Microsoft

Security and Compliance of Application Infrastructure in a Multi-Cloud World

Damir Bersinic
Azure Hybrid Cloud Technical Sales Lead – Canada
C+E Global Black Belt Team
damirb@microsoft.com

Gold Sponsors

Community Supporters

Customer environments and application requirements are evolving

How to govern and operate across disparate environments?

How to ensure security across the entire organization?

How to best enable innovation and developer agility?

How to meet regulatory requirements and overcome technical hurdles?

100's–1,000's of apps

- VMs
- Databases
- Containers
- Serverless

.NET, JS, Java, GO, php

Diverse infrastructure

- Datacenters
- Hosters
- Branch offices
- OEM hardware
- IoT devices
- Edge

Hybrid & Multi-Cloud

Microsoft Azure

aws

Google Cloud

Alibaba Cloud

vmware

ORACLE

IBM Cloud

Momentum to a hybrid and multicloud strategy

90%

of enterprises depend on hybrid

93%

of enterprises have a multicloud strategy

Source: Gartner Says a Massive Shift to Hybrid Infrastructure Services Is Underway
Source: Cloud Computing Trends: 2020 State of the Cloud Report | Flexera Blog

Hybrid and multicloud security is top of mind

Adaptable attackers

Attacks traverse laterally across silos and perimeters

Disparate security tools

Security tools are increasingly complex, and poorly integrated into the DevOps cycle

Overwhelming noise

It's harder than ever to find the signal in the noise

Azure is the only cloud platform built by a security vendor

Microsoft operates a $10B security business

More than 650,000 customers and 90 of the Fortune 100 trust Microsoft SCI solutions

Microsoft employs +8,500 security experts and committed $20B in security investment over the next 5 years

In 2020, 9 billion malware threats were blocked on endpoints by Microsoft 365 Defender

Microsoft processes over 24 trillion signals every 24 hours

Azure security is…

Built-in

Simplified and streamlined security, built directly into Azure

- All cloud resources, all layers of architecture
- Native controls for DevOps, scalable experiences for SecOps
- Broad policy support & actionable best practices

Modern

Protect, detect, and respond with AI and cloud scale

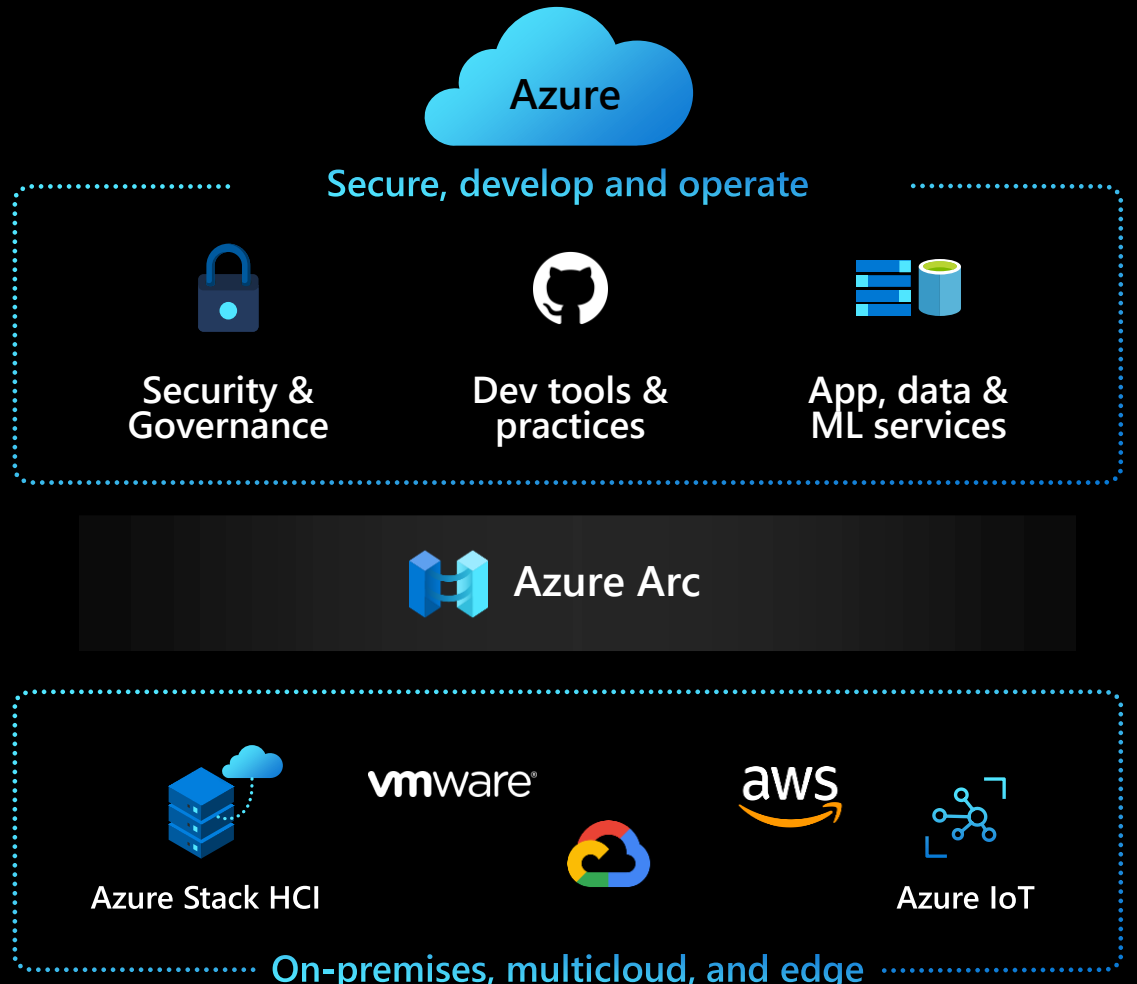
- Reduces false positives with AI trained on trillions of signals
- Streamlines common tasks with automation
- Scale quickly and optimize costs with the cloud

Holistic

Secures your entire organization and works with what you have

- Unified visibility, centrally managed
- Security across hybrid resources
- Multi-cloud posture management and threat protection with EASM and XDR

Innovate anywhere with Azure Arc



Use cases for hybrid and multicloud security

Azure AD

Identity and access management

Microsoft Defender for Cloud

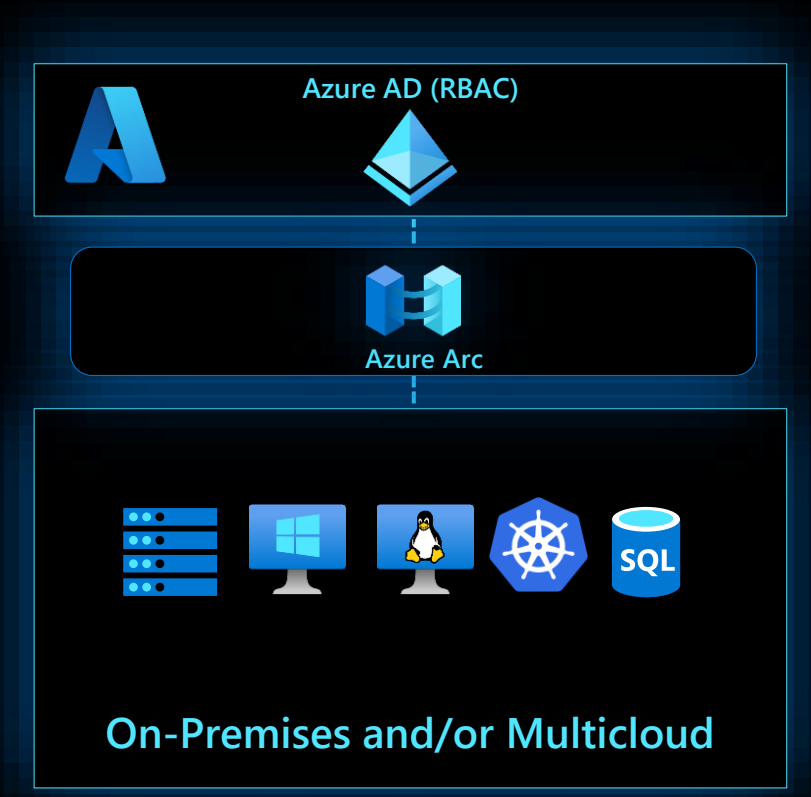
Cloud security posture management and protection

Microsoft Sentinel

Intelligent security analytics across the organization with a cloud-native SIEM

Centralized identity and access control

- Control and delegate access to Azure Arc-enabled resources from the Azure Portal with role-based access control (RBAC)
- Use managed identities to access other Azure resources that support Azure AD-based authentication



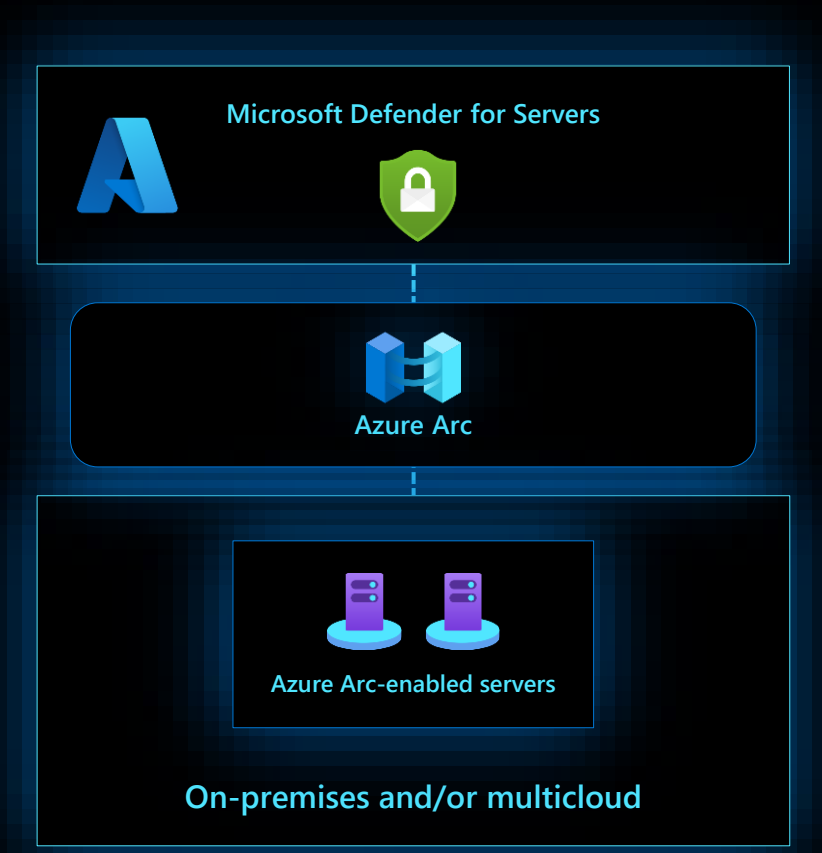
Microsoft Defender for Cloud

Assess, secure, and defend your hybrid and multicloud workloads

- **Continuously assess.** Understand your current security posture, identify and track vulnerabilities. Get a bird's eye-view of your security posture with Secure Score
- **Secure**. Harden connected resources and services by following customized and prioritized recommendations with Azure Security Benchmark
- **Defend**. Detect and resolve threats to those resources and services. With prioritized **security alerts**, focus on what matters the most and surface to the right audience

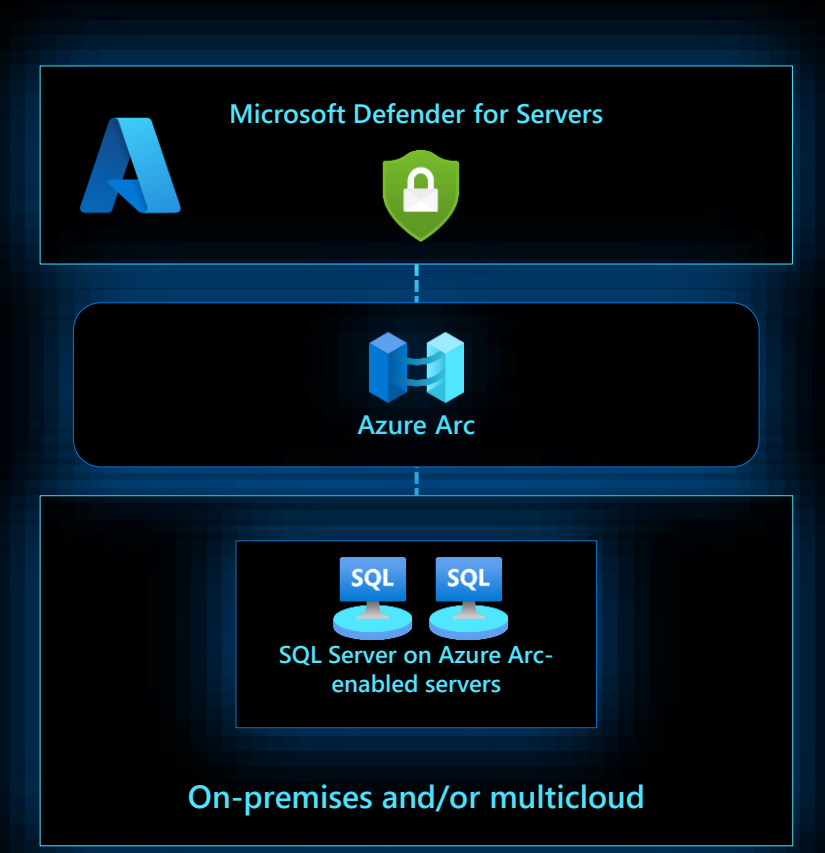
Deploy Defender for Servers anywhere

- Easily deploy as extensions in Azure without re-installing agents
- Vulnerability assessment built-in with flexibility to use tools like Qualys offering integrated vulnerability scanning for your connected machines
- Use Just-in-Time VM access to control access to commonly attacked management ports
- Block malware with adaptive application controls
- Set guardrails with Azure Policy integration, server owners can view and remediate to meet their compliance



Deploy Defender for databases (SQL) anywhere

- Monitor and remediate potential vulnerabilities for SQL Servers in Azure, on-premises or in other clouds
- Discover, track and remediate potential database vulnerabilities with assessment scans.
- Monitor for threats such as SQL injection, brute-force attacks, and privilege abuse with advanced threat protections

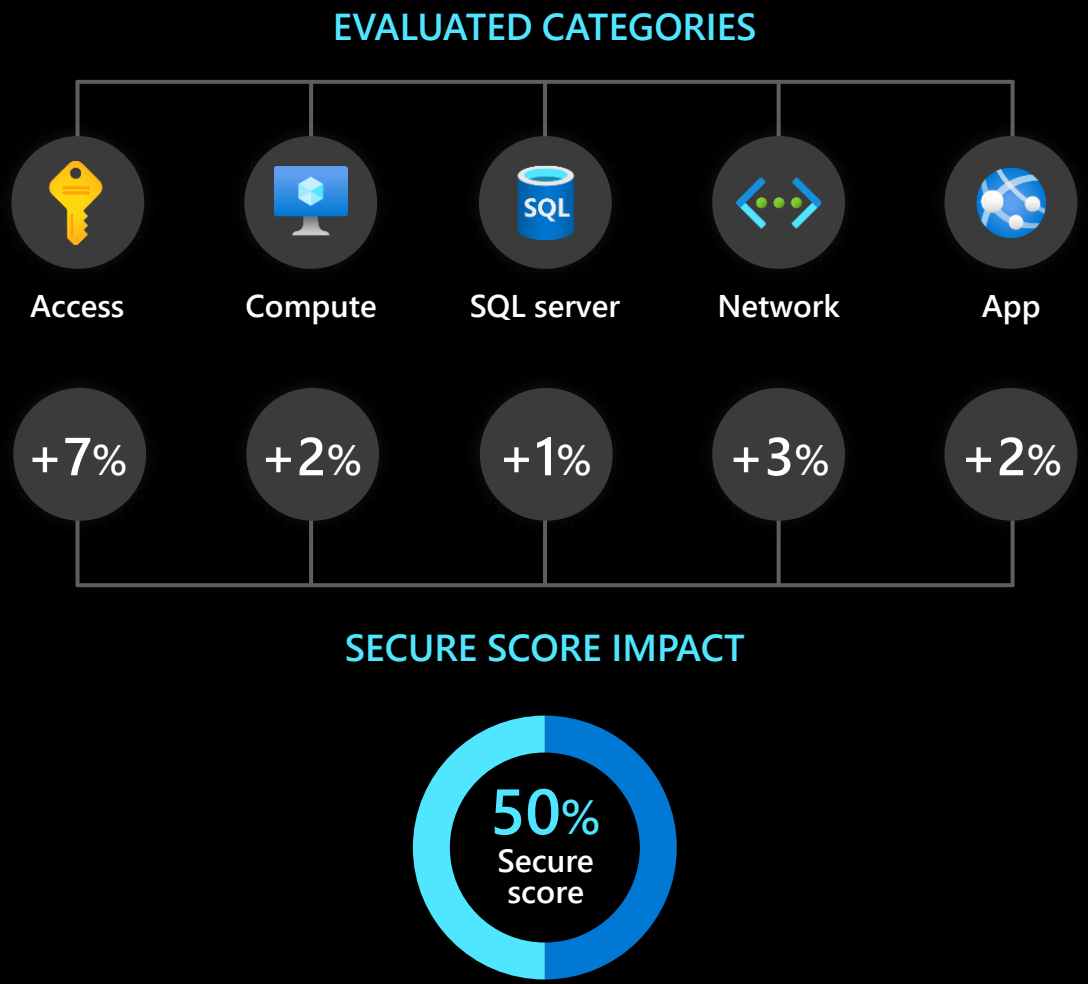


Deploy Defender for Containers anywhere

- Single pane of glass for Kubernetes security—including multi-cloud clusters
- **Environment hardening**—Defender for Containers protects Arc-enabled Kubernetes clusters by providing visibility into misconfiguration and guidelines to help mitigate identified threats

Continuous assessment and Security posture management

- Gain insights into the security state of your cloud workloads across Azure, AWS, and GCP
- Address security vulnerabilities with prioritized recommendations
- Improve your secure score and overall security posture in minutes
- Speed up regulatory compliance
- Granular control of secure score



Secure with tailored recommendations

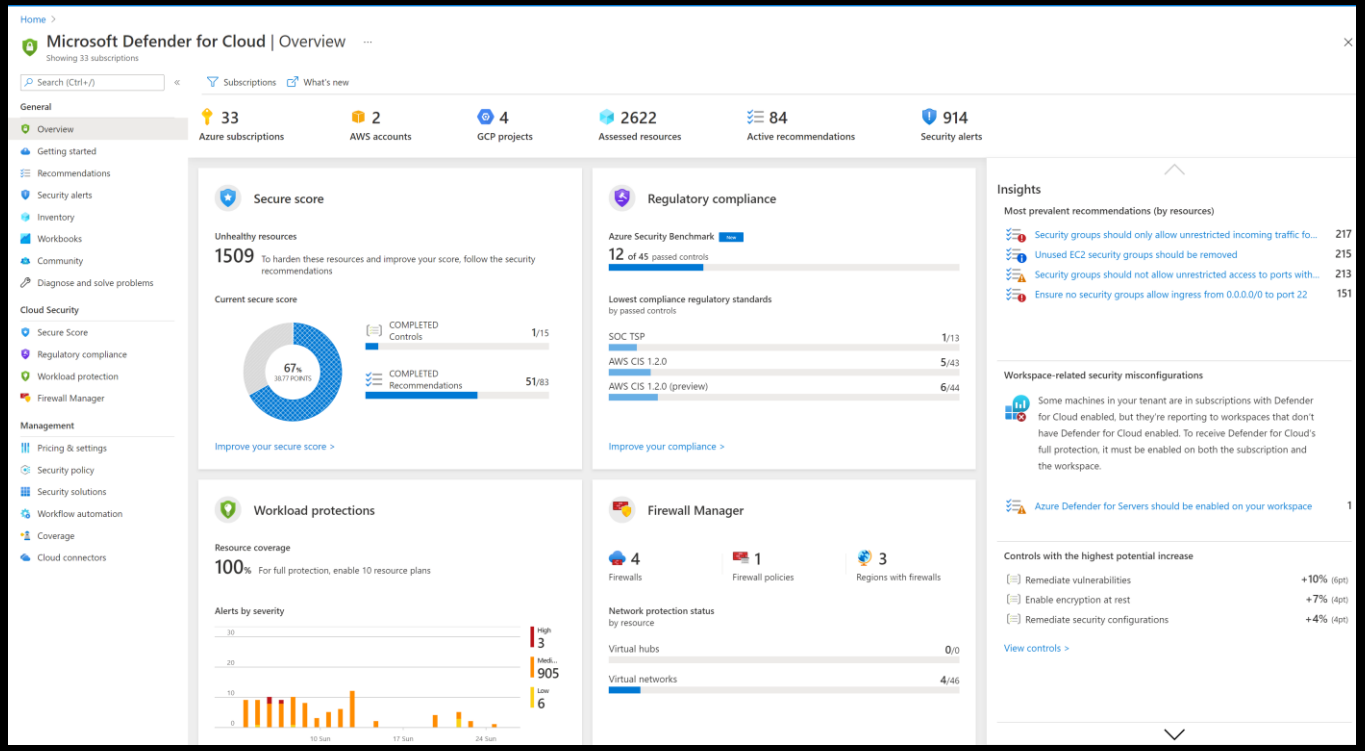
Unified resource view

- All your cloud resources in one place: Azure, AWS, on-premises, and other clouds
- Focused views for security posture, compliance, and workload protection

Clear & simple view

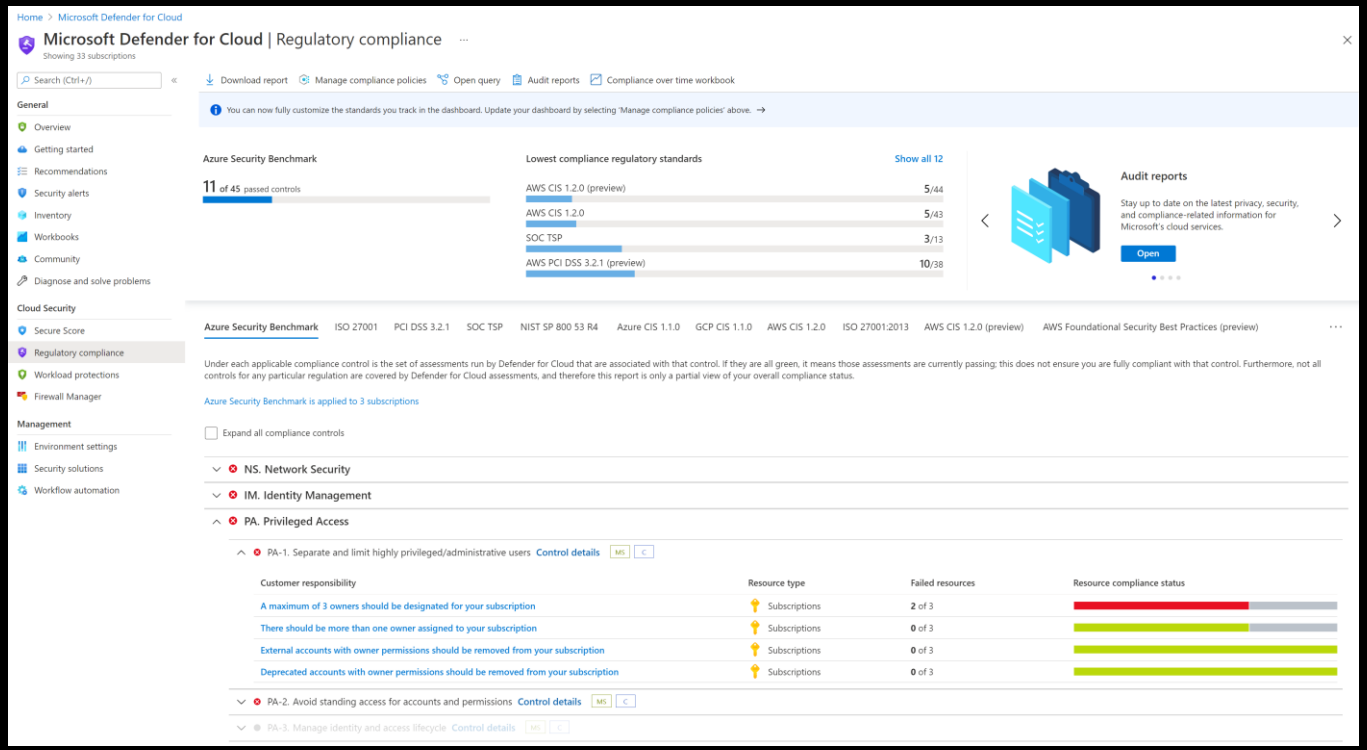
- Identify all your security related stats at a glance

Emphasis on visibility & clear KPIs



Compliance assessment and governance

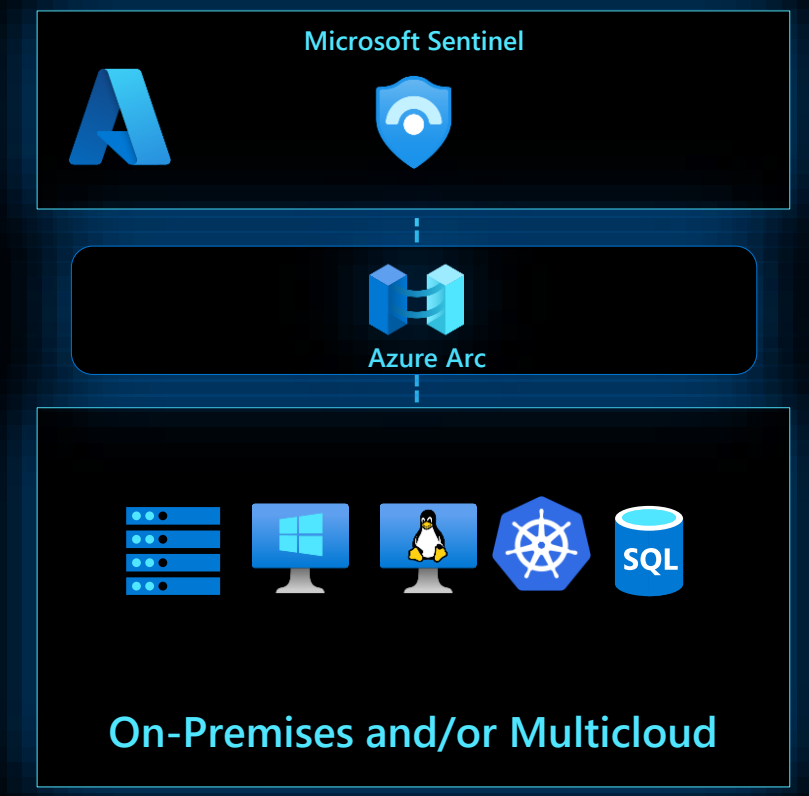
- Demonstrate compliance status, based on continuous assessments of your Azure and AWS resources
- Azure Security Benchmark monitoring enabled by default
- Mapped to the MITRE ATT&CK® framework
- Support for common industry and regulatory standards, as well as custom requirements
- Overview and reports of your compliance status



Microsoft Sentinel

Intelligent, scalable, and cloud native SIEM and SOAR solution.

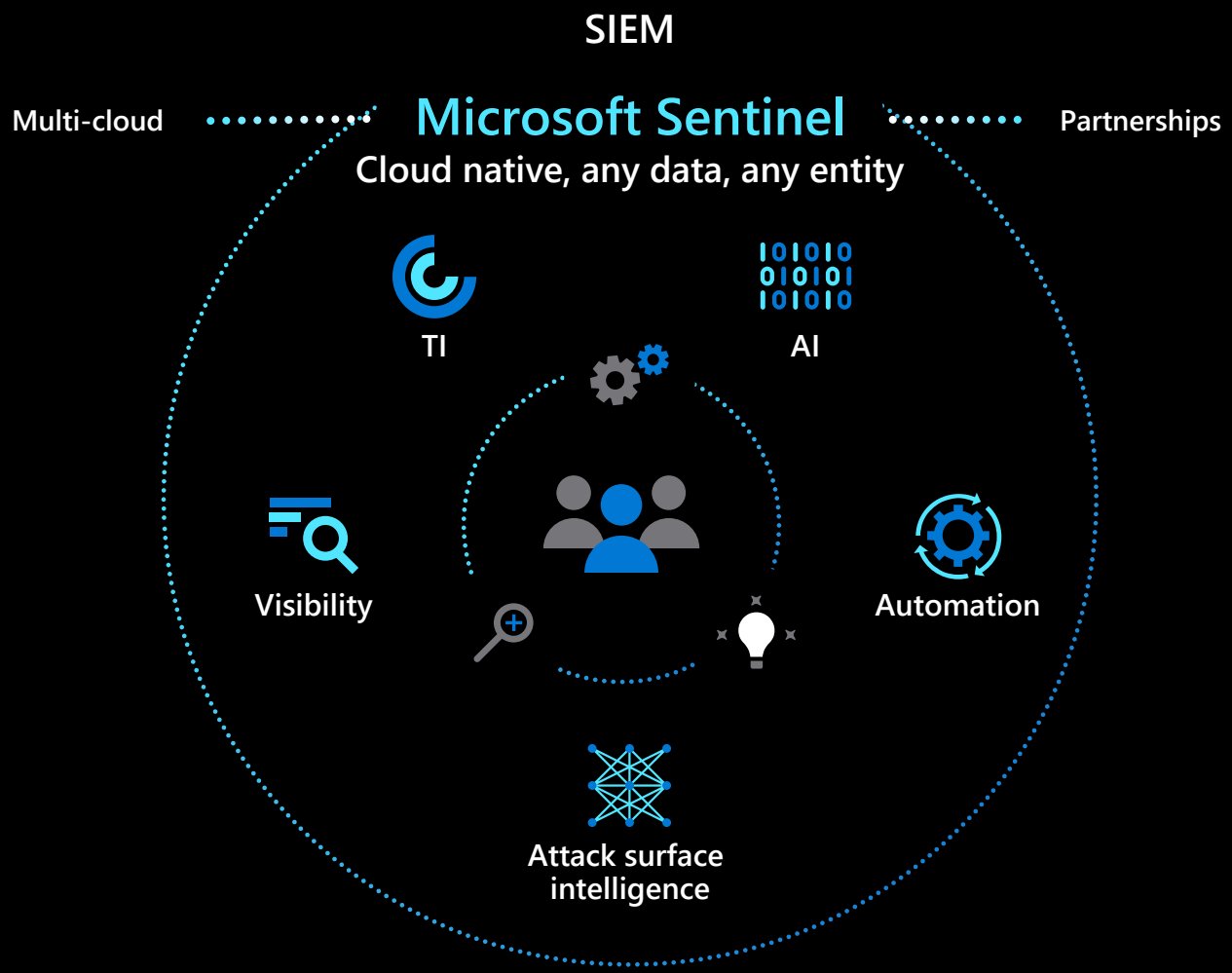
- **Collect** data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds
- **Detect** previously uncovered threats and minimize false positives using analytics and threat intelligence from Microsoft
- **Investigate** threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
- **Respond** to incidents rapidly with built-in orchestration and automation of common tasks



Gain insights across your entire enterprise

First cloud-native SIEM on a major cloud platform, with over 9,000 customers

- Collect security data at cloud scale and integrate with your existing tools
- Leverage AI to detect emergent threats, reducing false positives by 79% over three years[1]
- Respond rapidly with built-in orchestration and automation



1: Commissioned study-The Total Economic Impact™ of Microsoft Azure Sentinel, conducted by Forrester Consulting, 2020

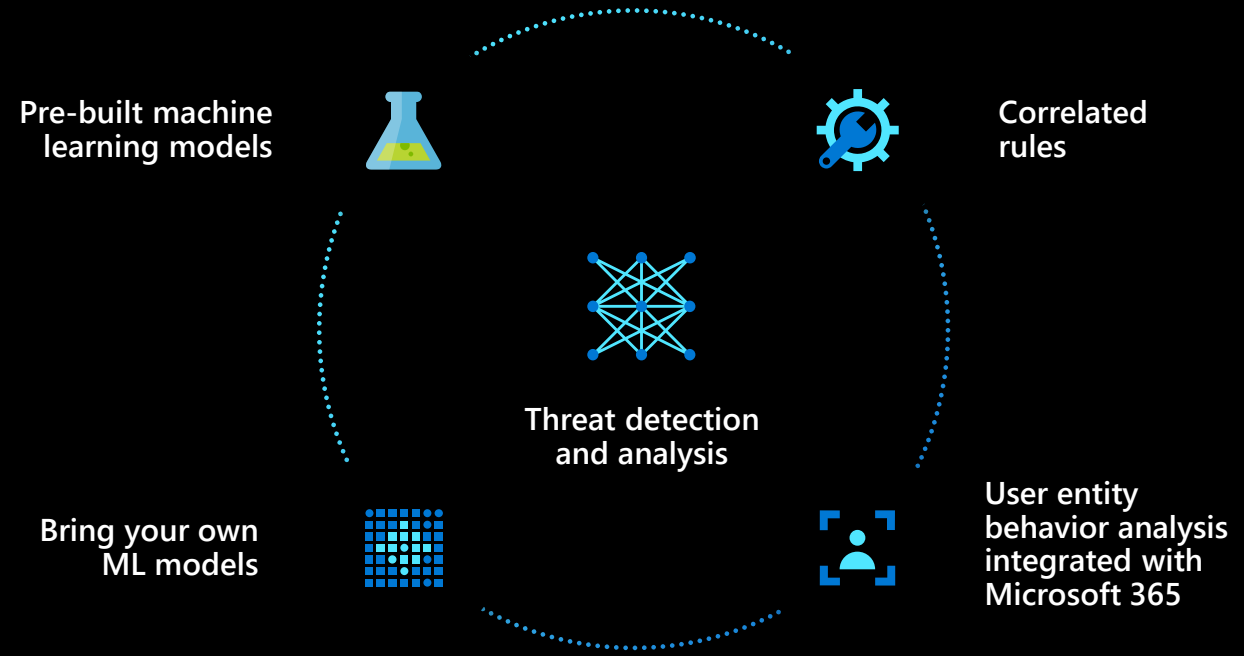
Optimize for your needs

- **Bring your own insights,** machine learning models, and threat intelligence
- Tap into our **security community** to build on detections, threat intelligence, and response automation

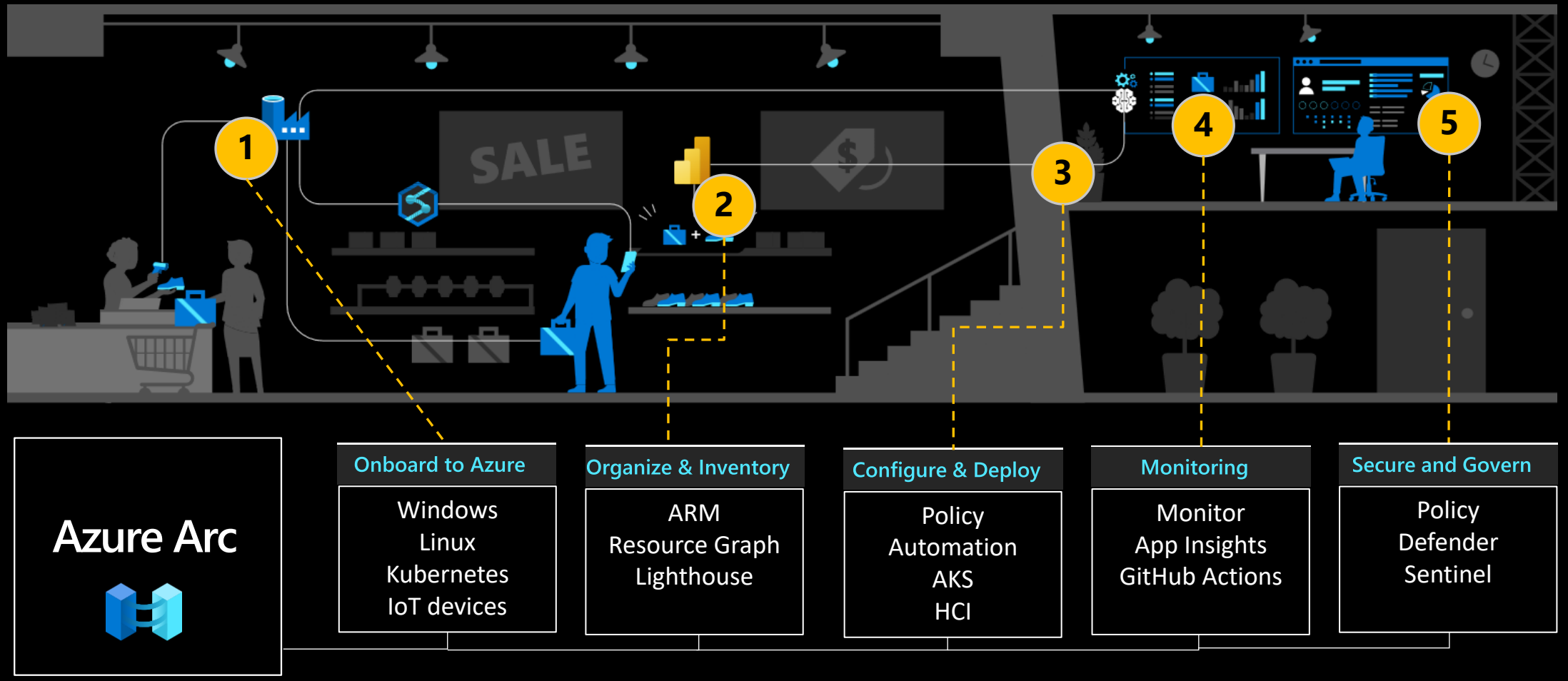
Detect threats and analyze security data quickly with AI

- ML models based on **decades of Microsoft security experience and learnings**
- Millions of signals filtered to few **correlated and prioritized incidents**
- Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%



How it works: Secure and govern digital estate



Example: Intelligent retail

Next steps

Onboard your non-Azure resources to Azure Arc. Use the Azure Arc Jumpstart to get going with ease.

Secure and protect your Arc-enabled resources by enabling Microsoft Defender for Cloud and Microsoft Sentinel.

Get best practices and guidance with the landing zone accelerator for Azure Arc

Gold Sponsors

Community Supporters

Microsoft

Thank you

Rabobank

Customer:
Rabobank
Industry:
Banking & Capital Markets
Size:
10,000+
Country:
Netherlands

Products and services:
Azure Arc
Azure Monitor
Microsoft 365 E5 Security
Microsoft Azure Active Directory
Microsoft Defender for Cloud
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Sentinel

Read full story here

Microsoft

"The difference we've experienced in visibility and threat detection since deploying Microsoft Security solutions is like night and day."

—Raoul van der Voort, Global Service Owner, Cyber Defense Center, Rabobank

Situation:

How does a venerable yet growing global entity balance cutting-edge security, agility, and costs against the demands of a multicloud, hybrid infrastructure that also contains several heterogenous systems? For Rabobank, the answer was clear.

Solution:

The company rolled out Microsoft Defender for Cloud to monitor hybrid, multicloud workloads and connected it with Microsoft Sentinel and Microsoft Defender for Endpoint for broad visibility.

Impact:

Rabobank has done away with several high-ticket license fees for non-Microsoft solutions amounting to €400,000 (USD460,000) in cost savings, reducing its vendor count from 20 down to four. But the heightened security it gained is priceless.

PROSEGUR

Customer:
Prosegur

Industry:
Professional Services

Size:
Corporate (10,000+ employees)

Country:
Spain

Products and services:
Microsoft Azure
Microsoft Azure Arc
Microsoft Azure Automation
Microsoft Azure Defender
Microsoft Azure Monitor
Microsoft Azure Security Center

Read full story here

Microsoft

"By using Azure Arc, we estimate that we'll save about 10 times the effort—and 10 times the cost—to patch and deploy any kind of hardening in Linux servers in comparison with the previous manual method."

—Iñigo Martinez Lasala, Director of Technology and Systems, Prosegur

Situation:

Based in Spain with operations around the world, security company Prosegur needed to easily manage and secure its servers. After many acquisitions, the company wanted to simplify management of its complex, hybrid, multicloud environment.

Solution:

After a successful proof of concept, Prosegur adopted Microsoft Azure Arc to help manage the company's infrastructure. In addition, it uses Azure Defender, Azure Security Center, and Azure Monitor to create a comprehensive security environment.

Impact:

With 700 servers moved and 5,000 total planned, Prosegur is managing its infrastructure on an almost unprecedented scale. The company boosted its security posture while also decreasing costs and minimizing manual tasks by technical staff.