Microsoft

Azure & Security: Overcoming Concerns

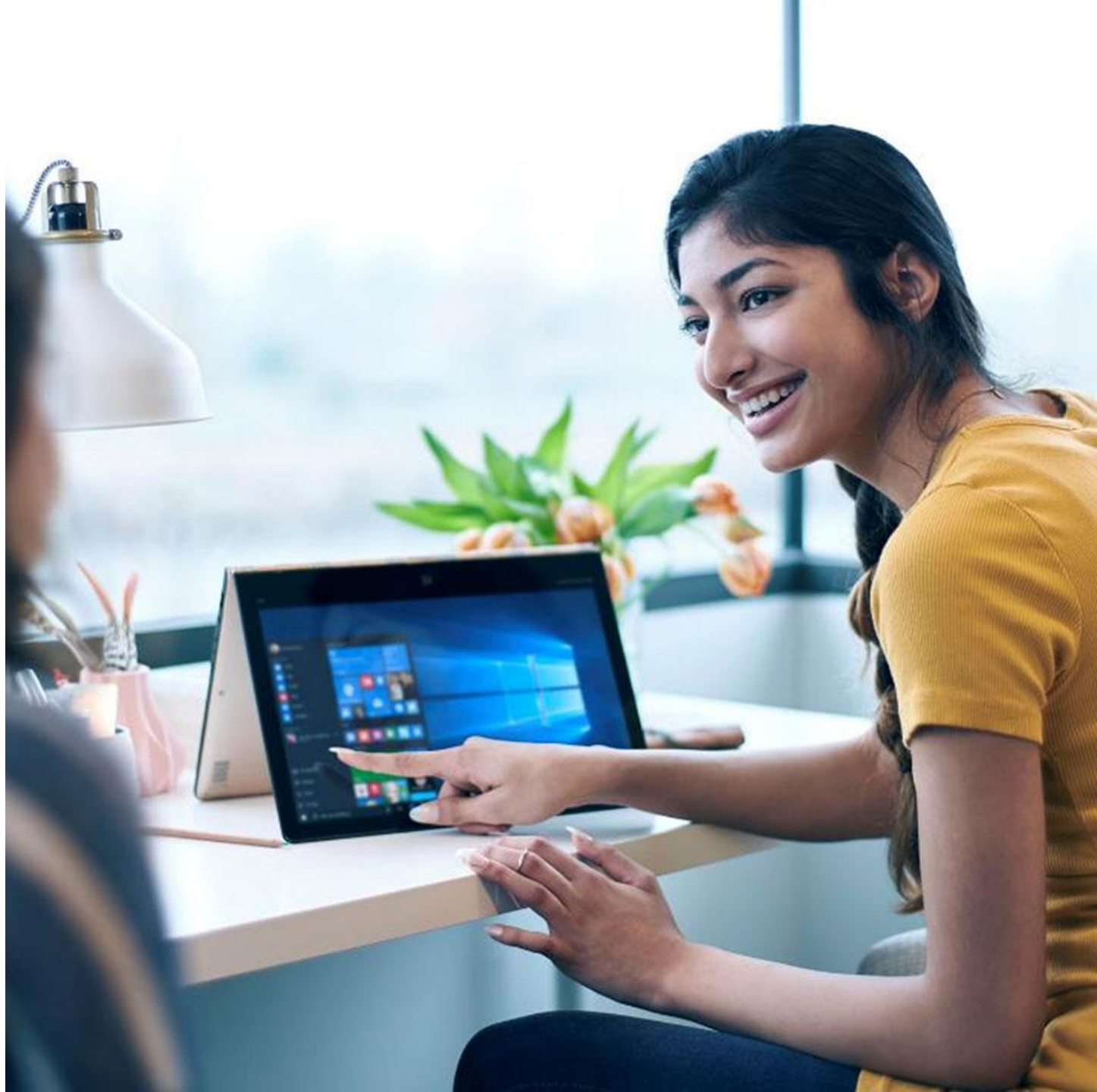
Paul Masschelin
Greg White

June 18, 2019

What you should learn today

- 3 Core Components of the Azure Security Model
- Security Landscape & Challenges
- How Microsoft Helps Protect You
- Key Strategies
- Importance of Compliance

3 Core Components of the Azure Security Model



Microsoft

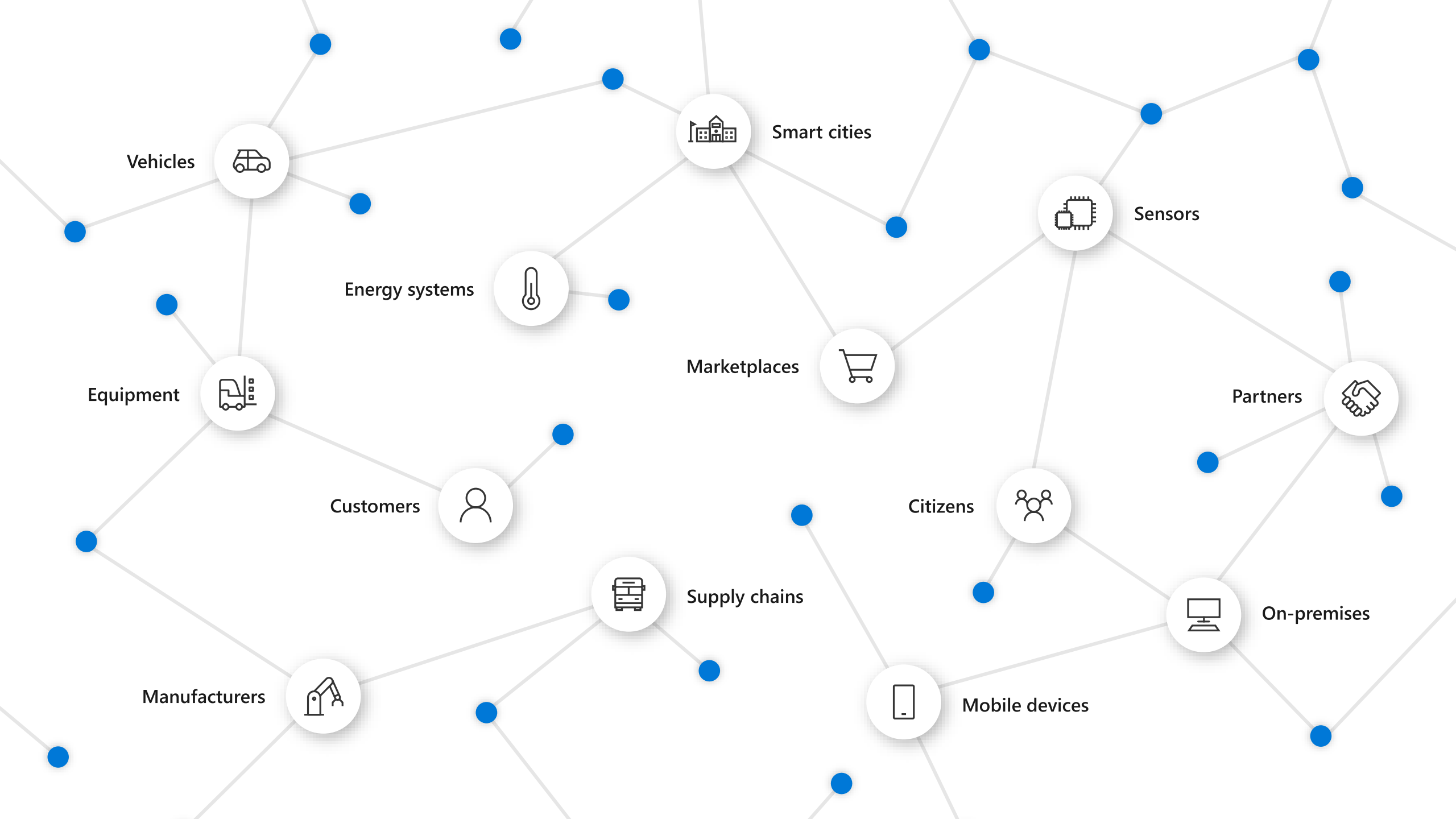
Security Landscape and Challenges

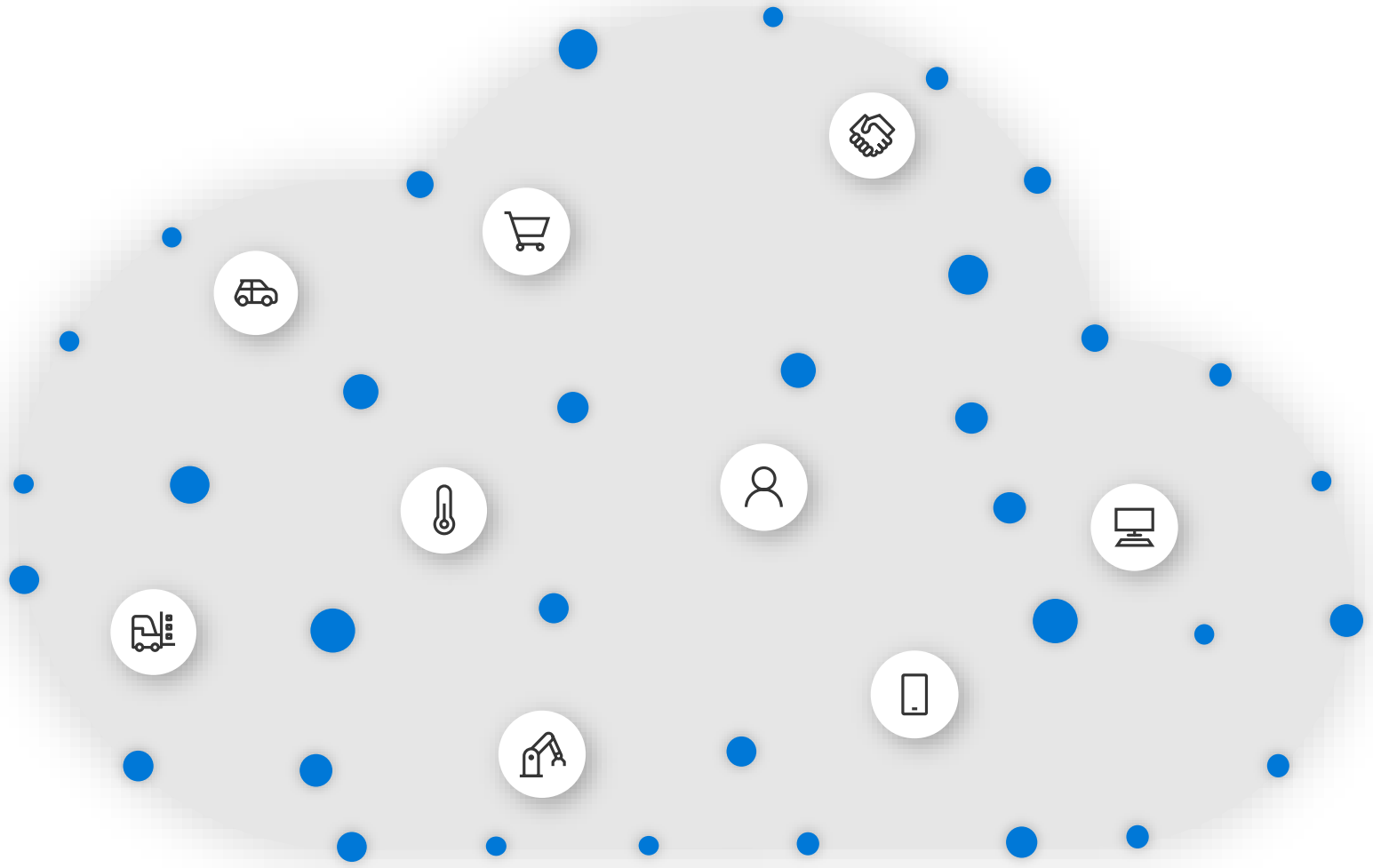
The cybersecurity landscape is rapidly changing

Cyberspace is the new battlefield

Security skills are in short supply

Virtually anything can be attacked

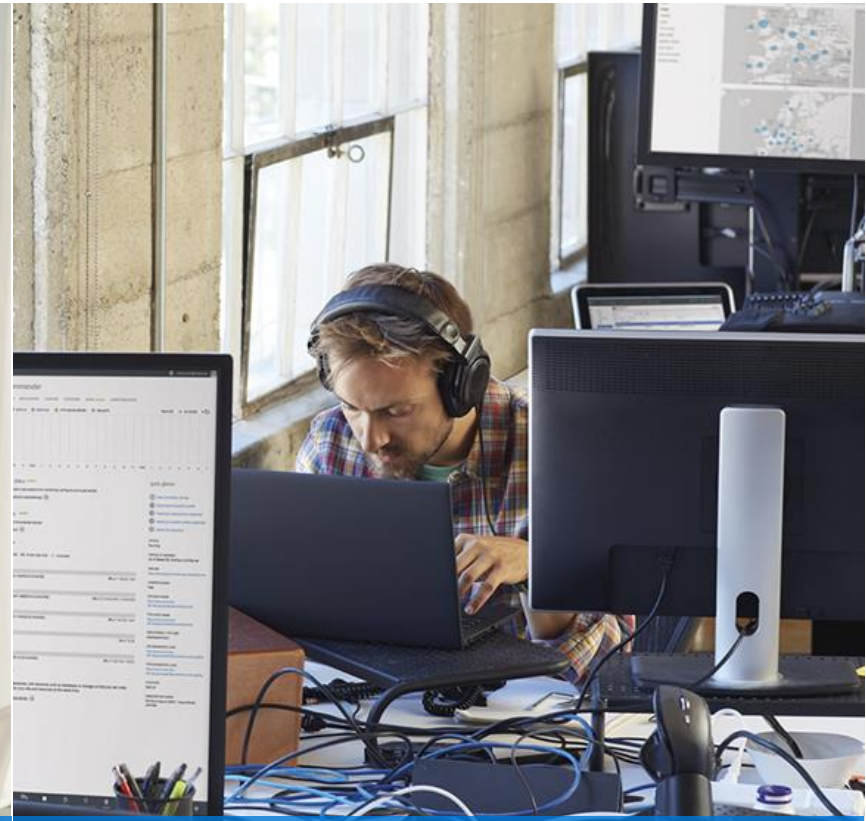

Vehicles
Smart cities
Sensors
Energy systems
Marketplaces
Equipment
Partners
Customers
Citizens
Supply chains
On-premises
Manufacturers
Mobile devices



Digital transformation is driving change

IT embracing change

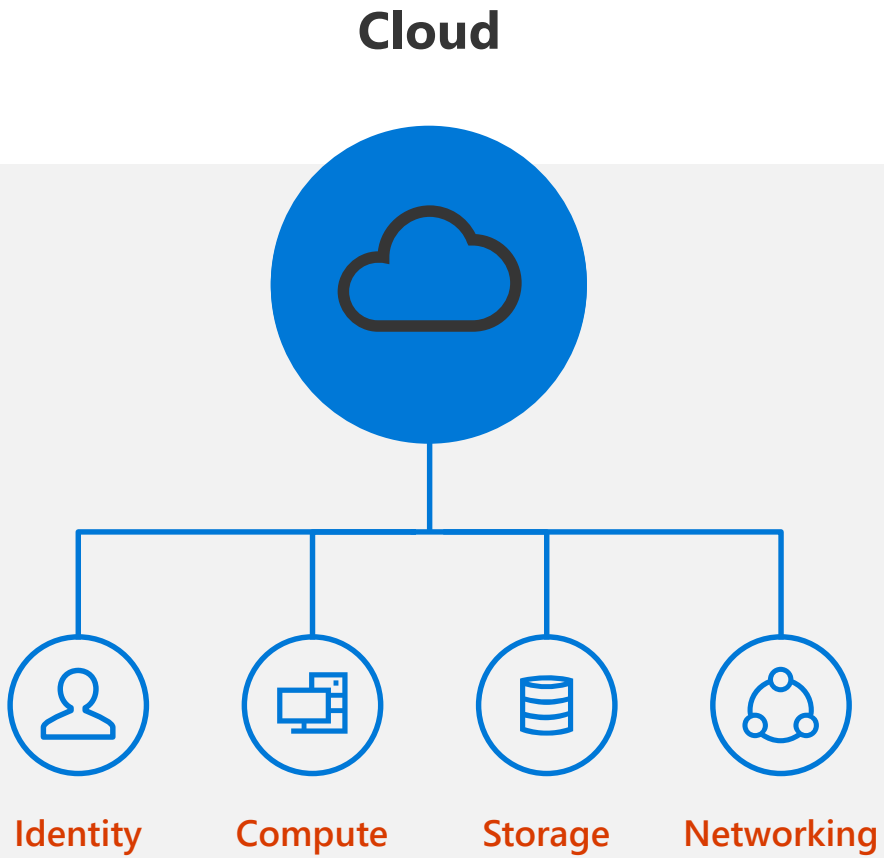
Business units



Developers

Rise of cloud workload owners | Security is everyone's issue | Need to expand beyond management contacts

Cloud adoption is growing



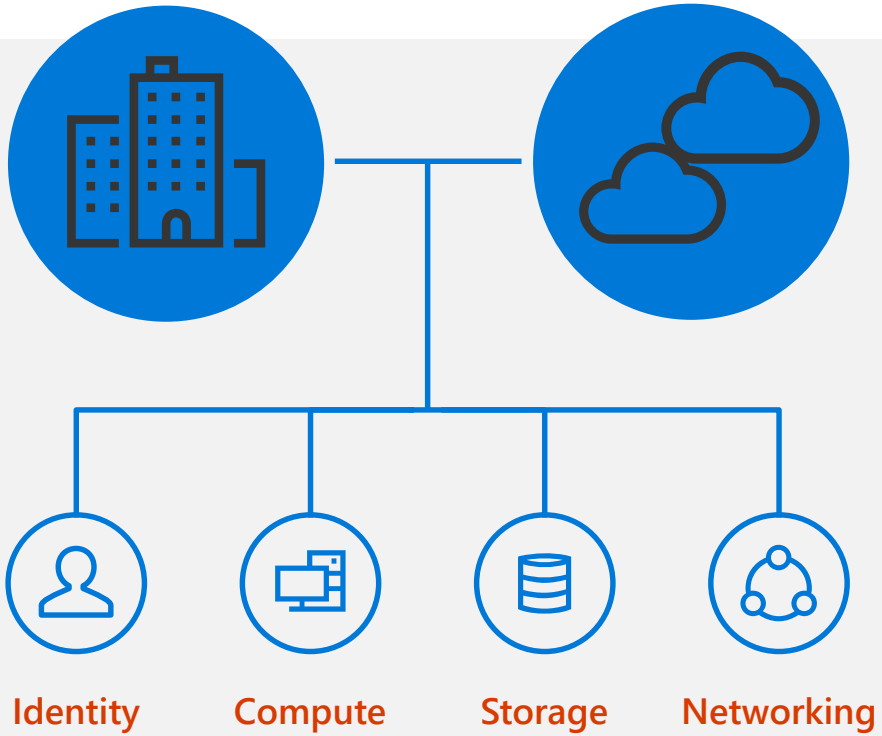
90%

of Fortune 500 use Microsoft Cloud

_1: Rightscale: 2017 State of Cloud Survey http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey#hybrid-cloud

While cloud is growing, hybrid is the most common approach

On-premises and Cloud



>67%

Enterprises adopting hybrid cloud in 2017[1]

_1: Rightscale: 2017 State of Cloud Survey http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey#hybrid-cloud

Securing Azure resources is a shared responsibility between Microsoft and the customer

MICROSOFT'S COMMITMENT

Securing and managing the cloud foundation

Physical assets

Datacenter operations

Cloud infrastructure

JOINT RESPONSIBILITY

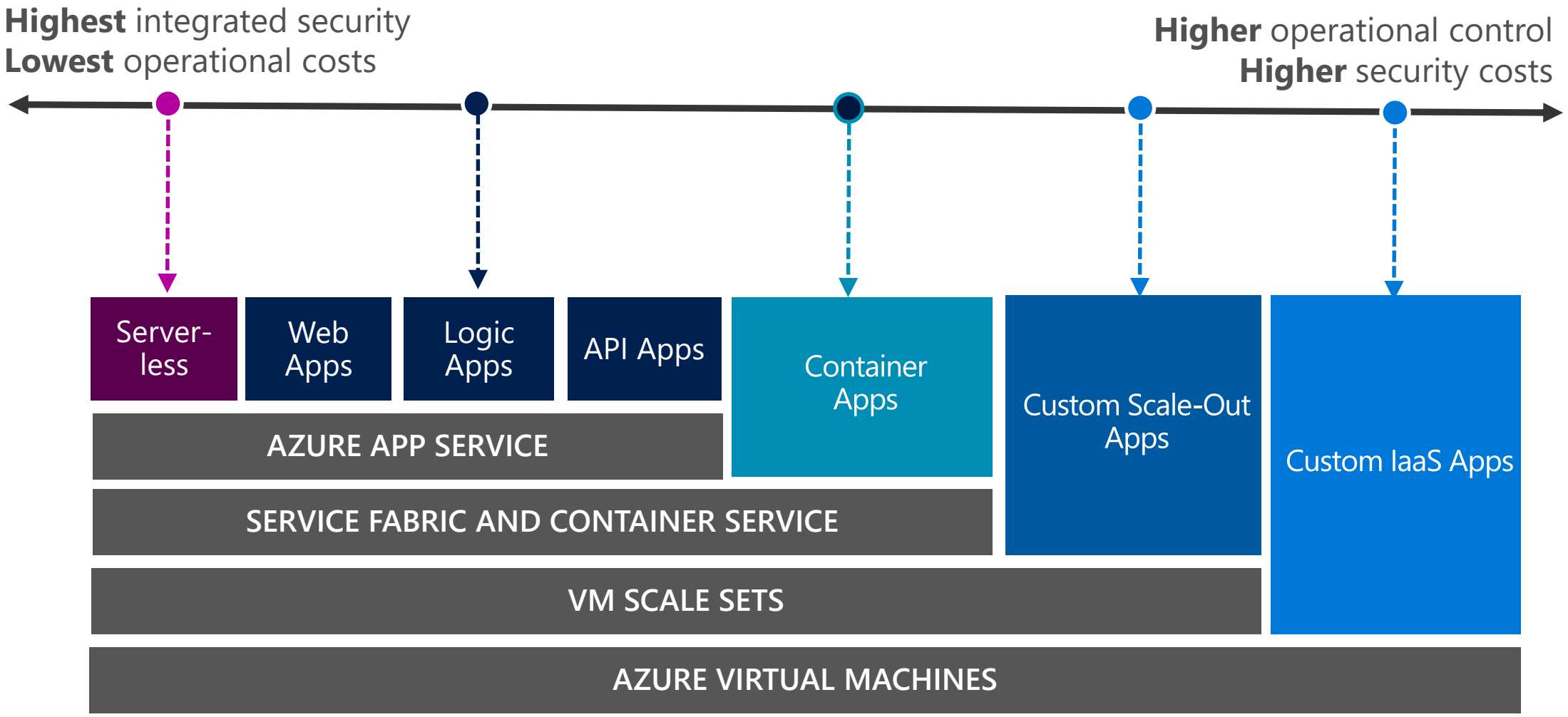
Securing and managing your cloud resources

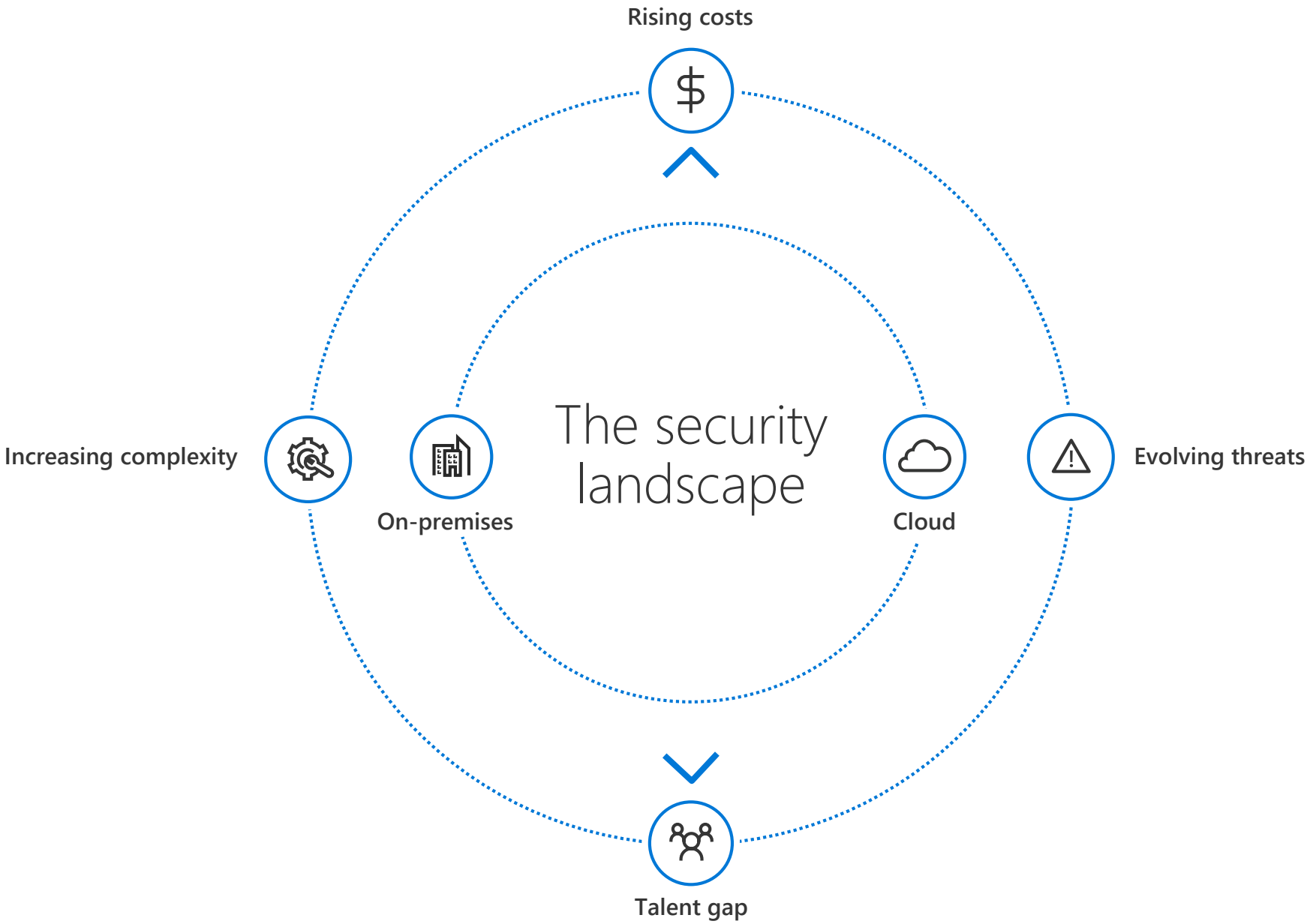
Virtual machines

Applications & workloads

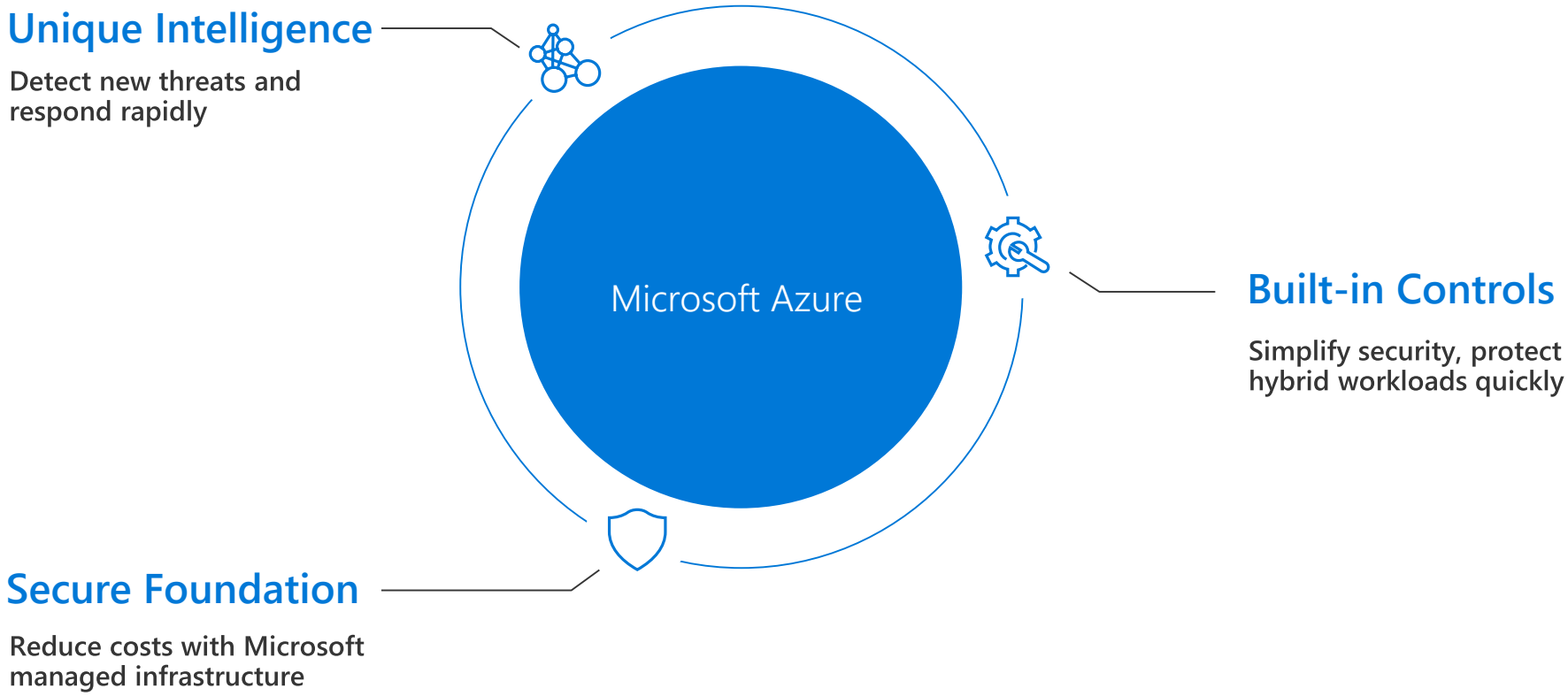
Data

Shared Responsibility within App Models




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

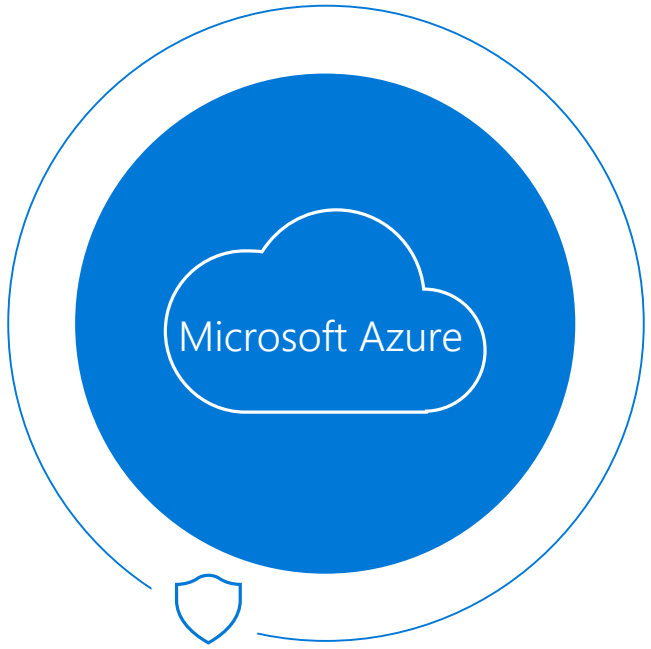
Strengthen security posture with Azure



Secure Foundation

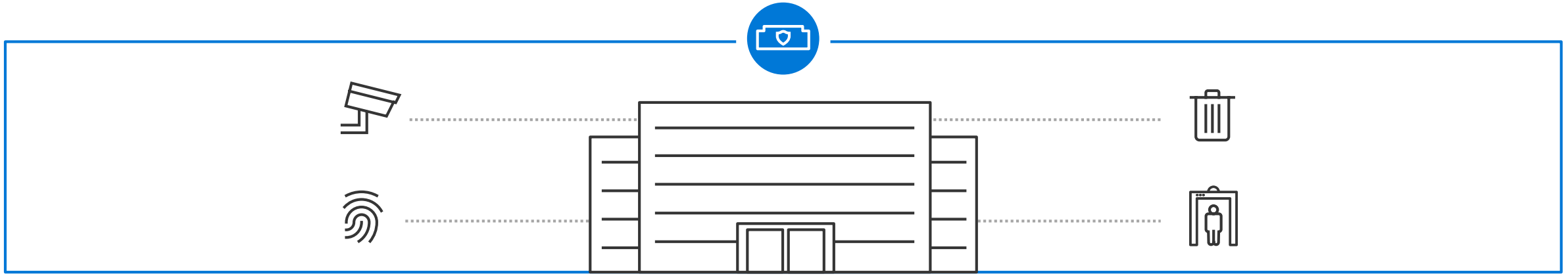
Microsoft managed

- Physical datacenter
- Azure infrastructure
- Operational security



Secure foundation

Physical datacenter security



Global datacenters designed and operated by Microsoft

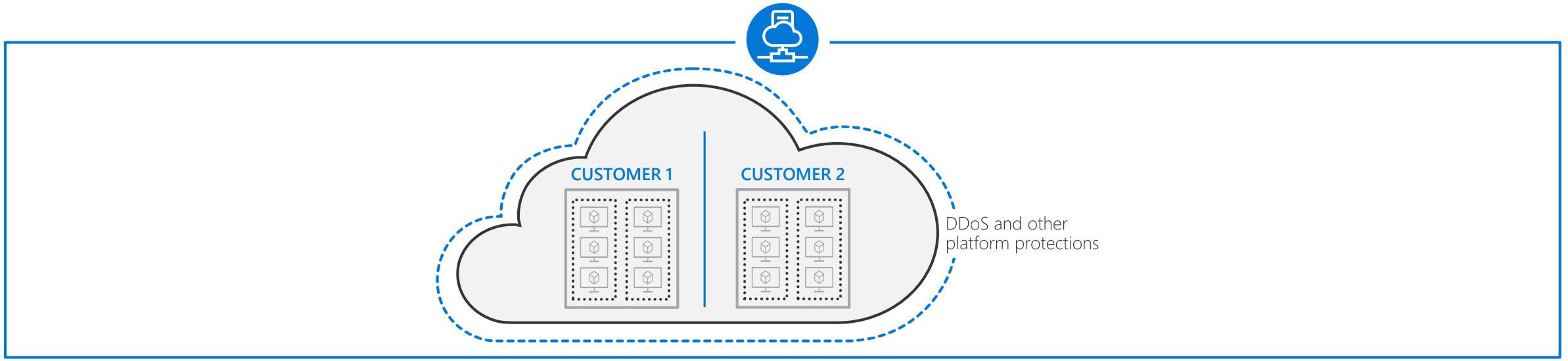
Protected by industry leading security systems

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

Secure Foundation

Operational security

Restricted access for Microsoft administrators

Identity isolation and secure operator workstations

Grants least privilege required to complete task

Incident response

Multi-step incident response process

Focus on containment & recovery

3500+ security professionals

Working to harden, patch and protect the platform

24x7 monitoring for threats; assume breach drills


Trust principles that run our business
SECURITY
PRIVACY
TRANSPARENCY
COMPLIANCE

Security

We will ensure that all your data is secure

We spend over $1 billion a year on cybersecurity.

3,500+ security professionals work to secure datacenters and hunt down attackers.

We block more than 5 billion distinct malware threats per month.

Privacy

We will ensure your data is private and is under your control

We used GDPR as a catalyst for broader efforts to improve data handling globally.

We have brought 4 privacy lawsuits against the U.S. government to protect customer privacy rights.

We build privacy into our services as part of the Microsoft Security Development Lifecycle.

Brad Smith, President and Chief Legal Officer

Transparency

We will be transparent about the collection and the uses of data

We provide geographic locations where customer data is stored.

We publish the number of legal demands for customer data that we receive from law enforcement agencies.

We provide visibility into what we do with customer data, how we protect it, and how they are in control.

Compliance

We will manage your data in accordance with the law of the land

We have the most comprehensive compliance coverage in the industry.

We committed to sharing our experiences in complying with complex regulations.

We make several resources available to help our customers along their Compliance journey.

Global

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO 9001:2015
- ISO 20000-1:2011
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Certification
- CSA STAR Attestation
- CSA STAR Self-Assessment
- WCAG 2.0 (ISO 40500:2012)

US Gov

- FedRAMP High
- FedRAMP Moderate
- EAR
- DFARS
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DoE 10 CFR Part 810
- NIST SP 800-171
- NIST CSF
- Section 508 VPATs
- FIPS 140-2
- ITAR
- CJIS
- IRS 1075

Industry

- PCI DSS Level 1
- GLBA
- FFIEC
- Shared Assessments
- FISC (Japan)
- APRA (Australia)
- FCA (UK)
- MAS + ABS (Singapore)
- 23 NYCRR 500
- HIPAA BAA
- HITRUST

Regional

- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP PROTECTED
- Canada Privacy Laws
- China GB 18030:2005
- China DJCP (MLPS) Level 3
- China TRUCS / CCCPPF
- EN 301 549
- EU ENISA IAF
- EU Model Clauses
- EU – US Privacy Shield
- GDPR
- Germany C5
- Germany IT-Grundschutz workbook
- India MeitY
- Japan CS Mark Gold
- Japan My Number Act
- Netherlands BIR 2012
- New Zealand Gov CC Framework
- Singapore MTCS Level 3
- Spain ENS
- Spain DPA
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

Industry

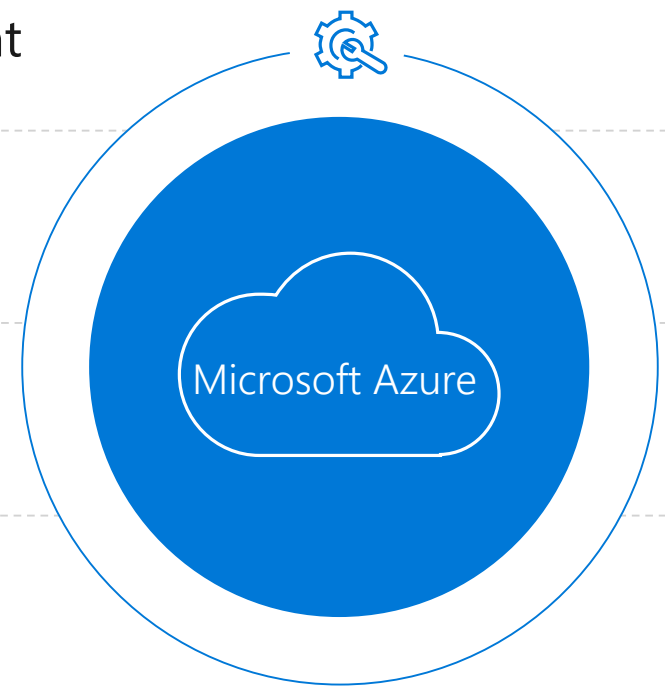
- 21 CFR Part 11 (GxP)
- MARS-E
- NHS IG Toolkit (UK)
- NEN 7510:2011 (Netherlands)
- FERPA
- CDSA
- MPAA
- DPP (UK)
- FACT (UK)
- SOX

microsoft.com/en-us/trustcenter/compliance/complianceofferings

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

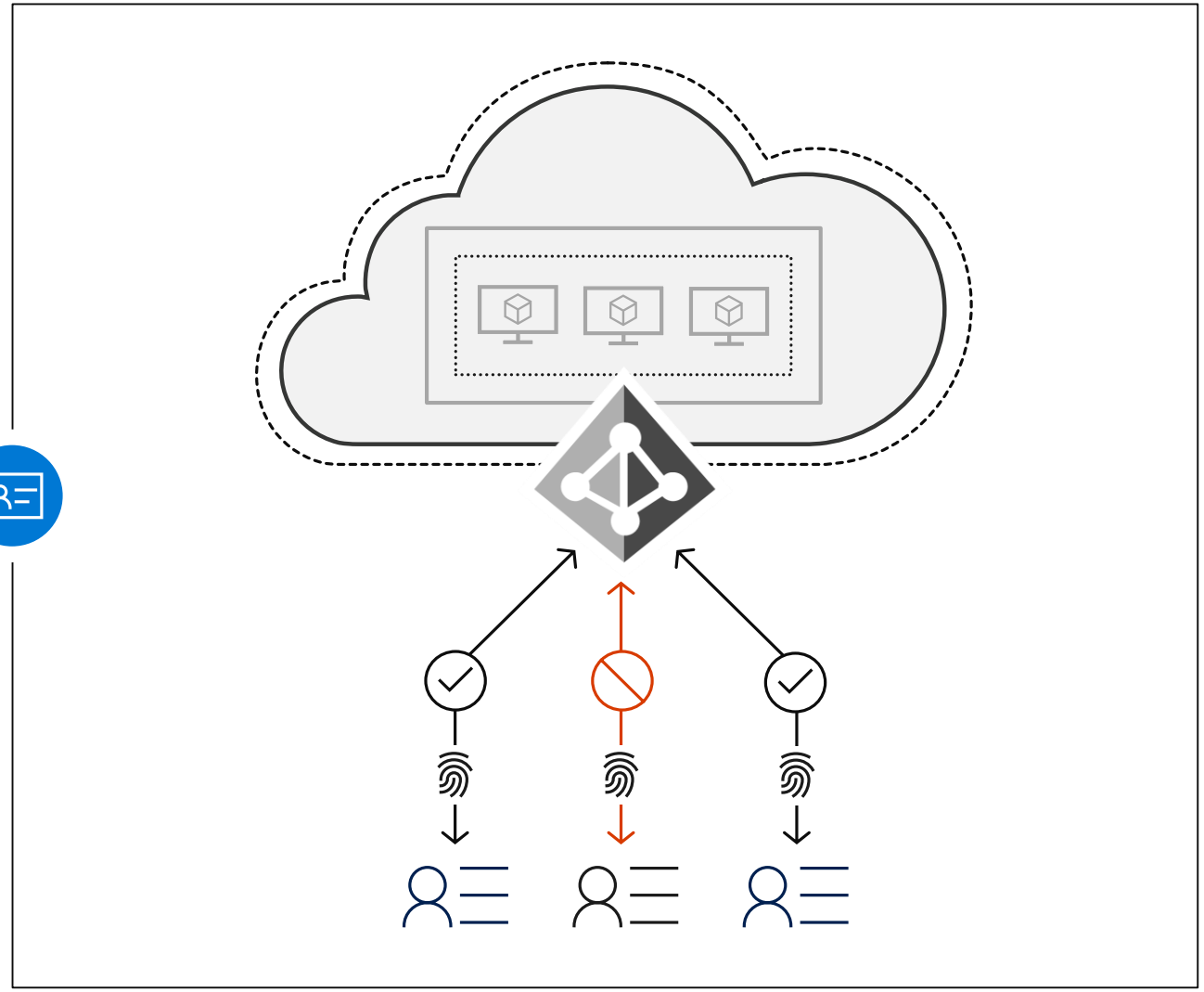
- Azure Active Directory Connect

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

1 Enable built-in encryption across resources

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

2 Encrypt data while in use

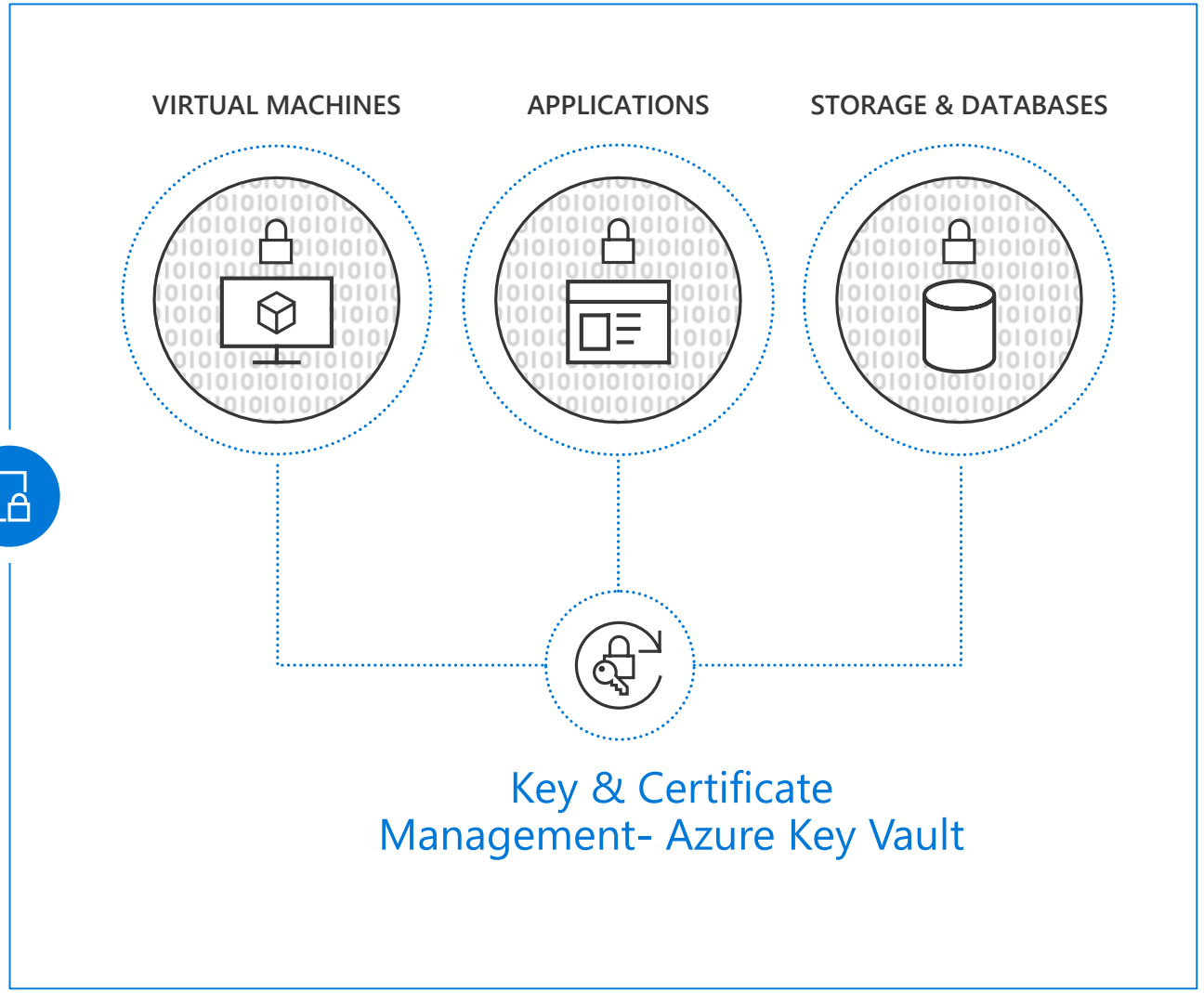
- Azure confidential computing

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 | Threat protection

Protect workloads against evolving attacks

1 Mitigate potential vulnerabilities proactively

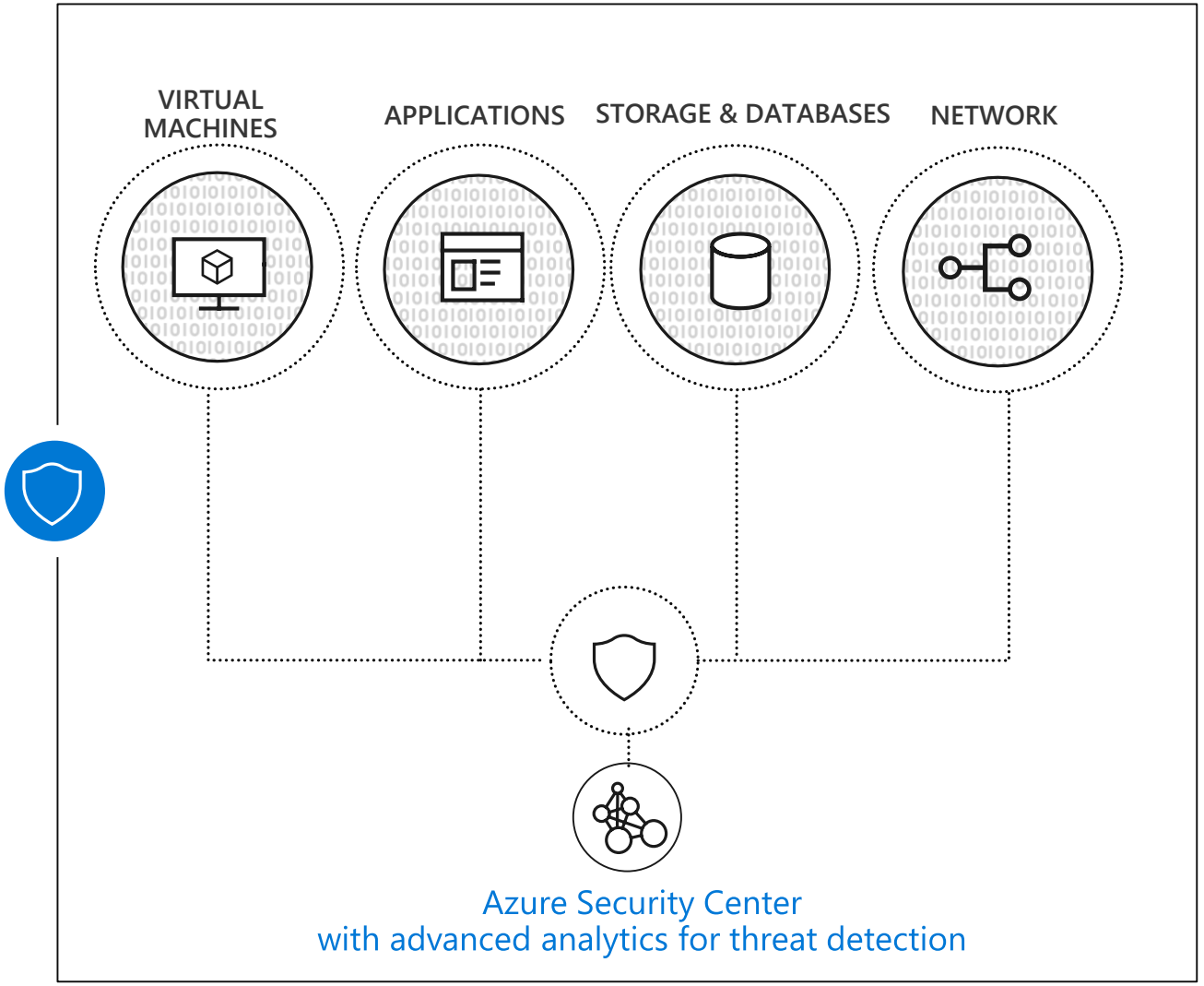
- Ensure up to date VMs with relevant security patches
- Enable host anti-malware

2 Reduce surface area of attack

- Enable just in time access to management ports
- Configure Application Whitelisting to prevent malware execution

3 Detect threats early and respond faster

- Use actionable alerts and incidents
- Interactive investigation tool and playbooks to orchestrate responses



Built-in Controls | Security Management

Enable visibility and control across hybrid workloads

1 Enable centralized view of security state across cloud and on-premises workloads

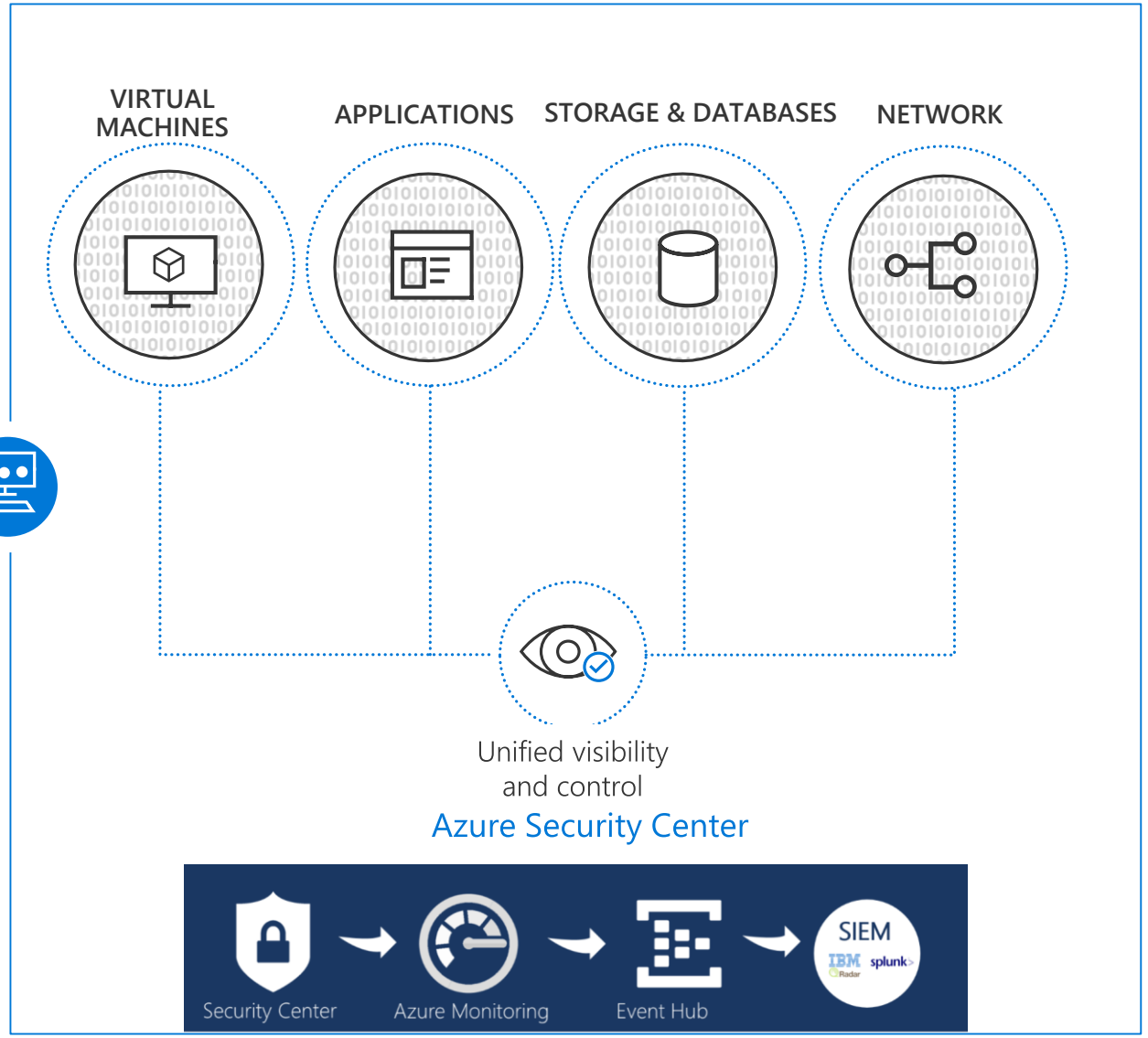
- Monitor security across all subscriptions and environments

2 Ensure compliance to your requirements

- Configure centralized security policy and view compliance score across different resources in a central dashboard

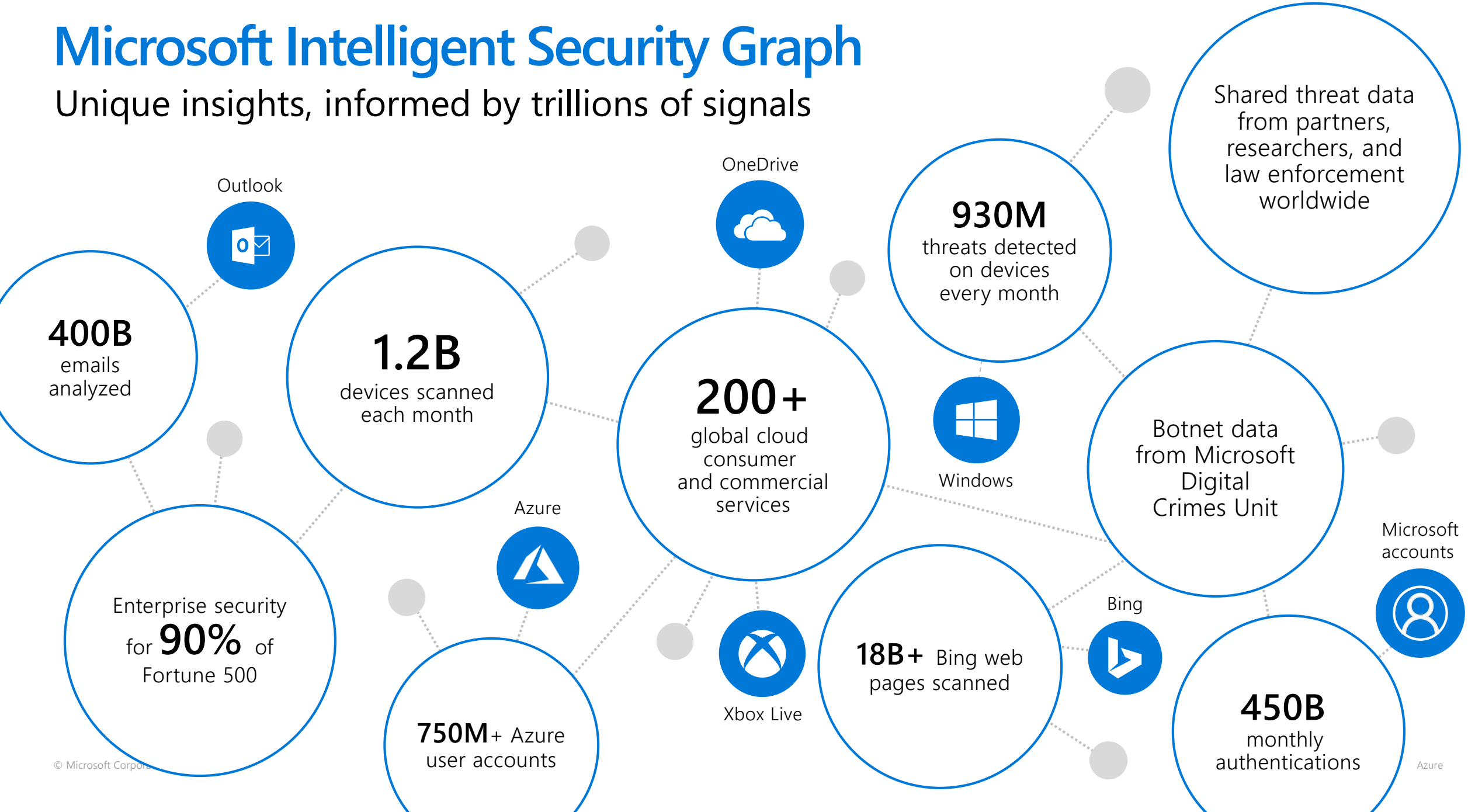
3 Integrate auditing, logging with existing processes

- Configure auditing, logging and use Log Analytics for advanced analysis
- Export security data to existing SIEM solutions

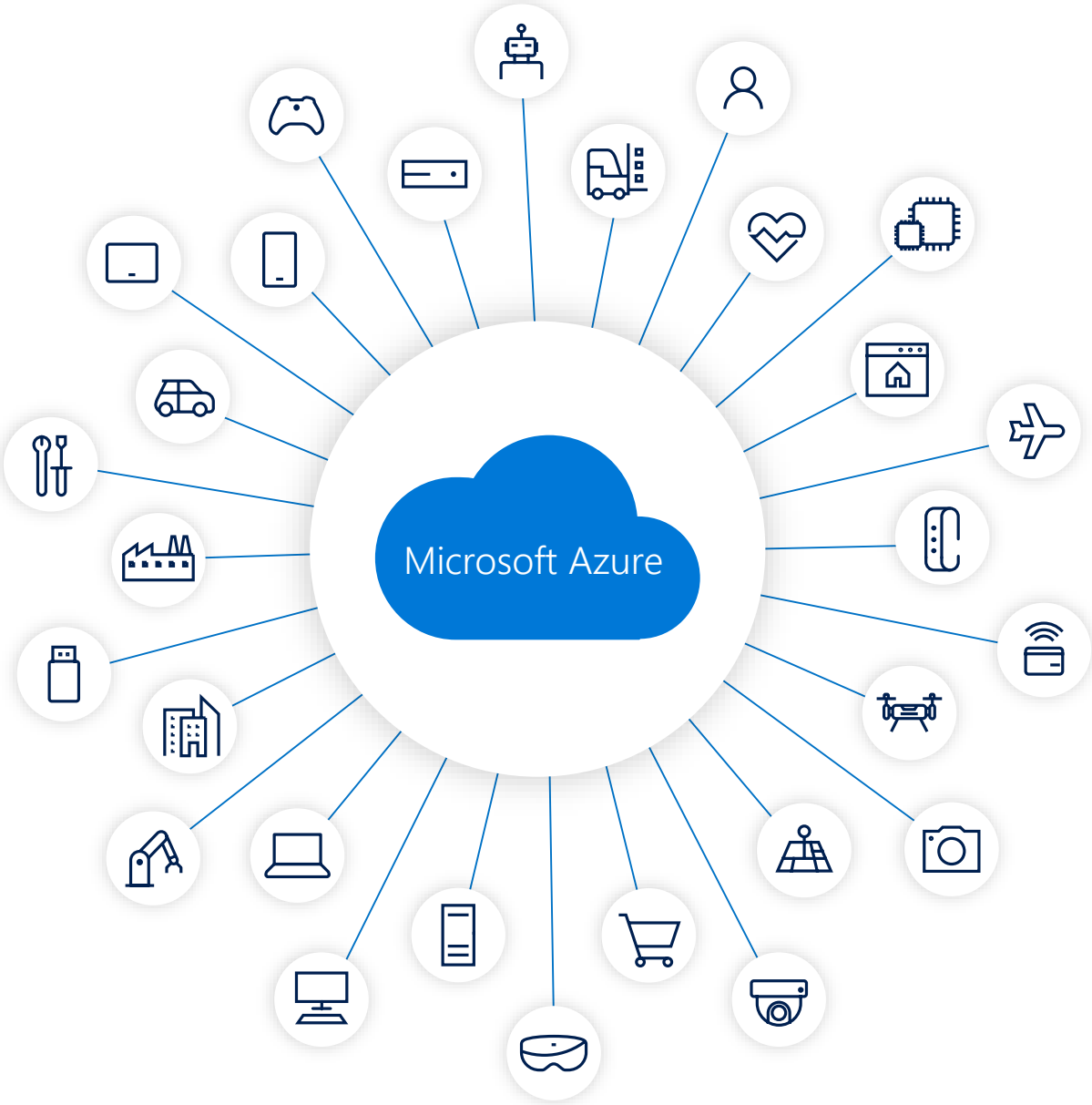


Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals

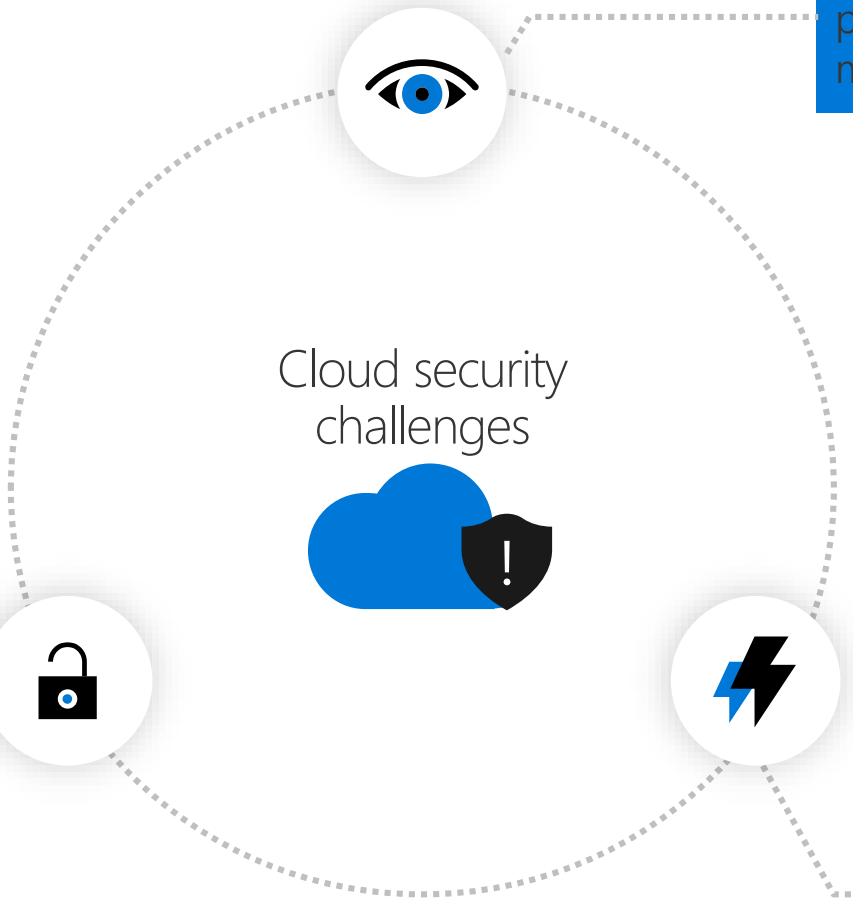


Gain unmatched security with Azure



Visibility into security and compliance

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



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 from an average of 102 to 130.**

*Source: Verizon's 2017 Data Breach Investigations Report
**Source: Ponemon: 2017 Cost of Cybercrime Study

Azure Security Center

Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

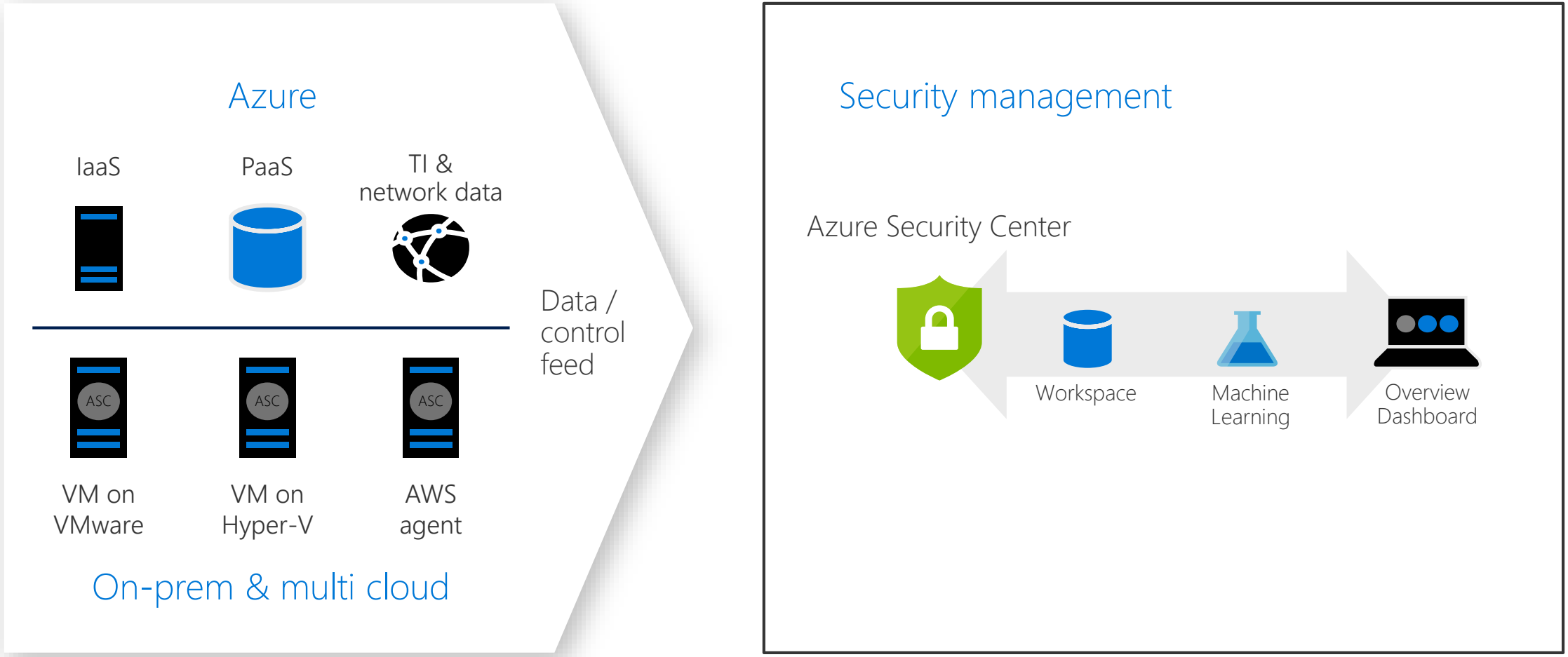
For servers

For cloud native workloads

For databases and storage

Get secure faster

Azure Security Center Architecture

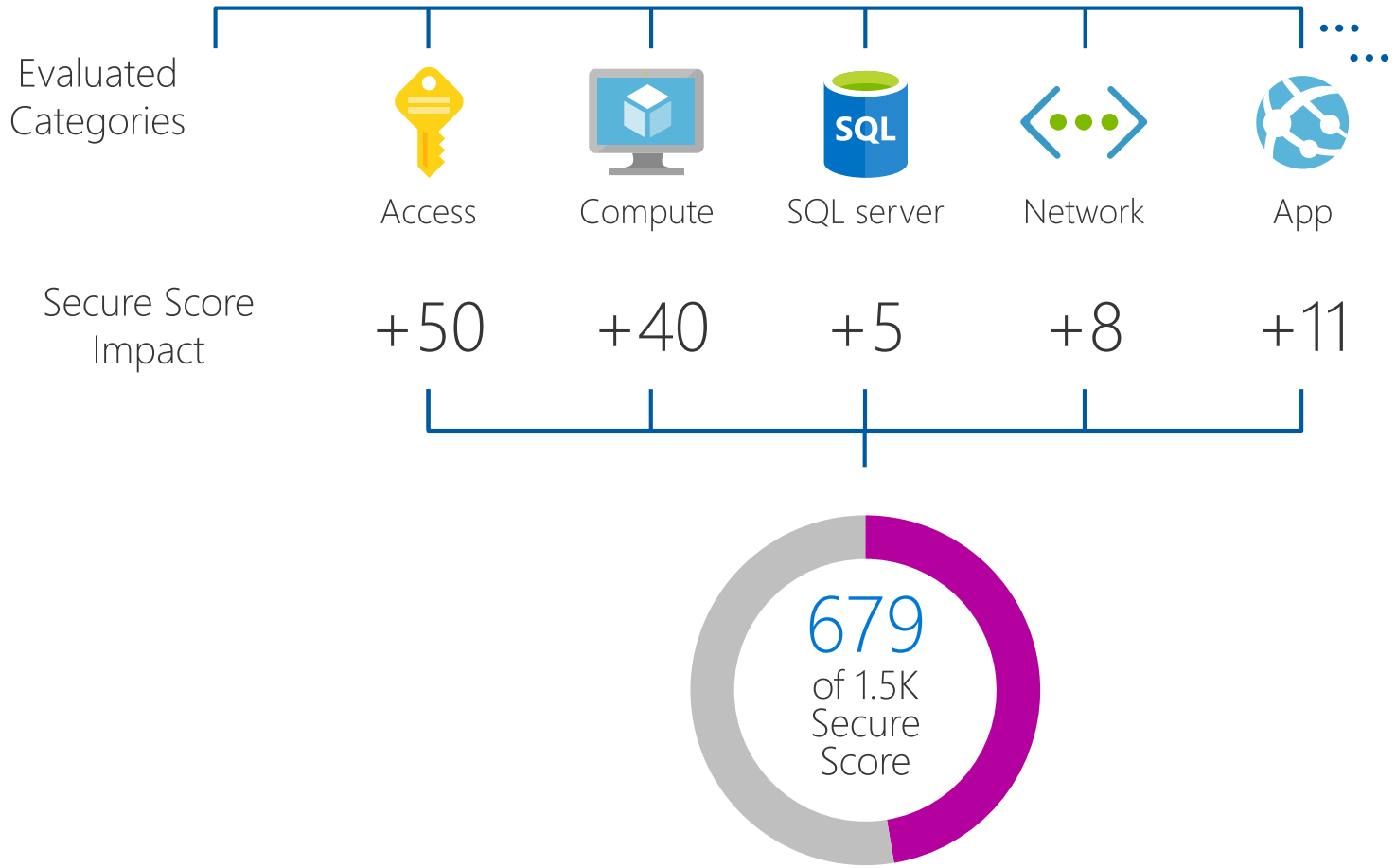


Prioritize your response to security issues with Secure Score

Gain instant insight into the security state of your cloud workloads

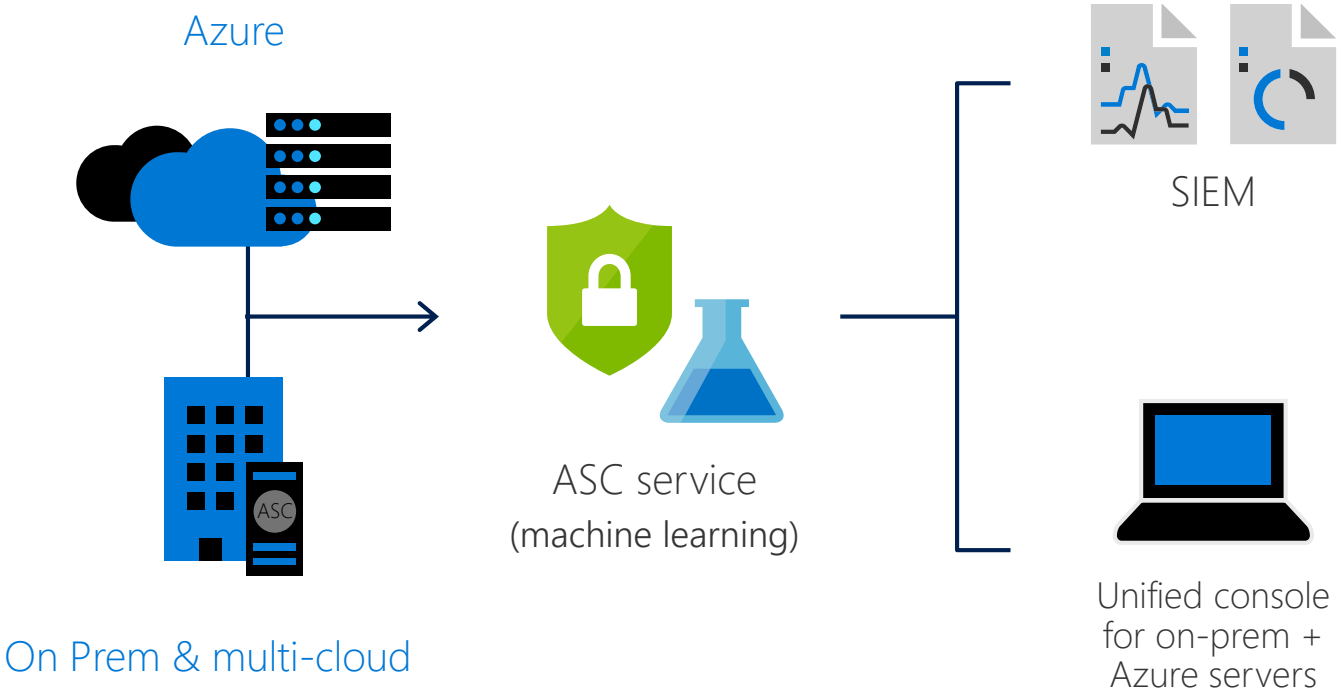
Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes



Get secure faster

- Automatically discover and onboard Azure resources
- Gain a unified view of security across your hybrid cloud workloads
- Integrate with existing SIEM or partner solutions to streamline threat mitigation
- Assess compliance in a click



Pricing

Features	Free (Azure resources only)	Standard (Hybrid incl. Azure)
Security policy, assessment, and recommendations	✔	✔
Connected partner solutions	✔	✔
Just-in-time VM Access	--	✔
Adaptive application controls	--	✔
File integrity monitoring	--	✔
Advanced threat detection for networks, VMs/servers, and Azure services	--	✔
Threat intelligence	--	✔
Virtual machines		✔
App Services		✔
SQL databases		✔
Price	Free	$15 / node / month

Take actions today

Enable Azure Security Center to assess your secure score

Start trial for Security Center standard to get advanced threat protection

Onboard on-premises and other cloud workloads

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

Microsoft Azure

Thank you