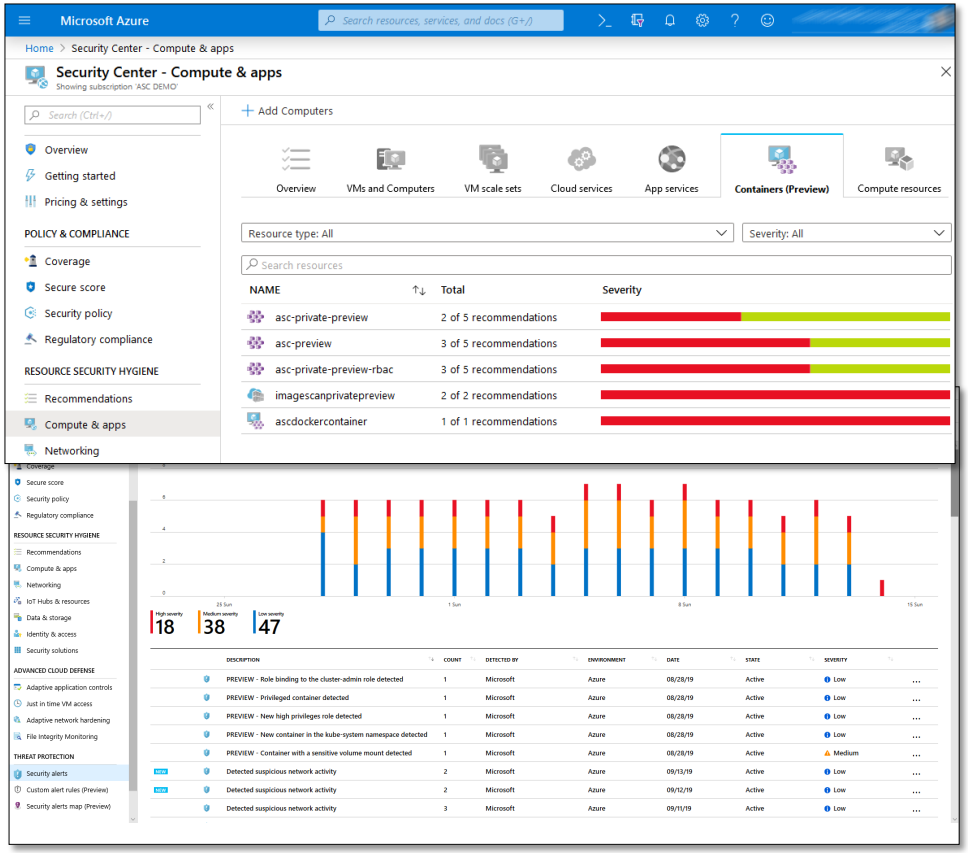
Now available in standard Azure security center with the new container service add-on

Protecting Container hosts (IaaS)

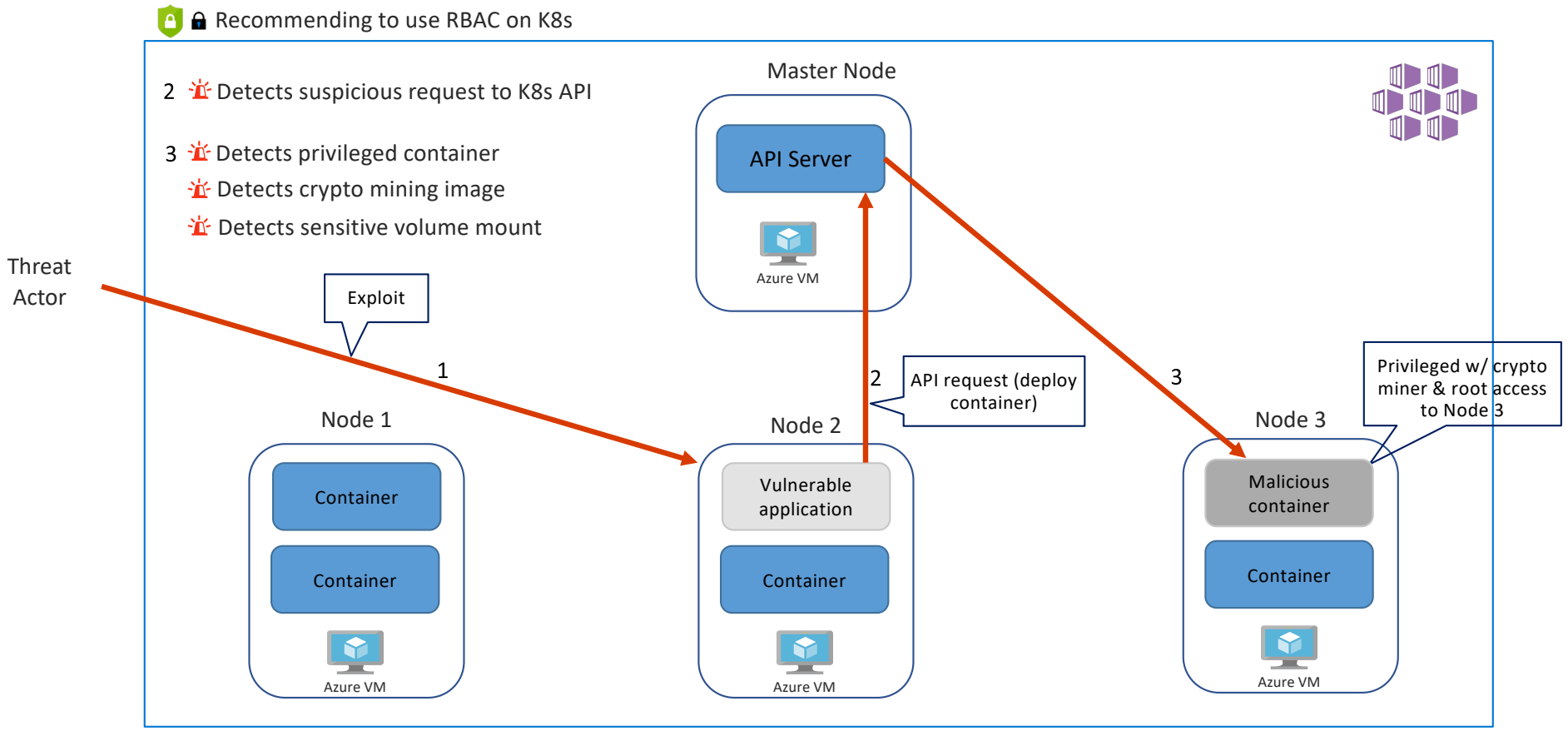
- CIS Docker Benchmark assessment
- Node Threat Protection

Protecting AKS

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

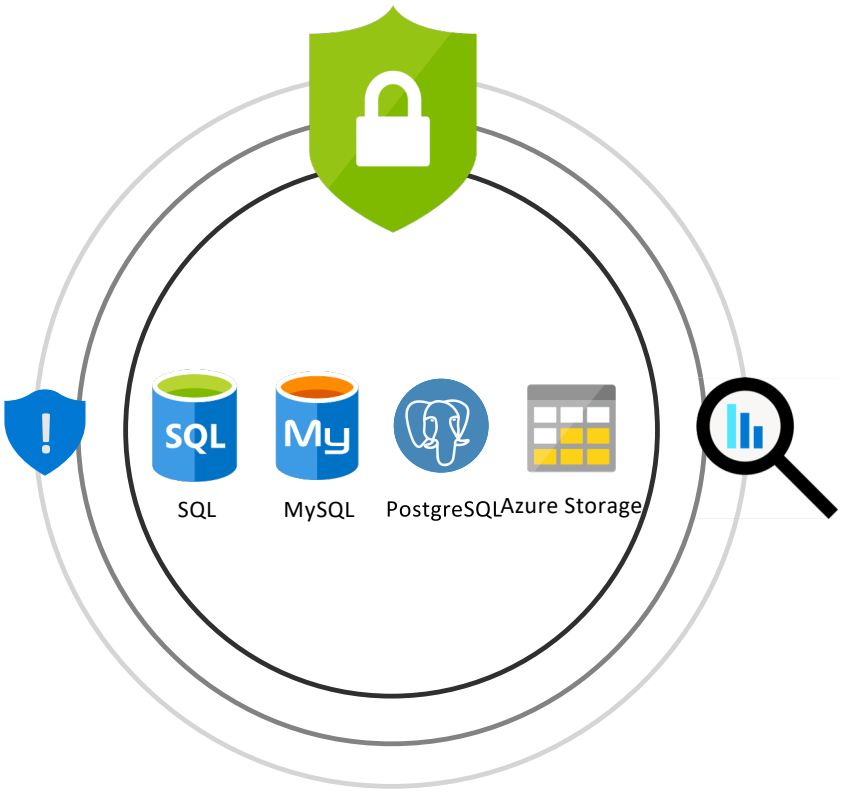


Protecting against advanced cloud threats



Protect data services from threats

- Prevent & detect threats targeting your Azure SQL databases, 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 advanced protection capabilities for data services

NEW

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…

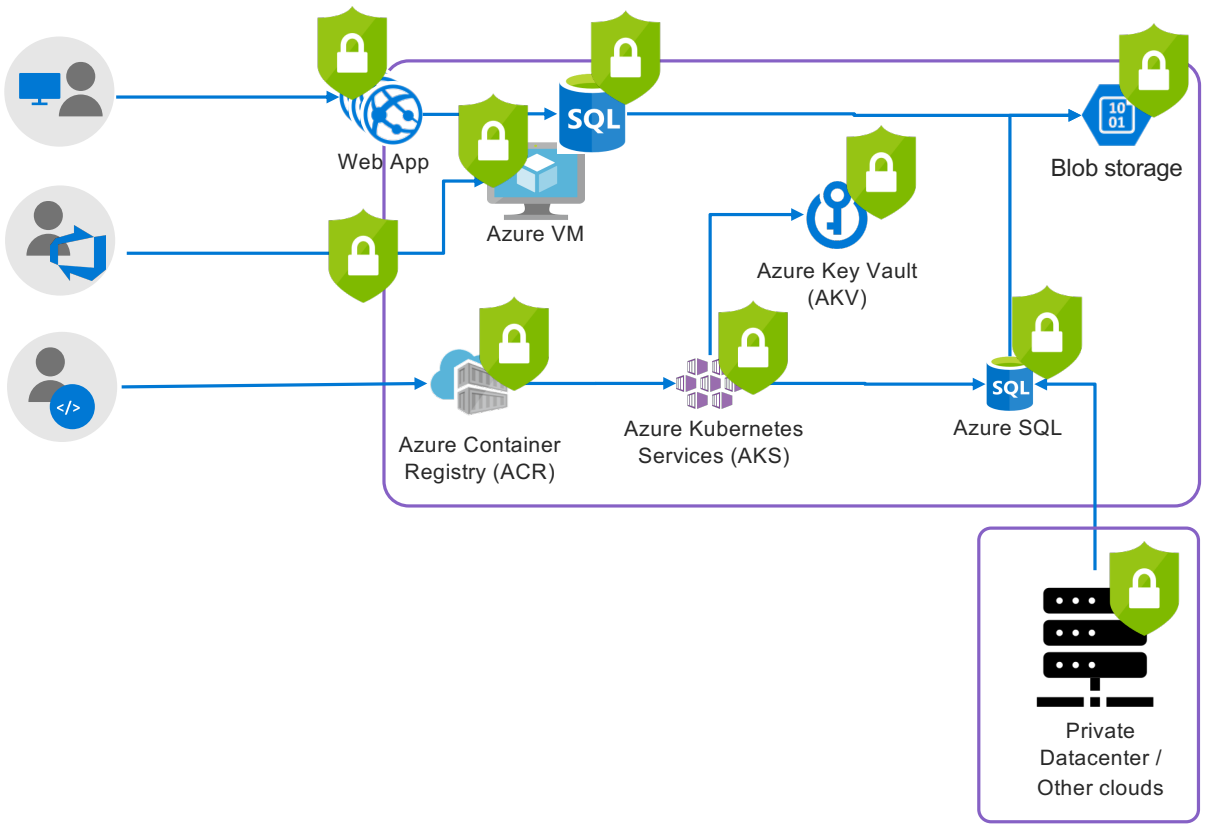
Storage account detections

- 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

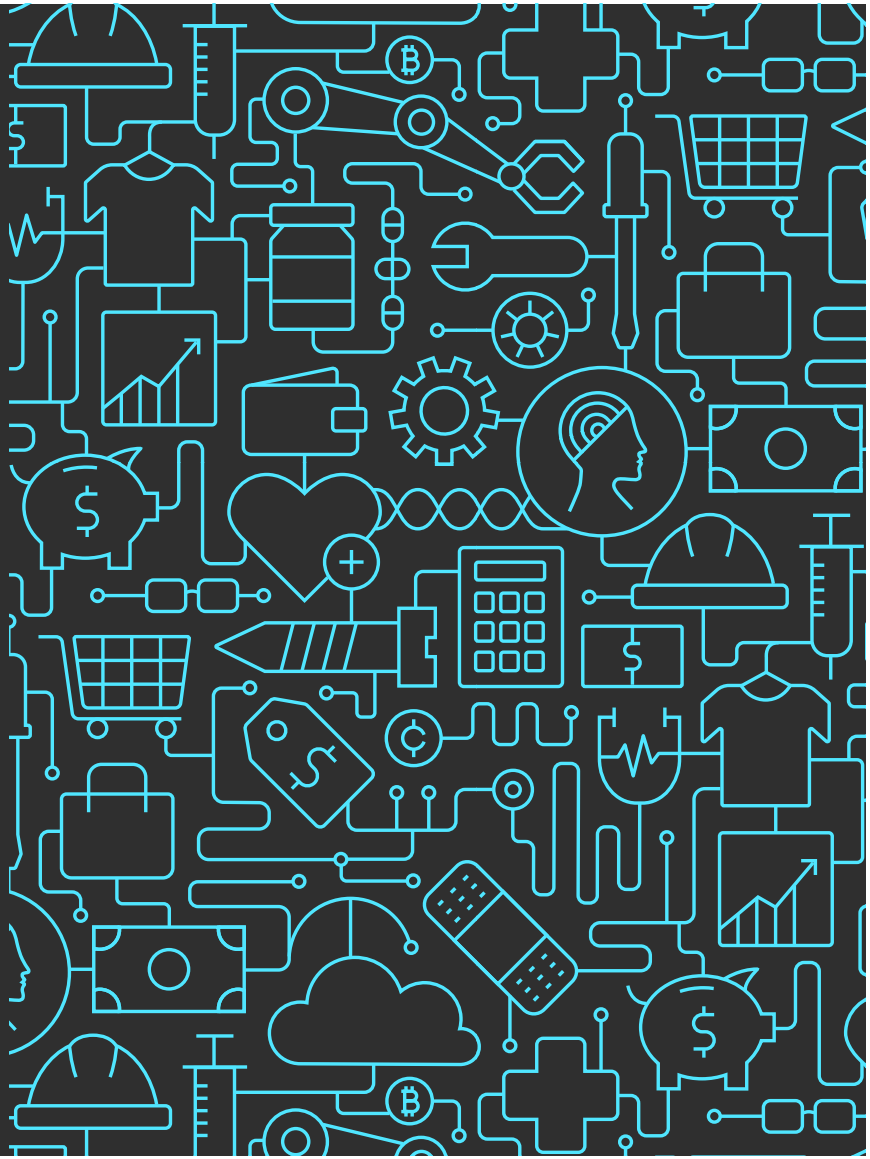
- Access from a suspicious location, Tor network
- Unusual policy change or listing and secret get
- Unusual volume or pattern of Key Vault operations
- And more…

Example solution architecture on Azure



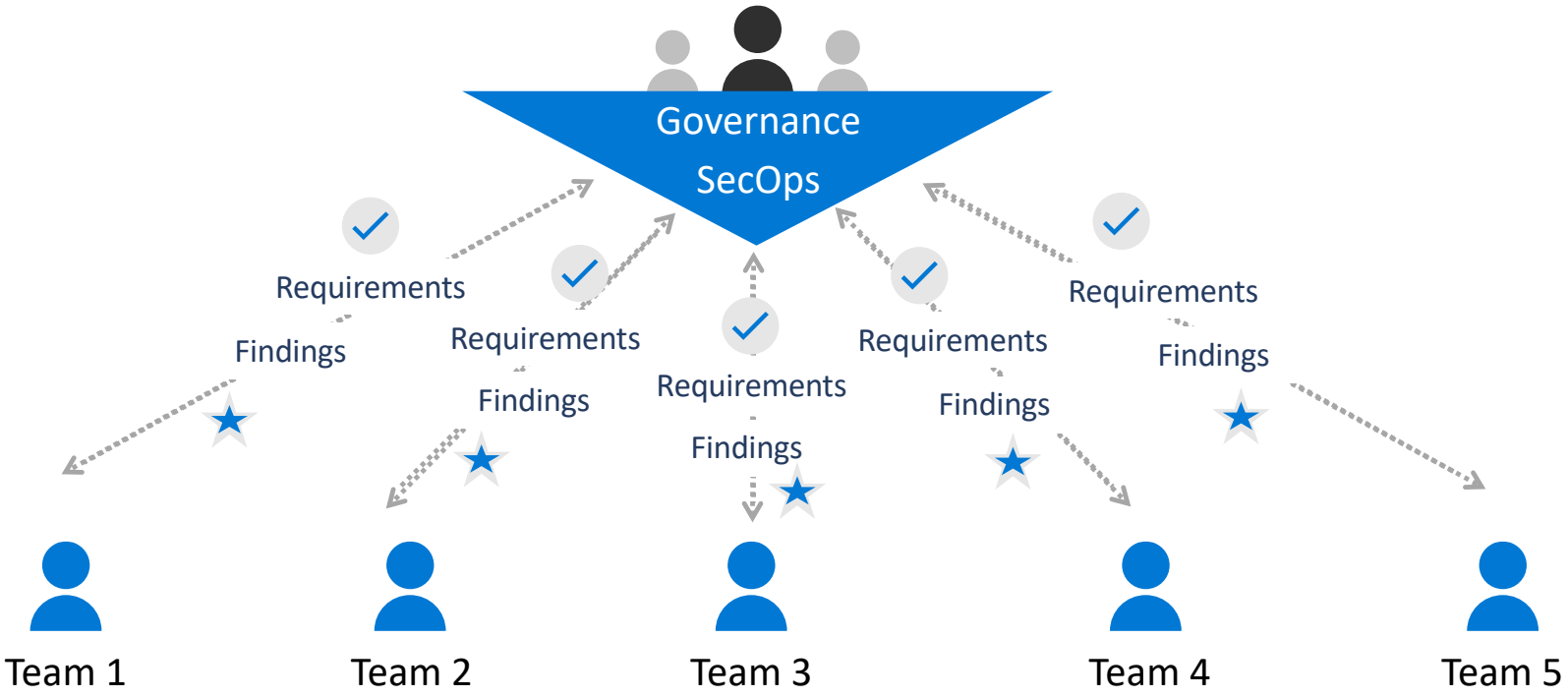
Microsoft

Azure security center enterprise integrations



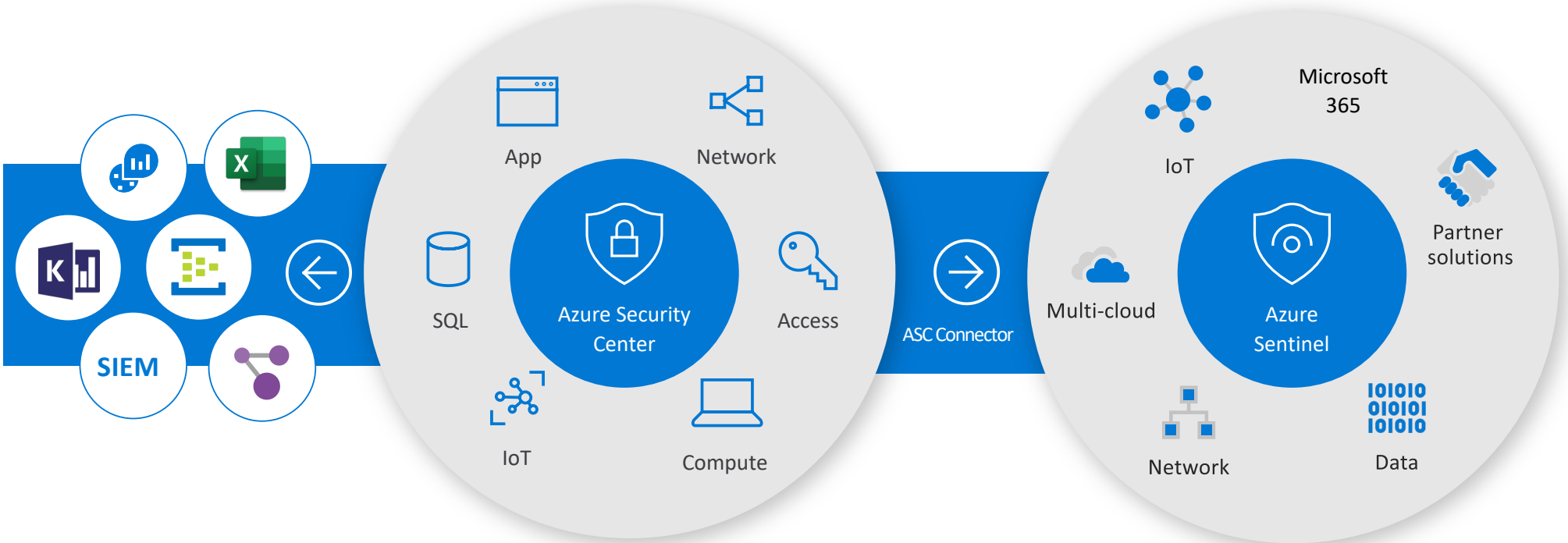
Driving threat protection through the organization

Through a central SecOps & cloud governance role



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

NEW



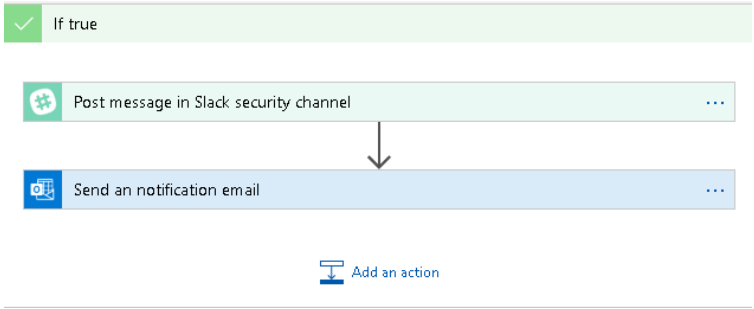
Azure Security Center
Cloud Workload Protection

Azure Sentinel
Cloud Native SIEM

Automate workflows with ASC

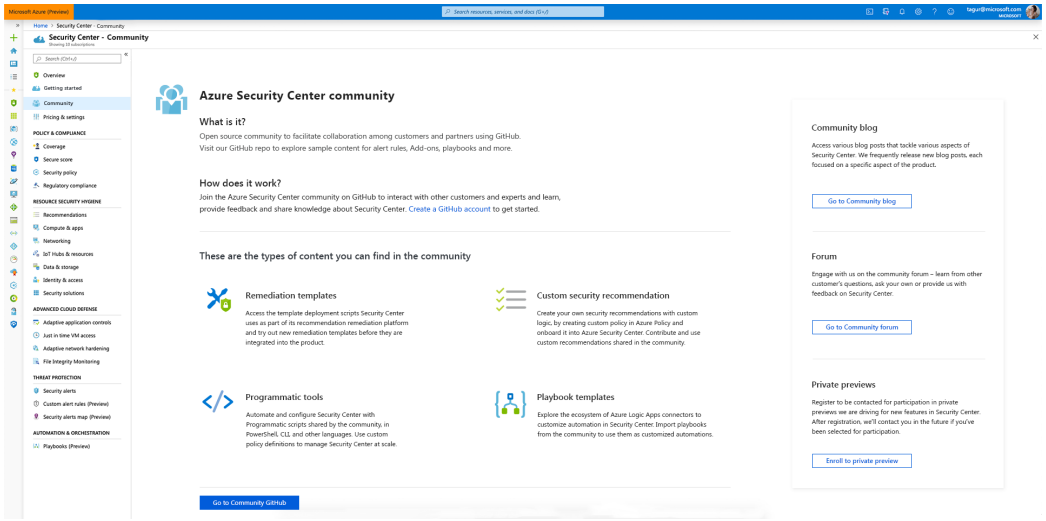
Automate workflows with ASC

- 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

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**

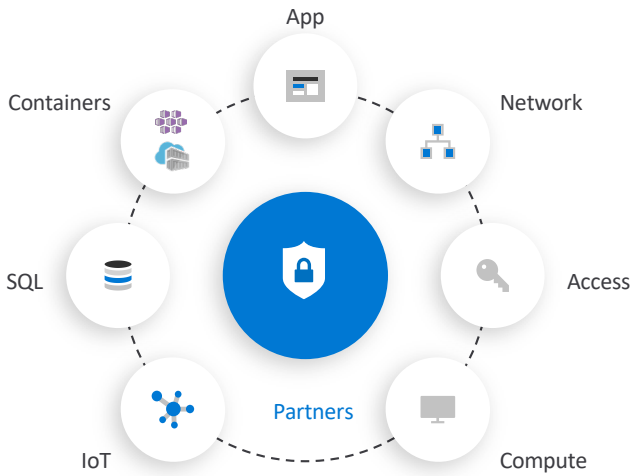
Built-in vulnerability assessment with Security Center Standard

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

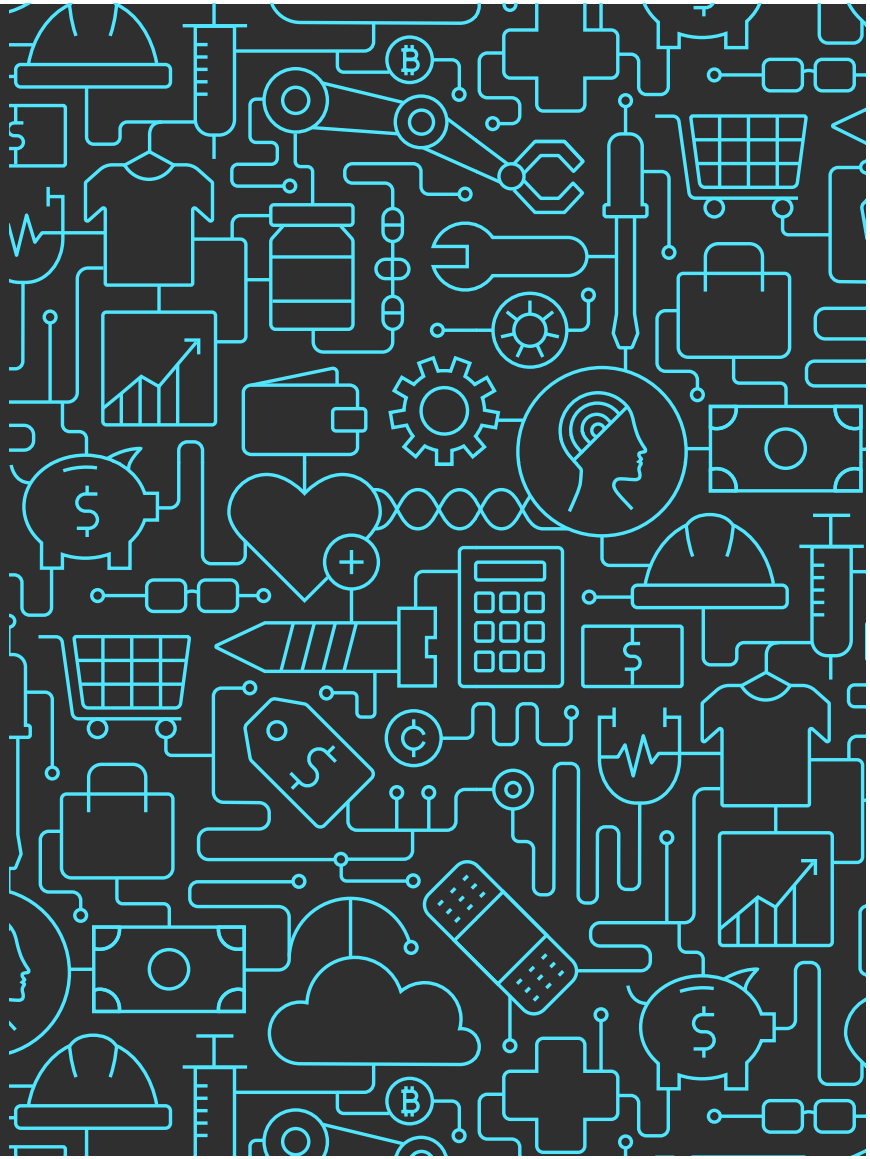
Improved reporting and export for Security Center alerts and recommendations

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

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

Microsoft

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**

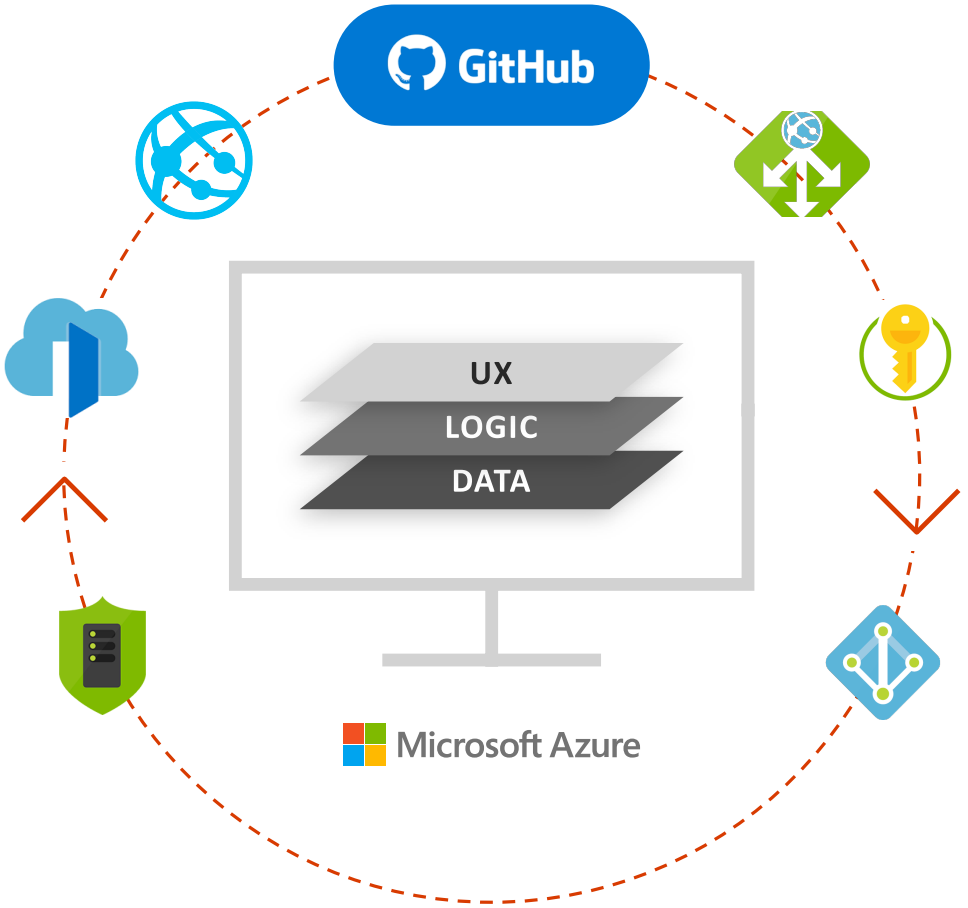
  Azure provides you with security tools at the data, network, identity and runtime

  Encryption at rest, in transit, and in use

- **Guidance to help you succeed**

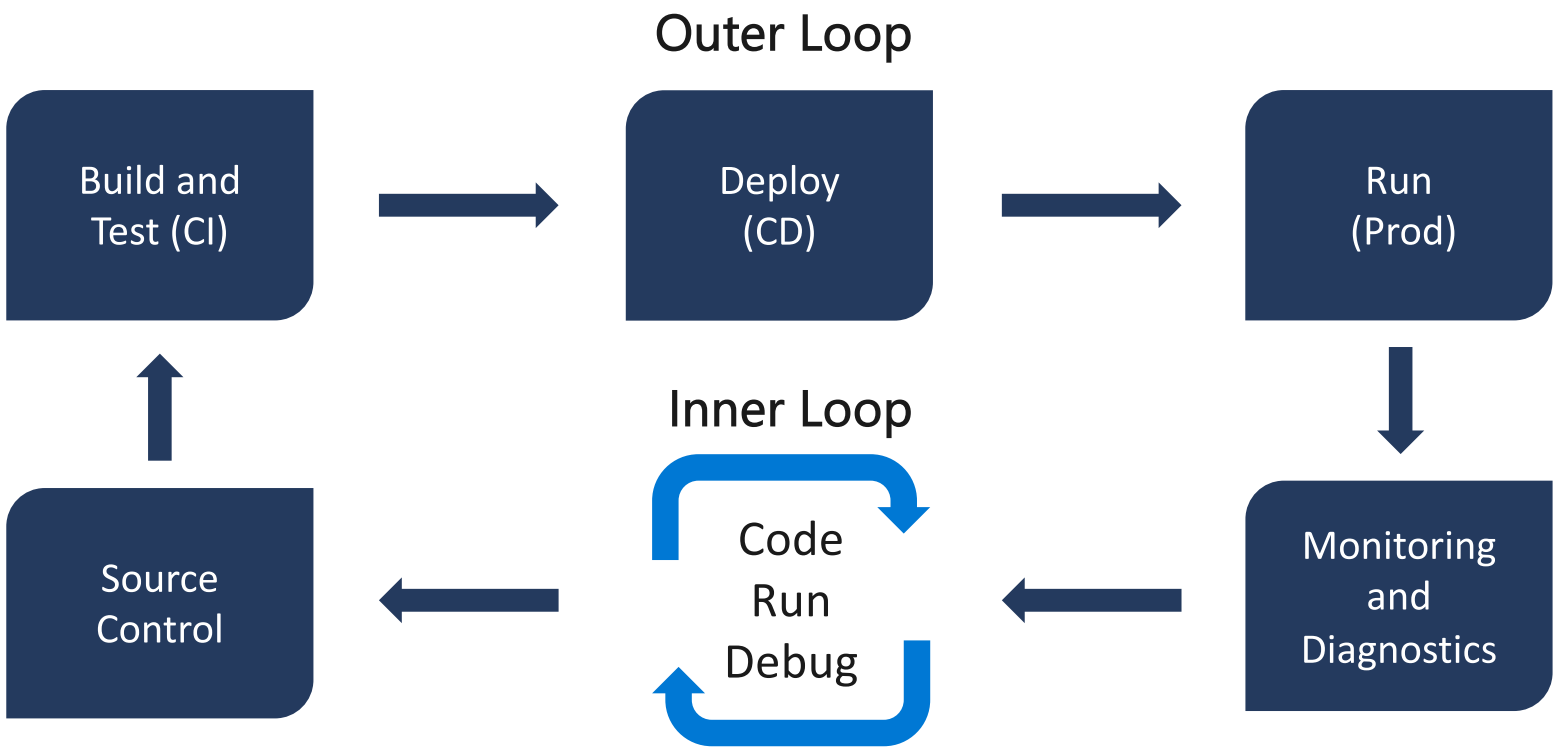
  Best practices documentation

  Secure Devops toolkit



Secure DevOps

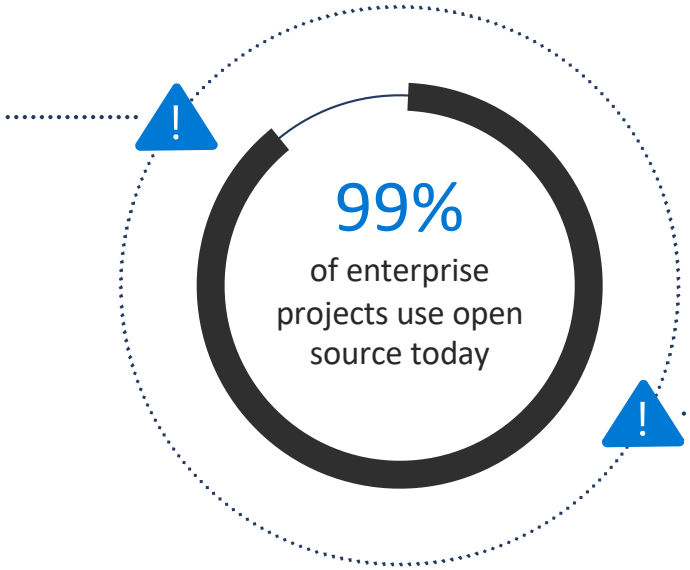
Inner and Outer Loop Development



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**

GitHub

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

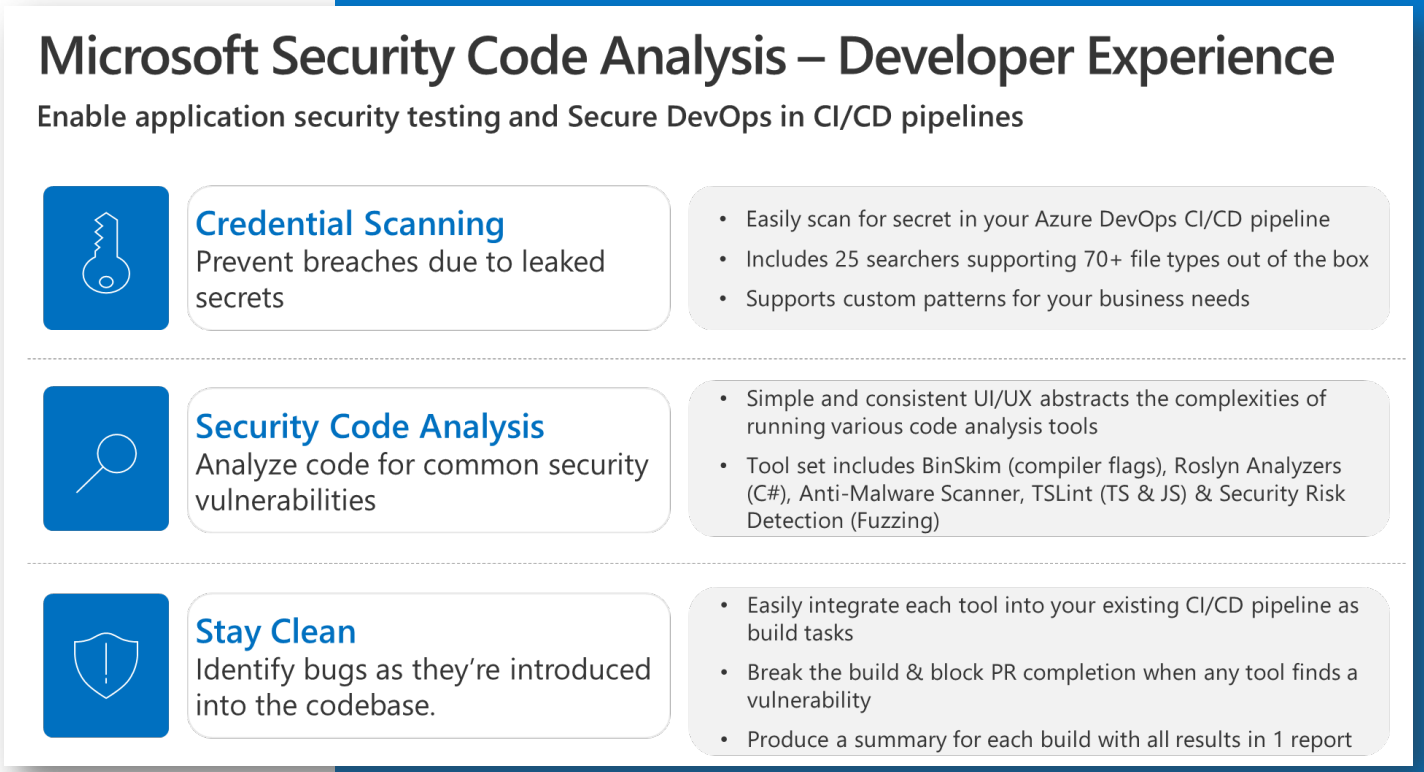
The extension can ensure the tools stay up-to-date and you never have to worry about managing updates

Available today

(via Support)

A 1st Step

Outer loop

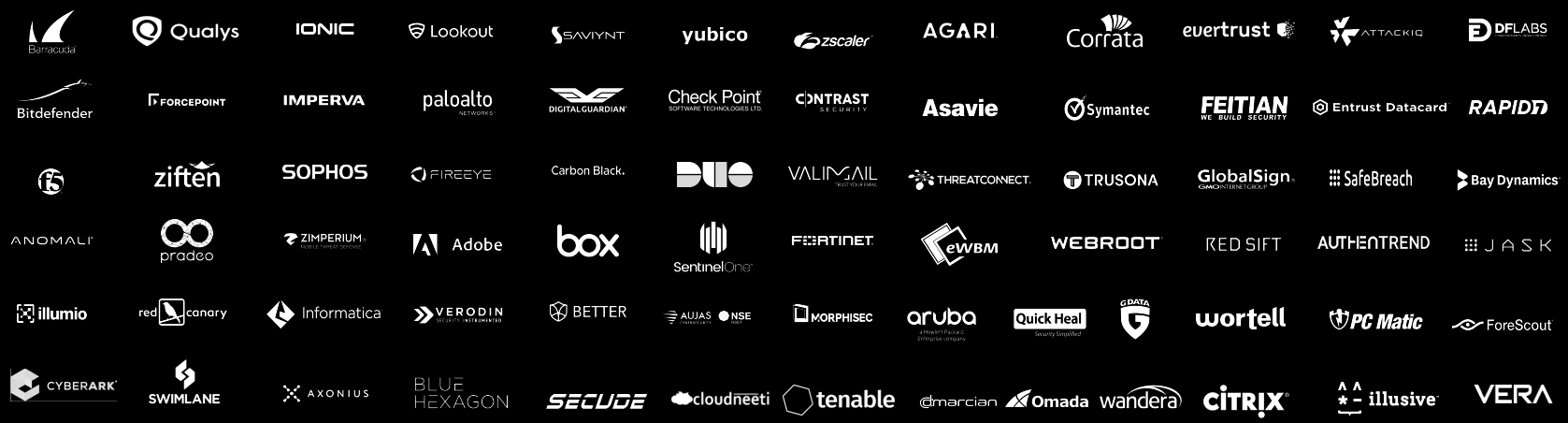


Available today

(via Support)

A 1st Step

Partners


Barracuda
Qualys
IONIC
Lookout
SAVIYNT
yubico
zscaler
AGARI
Corrata
evertrust
ATTACKIQ
DFLABS
Bitdefender
FORCEPOINT
IMPERVA
paloalto NETWORKS
DIGITAL GUARDIAN
Check Point SOFTWARE TECHNOLOGIES LTD.
CONTRAST SECURITY
Asavie
Symantec
FEITIAN WE BUILD SECURITY
Entrust Datacard
RAPID7
ziften
SOPHOS
FIREEYE
Carbon Black.
DUO
VALIMAIL
THREATCONNECT
TRUSONA
GlobalSign
SafeBreach
Bay Dynamics
ANOMALI
pradeo
ZIMPERIUM
Adobe
box
SentinelOne
FORTINET
eWBM
WEBROOT
RED SIFT
AUTHENTREND
JASK
illumio
red canary
Informatica
VERODIN
BETTER
AUJAS
NSE
MORPHISEC
aruba
Quick Heal
G DATA
wortell
PC Matic
ForeScout
CYBERARK
SWIMLANE
AXONIUS
BLUE HEXAGON
SECUDE
cloudneeti
tenable
@marcian
Omada
wandera
CITRIX
illusive
VERA

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

Microsoft

Thank you!

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

ASC Tech Community Page