Microsoft

Microsoft Azure Security Overview

Claire Lieu — Program Manager

Mark Vayman — Principal Program Manager

Microsoft Azure

Microsoft Azure

Unified platform for modern business

Azure Regions

54

Azure regions announced

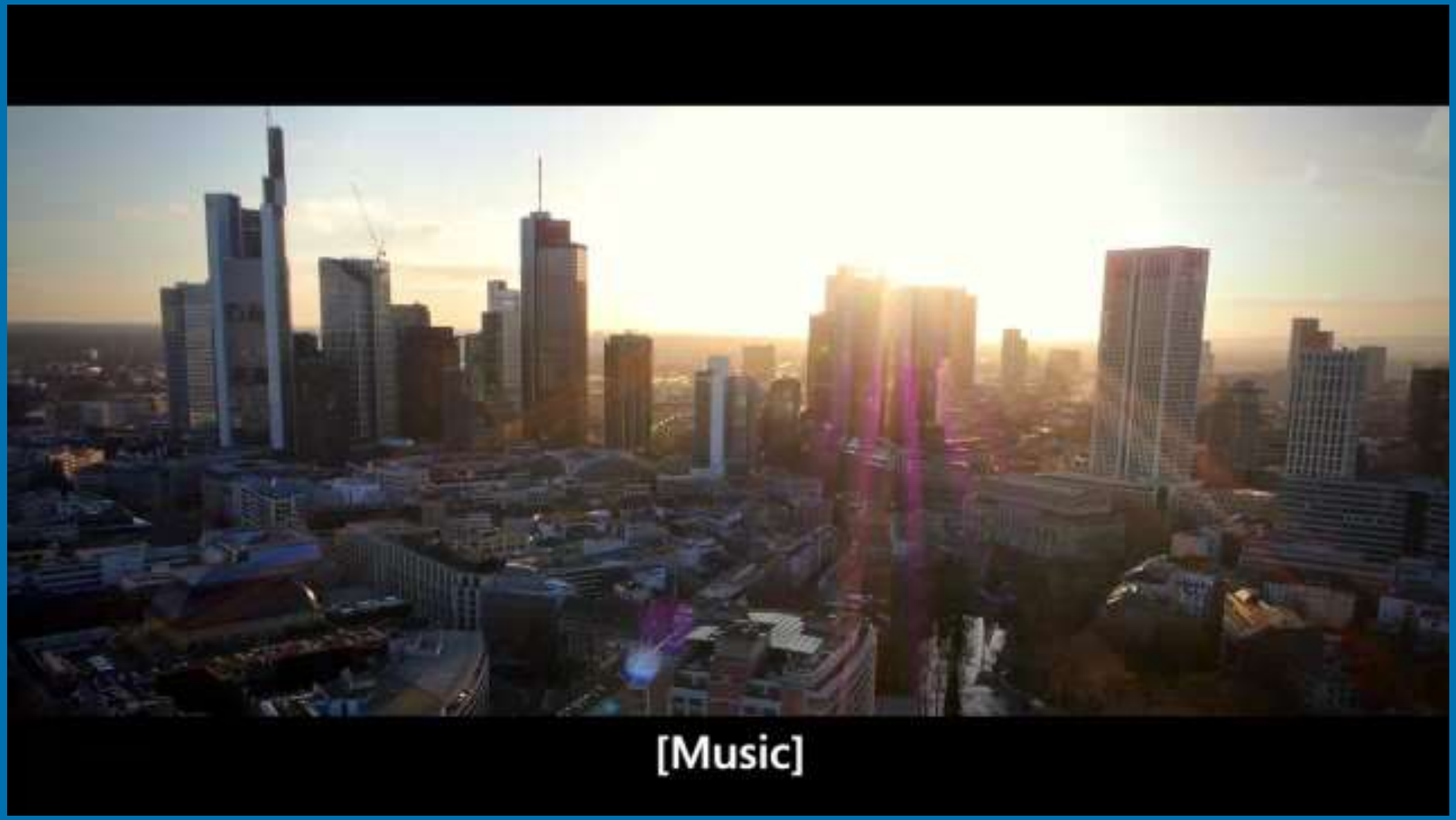
Compute

Data Storage

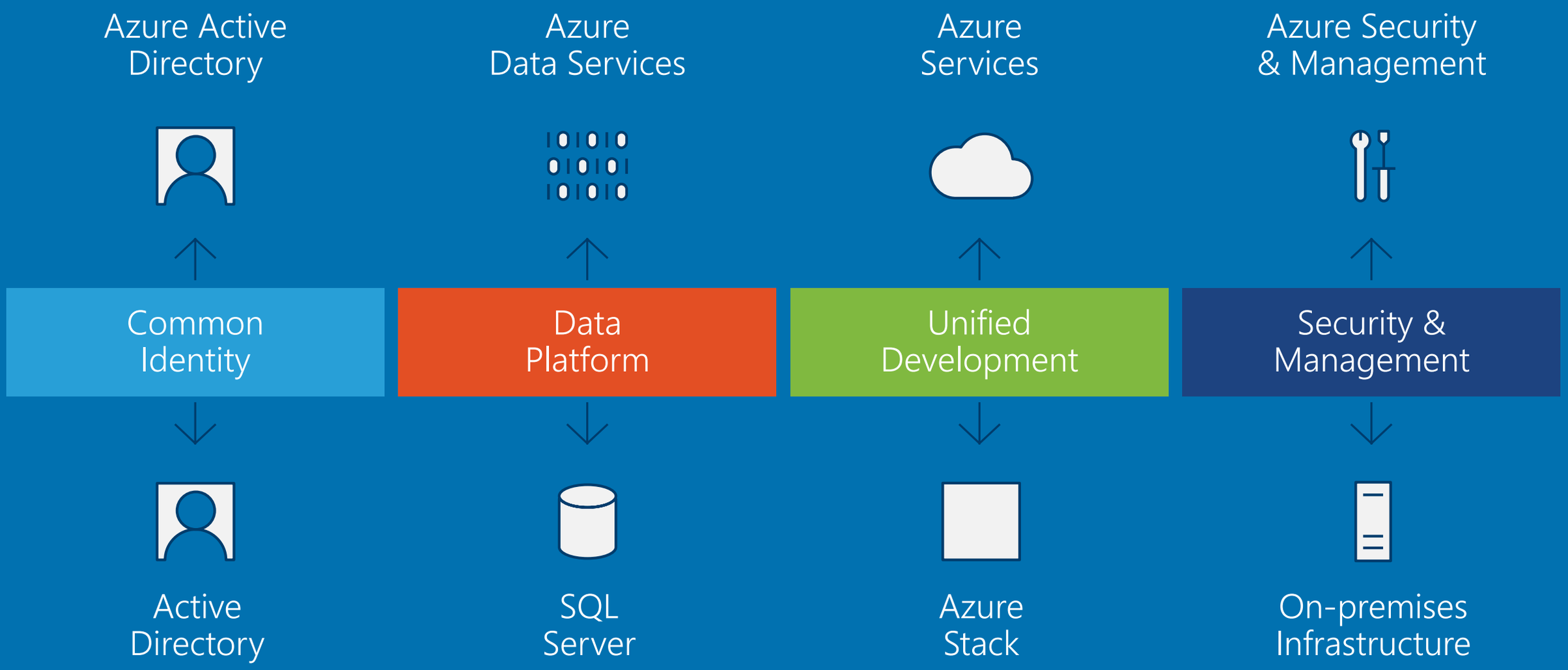
Network Services

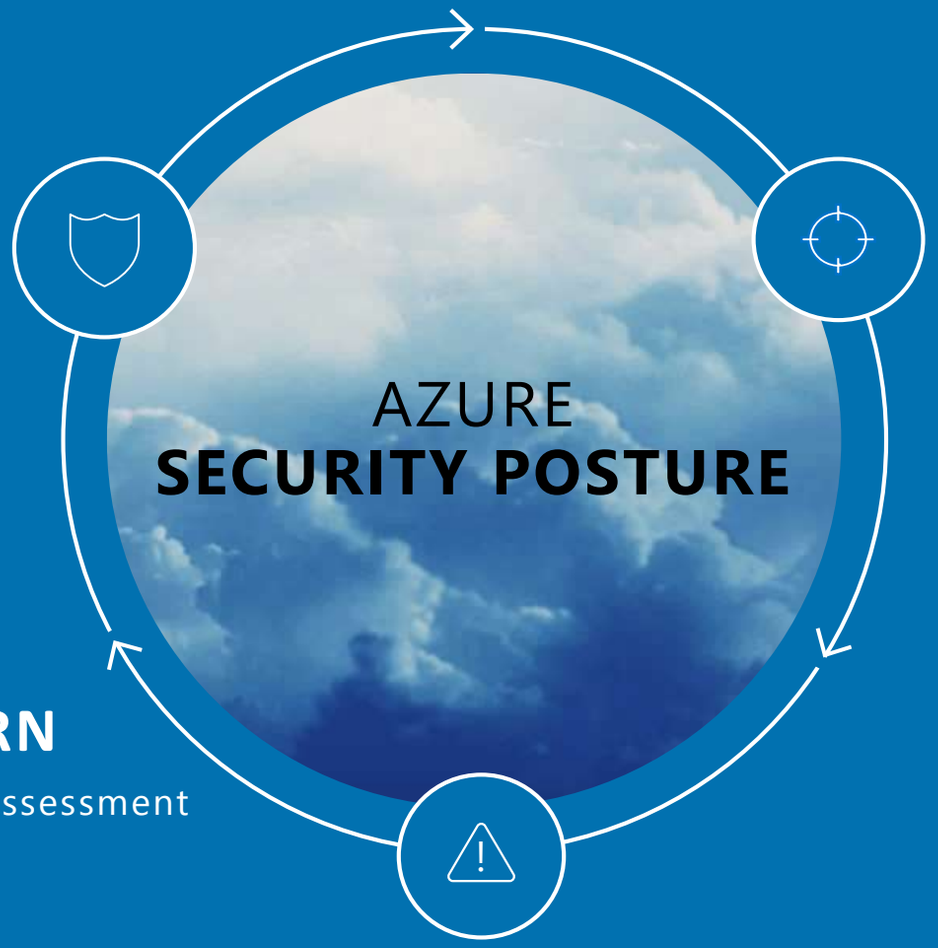
App Services

Satya Nadella on Customer Security & Privacy

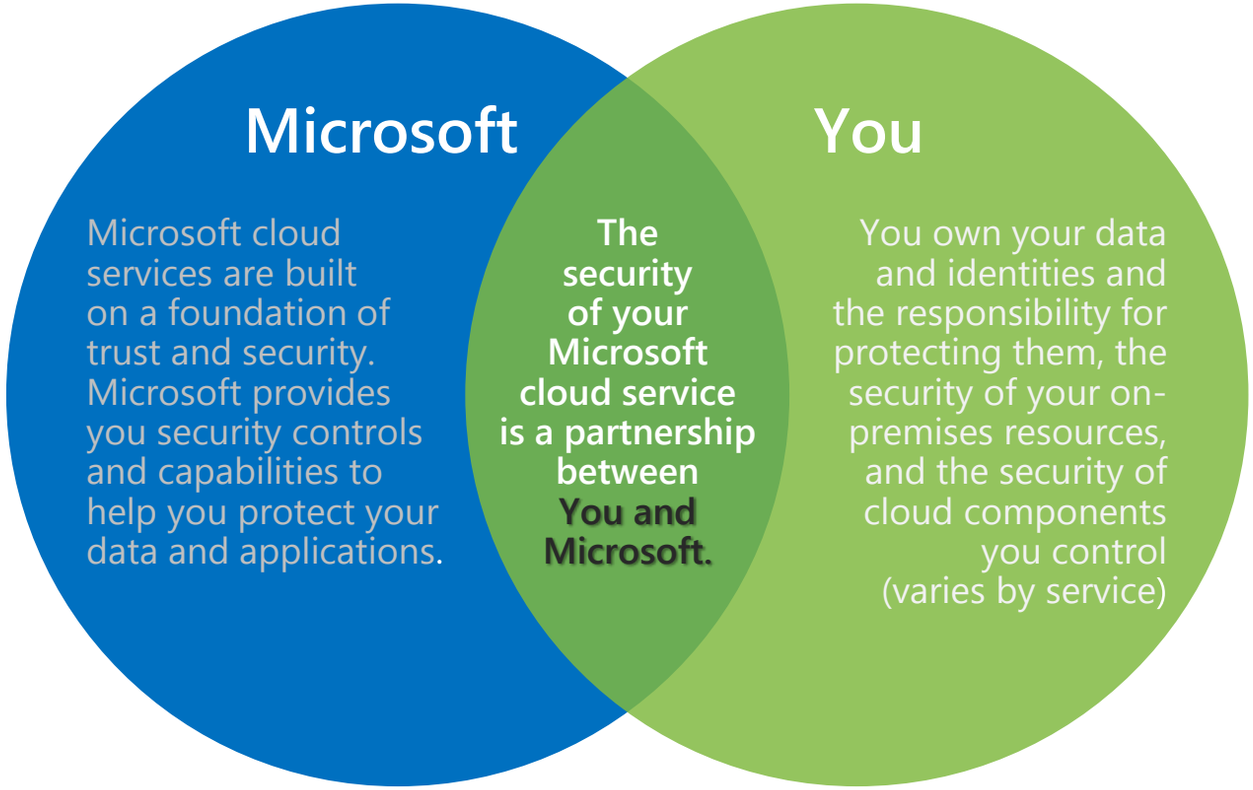


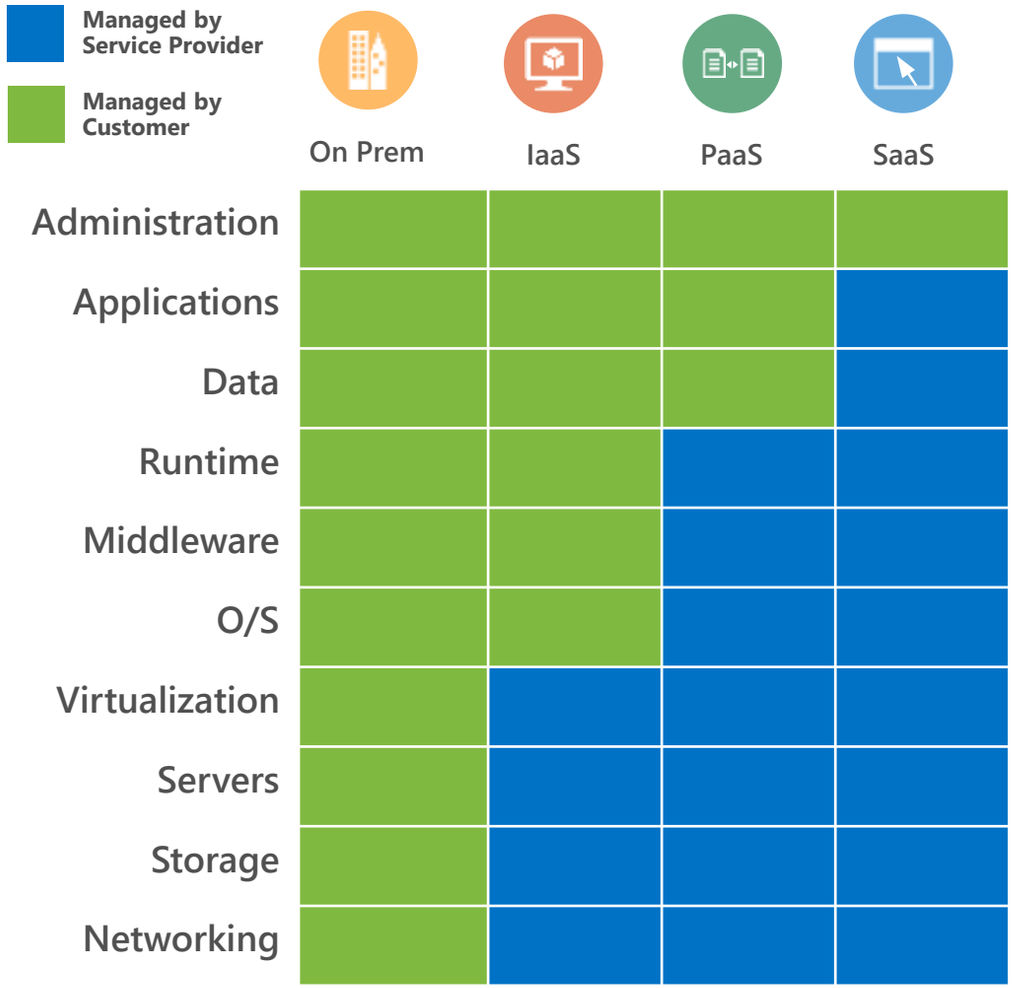
Only consistent hybrid cloud




ASSUME BREACH
PROTECT
Security Development Lifecycle
Threat Modeling
Code Review
Security Testing
Network/User/Data/System security
DETECT
Auditing and Certification
Live Site Penetration Testing
Centralized Logging and Monitoring
Fraud and Abuse Detection
AZURE
SECURITY POSTURE
LEARN
Post-Breach Assessment
RESPOND
Breach Containment
Coordinated Security Response
Customer Notification

Cloud Services Security is a Shared Responsibility





Security Development Lifecycle

Education

Administer and track security training

Process

Guide product teams to meet SDL requirements

Accountability

Establish release criteria & sign-off as part of FSR

Incident Response (MSRC)

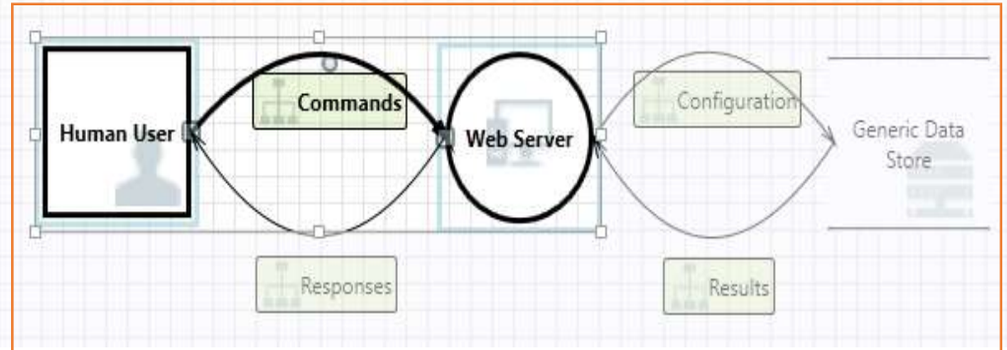
Training → Requirements → Design → Implementation → Verification → Release → Response

Ongoing Process Improvements

Secure Development Lifecycle

Empowering You

- Secure Development Lifecycle - https://www.microsoft.com/en-us/sdl/
- Tools to enable writing and releasing secure code



Threat Modelling Tool

TMT2016

Visual Studio

CREDSCAN

Detecting creds in source & more

GitHub

Microsoft Visual Studio Team Services

Credential Scanner

GitHub, VS-IDE Integration

.NET Framework

Static Analysis for .NET

Roslyn, Security Analyzers

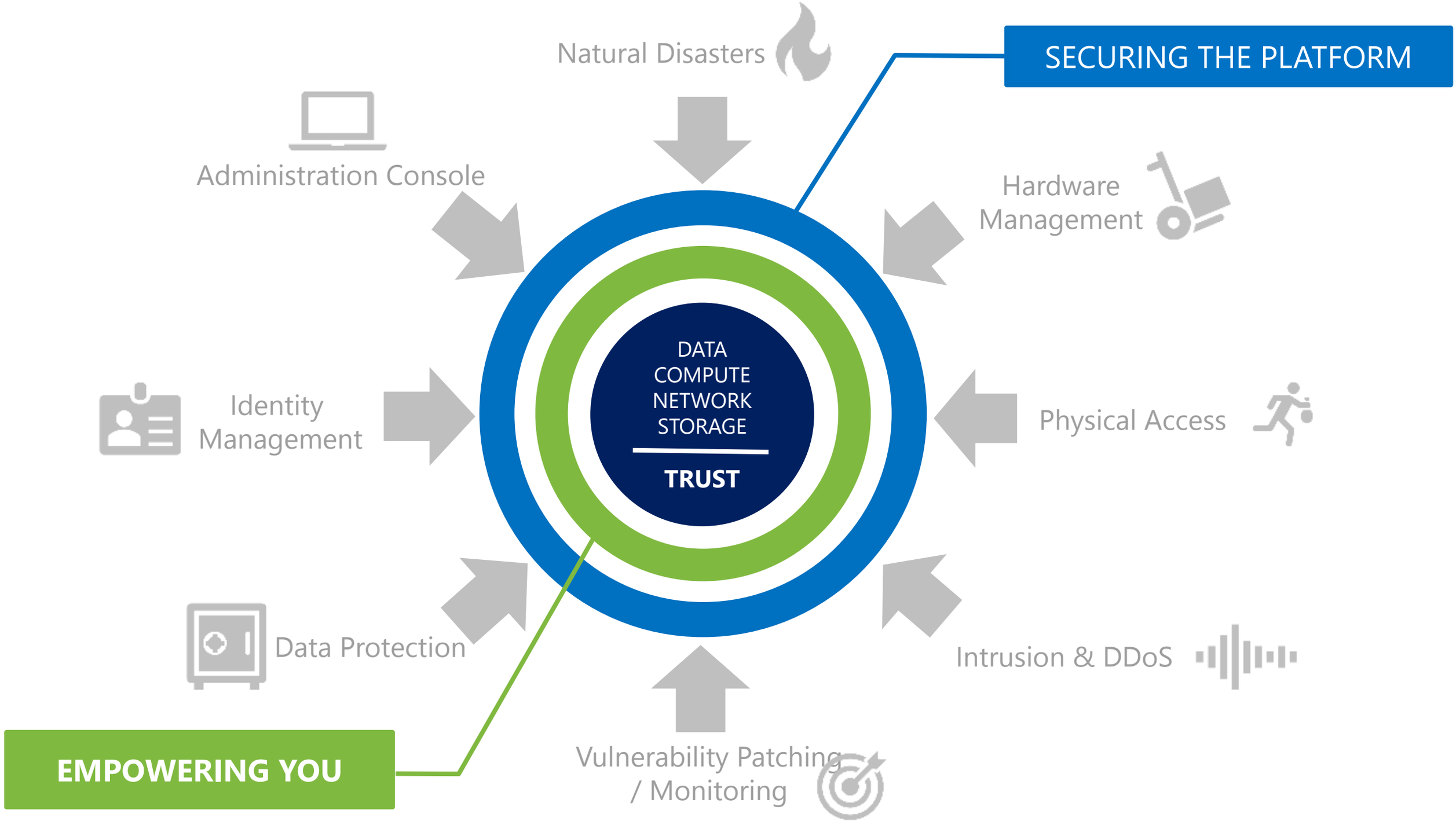
Microsoft / binskim

Binary Static Analysis Tool [GitHub]

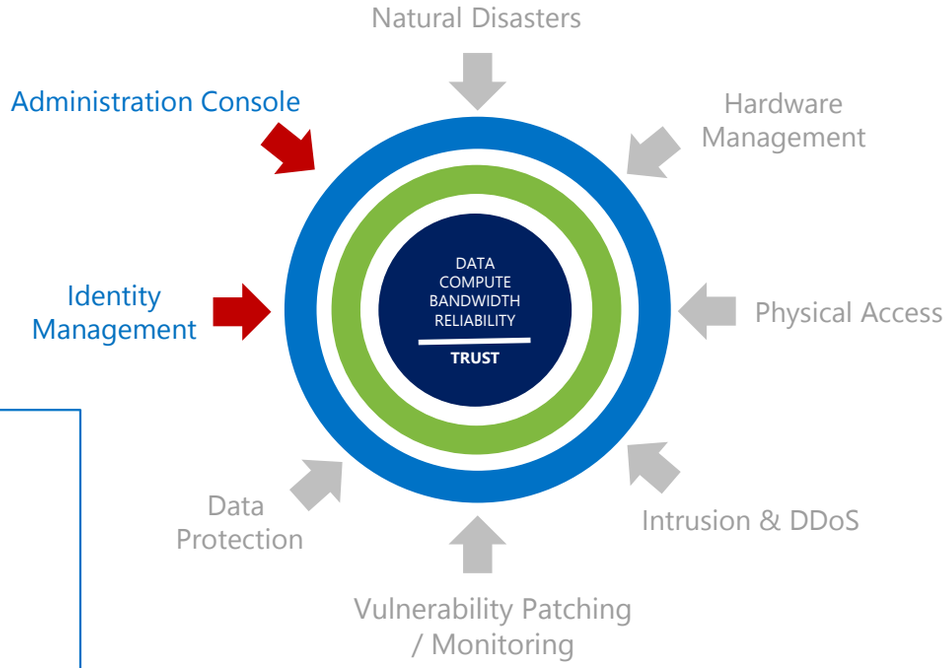
provides security and correctness results for Windows portable executables

Secure Code Analysis VSTS Extension (Private Preview)

Contact: sdt-vsts@microsoft.com


SECURING THE PLATFORM
Natural Disasters
Administration Console
Hardware Management
DATA
COMPUTE
NETWORK
STORAGE
TRUST
Identity Management
Physical Access
Data Protection
Intrusion & DDoS
Vulnerability Patching / Monitoring
EMPOWERING YOU

Administration Console and Identity Management



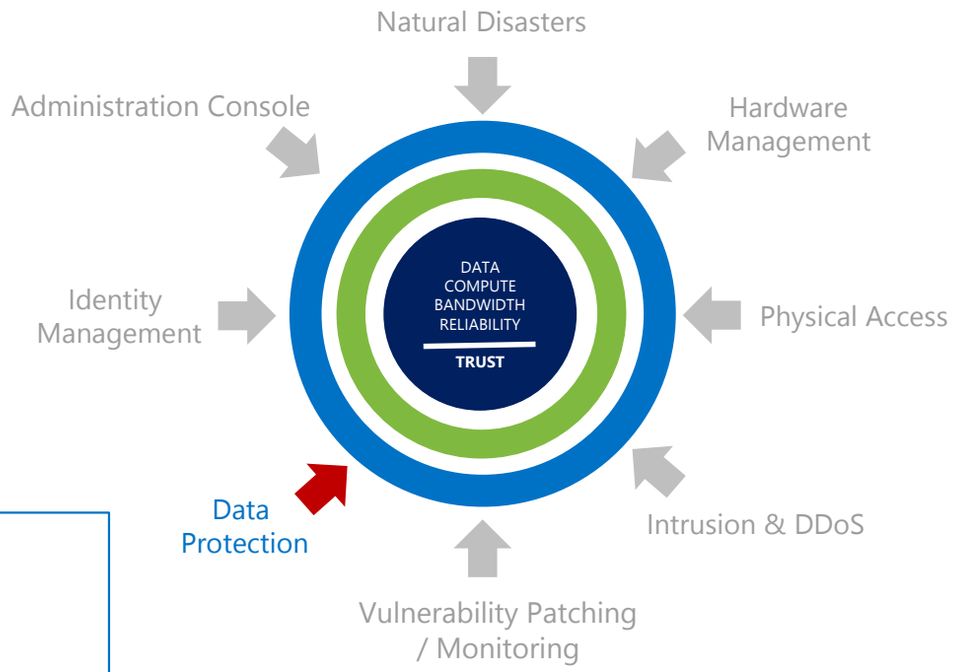
Securing the Platform

- Locked down Secure Admin Workstation
  - Secure Boot, HW security, no admin, restricted browsing,
  - AppLocker & Device Guard, Software Center, App security review
  - Dedicated identity and resource forests
- Multi-factor authentication with physical or virtual smartcard
- Least and Temporarily Privilege, Just in Time elevation
- Access Control and Monitoring

Empowering You

- Privileged Access Workstation guidance on TechNet [link]
- Multi-factor authentication
- AAD Conditional Access (Location, Compliant devices)
- Just in Time access to IaaS
- AAD Monitoring

Data Protection



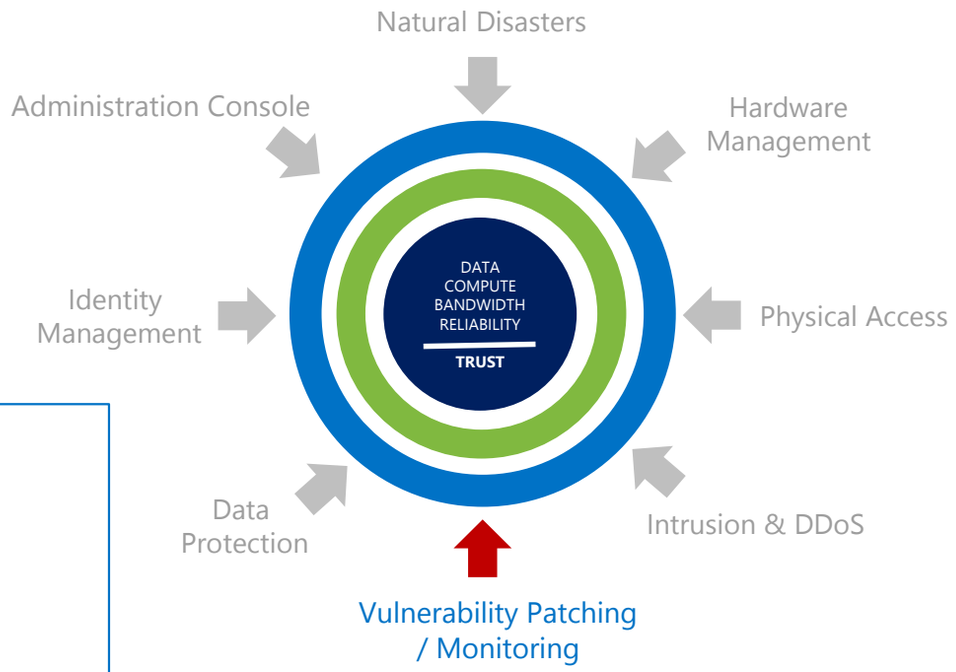
Securing the Platform

- Azure Key Vault & internal key management solution
- Bitlocker
- Access Control with Just In Time elevation and monitoring
- Data segregation (multi-tenant)

Empowering you

- Azure Key Vault with Hardware Security Modules (“HSM”)
- Virtual machine encryption
- Storage encryption
- Transparent data layer encryption (“TDLE”) for SQL
- Data destruction policy

Vulnerability Patching / Monitoring



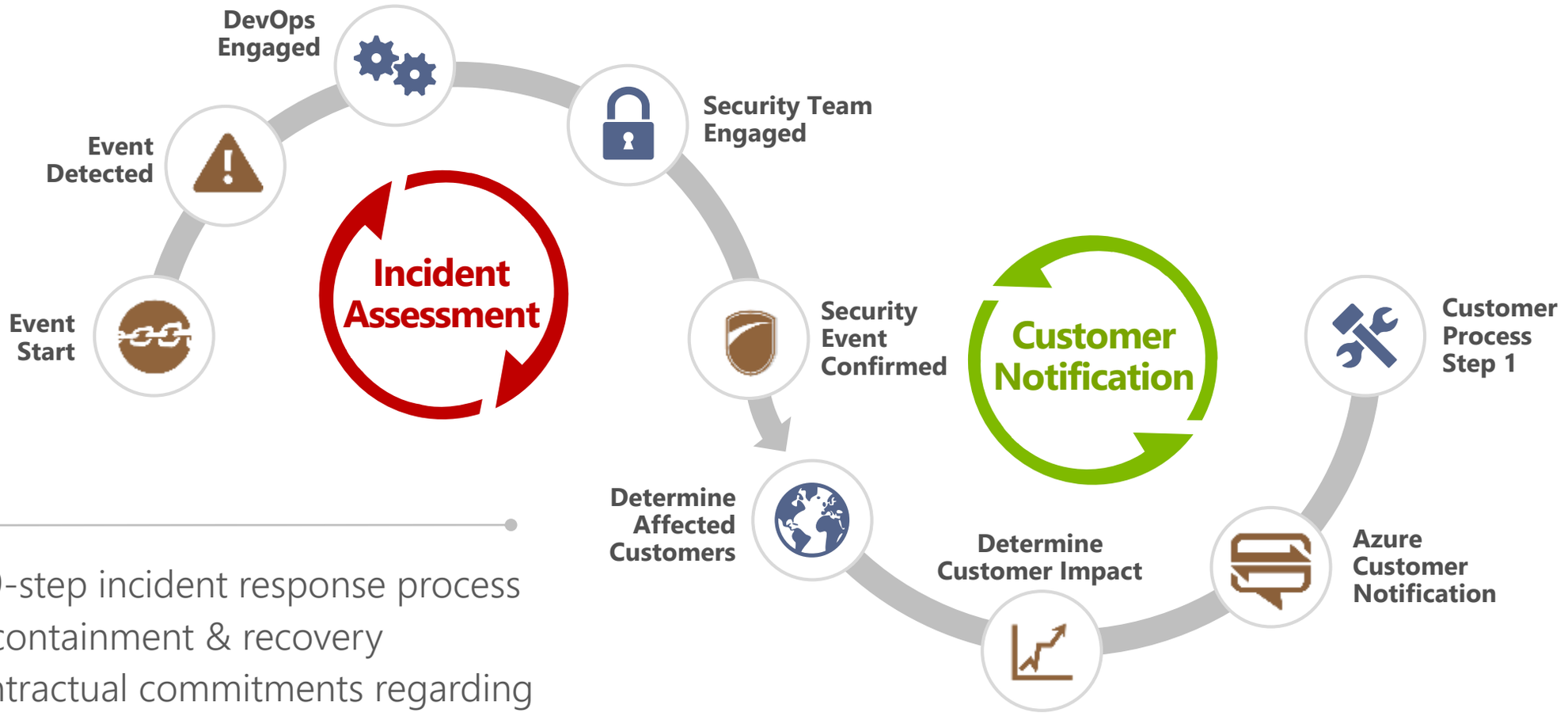
Securing the Platform

- Access Control and Monitoring
- Baseline configuration
- Antimalware
- Update monitoring and management
- Vulnerability scanning

Empowering you

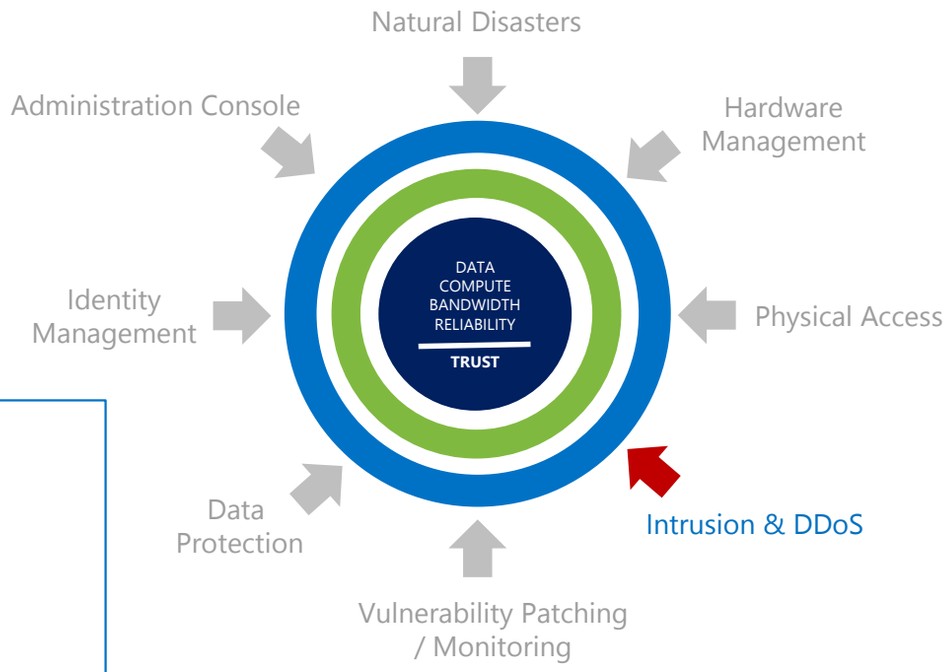
- Azure Security Center
- Antimalware
- Baseline configuration monitoring
- Update monitoring
- Vulnerability scanning (3rd party solution)
- Security detections
- Web Application Firewall
- SIEM integration with Azure Monitor

Incident Response



- ✓ In-depth 9-step incident response process
- ✓ Focus on containment & recovery
- ✓ Makes contractual commitments regarding customer notification + provides forensics

Intrusion and DDoS



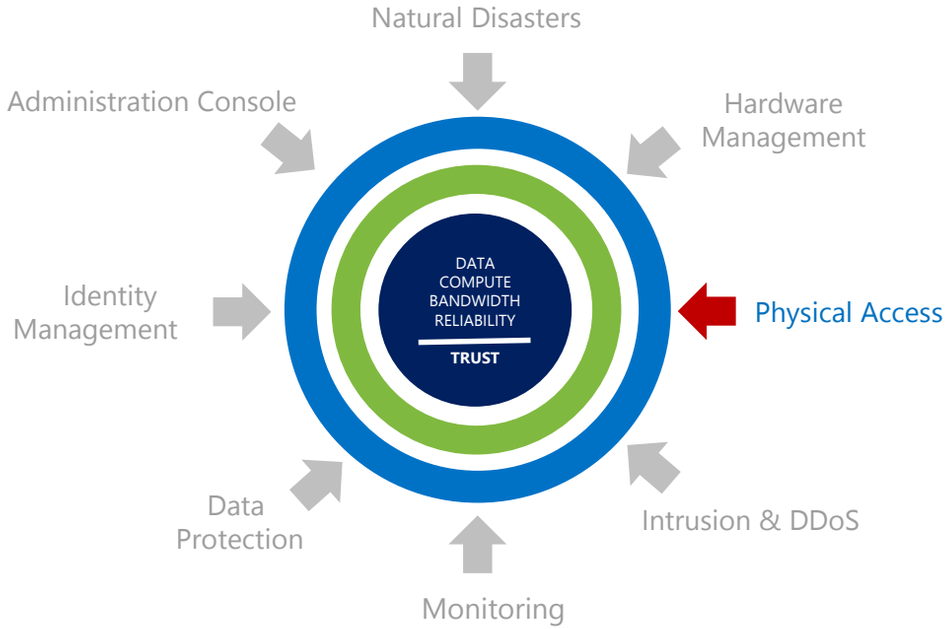
Securing the Platform

- Segmentation
- Access Control Lists
- Intrusion Detection
- Host firewall
- Edge vulnerability scanning
- DDoS protection

Empowering you

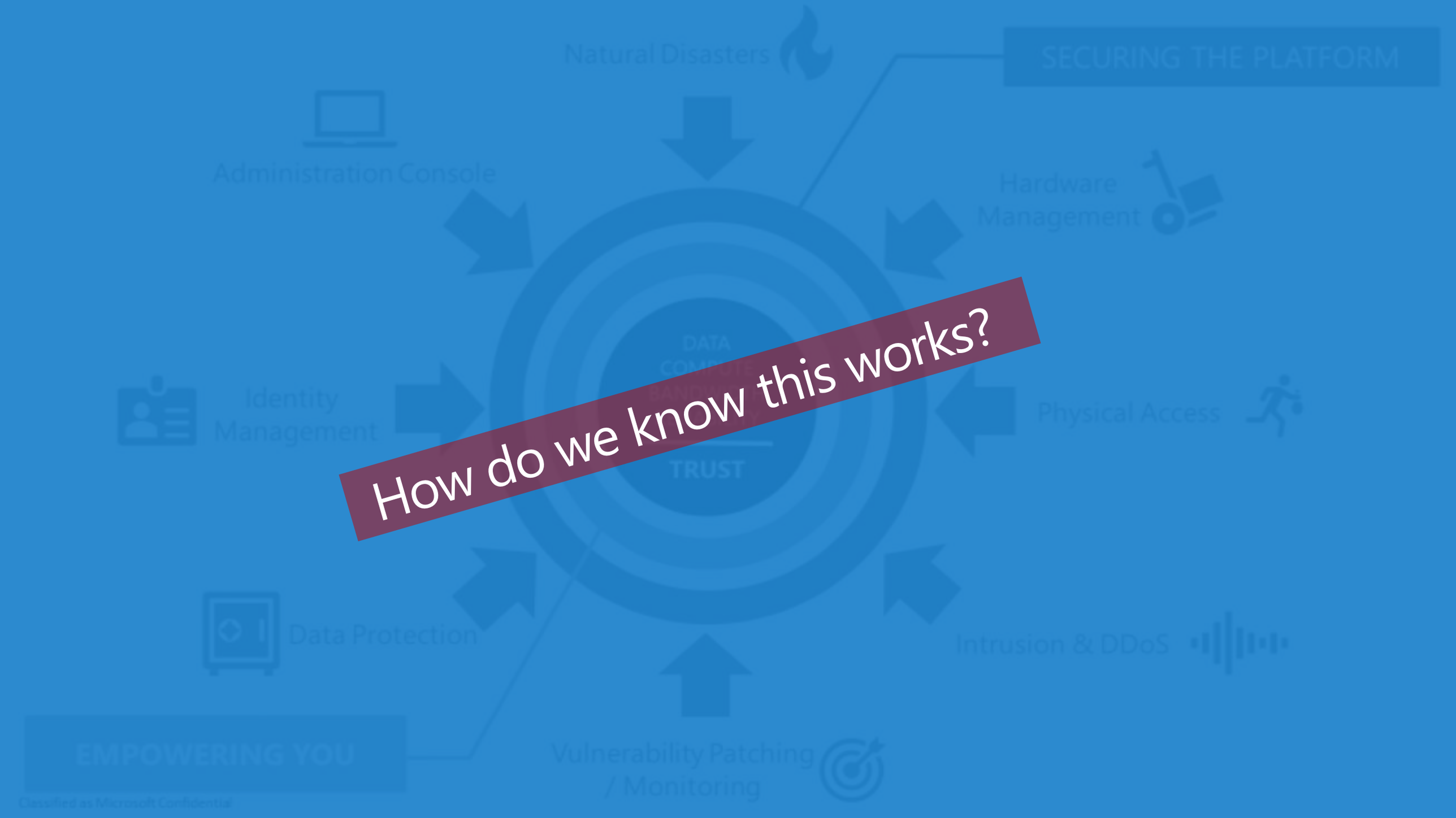
- Host firewall (IaaS)
- Virtual Networks (private IP space for your services)
- Network Security Groups
- Virtual Private Networks
- Just-in-Time VM access (Azure Security Center)
- Network access rules in AAD

Data Center Security



Securing the Platform

- Multiple layers of physical security
- 24/7/365 surveillance and protection
- Vehicle and individual access checkpoints
- Multi-factor biometric entry point
- Metal detectors
- State-of-the-art fire suppression systems



How do we know this works?

RED team vs. BLUE team

Red Team

- Dedicated adversary performing targeted and persistent attacks against our Microsoft Online Services.
- Attack and penetrate environments using the same steps adversary's kill chain
- Mean Time to Compromise (MTTC) + Mean Time to Privilege Escalation (MTTP)

Recon → **Delivery** → **Foothold** → **Persist** → **Move** → **Elevate** → **Exfiltrate**

Blue Team

- Dedicated set of security responders or members from across the Security Incident Response, Engineering and Operations organizations.
- Estimated Time to Detection (ETTD) + Estimated Time to Recovery (ETTR)

Gather → Detect → Alert → Triage → Context → Plan → Execute

Azure is a market leader in compliance coverage

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

Regional

- Argentina PDPA
- Australia CCSL / IRAP
- 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
- 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

https://aka.ms/AzureCompliance

Compliance Control

Microsoft Trust Center

Microsoft | Microsoft 365 | Azure | Office 365 | Dynamics 365 | SQL | Windows 10 | More

Trust Center | Compliance | Security | Privacy | Products | Services | Industry | Resources

HIPAA and the HITECH Act

The Health Insurance Portability and Accountability Act (HIPAA) is a US healthcare law that establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information. It applies to covered entities—doctors' offices, hospitals, health insurers, and other healthcare companies—with access to patients' protected health information (PHI), as well as to business associates, such as cloud service and IT providers, that process PHI on their behalf. (Most covered entities do not carry out functions such as claims or data processing on their own; they rely on business associates to do so.)

The law regulates the use and dissemination of PHI in four general areas:

- Privacy, which covers patient confidentiality.
- Security, which deals with the protection of information, including physical, technological, and administrative safeguards.
- Identifiers, which are the types of information that cannot be released if collected for research purposes.
- Codes for electronic transmission of data in healthcare-related transactions, including eligibility and insurance claims and payments.

The scope of HIPAA was extended with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Together, HIPAA and HITECH Act rules include:

- The HIPAA Privacy Rule, which focuses on the right of individuals to control the use of their personal information, and covers the confidentiality of PHI, limiting its use and disclosure.
- The HIPAA Security Rule, which sets the standards for administrative, technical, and physical safeguards to protect electronic PHI from unauthorized access, use, and disclosure. It also includes such organizational requirements as Business Associate Agreements (BAAs).
- The HITECH Breach Notification Final Rule, which requires giving notice to individuals and the government when a breach of unsecured PHI occurs.

HIPAA regulations require that covered entities and their business associates—in this case, Microsoft when it provides services, including cloud services, to covered entities—enter into contracts to ensure that those business associates will adequately protect PHI. These contracts, or BAAs, clarify and limit how the business associate can handle PHI, and set forth each party's adherence to the security and privacy provisions set forth in HIPAA and the HITECH Act. Once a BAA is in place, Microsoft customers—covered entities—can use its services to process and store PHI.

Currently there is no official certification for HIPAA or HITECH Act compliance. However, those Microsoft services covered under the BAA have undergone audits conducted by accredited independent auditors for the Microsoft ISO/IEC 27001 certification.

Microsoft enterprise cloud services are also covered by FedRAMP assessments. Microsoft Azure and Microsoft Azure Government received a Provisional Authority to Operate from the FedRAMP Joint Authorization Board; Microsoft Dynamics 365 U.S. Government received an Agency Authority to Operate from the US Department of Housing and Urban Development, as did Microsoft Office 365 U.S. Government from the US Department of Health and Human Services.

Frequently asked questions

Expand all

- Can my organization enter into a BAA with Microsoft?
- Does having a BAA with Microsoft ensure my organization's compliance with HIPAA and the HITECH Act?
- Can Microsoft modify my organization's BAA?
- How can I get copies of the auditor's reports?
- How can I learn more about complying with HIPAA and the HITECH Act?

  To assist customers with this task, Microsoft has published these guides:

  - *HIPAA/HITECH Act implementation guidance* for Azure and for Dynamics 365 and Office 365. Written for privacy, security, and compliance officers and others responsible for HIPAA and HITECH Act implementation, they describe concrete steps your organization can take to maintain compliance.
  - Practical guide to designing secure health solutions using Microsoft Azure helps you better understand what it takes to successfully adopt a cloud service in a secure manner.
  - Addressing HIPAA security and privacy requirements in the Microsoft Cloud offers a brief overview of regulation requirements. It also provides a detailed analysis of how Microsoft's cloud services were built with methodologies that map to those requirements, and guidance on how to build compliance-ready solutions.

Recommended resources

HIPAA Omnibus Rule (The final regulations modifying HIPAA rules)

Microsoft Common Controls Hub Compliance Framework

Microsoft Online Services Terms

Microsoft Cloud for Government

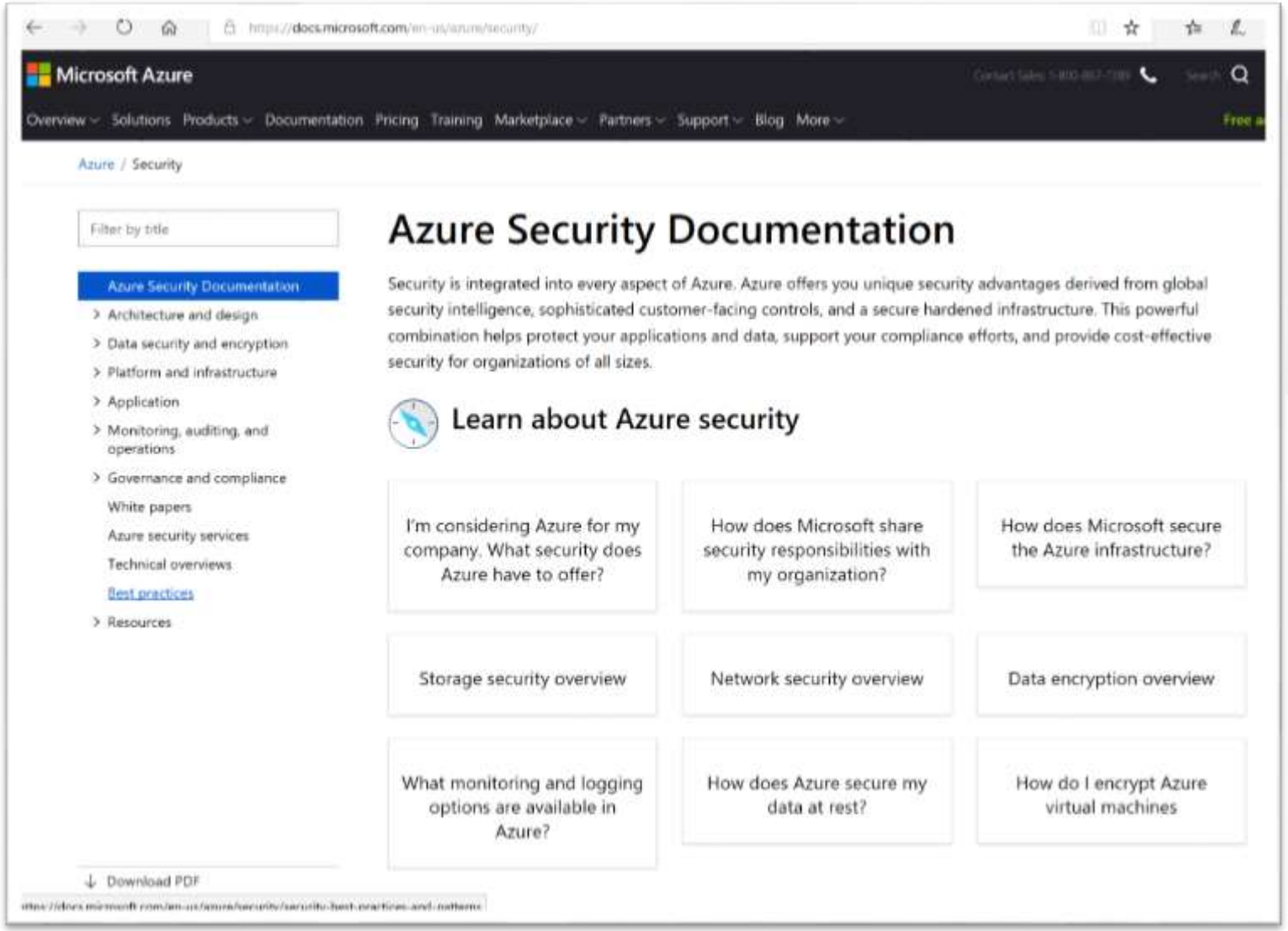
Understanding HIPAA Compliance with Azure (May 19, 2016)

Azure HIPAA implementation guidance

See all resources >

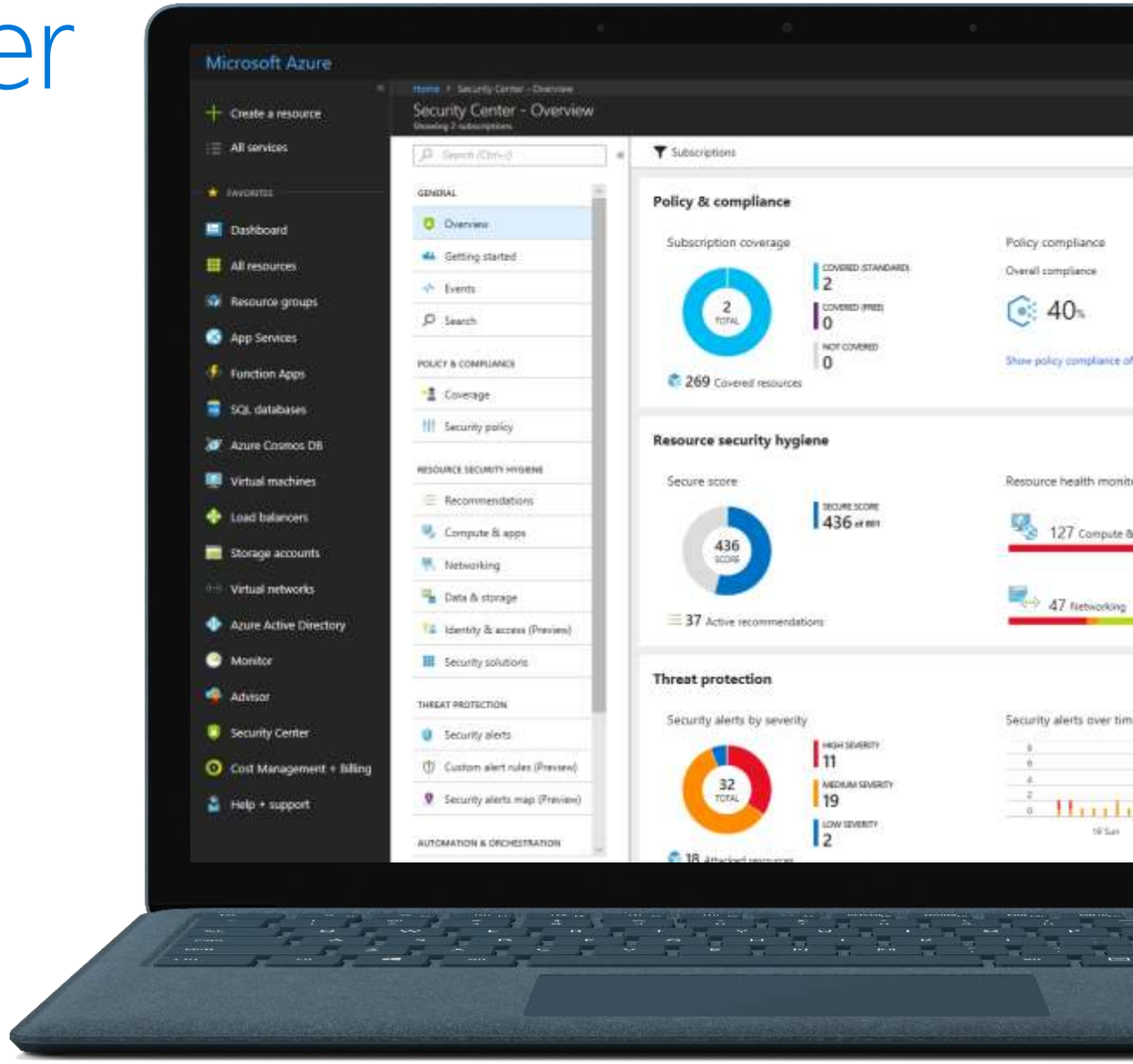
Azure Security Documentation

Azure Security Documentation



Azure Security Center

- ✓ Protection through best practices
- ✓ Detect threats and attacks
- ✓ Remediate issues



Demo

Azure is an open and flexible cloud

Any language and any data source in any operating system for any device

DevOps

Nagios XI, VAGRANT, GRUNT, gradle, Gradle, Clients, Xamarin, APACHE CORDOVA

Management

CHEF, puppet labs, ANSIBLE, SALTSTACK, mist.io, libcloud, SCALR

Applications

Joomla!, Drupal, PaaS & DevOps, apprenda, Jelastic, CLOUD FOUNDRY

App frameworks & tools

php, nodeJS, Java, Ruby, IntelliJ IDEA, eclipse

Databases & middleware

hadoop, redis, cleardb, cloudera, MySQL, mongoDB, Couchbase

Infrastructure

redhat, suse, bitnami, ORACLE LINUX, FreeBSD, docker

Identity & Access: Azure AD Overview

Enterprise Cloud

Azure Active Directory (AAD) offers identity and access management in the cloud w/ federation to enterprise AD

Azure AD: Single Sign-on

Developers can integrate their app with Azure AD for single sign-on functionality

Multi-Factor Authentication

Strong authentication adds an extra layer of security for user logins.

Role Based Access Control

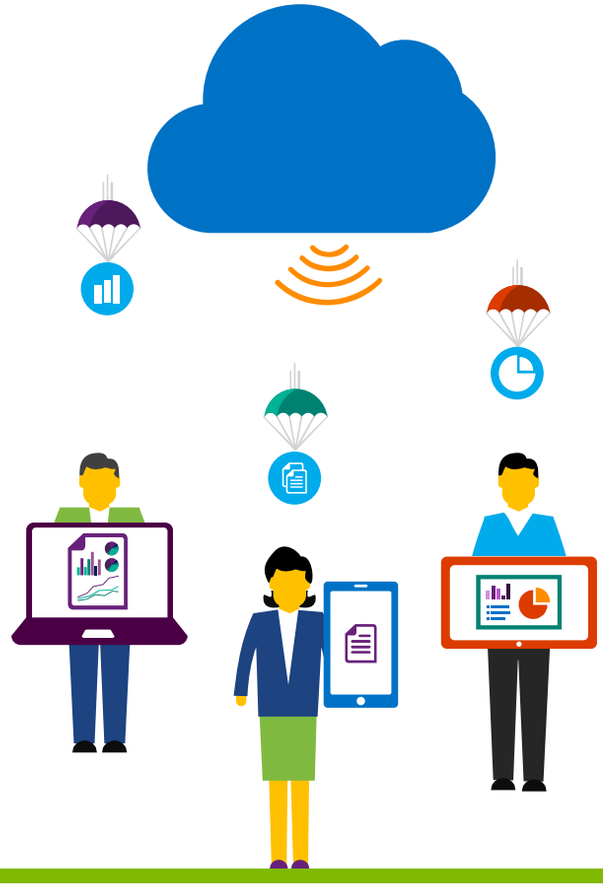
Role-based access; grant least privilege required for task

Privileged Identity Mgmt

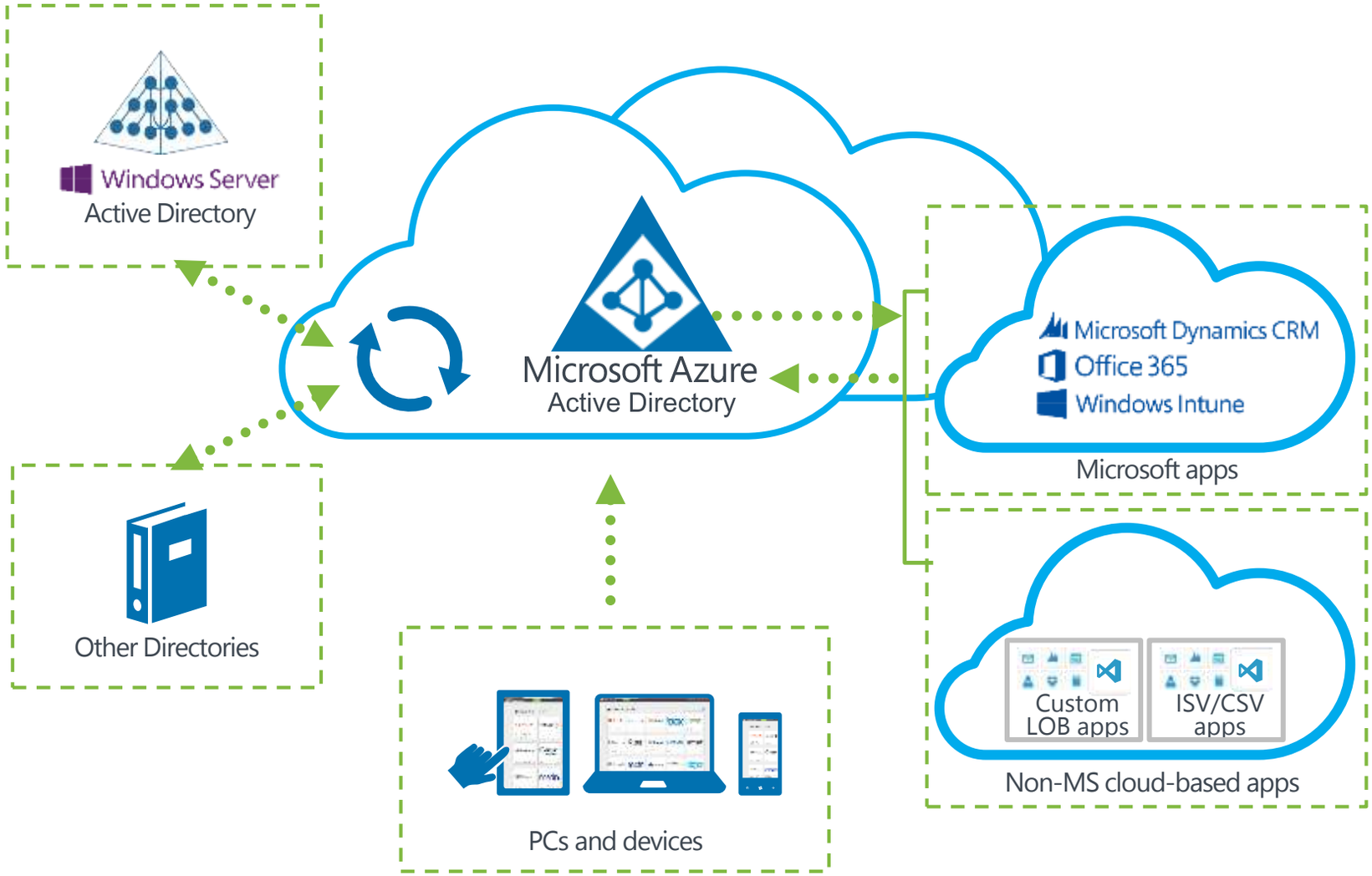
Manage, control and monitor access to Azure AD and O365 resources thru membership in built-in admin roles.

Security Monitoring

Security reports monitor access patterns that help identify potential threats.



Identity & Access: Single Sign-On Scenario



- ✓ Review reports and mitigate potential threats
- ✓ Can enable Multi-Factor Authentication

Data protection

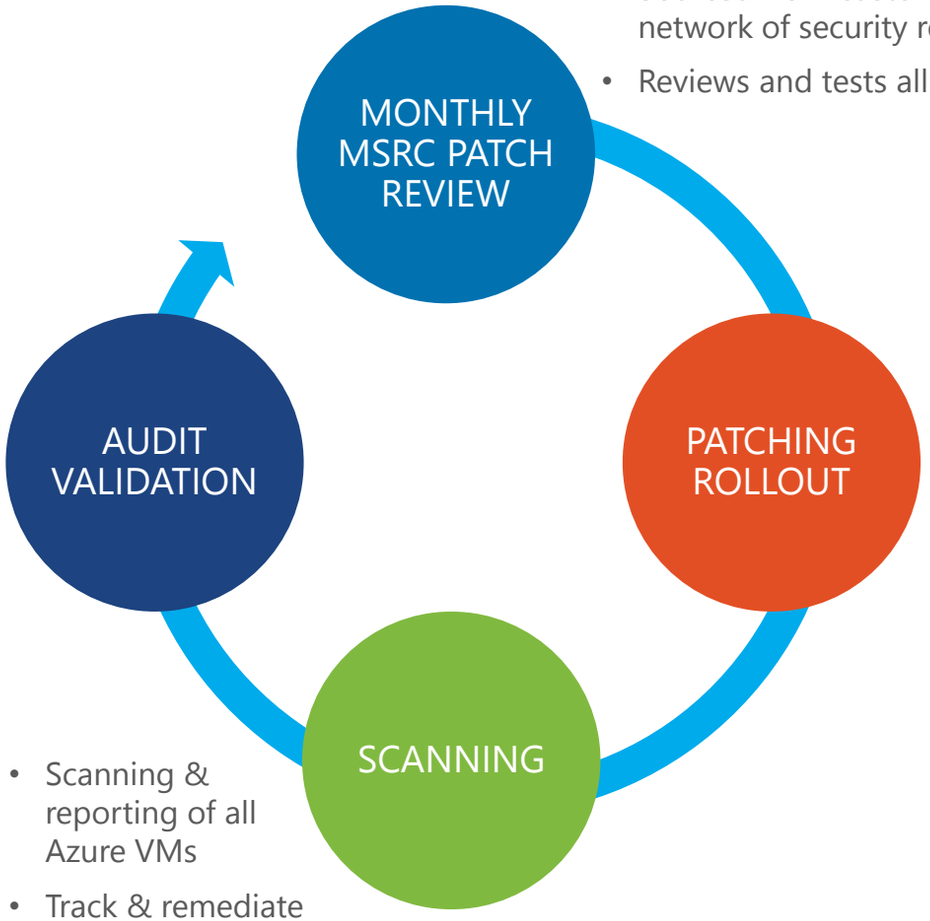
Azure provides customers with strong data security – both by default and as customer options

Data segregation	At-rest data protection
Logical isolation segregates each customer's data from that of others.	Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection	Encryption
Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.	Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy	Data destruction
Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.	When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer's data inaccessible.

Update Management



- Monitor 100,000+ vulnerability reports
- Sourced from customers & worldwide network of security researchers
- Reviews and tests all changes

- Prioritize critical updates
- Monthly OS releases with patches

- Scanning & reporting of all Azure VMs
- Track & remediate any findings

- Reconciliation report
- Resolution summary

AZURE:

✓ Apply patch management as a service

✓ Rigorously reviews & tests all changes

CUSTOMER:

✓ Applies similar patch management strategies for their Virtual Machines

Visualizing the security layers