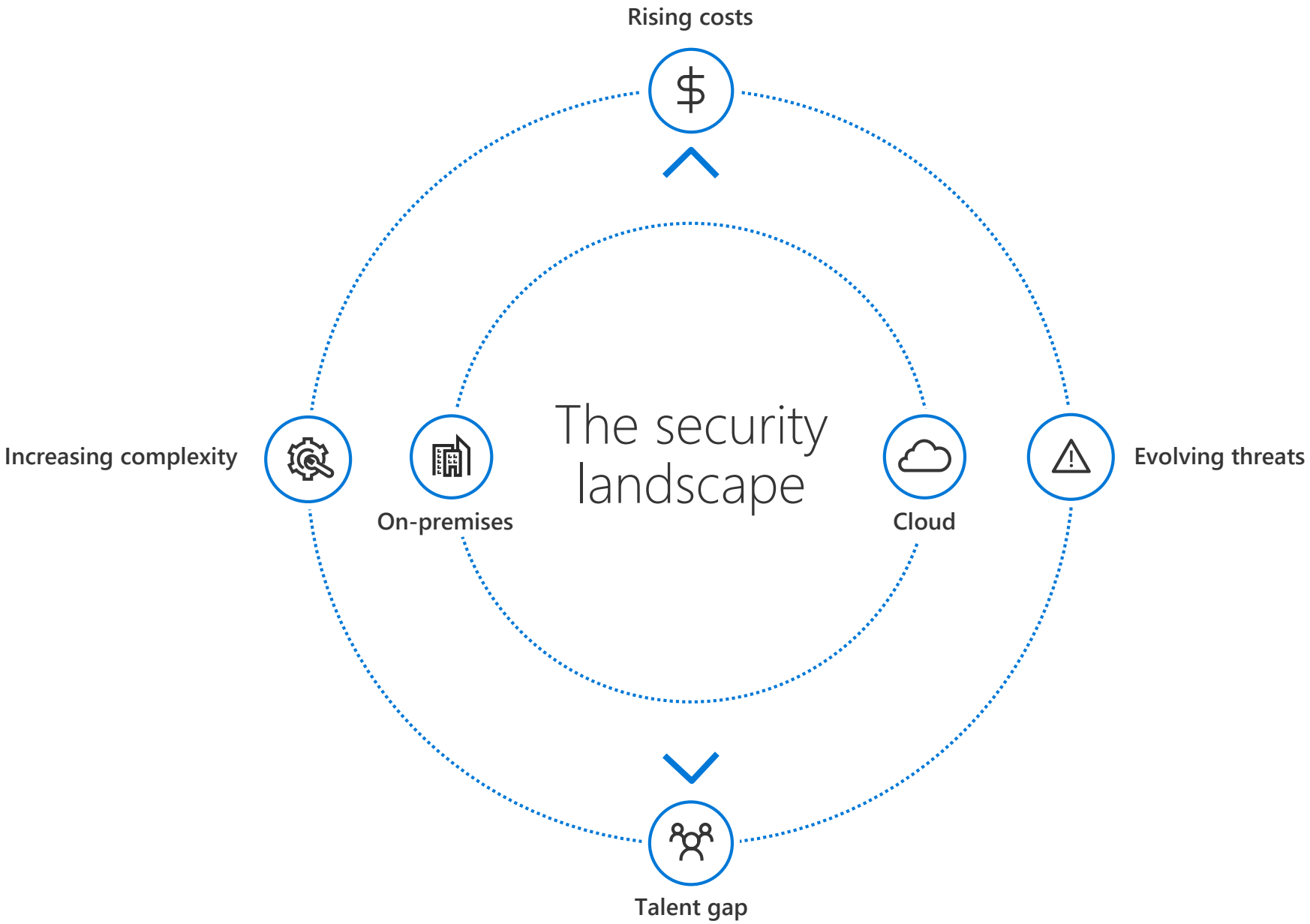
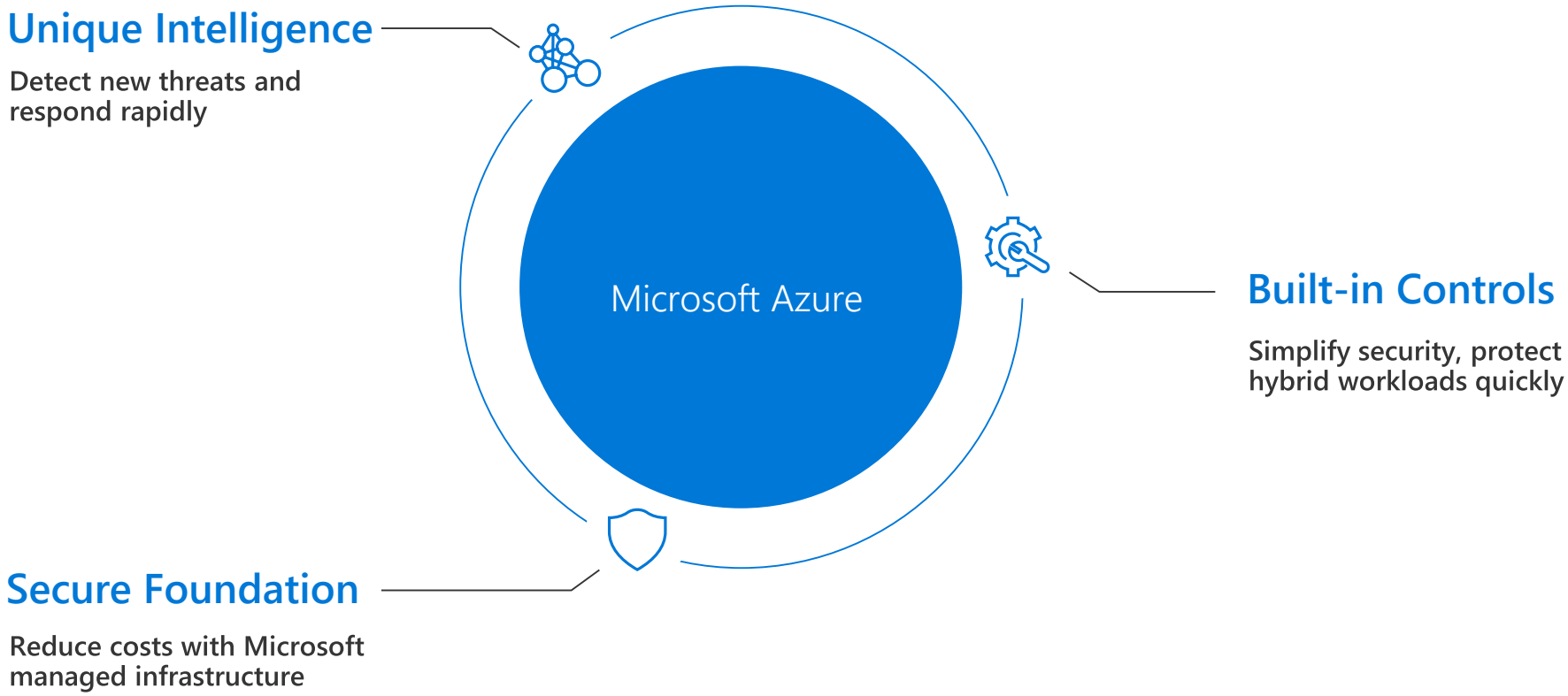
Microsoft

Azure security

Benjamin Tokgöz
Microsoft


Rising costs
Increasing complexity
On-premises
The security landscape
Cloud
Evolving threats
Talent gap

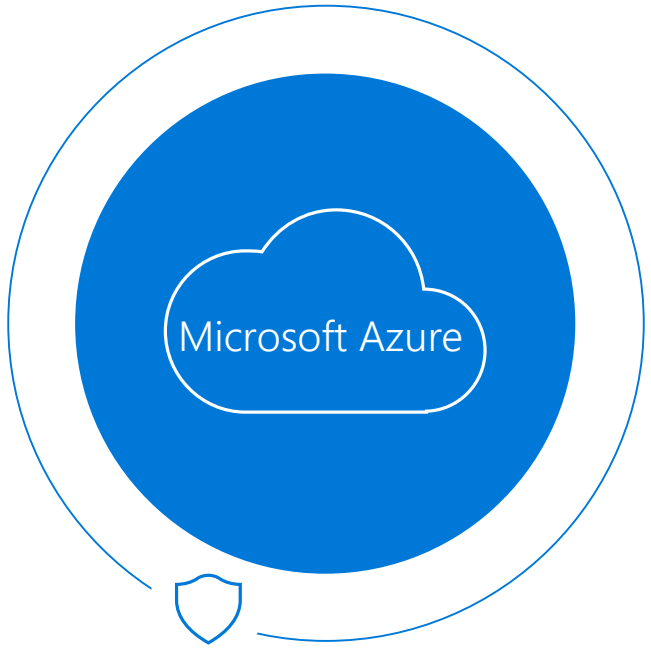
Strengthen security posture with Azure



Secure Foundation

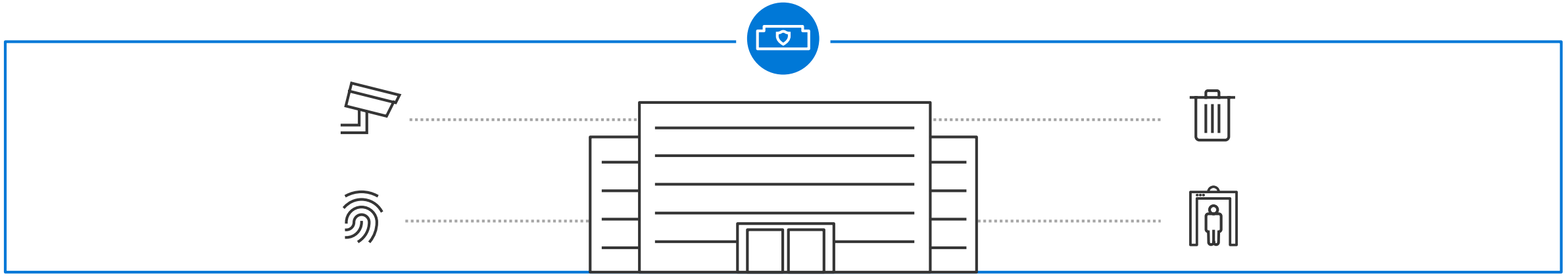
Microsoft managed

- Physical datacenter
- Azure infrastructure
- Operational security



Secure foundation

Physical datacenter security



Global datacenters designed and operated by Microsoft

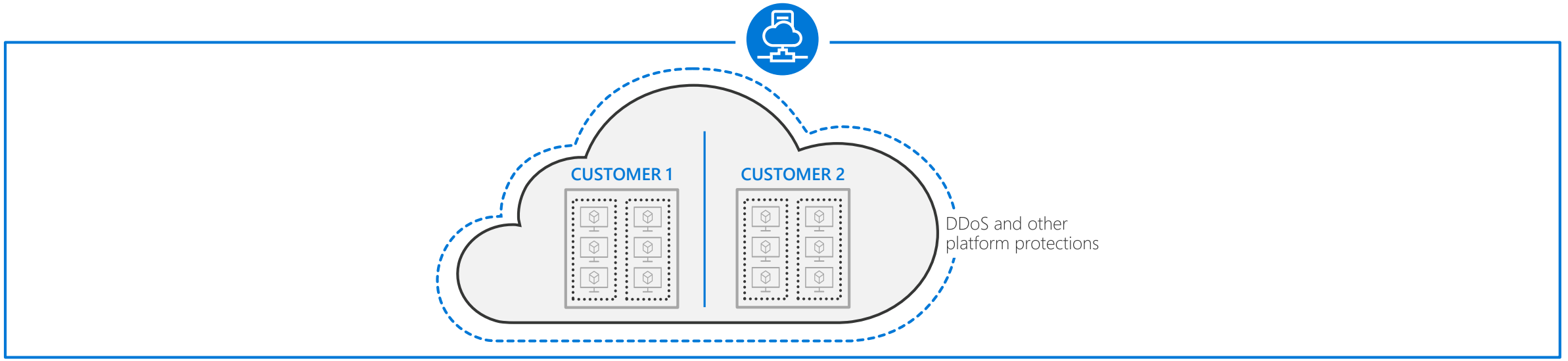
Protected by industry leading security systems

Extensive layers of protection

Helps reduce unauthorized physical access

Secure foundation

Azure infrastructure security



Securing customer data

Data, network segregation. Platform level protections like DDoS

Secure hardware

Custom-built hardware with integrated security and attestation

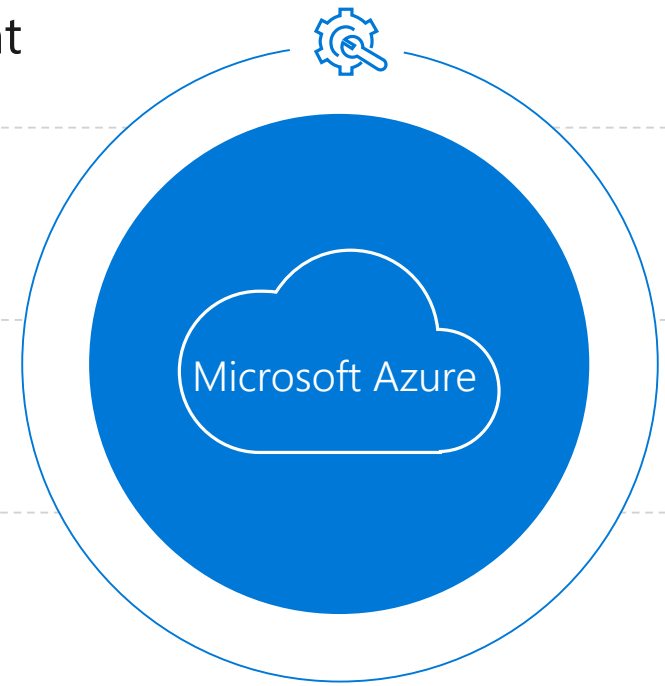
Continuous testing

War game exercises by Microsoft teams, continuous monitoring

Built-in Controls + Partner Integration

Defense-in-depth strategies

- Identity & access management
- Data protection
- Network security
- Threat protection
- Security management



Integrated partner solutions

Built-in Controls | Identity and access management

Manage and control user identity and access

1 Extend on-premises directory to the cloud/same sign-on/single sign-on

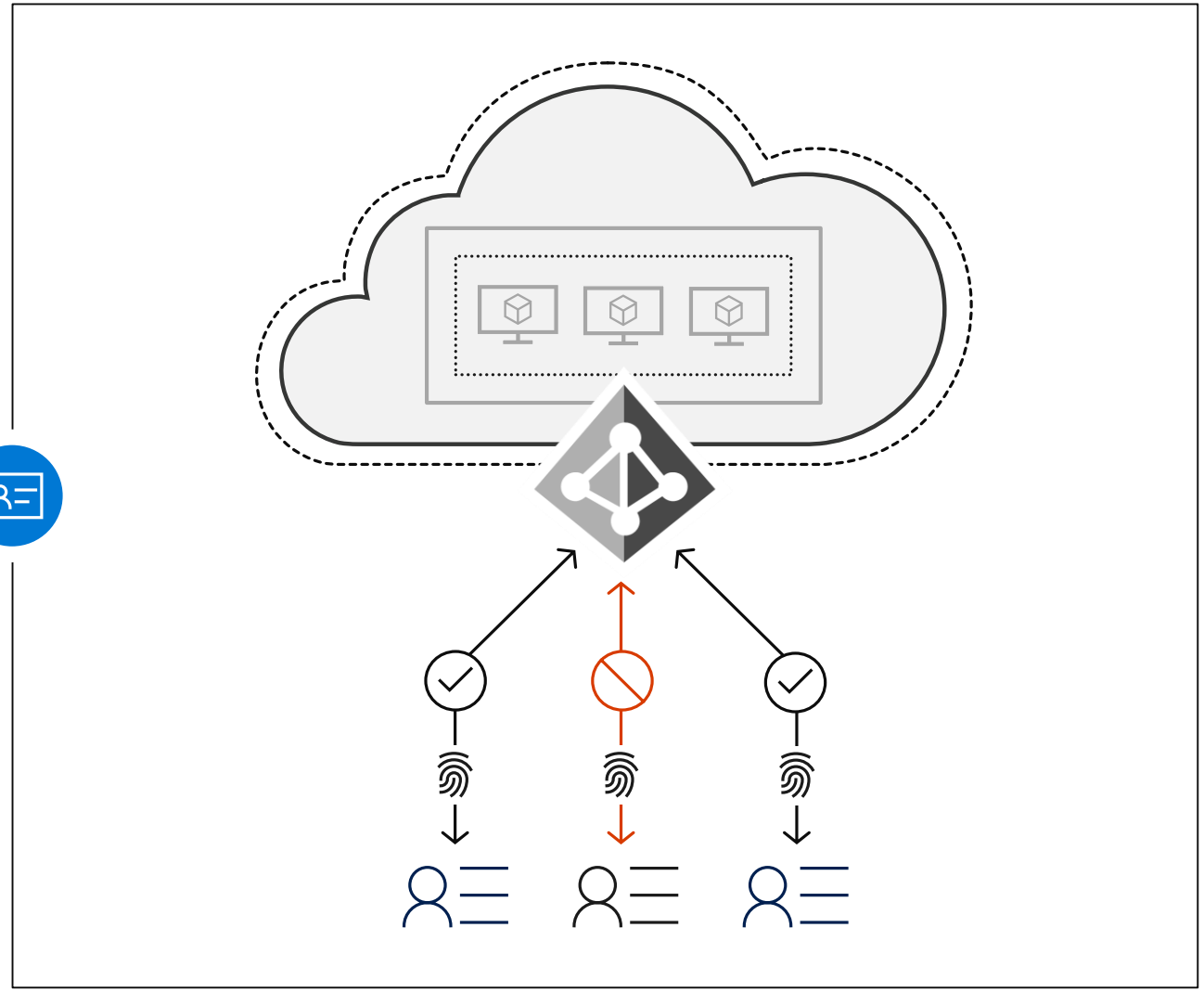
- Azure Active Directory Connect

2 Use principle of least privilege

- Azure Role Based Access Control
- Azure Active Directory Conditional Access based policy

3 Enable additional identity protection

- Configure Multi-factor authentication
- Monitor and control privileged accounts with Azure AD PIM
- Enable additional threat protection with Azure AD Identity Protection



Built-in Controls | Data protection

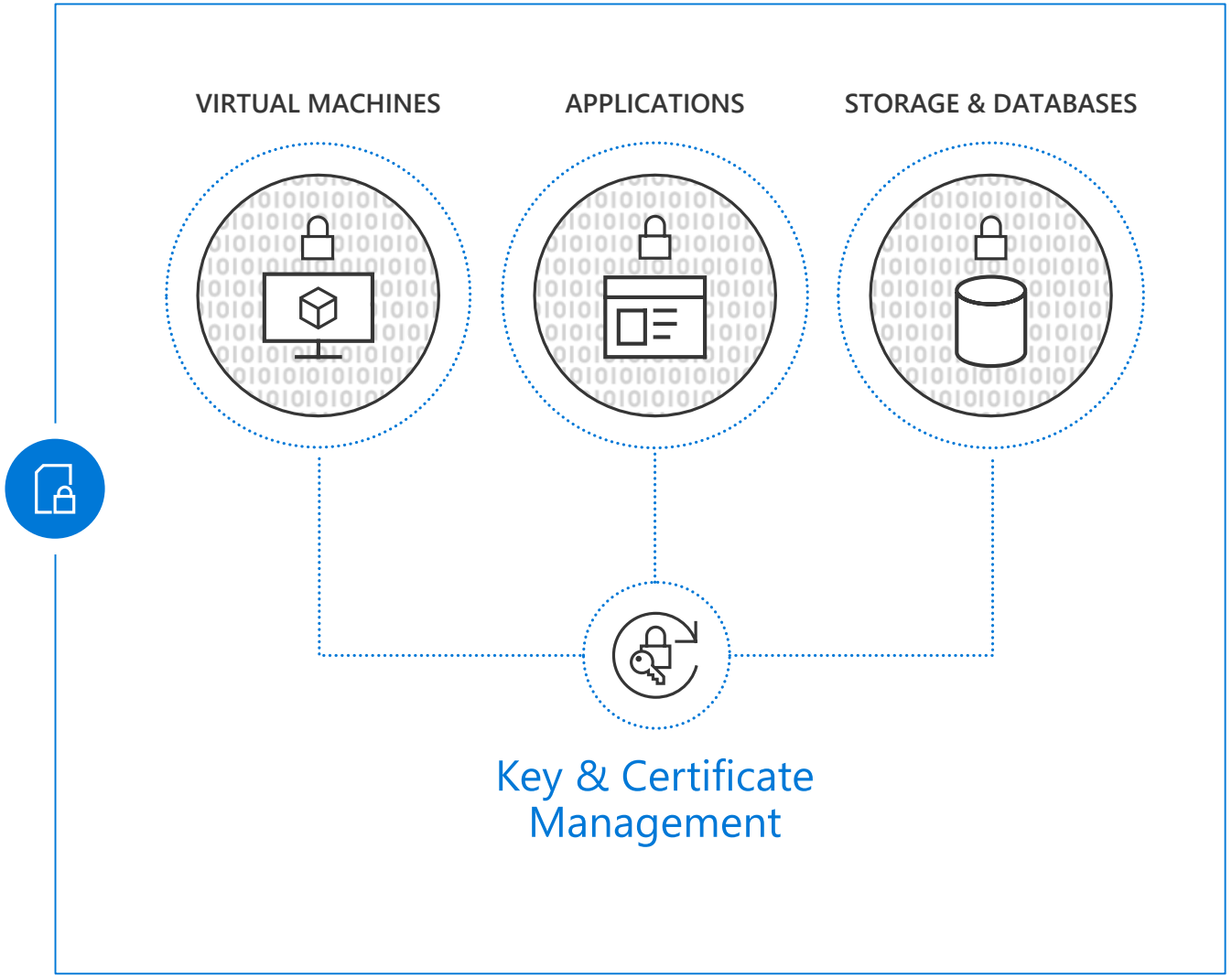
Encrypt data and communications

Enable encryption across workloads to protect data

Integrated options across disks, storage, SQL

Safeguard keys and other secrets using HSMs

Maintain control over encrypted data — grant and revoke key use by your own and third party applications as needed



Built-in Controls | Data protection

Encrypt data and communications

1 Enable built-in encryption across resources

- Azure Storage Service Encryption
- Azure Disk Encryption
- SQL TDE/Always Encrypted

2 Encrypt data while in use

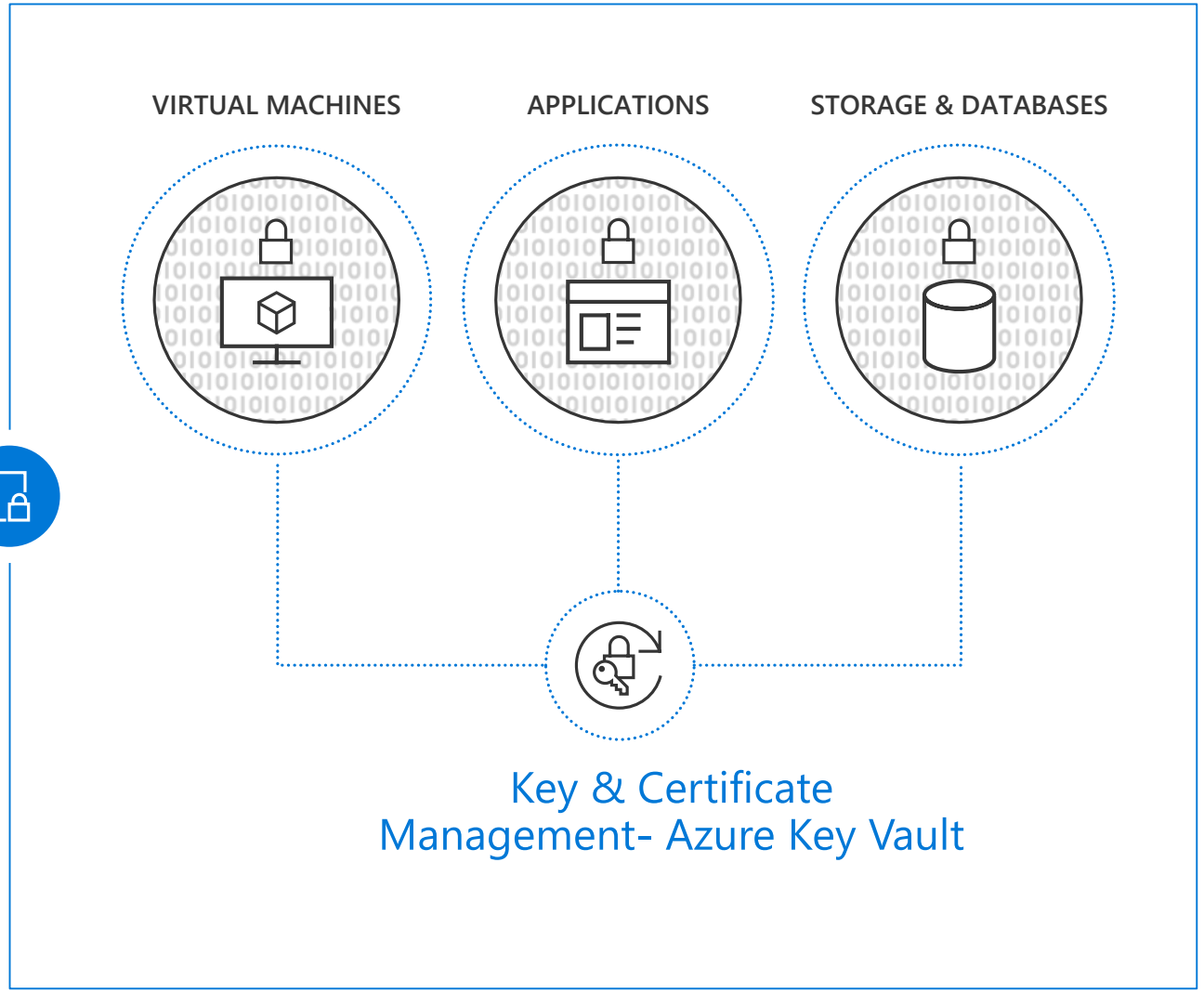
- Azure confidential computing

3 Use delegated access to storage objects

- Shared Access Signature enables more granular access control

4 Use a key management system

- Keep keys in a hardware HSM/don't store key in apps/GitHub
- Use one Key Vault per security boundary/per app/per region
- Monitor/audit key usage-pipe information into SIEM for analysis/threat detection
- Use Key Vault to enroll and automatically renew certificates



Built-in Controls | Network security

Strengthen network access controls

1 Configure network access rules, segmentation

- Set-up appropriate Network security group (NSG) or Application security group rules & Azure Firewall
- Use Virtual Network Appliance to enable additional filtering

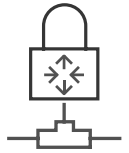
2 Avoid exposure to the Internet with dedicated WAN links

- Use Site to site VPN
- Azure ExpressRoute

3 Enable additional protections to ensure application availability

- Use Application Gateway & Web Application Firewall
- Configure DDoS Protection Standard

Network security groups



VPN

Web Application Firewall, Azure Firewall

DDoS Protection

Partner Solutions

Extend your existing security solution to Azure with Marketplace

Identity & access management

- RSA
- Omada
- PingIdentity.
- DUO
- SailPoint

Data protection

- gemalto (security to be free)
- SafeNet (The Foundation of Information Security)
- THALES
- SECURED BY CRYPTERON

Network security

- Palo Alto Networks
- Check Point SOFTWARE TECHNOLOGIES LTD.
- f5
- cisco
- Barracuda

Threat protection

- Symantec
- McAfee
- Qualys Inc
- RAPID7
- aqua

Security management

- HPE ArcSight
- Splunk
- IBM QRadar
- ALERT LOGIC

And **hundreds** more with new partners integrating every month

Built-in Controls

Simplify security with Azure services

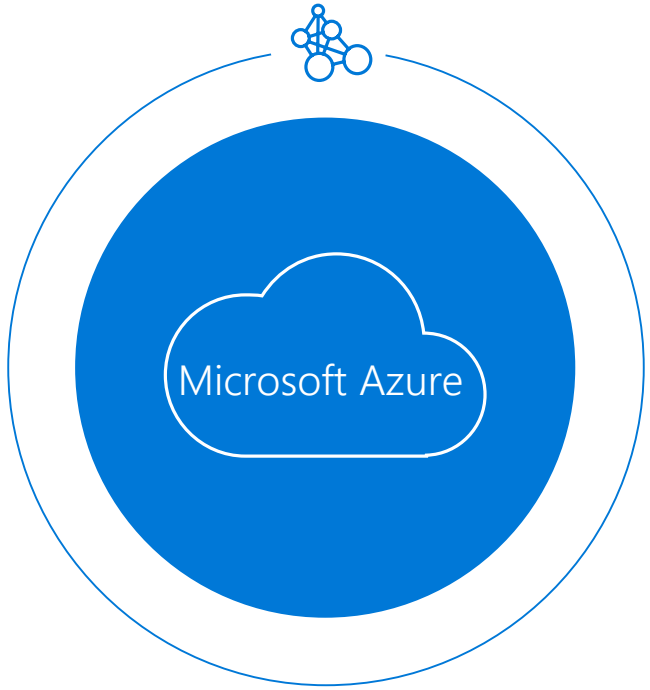
Identity & access management	Data protection	Network security	Threat protection	Security management
Azure Active Directory	Encryption (Disks, Storage, SQL)	VNET, VPN, NSG	Azure Security Center	
Multi-Factor Authentication	Azure Key Vault	Application Gateway (WAF), Azure Firewall	Microsoft Antimalware for Azure	Azure Log Analytics
Role Based Access Control	Confidential Computing	DDoS Protection Standard		
Azure Active Directory (Identity Protection)		ExpressRoute		

+ Partner Solutions

Unique Intelligence

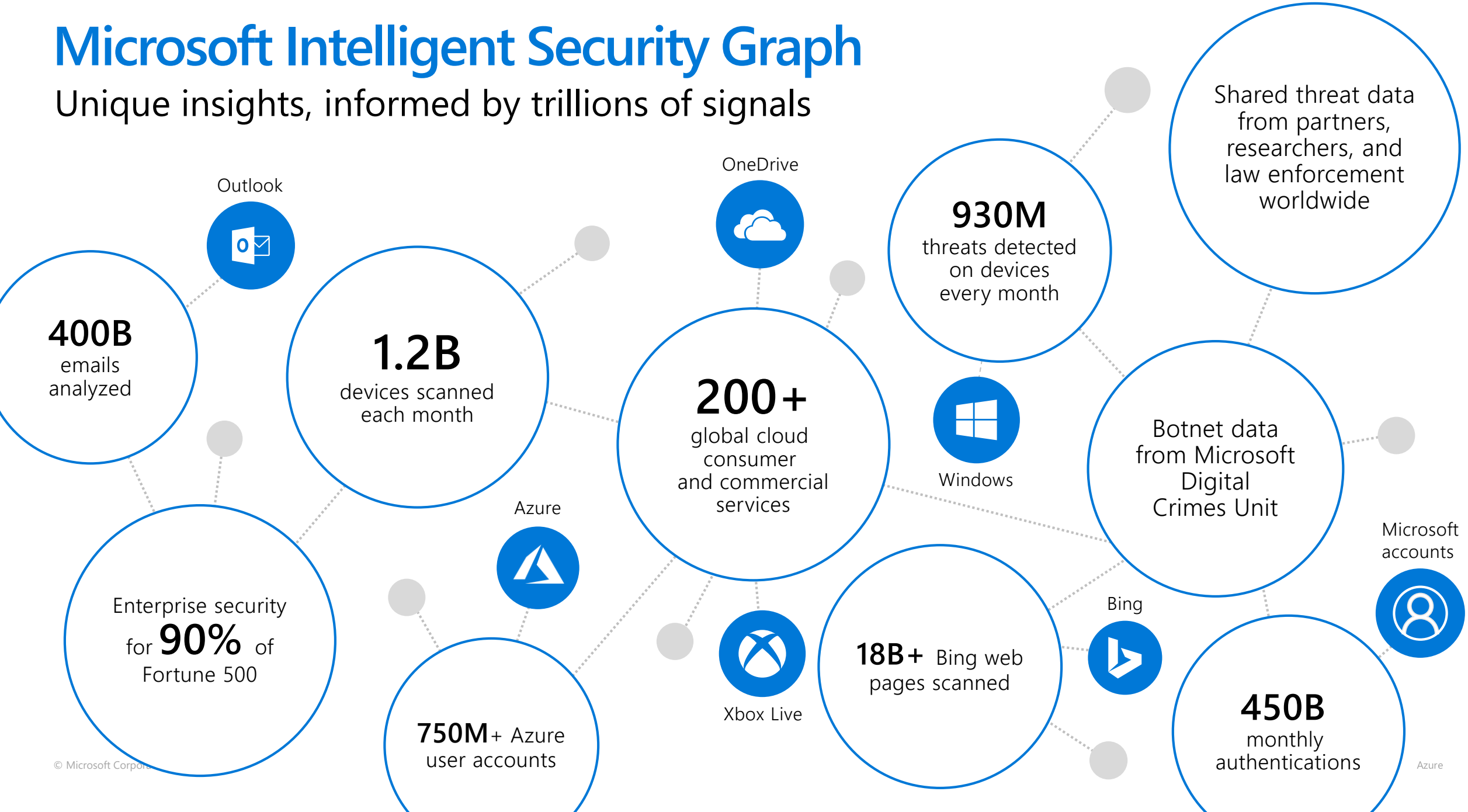
Integrated with Microsoft services

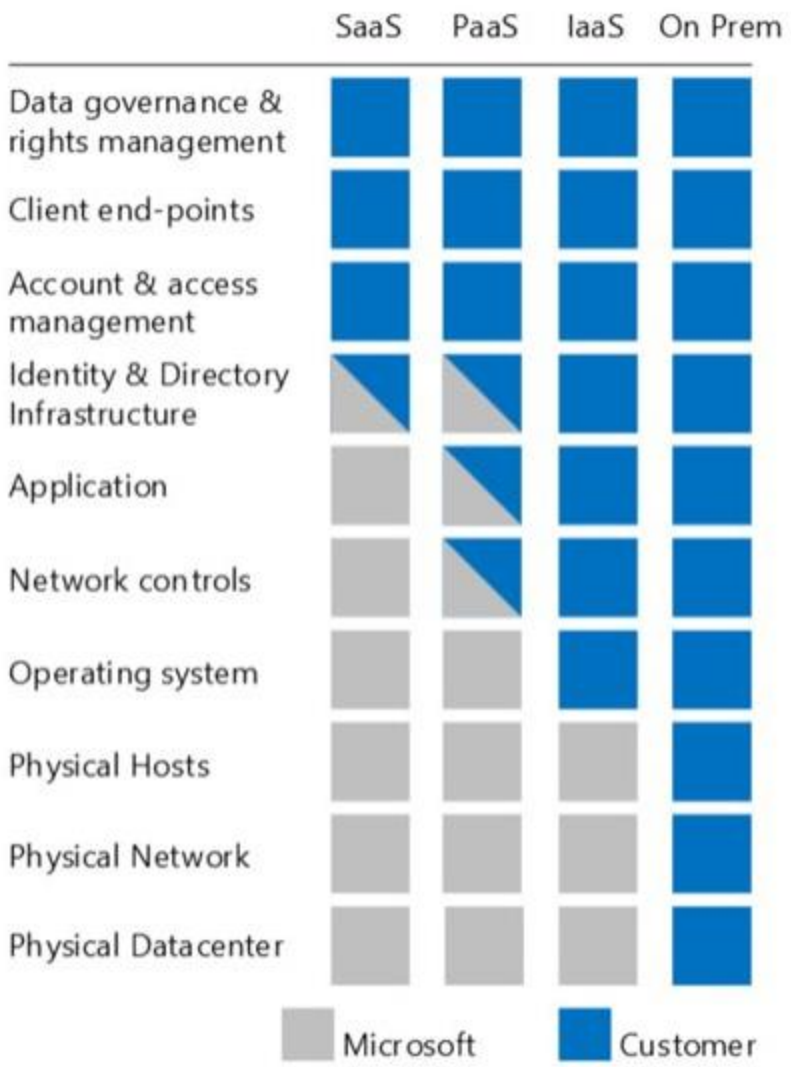
- Machine learning
- Threat intelligence
- Behavior analytics



Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals





The Cloud principles

Only you own and manage your data.

The Cloud supports you with the underlying infrastructure.

Microsoft

Security Center

Microsoft Azure Security Center

Unify security management and enable advanced threat protection for hybrid cloud workloads

Unified visibility and control

Adaptive threat prevention

Intelligent detection and response

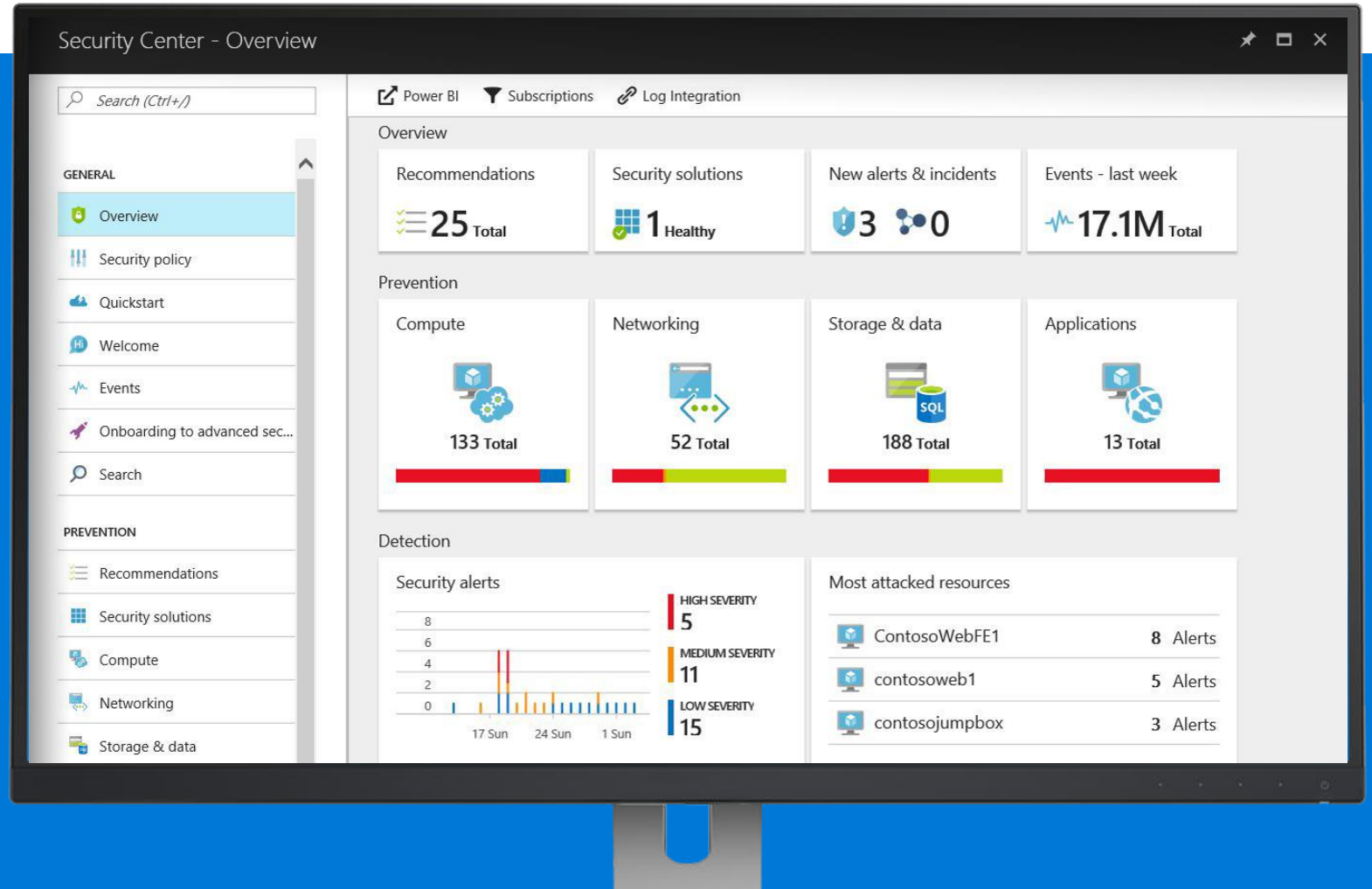
Understand security state across hybrid workloads

Built-in Azure, no setup required

- Automatically discover and monitor security of Azure resources

Gain insights for hybrid resources

- Easily onboard resources running in other clouds and on-premises



Analyze security information from variety of sources

Integrated partners

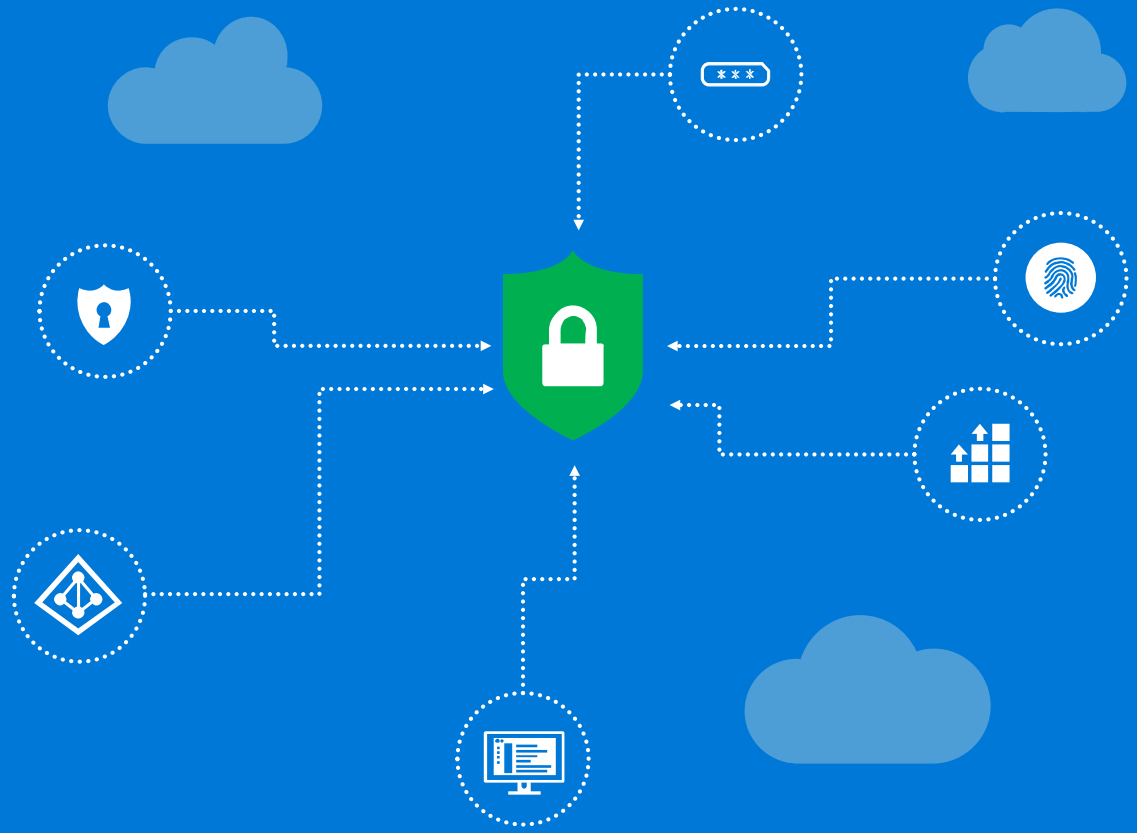
- Connected security solutions running in Azure, e.g. firewalls and antimalware solutions

Microsoft security

- Azure Active Directory Information Protection
- Advanced Threat Analytics

Many others

- Any security solution that supports Common Event Format (CEF)



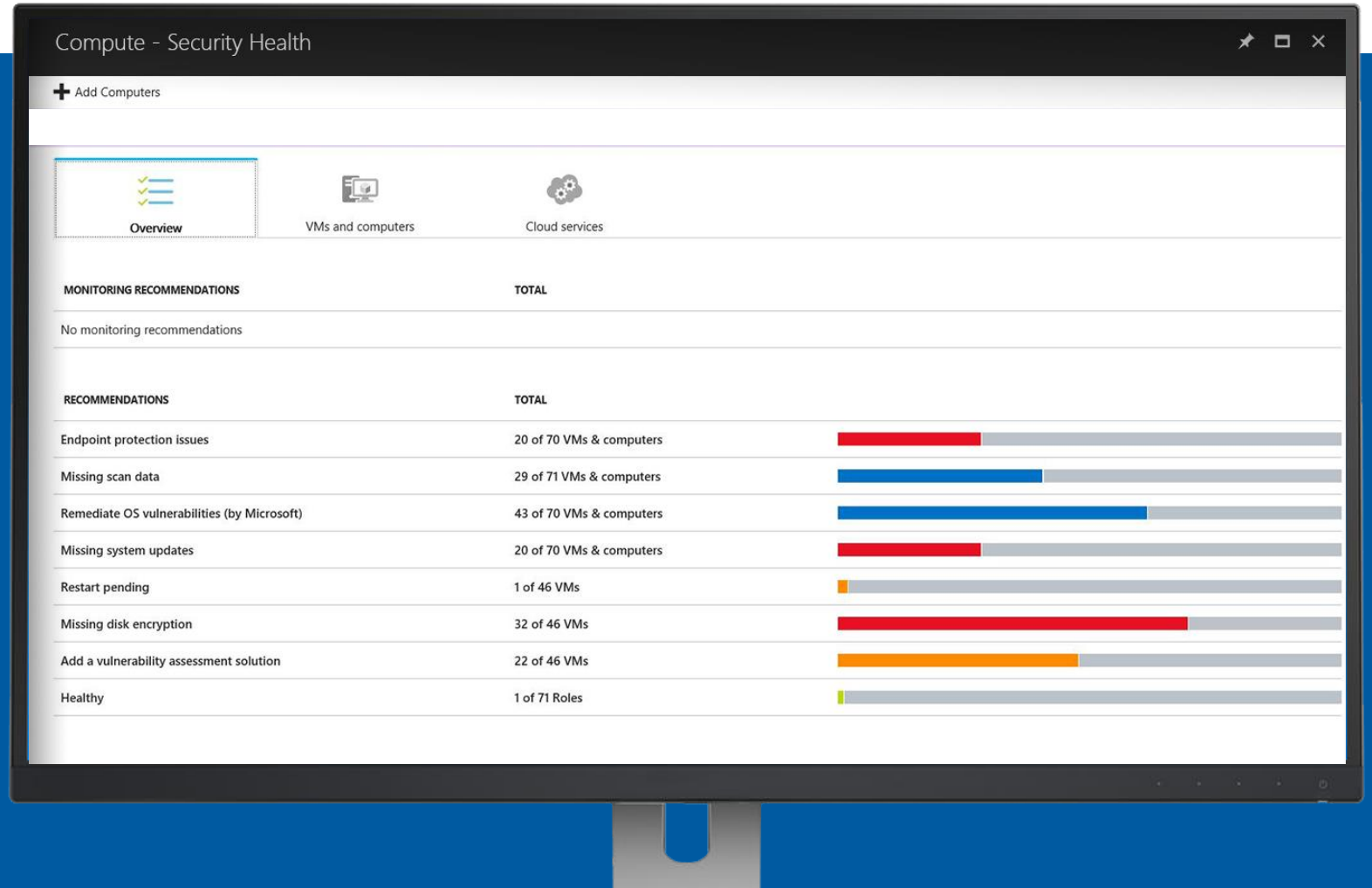
Identify and remediate vulnerabilities quickly

Continuous assessment of machines, networks, and Azure services

- Hundreds of built-in security assessments, or create your own

Fix vulnerabilities quickly

- Prioritized, actionable security recommendations



Demo

Microsoft