Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
  - AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

Unmanaged & Mobile Devices

- Intune MDM/MAM

Managed Clients

- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS

Security Appliances

Express Route

Intranet Servers

- Windows Server 2016 Security
  Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring

S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft

Attack services are inexpensive

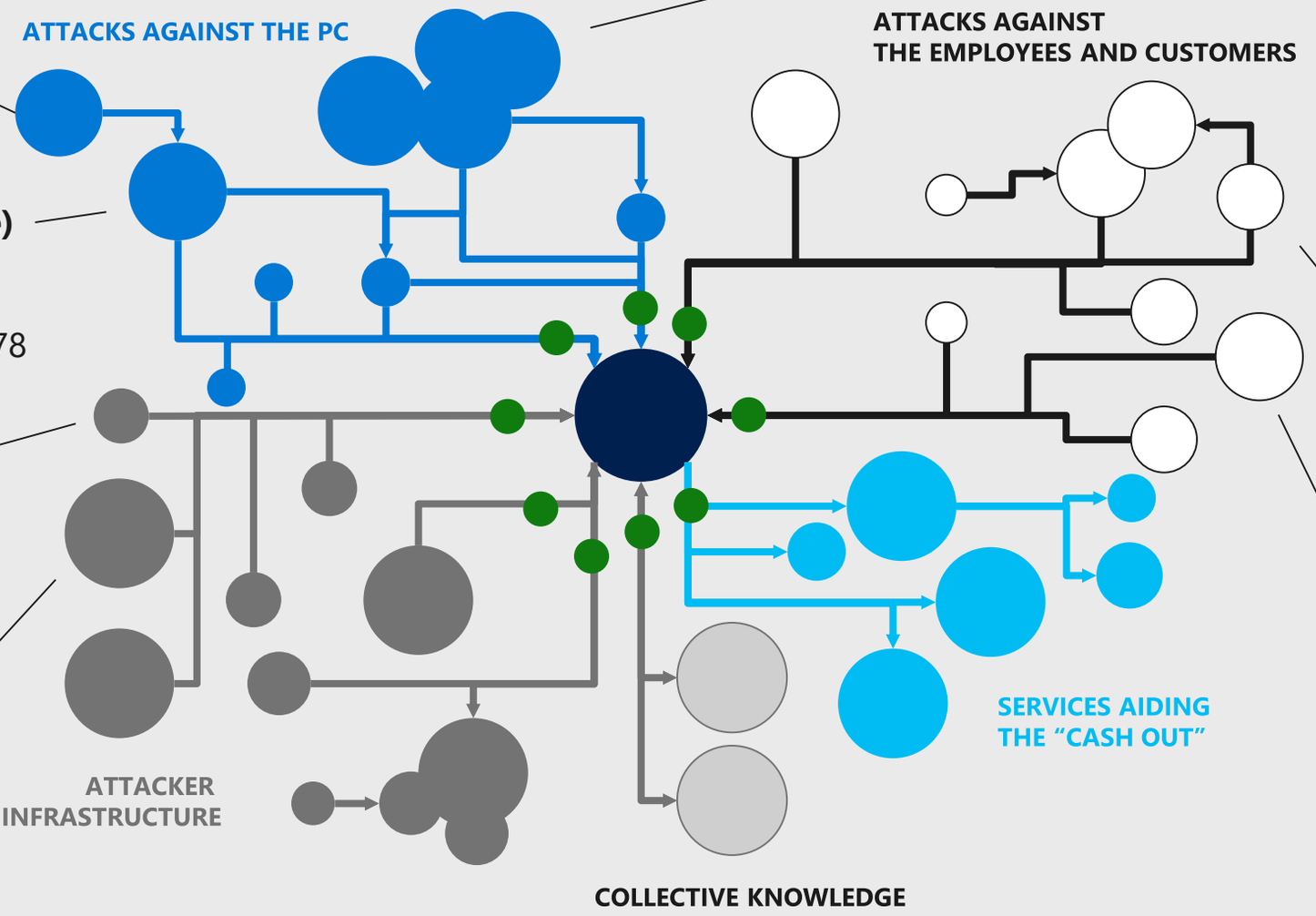
Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges
- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

Proxy services to evade IP geolocation prices vary
As low as $100 per week for 100,000 proxies.

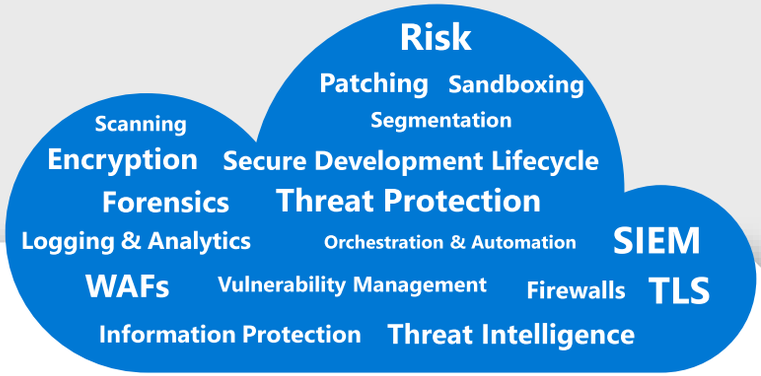


Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

Transforming from Legacy to Cloud

Evolving architecture, tools, skills, & practices



Architectures change, but principles & outcomes remain the same

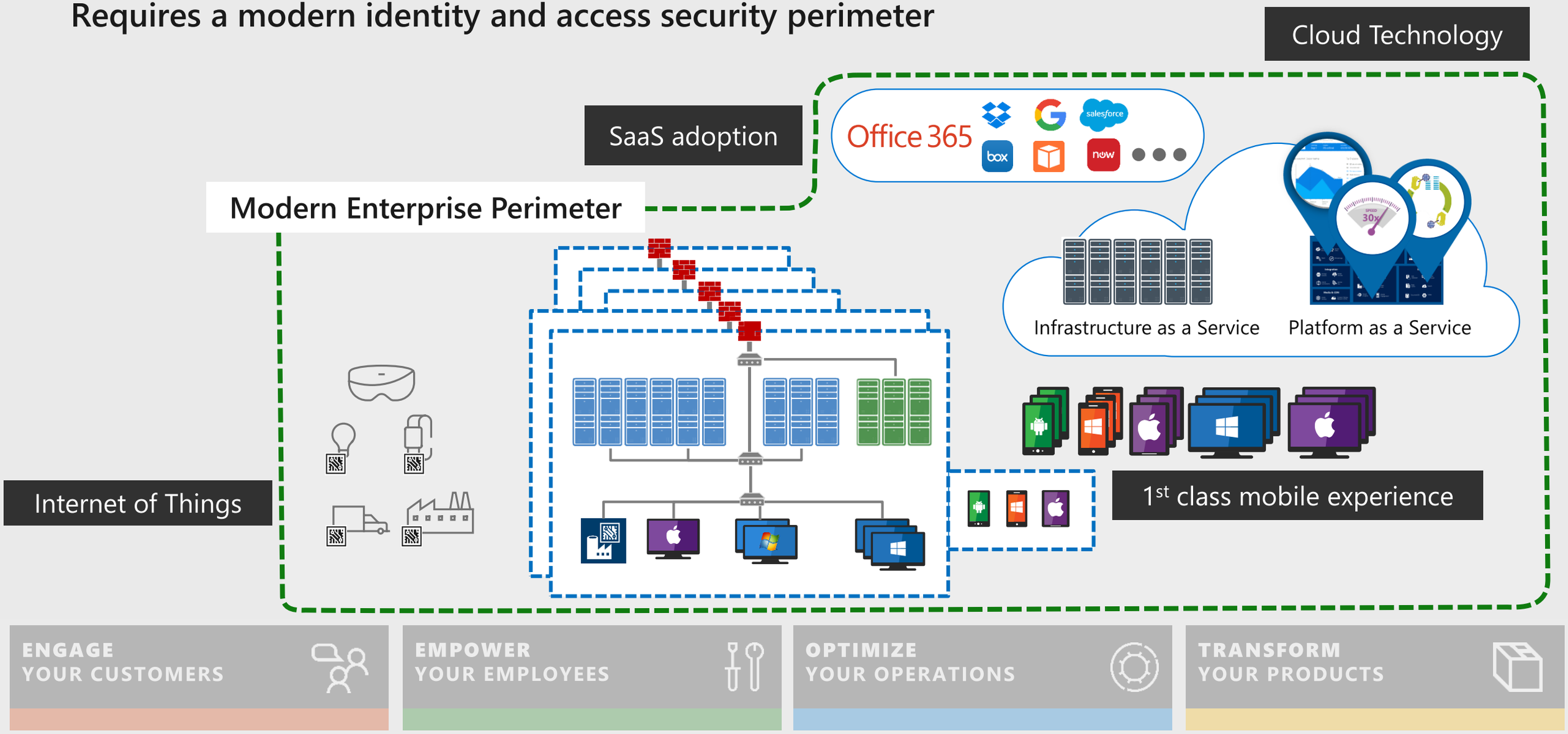
Roles, responsibilities, and skillsets will evolve

Controls, tools, and processes will evolve

Note: Legacy ‘technical debt’ persists with legacy workloads/applications in IaaS

Your enterprise in transformation

Requires a modern identity and access security perimeter



ENGAGE YOUR CUSTOMERS

EMPOWER YOUR EMPLOYEES

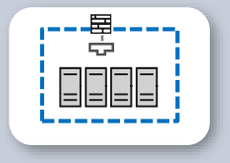
OPTIMIZE YOUR OPERATIONS

TRANSFORM YOUR PRODUCTS

Building a resilient cybersecurity program

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	Customer	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and Identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Customer	Customer
Applications	Microsoft	Customer	Customer	Customer
Network Controls	Microsoft	Customer	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

ESTABLISH A MODERN PERIMETER

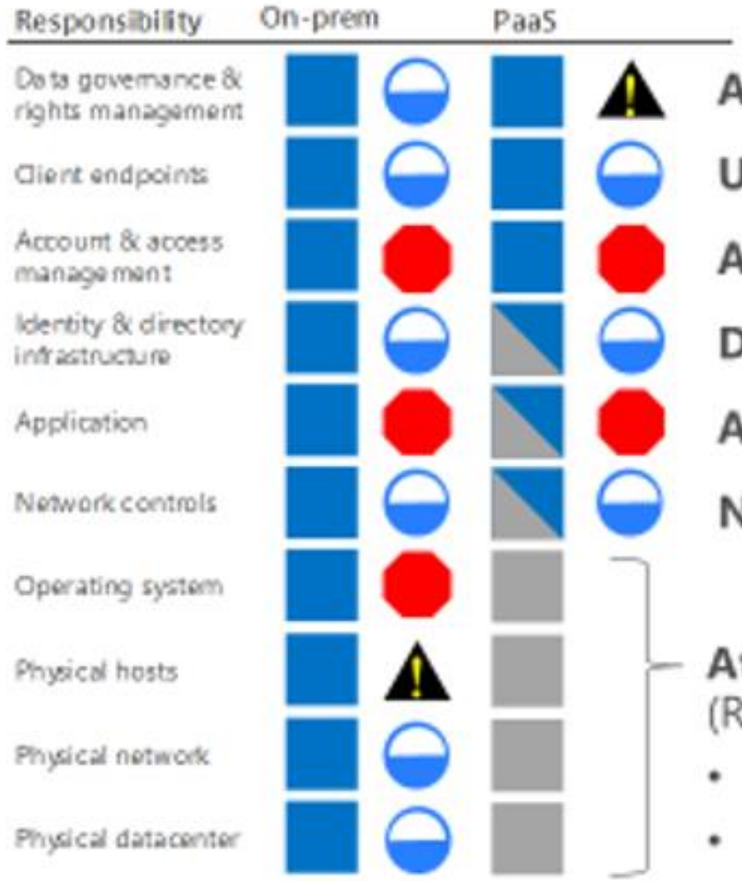


MODERNIZE INFRASTRUCTURE SECURITY

“TRUST BUT VERIFY” EACH CLOUD PROVIDER

Microsoft Customer

Security advantages of PaaS



Application data – **Depends on key/data management**

User/endpoints – **Depends on least privilege design**

Admin access – **One account → access to all apps / data / infra**

Directory – **Depends on identity system / app authentication**

Application code – **One exploit can lead to access of all data**

Network configuration – **Depends on TLS usage**

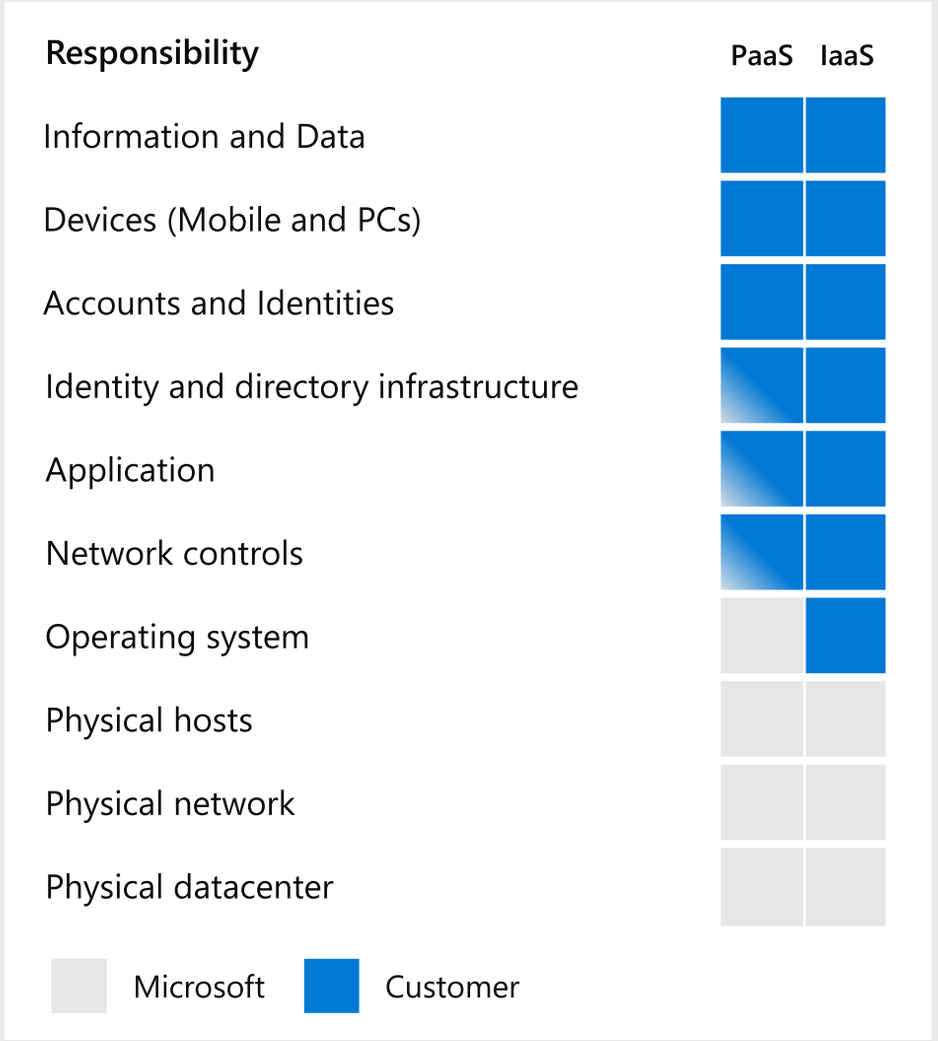
Attack Azure Infrastructure – Extremely low attack return on investment (ROI) for a single tenant

- Active security monitoring & engineering make attack very expensive
- Expense limits potential attackers to small pool with larger budgets

Always attractive target

App design can quickly deter attacker

Security Responsibilities Transfer to Azure



Transferred for PaaS

Security Patches

Feature Upgrades

VMs/Containers security –
OS and Middleware Installation, Maintenance, troubleshooting, etc.

Azure Marketplace
fits PaaS or IaaS model

Transferred for IaaS and PaaS

Denial of Service*

Racking/Stacking Servers, Delays in Adding Capacity

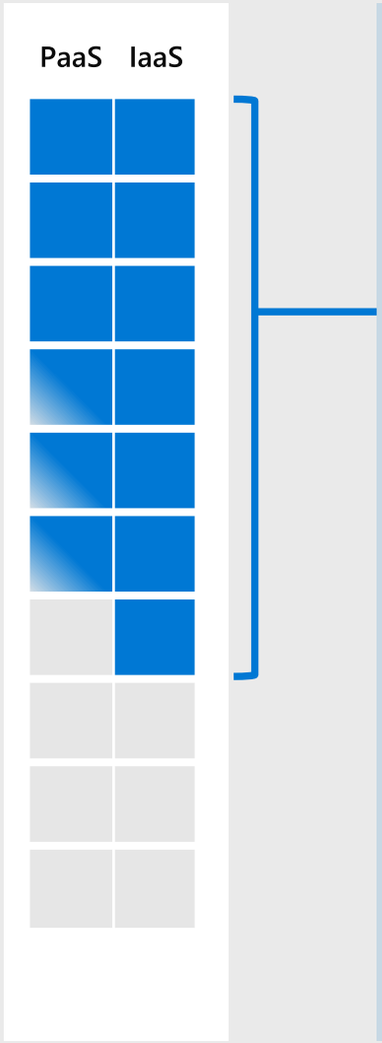
Fabric/Virtualization Patching, Maintenance & Troubleshooting

Fabric Availability / Uptime
→ SLA from Microsoft

Attacks on

- Physical Attacks
- Virtualization Fabric
- Hardware/Firmware
- Network Infrastructure

Azure Threats – Mix of Old & New…



EXISTING TECHNIQUES (AT COMPARABLE LEVELS)

EXPLOIT/ENTER	TRAVERSAL	MONETIZATION
SOCIAL ENGINEERING	CREDENTIAL THEFT & ABUSE (HASHES, SSH…)	RANSOMWARE
PHISHING	SCAN & EXPLOIT	TARGETED DATA THEFT
GEO-FILTERING EVASION WITH PROXY		COMMODITY BOTNET/DDOS/ETC
●●●	●●●	●●●

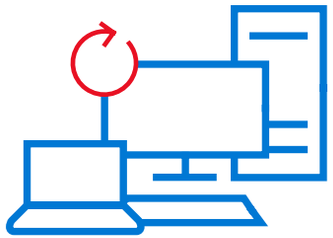
New Techniques (☆) or Very High Usage (⌂)

☆ ACQUIRE TENANT KEYS FROM GITHUB/ETC	☆ PIVOT TO ON PREMISES FROM CLOUD	⌂ CRYPTOMINERS – (WEBSERVERS, VISITORS)
⌂ RDP/SSH PASSWORD SPRAY & BRUTE FORCE		

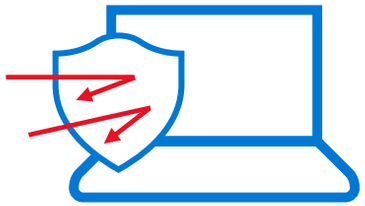
Designing for Failure – The Mindshift

THEN

Reliability:
Designed not to fail

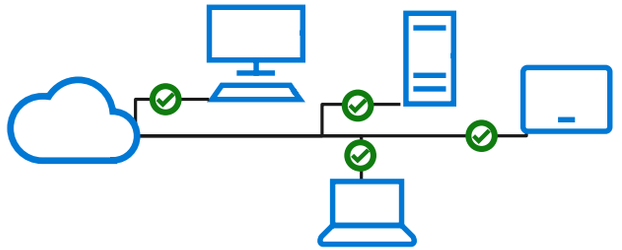


Prevent:
Every possible attack

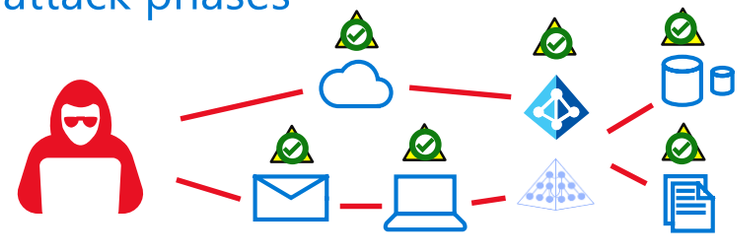


NOW

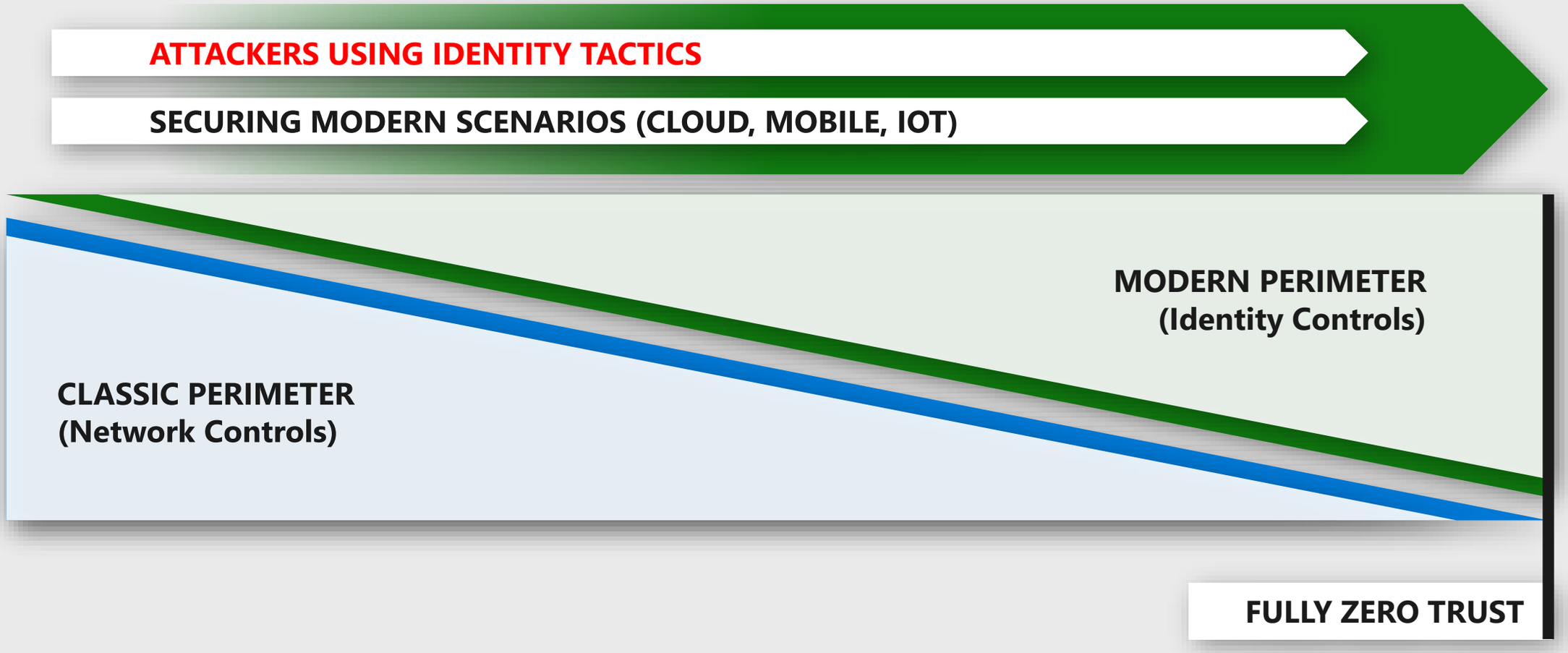
Resilience:
Designed to recover quickly



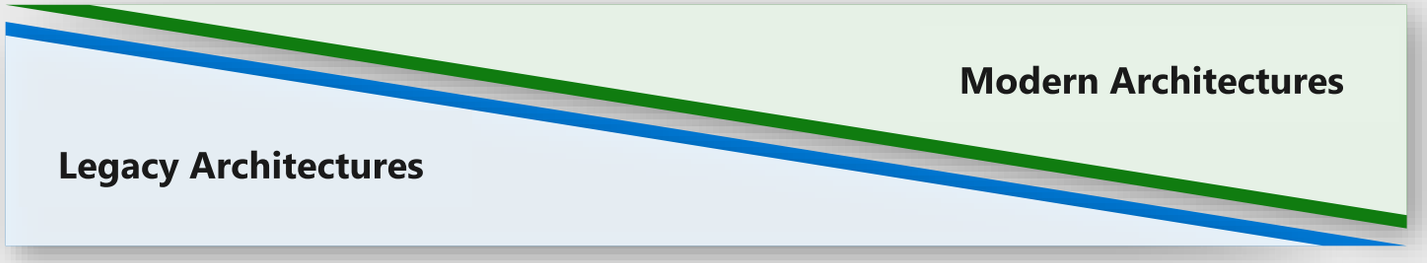
Assume Compromise:
Protect, detect, and respond along attack phases



Running Dual Perimeters



Evolution of Roles and Responsibilities



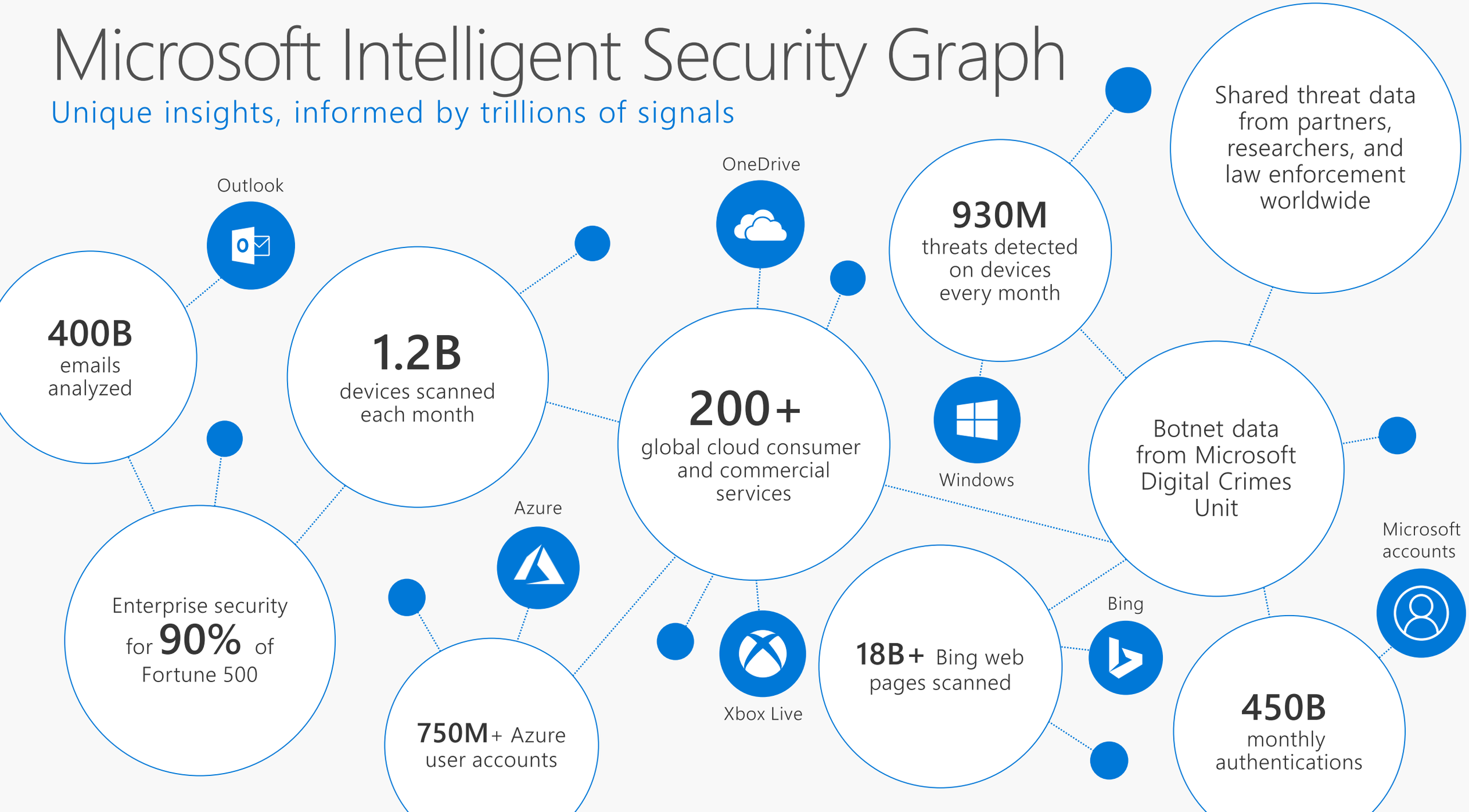
"STOP THE PRESSES!" → CONTINUOUS VALIDATION

Security roles will change with architectural/operational models

Manual Resource Administration	**Administration**	Author & Govern Automation
Containment with Network	Network → **Containment**	Containment at all layers (Net, App, ID, Data, etc.)
Quality Check Before Release	**Development**	Security SME in DevOps process
Project based Engagement	**Architecture**	Continuous Engagement & Improvement

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Microsoft protecting Microsoft

Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more...

Traditional Defenses

Corporate Infrastructure + Cloud Infrastructure

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt

Attackers View

People

Background Checks
Security Training
Conferences

Least Privilege

Least Privilege Access
Just-in-time Access
and more...

Authentication

Multi-factor Auth
Anomaly Detection

Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

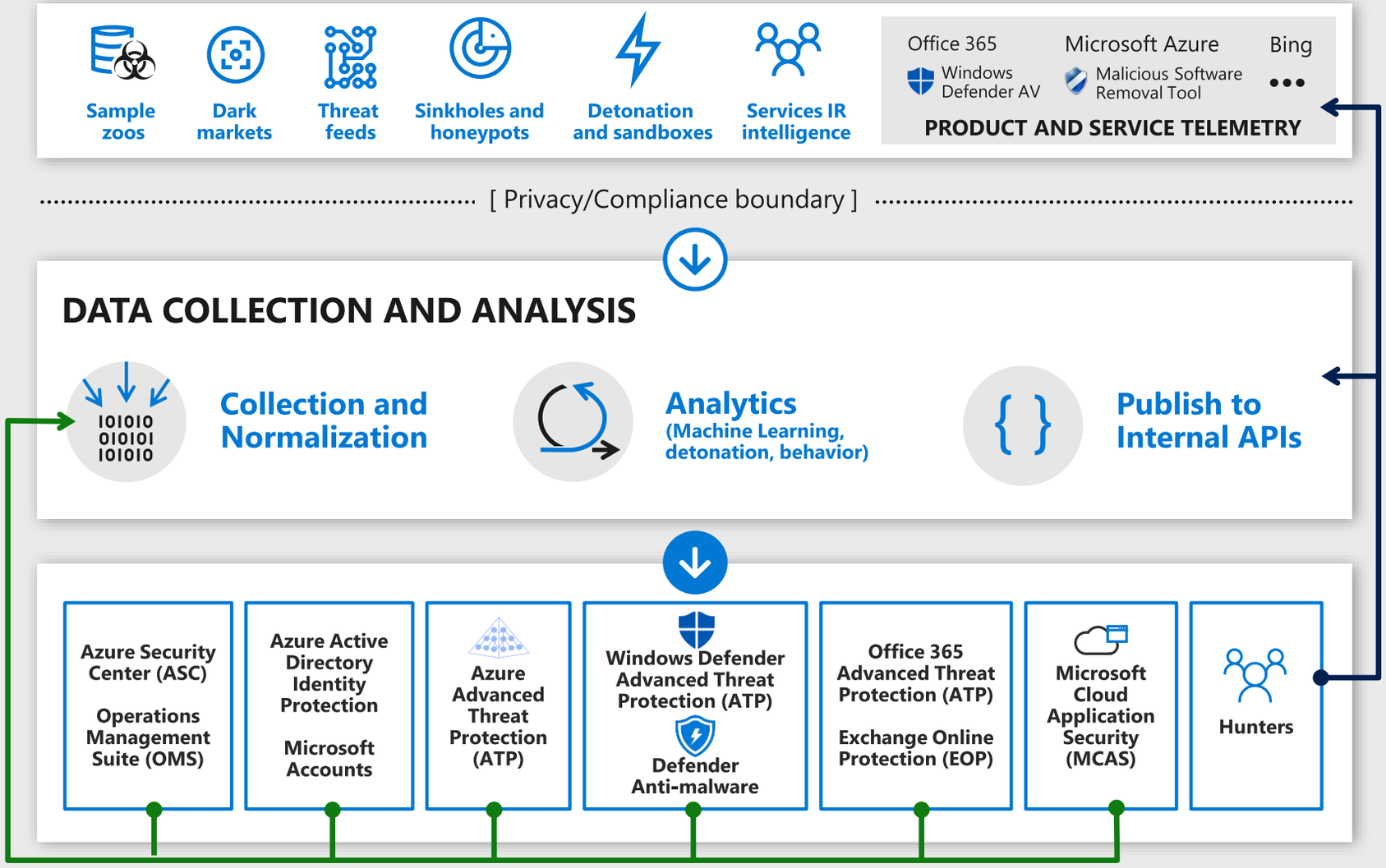
Automated Assessments
Secure DevOps toolkit
and more...

Security Development Lifecycle

Continuous Logging & Monitoring
Incident Response
CDOC (24x7 SOC)

Monitoring & Vigilance

Inside The Intelligent Security Graph

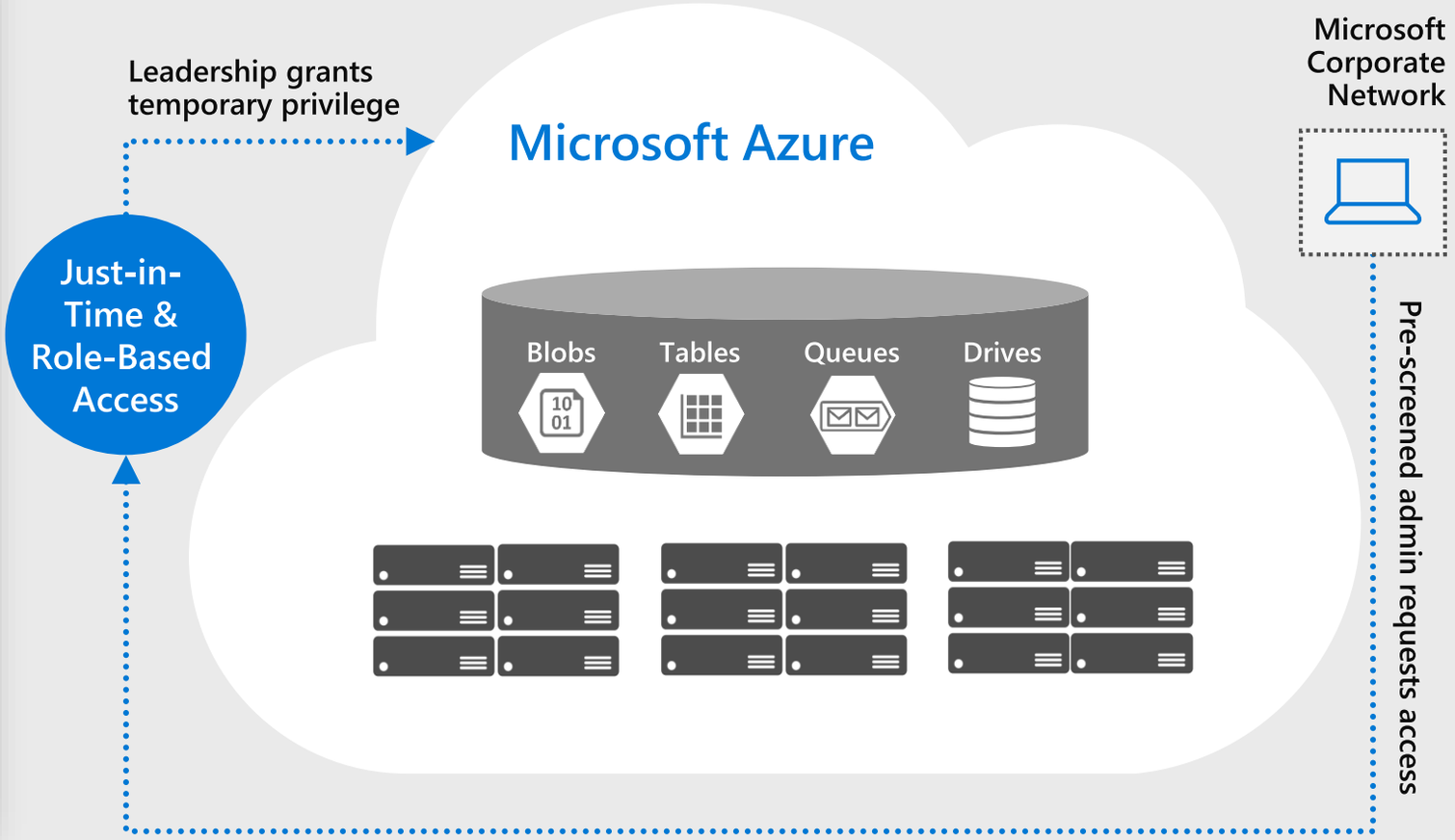


- Products instrumented to strict privacy/compliance standards
  See Microsoft Trust Center
- Analytics help fuel new discoveries
- Products send data to graph
- Products use Interflow APIs to access results
- Products generate data which feeds back into the graph
- Hunters identify attacks, improve analytics, feed back into product design

Employee Access Management

Just-in-Time (JIT) Administrative Privileges + Just Enough Access Through RBAC

- No standing access to the customer data
- Grants least privilege required to complete task
- Multi-factor authentication required for all administration
- Access requests are audited, logged, and reviewed

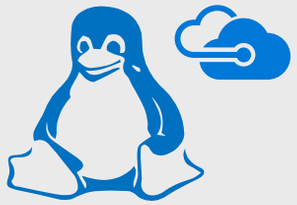


Integrating with your existing solution portfolio

Microsoft Intelligent Security Association

Active in security and open source communities

Top contributor
to GitHub in 2016



~50% of IaaS VMs
in Azure run Linux

Board Membership

cloud security alliance®

security advisor alliance

THE LINUX FOUNDATION

fido alliance simpler stronger authentication

FINANCIAL SERVICES Information Sharing and Analysis Center

Key Challenges and Strategic Opportunities

Identity-based attacks are up 300% this year	Adopt identity-based protection
Information is your most attractive target	Protect information wherever it goes
Attackers constantly evolving techniques	Detect attacks faster and automate response
Most enterprises report using more than 60 security solutions	Use tools that integrate investigation experience and provide guidance

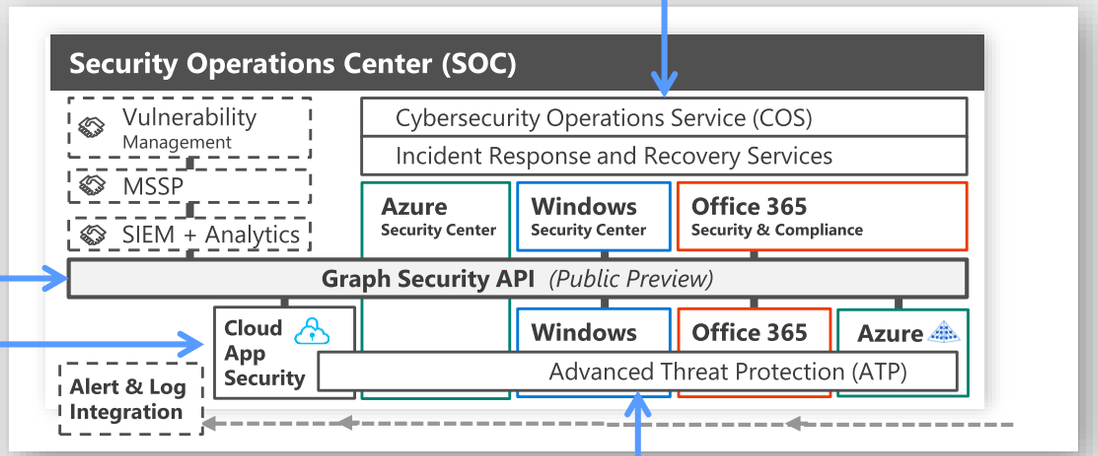
Security Operations Center (SOC)

CHALLENGES

- **Traditional SIEM centric model results in**
  - **High Event Volume** and associated cost
  - **Alert Overload** - too many false positives
  - **Poor Investigation Workflow**
- **Security expertise wasted on**
  - Manual integration of tools/intelligence
  - Constantly evaluating products

MICROSOFT'S APPROACH

- ✓ Assist with **Incident Response and Recovery** as well as proactively **hunting for adversaries**
- ✓ **Integrate existing SOC tools** and Microsoft capabilities with **Graph Security API (public preview)**
- ✓ Anomaly detection, alerts, and investigation across **SaaS applications** with Cloud App Security
- ✓ Advanced Threat Protection provides **integrated investigation experience** across Windows/Linux/Mac desktops and servers, Office 365, Active Directory, and Azure Tenants.
- ✓ Intelligent Security Graph provides **integrated intelligence** for detection



Intelligent Security Graph

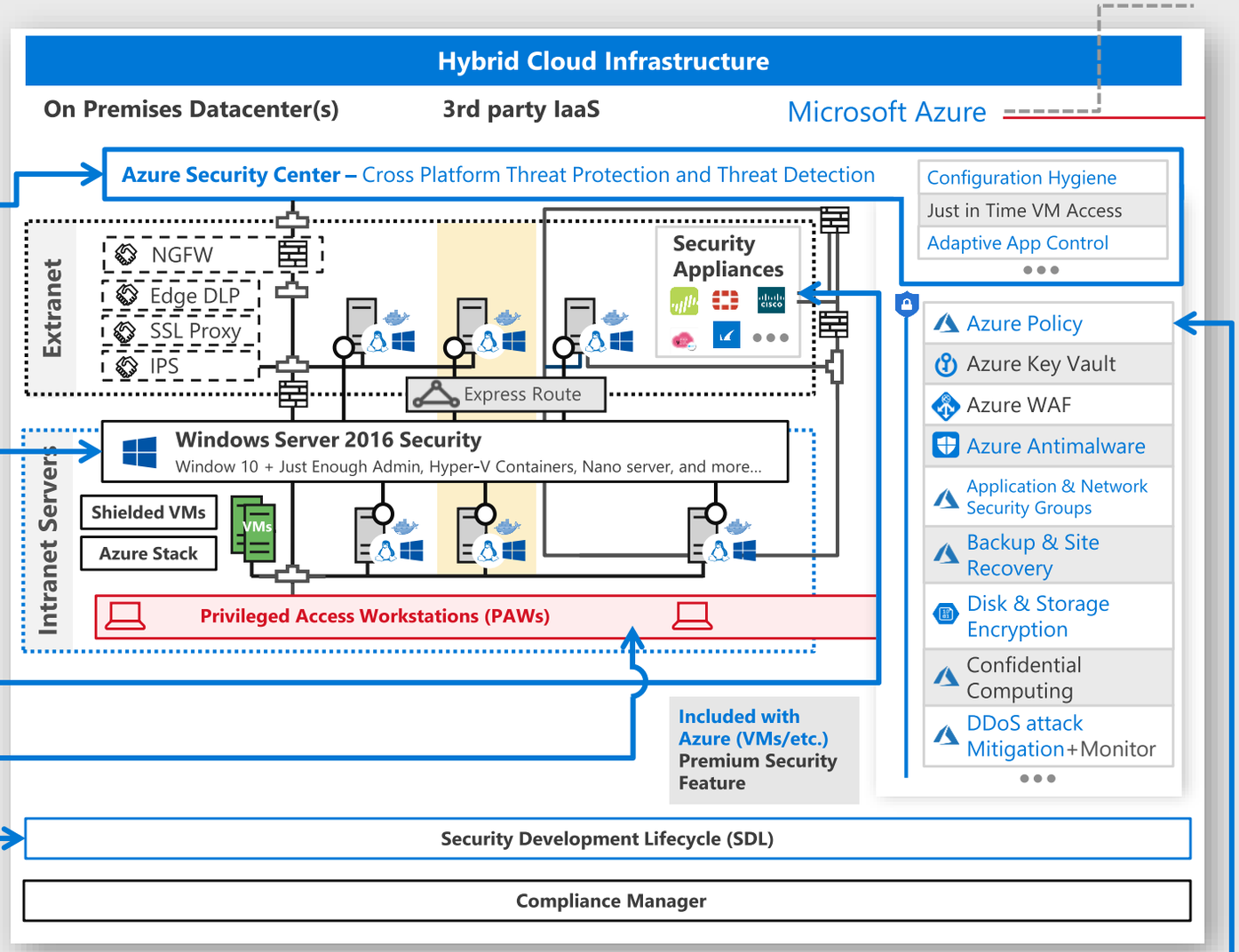
Hybrid Cloud Infrastructure

CHALLENGES

- **Limited experience and toolsets** for securing hybrid architecture and Platform as a Service
- **Critical Risks** - Privilege management and security hygiene critical for cloud workloads

MICROSOFT'S APPROACH

- ✓ **Cross-Platform and Cross-Cloud** – security capabilities to enable visibility and control
- ✓ **Deep Azure Defenses** – Integrated with platform to secure Azure workloads, assess compliance
- ✓ **On Premises security** investments to modernize security and leverage cloud learnings + technology
- ✓ **Marketplace –** Integrate existing capabilities and skills
- ✓ **Privilege Management** – Protect against high impact attacks against privileged accounts
- ✓ **Secure Development Lifecycle (SDL)** – Securing applications and PaaS workloads



Azure has the most comprehensive compliance coverage in the industry

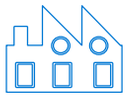
Global

- ☑ CSA STAR Attestation
- ☑ CSA STAR Certification
- ☑ CSA STAR Self-Assessment
- ☑ ISO 22301
- ☑ ISO 27001
- ☑ ISO 27017
- ☑ ISO 27018
- ☑ SOC 1 Type 2
- ☑ SOC 2 Type 2

U.S. Government

- ☑ CJIS
- ☑ DoD DISA SRG Level 2
- ☑ DoD DISA SRG Level 4
- ☑ DoD DISA SRG Level 5
- ☑ FedRAMP
- ☑ FIPS 140-2
- ☑ High JAB P-ATO
- ☑ IRS 1075
- ☑ ITAR
- ☑ Moderate JAB P-ATO
- ☑ Section 508 VPAT
- ☑ SP 800-171

Industry

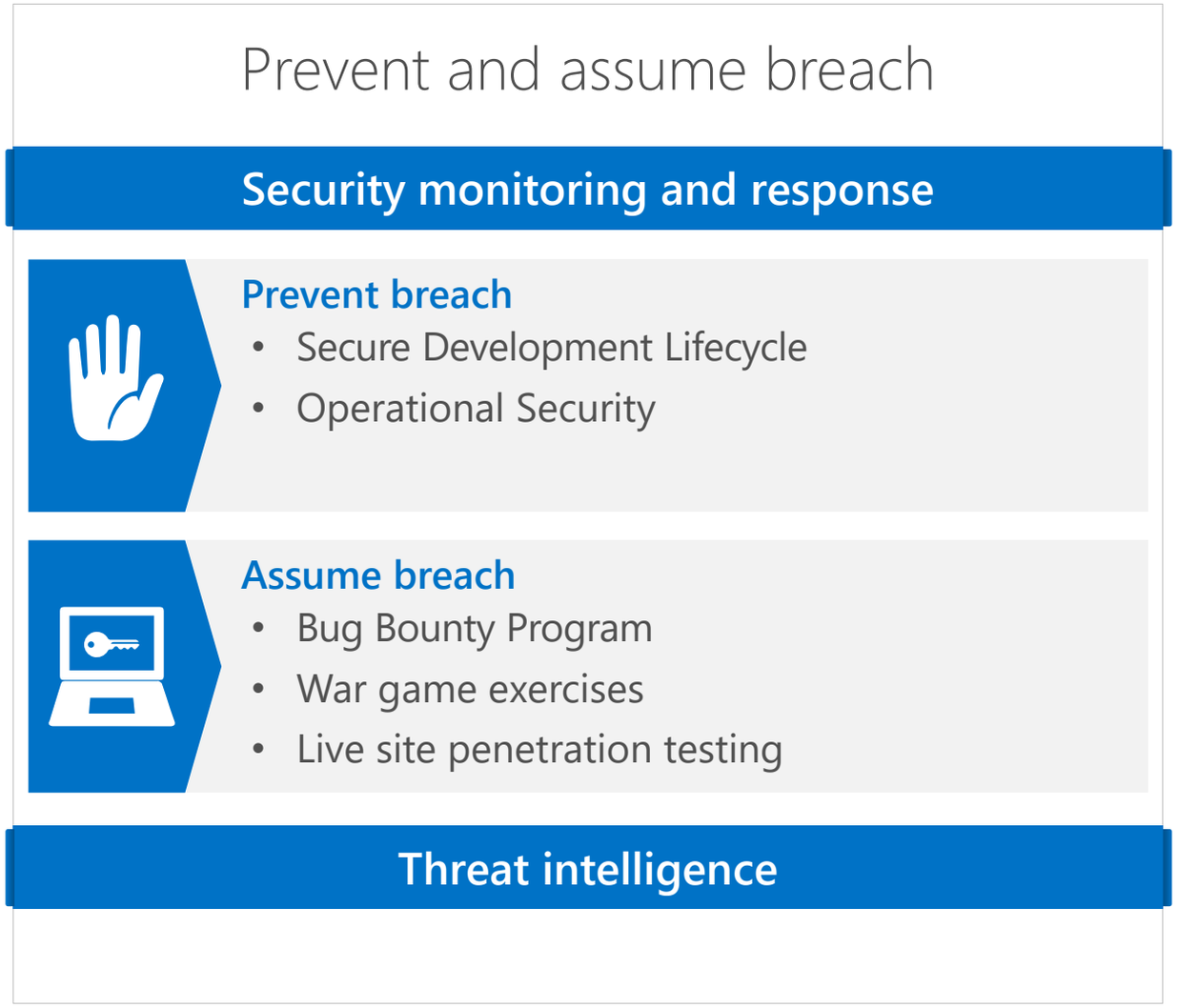


- ☑ CDSA
- ☑ FACT UK
- ☑ FERPA
- ☑ FFIEC
- ☑ FISC Japan
- ☑ GLBA
- ☑ GxP 21 CFR Part 11
- ☑ HIPAA / HITECH
- ☑ HITRUST
- ☑ IG Toolkit UK
- ☑ MARS-E
- ☑ MPAA
- ☑ PCI DSS Level 1
- ☑ Shared Assessments

Regional

- ☑ Argentina PDPA
- ☑ Australia IRAP/CCSL
- ☑ Canada Privacy Laws
- ☑ China DJCP
- ☑ China GB 18030
- ☑ China TRUCS
- ☑ ENISA IAF
- ☑ EU Model Clauses
- ☑ EU-US Privacy Shield
- ☑ Germany IT Grundschutz
- ☑ India MeitY
- ☑ Japan CS Mark Gold
- ☑ Japan My Number Act
- ☑ New Zealand GCIO
- ☑ Singapore MTCS
- ☑ Spain DPA
- ☑ Spain ENS
- ☑ UK G-Cloud

Prevent and assume breach



Prevent breach – A methodical Secure Development Lifecycle and Operational Security minimizes probability of exposure

Assume breach – Identifies & addresses potential gaps:

- Ongoing live site testing of security response plans improves mean time to detection and recovery
- Bug bounty program encourages security researchers in the industry to discover and report vulnerabilities
- Reduce exposure to internal attack (once inside, attackers do not have broad access)

Latest **Threat Intelligence** to prevent breaches and to test security response plans

State of the art **Security Monitoring and Response**

Operational security

Security Monitoring and Response

Data & Keys	User	Application	Host System	Internal Network	Network Perimeter	Facility
Data Protection Access control, encryption, key management	**Admin Access** Identity management, dual-factor authentication, training and awareness, screening, Least and Temporary Privilege	**Application Security** Access control, monitoring, anti-malware, vulnerability scanning, patch and configuration management	**Host Protection** Access control, monitoring, anti-malware, vulnerability scanning, patch and configuration management	**Network Security** Segmentation, intrusion detection, vulnerability scanning	**Network Security** Edge ACLs, DOS, intrusion detection, vulnerability scanning	**Physical Security** Physical controls, video surveillance, access control

Threat Intelligence Feed

Physical security of datacenters

Perimeter

- Barriers
- Fencing

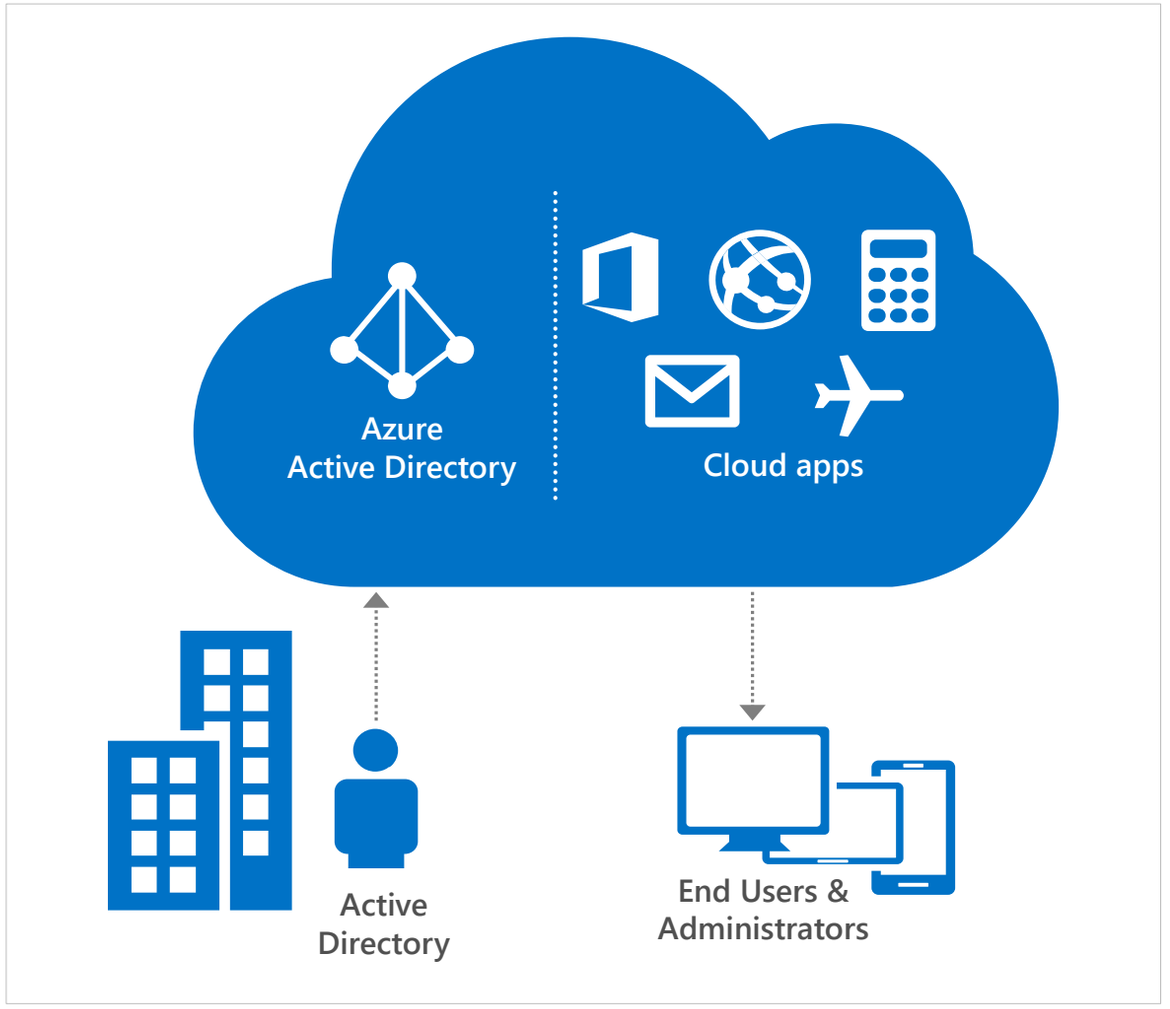
Building

- Seismic bracing
- Security operations center
- 24X7 security staff
- Days of backup power

Computer room

- Cameras
- Alarms
- Two-factor access control: Biometric readers & card readers

Identity & access management



AZURE

- Uses Azure AD to govern access to the management portal with granular access controls for users and groups on subscription or resource groups
- Provides enterprise cloud identity and access management for end users
- Enables single sign-on across cloud applications
- Offers Multi-Factor Authentication for enhanced security

CUSTOMER

- Centrally manages users and access to Azure, O365, and hundreds of pre-integrated cloud applications
- Builds Azure AD into their web and mobile applications
- Can extend on-premises directories to Azure AD

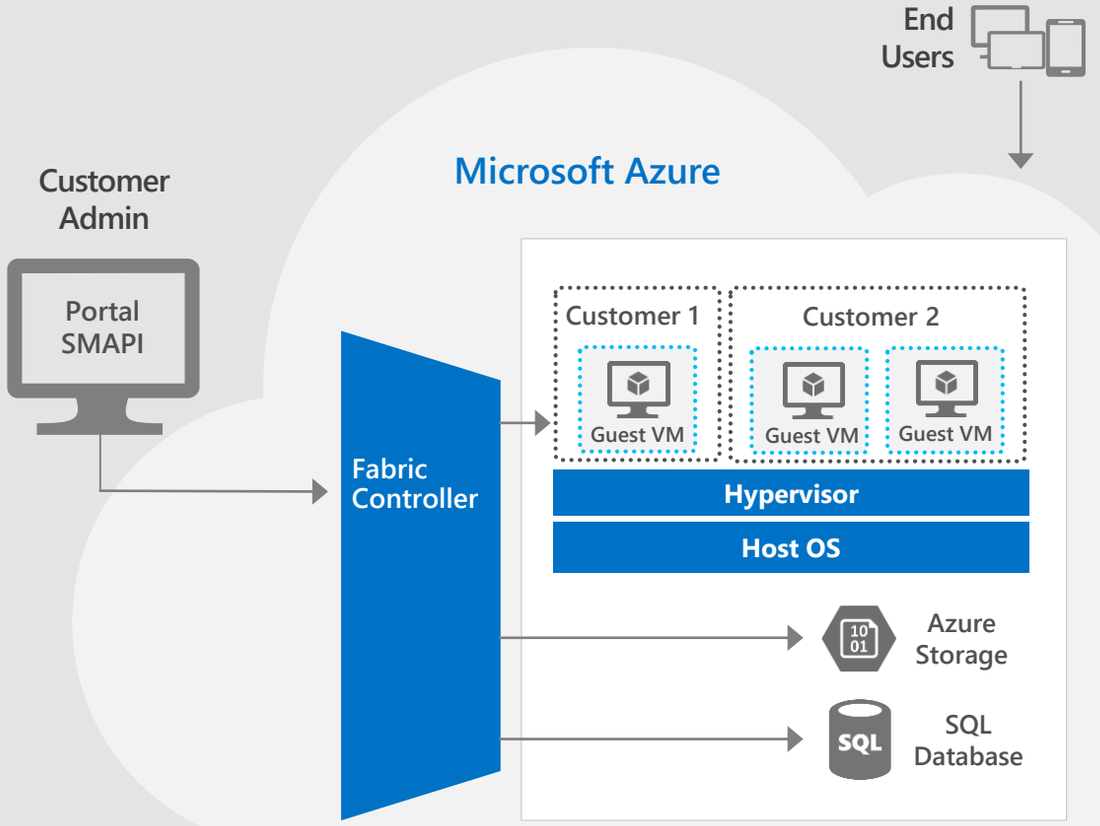
Architected for more secure multi-tenancy

Azure

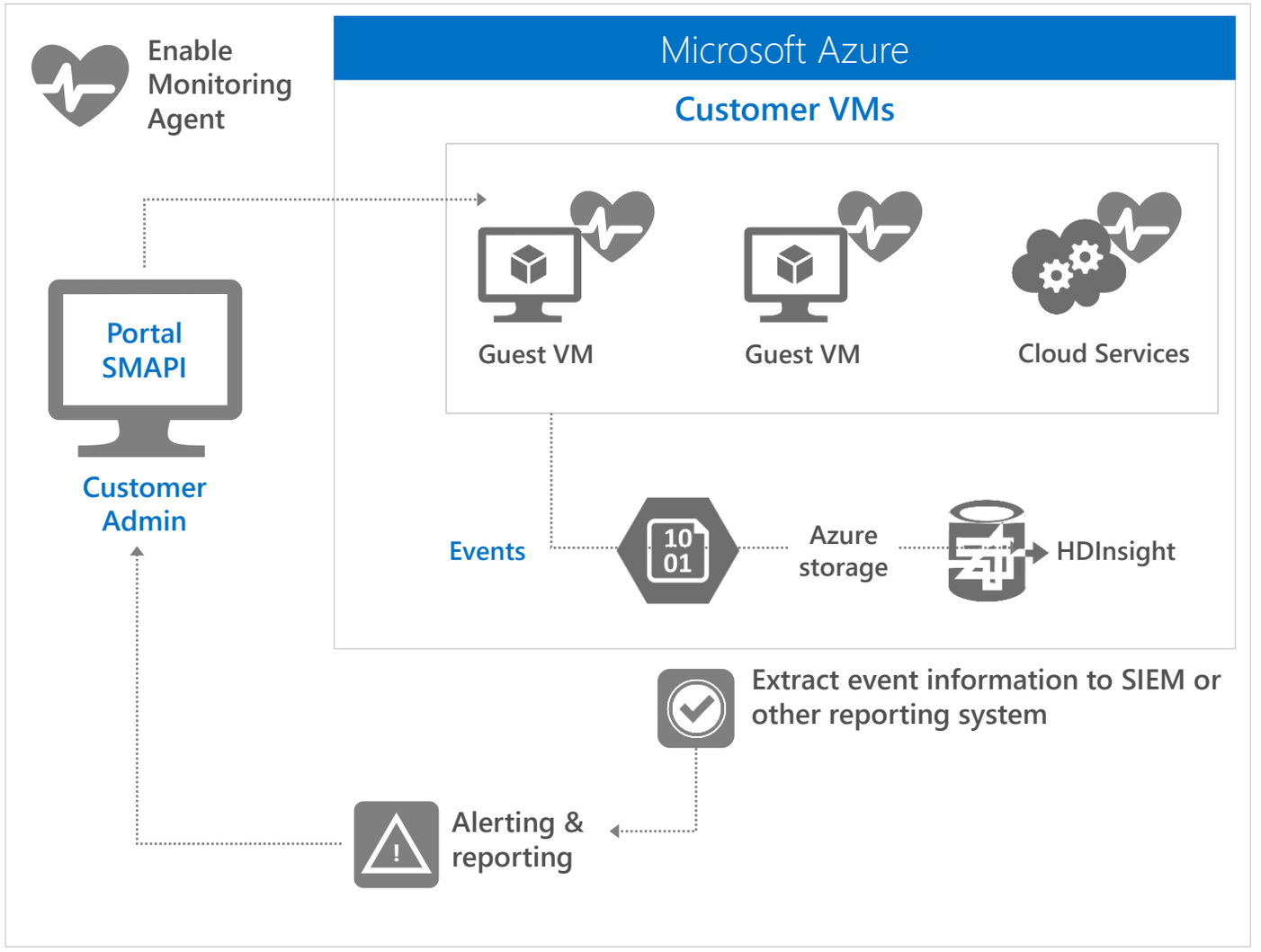
- Centrally manages the platform and helps isolate customer environments using the Fabric Controller
- Runs a configuration-hardened version of Windows Server as the Host OS
- Uses Hyper-V, a battle tested and enterprise proven hypervisor
- Runs Windows Server and Linux on Guest VMs for platform services

Customer

- Manages their environment through service management interfaces and subscriptions
- Chooses from the gallery or brings their own OS for their Virtual Machines



Monitoring & alerts



AZURE

- Performs monitoring & alerting on security events for the platform
- Enables security data collection via Monitoring Agent or Windows Event Forwarding

CUSTOMER

- Configures monitoring
- Exports events to SQL Database, HDInsight or a SIEM for analysis
- Monitors alerts & reports
- Responds to alerts

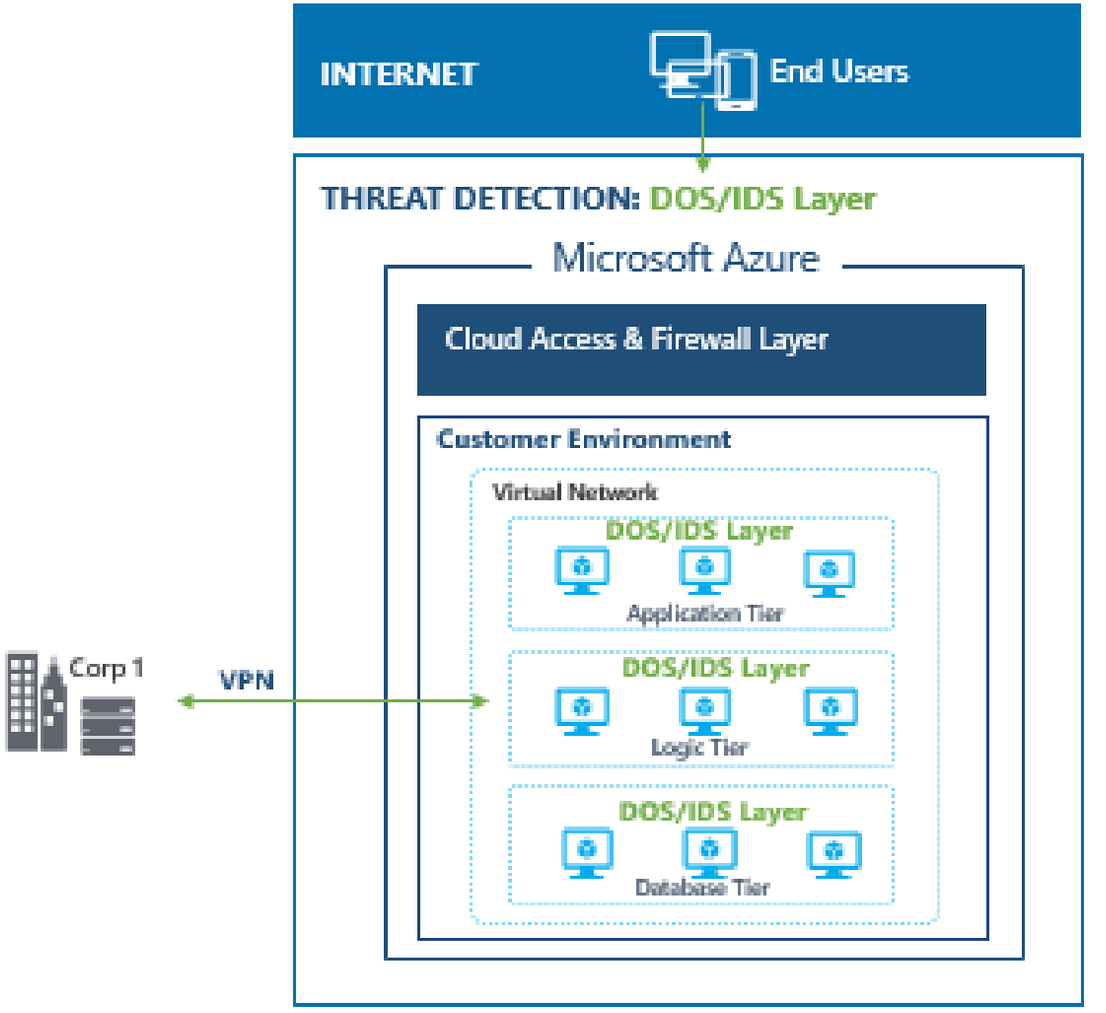
Threat detection

Azure

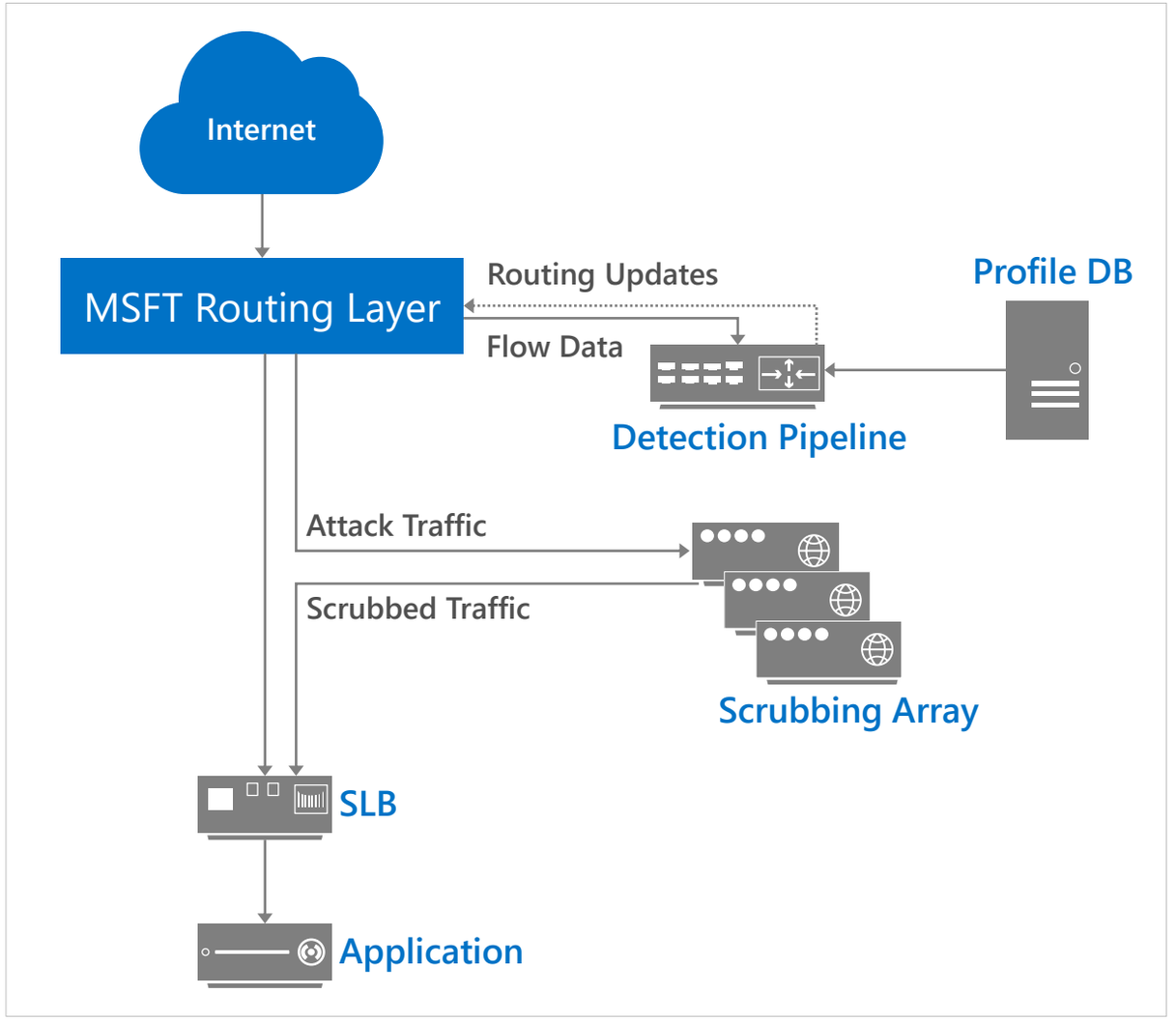
- Performs big data analysis of logs for intrusion detection & prevention for the platform
- Employs denial of service attack prevention measures for the platform
- Regularly performs penetration testing

Customer

- Can add extra layers of protection by deploying additional controls, including DOS, IDS, web application firewalls
- Conducts authorized penetration testing of their application



DDoS system overview



SUPPORTED DDOS ATTACK PROFILES

- TCP SYN
- UDP/ICMP/TCP Flood

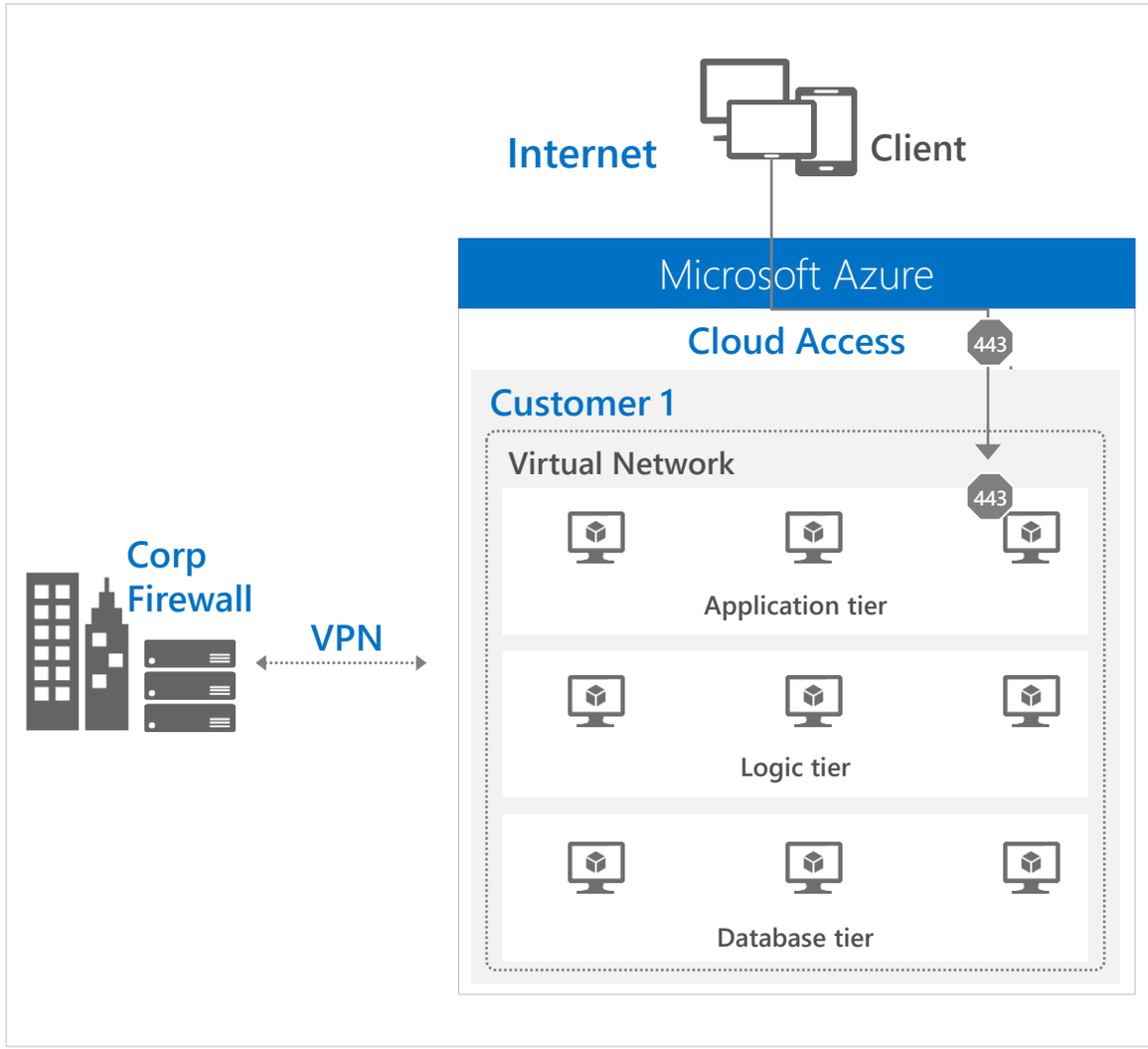
DETECTION PROCESS

- Traffic to a given /32 VIP Inbound or Outbound is tracked, recorded, and analyzed in real time to determine attack behavior

MITIGATION PROCESS

- Traffic is re-routed to scrubbers via dynamic routing updates
- Traffic is SYN auth. and rate limited

Firewalls



AZURE

- Restricts access from the Internet, permits traffic only to endpoints, and provides load balancing and NAT at the Cloud Access Layer
- Isolates traffic and provides intrusion defense through a distributed firewall

CUSTOMER

- Applies corporate firewall using site-to-site VPN
- Configures endpoints
- Defines access controls between tiers and provides additional protection via the OS firewall

Network protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises datacenters with Azure VMs

Virtual Networks

Customers can connect one or more cloud services using private IP addresses.

Network Security Groups

Customers can control over network traffic flowing in and out of customer services in Azure.

VPN

Customers can securely connect to a virtual network from anywhere.

ExpressRoute

Customers can create private connections between Azure datacenters and infrastructure that's on your premises or in a colocation environment.

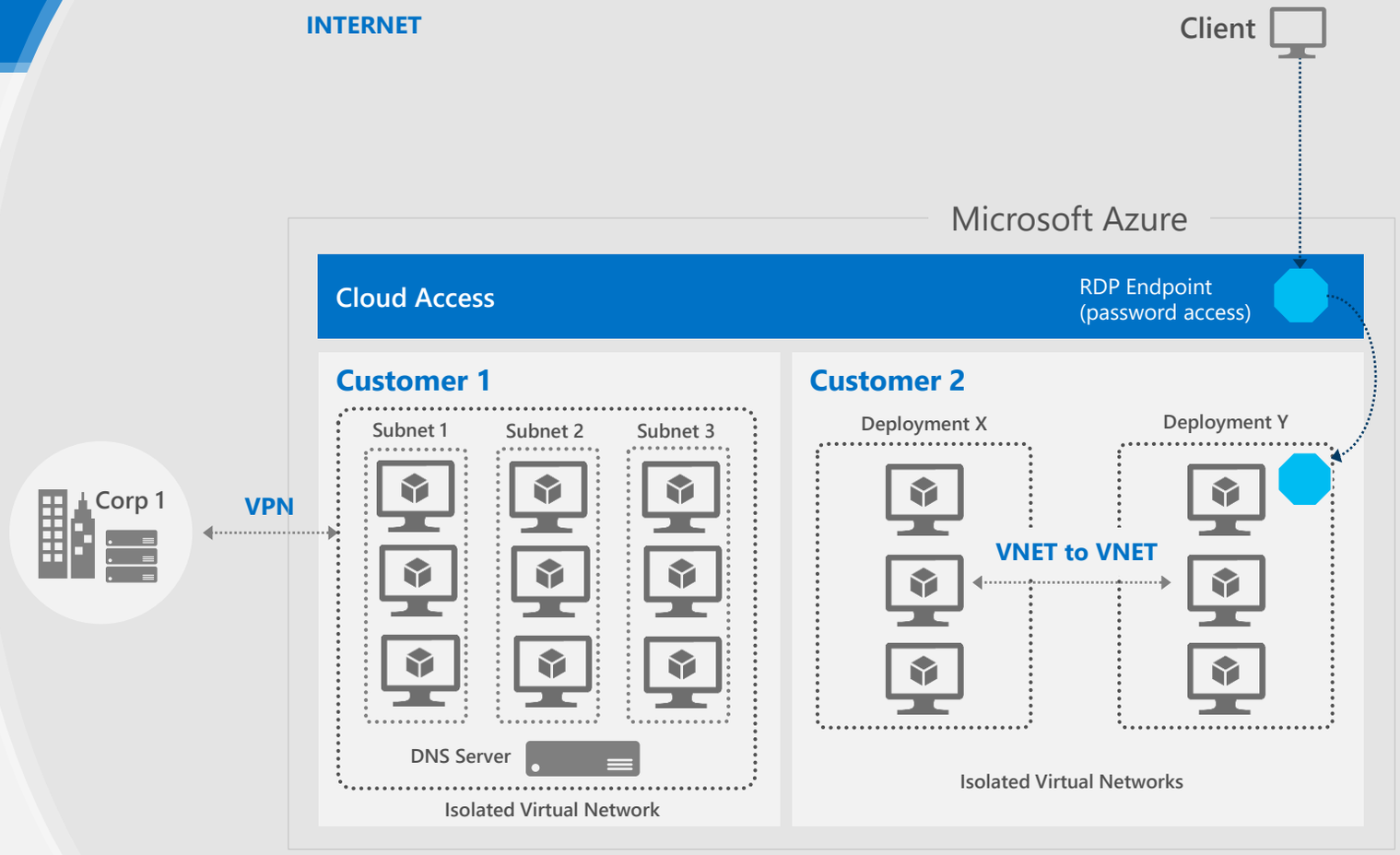
Virtual networks

Azure

- Allows customers to create isolated virtual private networks

Customer

- Creates Virtual Networks with Subnets and Private IP addresses
- Enables communications between their Virtual Networks
- Can bring their own DNS
- Can domain join their Virtual Machines



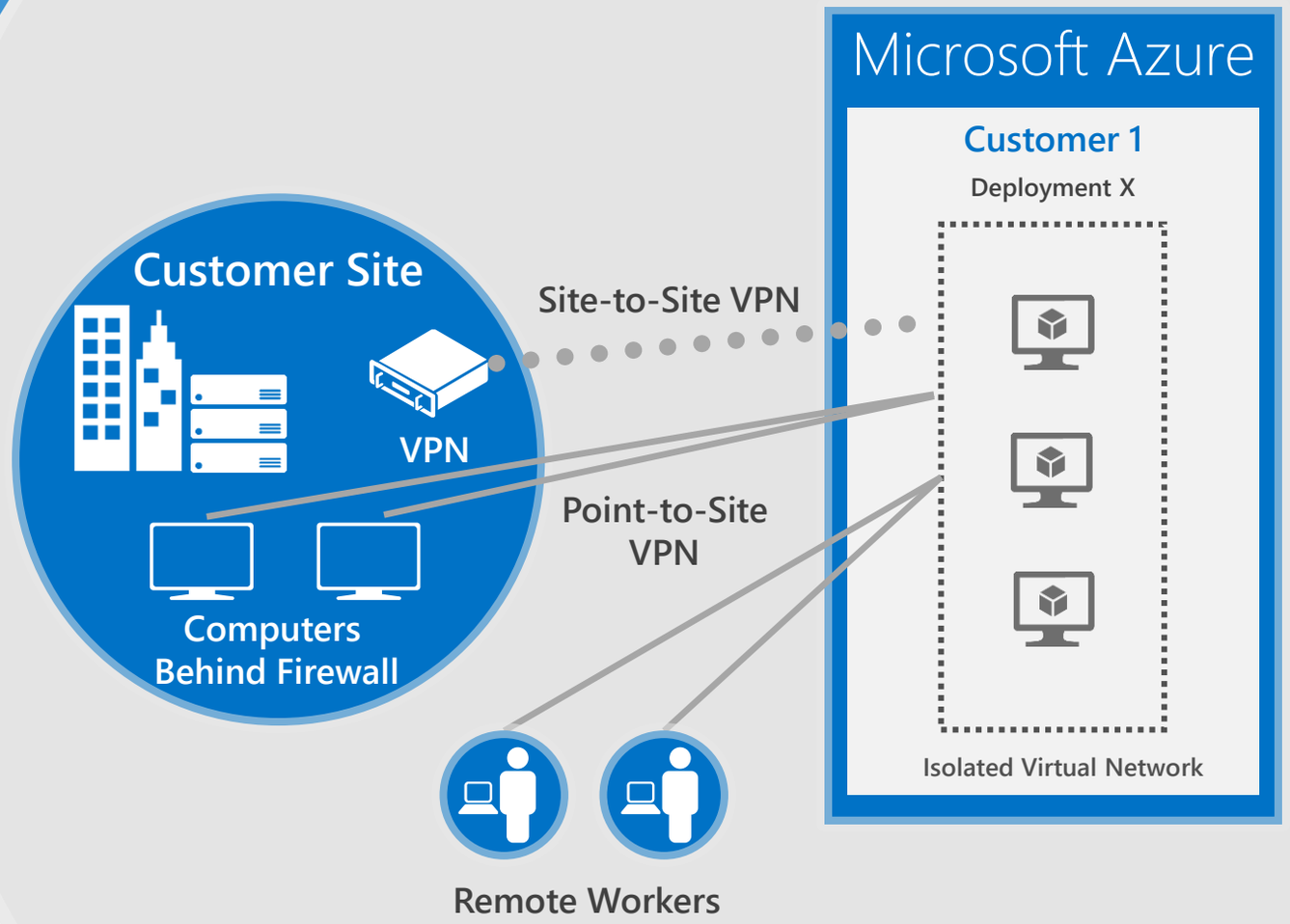
VPN connections

Azure

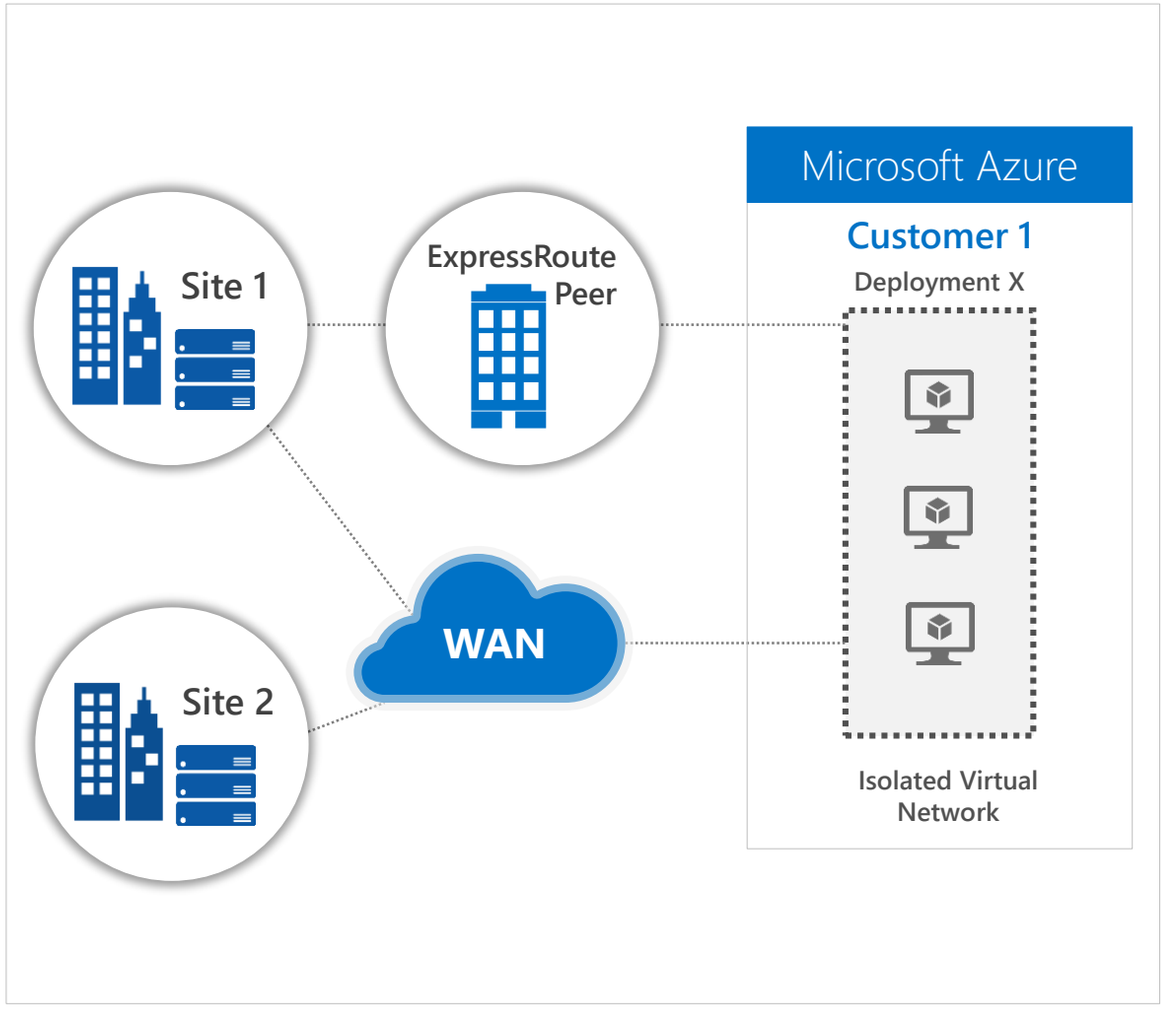
- Enables connection from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs
- Offers forced tunneling capabilities to enable customers to mandate all internet-bound traffic to go through the Site-to-Site tunnel

Customer

- Configures the VPN client in Windows
- Manages certificates, policies, and user access



ExpressRoute connections



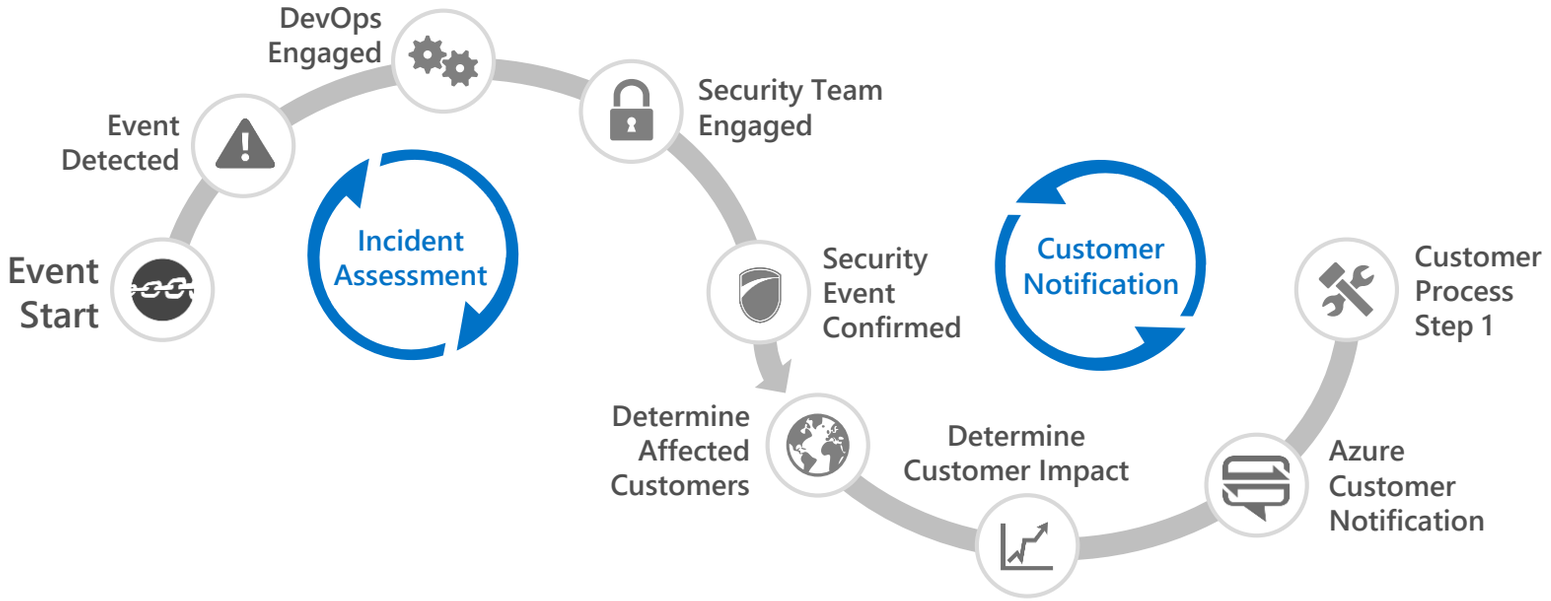
AZURE

- Offers private fiber connections via ExpressRoute
- Enables access to Compute, Storage, and other Azure services

CUSTOMER

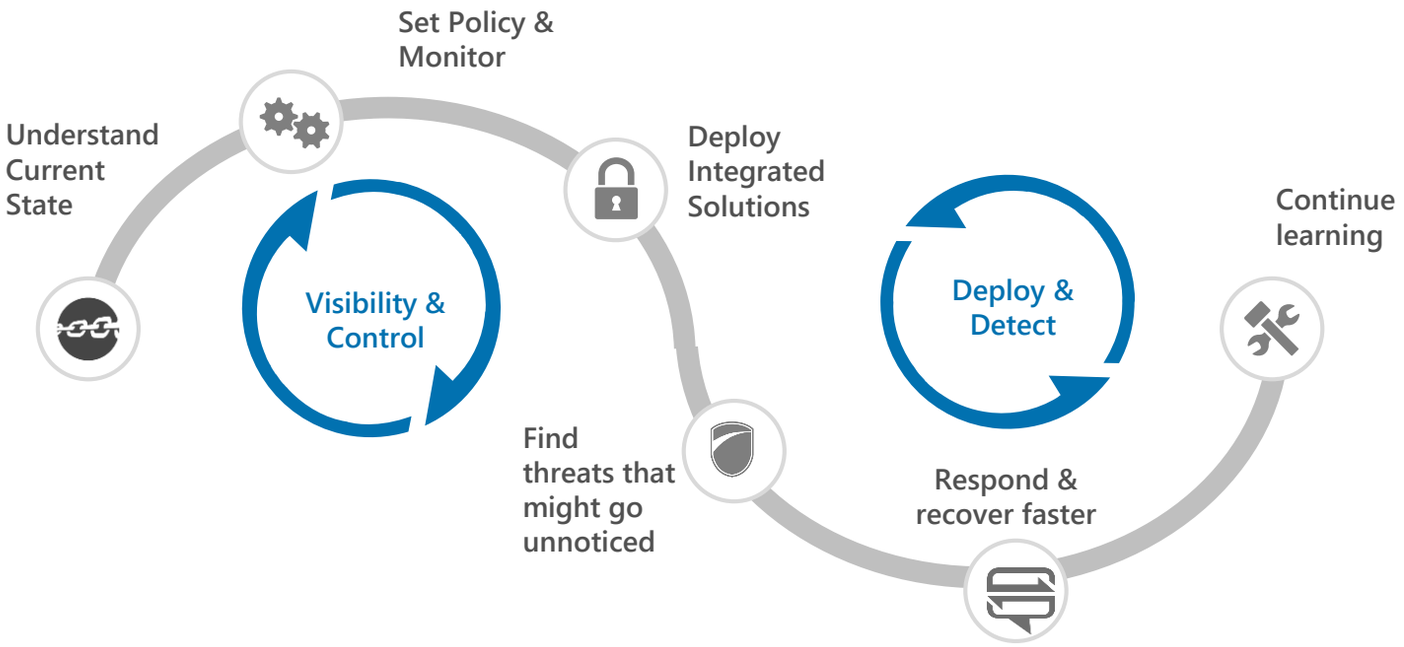
- Can establish connections to Azure at an ExpressRoute location (Exchange Provider facility)
- Can directly connect to Azure from your existing WAN network (such as an MPLS VPN) provided by a network service provider
- Can now authorize other Azure accounts to use a common ExpressRoute circuit
- Manages certificates, policies, and user access

Azure incident response



- Leverages a 9-step incident response process
- Focuses on containment & recovery
- Analyzes logs and VHD images in the event of platform-level incident and provides forensics information to customers when needed
- Makes contractual commitments regarding customer notification

Azure Security Center



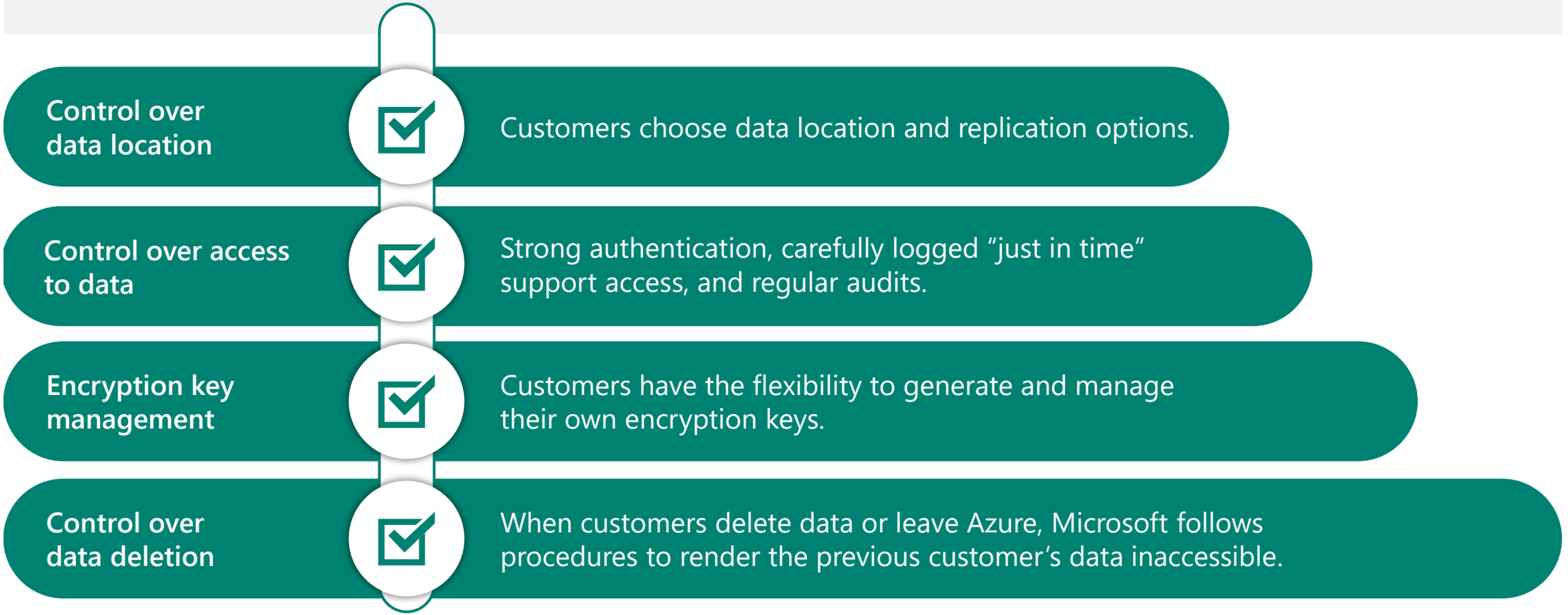
- ✓ Gain visibility and control
- ✓ Integrated security, monitoring, policy management
- ✓ Built in threat detections and alerts
- ✓ Works with broad ecosystem of security solutions

Check Point SOFTWARE TECHNOLOGIES LTD.
TREND MICRO
IMPERVA SECURESPHERE
CLOUDFLARE
Barracuda
f5
CISCO
IMPERVA INCAPSULA
FORTINET

Security Management | Encryption | Secure Networking | Partner Solutions

Customer data

When a customer utilizes Azure, they own their data.



Choice of Data Location & Replication

AZURE:

- ✓ Provides 3 copies of data in each datacenter
- ✓ Offers geo-replication in a datacenter 400+ miles away

CUSTOMER:

- ✓ Chooses where data resides
- ✓ Configures data replication options

Data protection

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

Data segregation

Logical isolation segregates each customer's data from that of others.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

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.

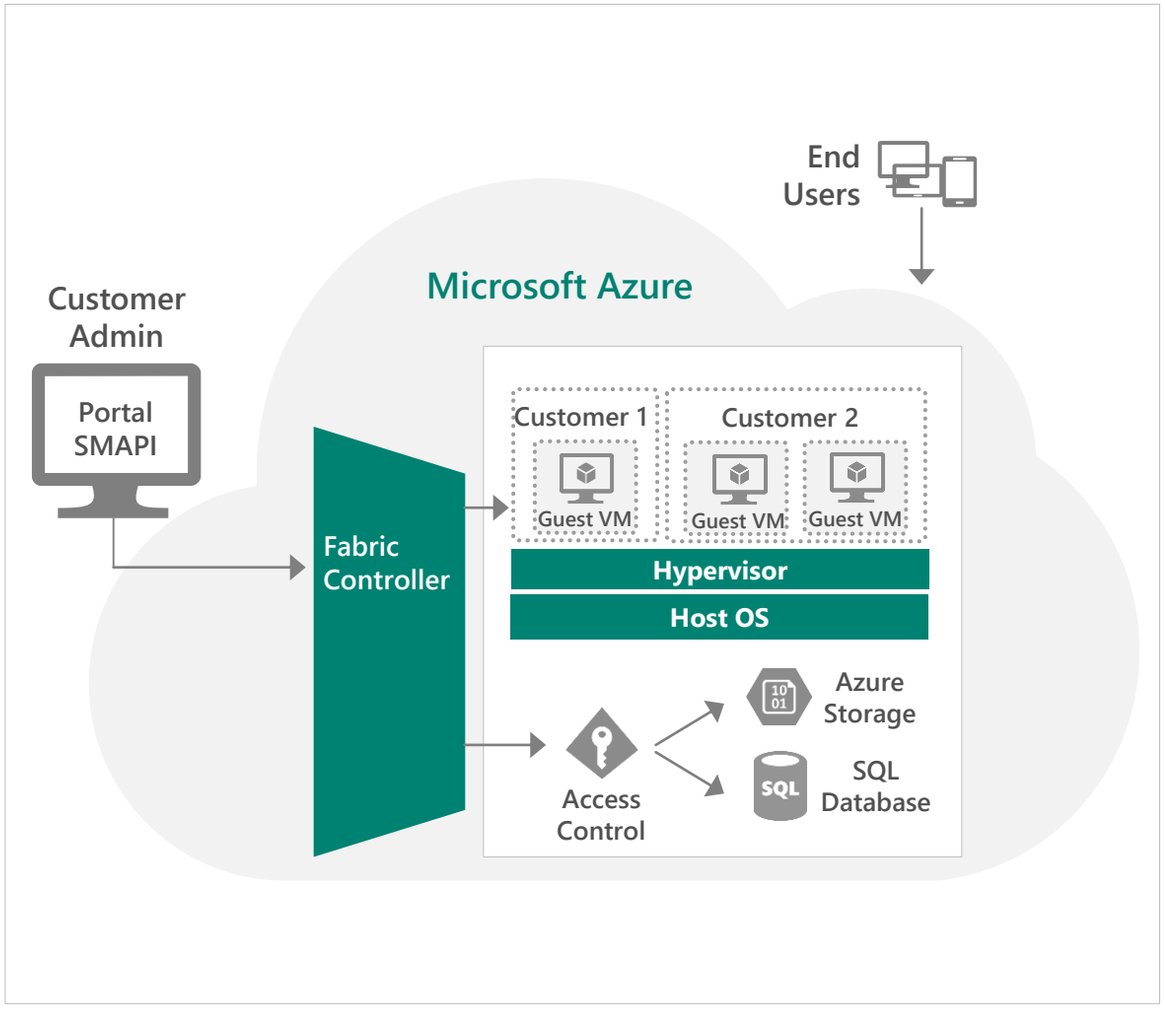
Data redundancy

Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

Data destruction

When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer's data inaccessible.

Data segregation



Storage Isolation

- Access is through Storage account keys and Shared Access Signature (SAS) keys
- Storage blocks are hashed by the hypervisor to separate accounts

SQL Isolation

- SQL Database isolates separate databases using SQL accounts

Network Isolation

- VM switch at the host level blocks inter-tenant communication

Encryption in transit

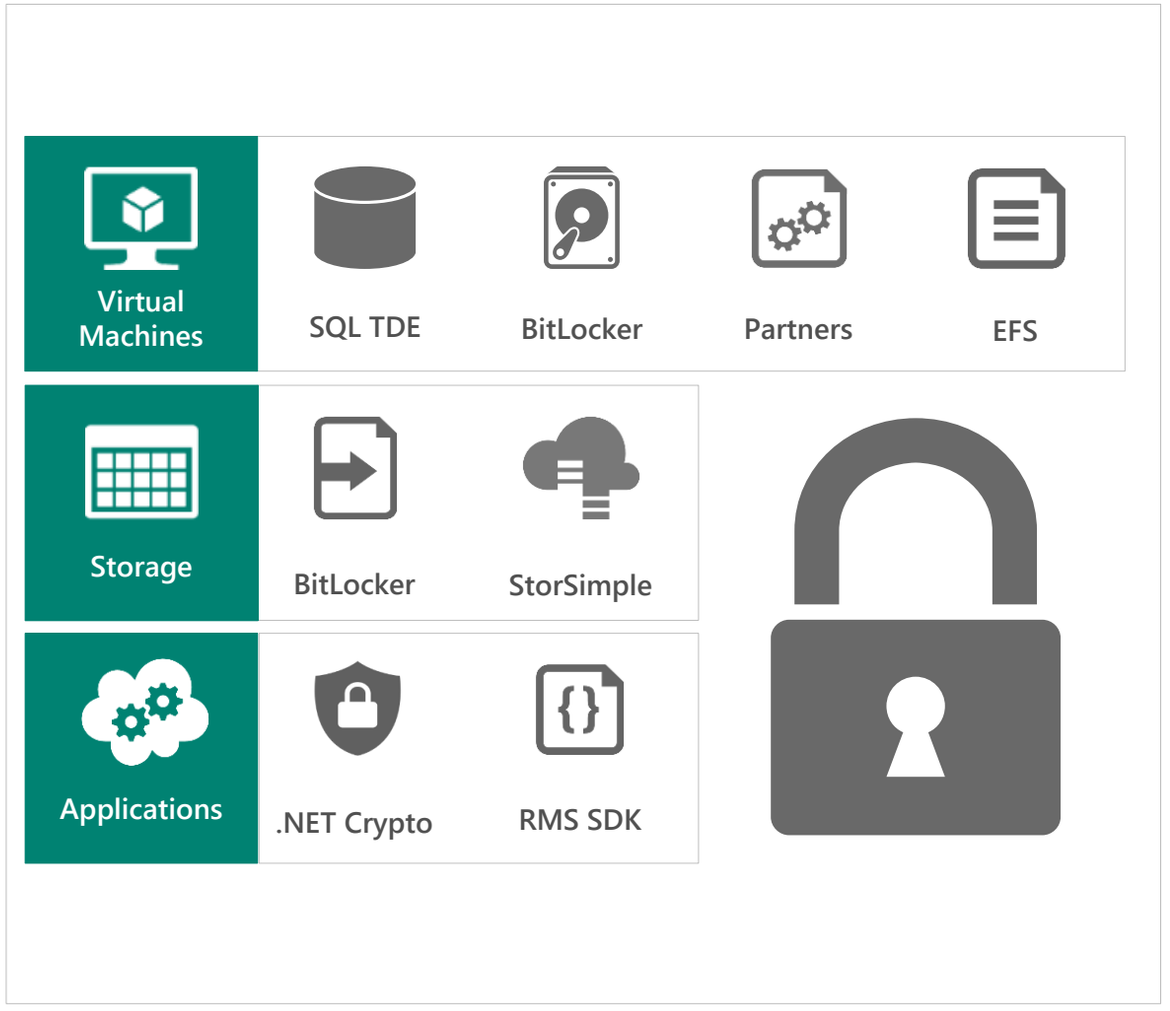
Azure

- Encrypts most communication between Azure datacenters
- Encrypts transactions through Azure Portal using HTTPS
- Supports FIPS 140-2

Customer

- Can choose HTTPS for REST API (recommended)
- Configures HTTPS endpoints for application running in Azure
- Encrypts traffic between Web client and server by implementing TLS on IIS

Encryption at rest



Virtual Machines

- Data drives – full disk encryption using BitLocker
- Boot drives – BitLocker and partner solutions
- SQL Server – Transparent Data and Column Level Encryption
- Files & folders – EFS in Windows Server

Storage

- BitLocker encryption of drives using Azure Import/Export service
- StorSimple with AES-256 encryption
- Server-side encryption of Blob Storage using AES-256
- Client-side encryption w/.NET and Java support

Applications

- Client Side encryption through .NET Crypto API
- RMS Service and SDK for file encryption by your applications

Data encryption

Customers want to encrypt data in the cloud and manage the keys by themselves

Layer	Encryption support	Key Management	Comments
Application	• .NET encryption API	Managed by customer	.NET Cryptography documentation
	• RMS SDK – encrypt data by using RMS SDK	Managed by customer via on-prem RMS key management service or RMS online	RMS SDK documentation
Platform	• SQL TDE/CLE on SQL server on Azure IAAS servers	Managed by customers	SQL TDE/CLE documentation
	• SQL Azure TDE and Column Encryption features in progress	Managed by customers	
	• StorSimple – provides primary, backup, archival	Managed by customers	Supports AES-256 to encrypt data in StorSimple StorSimple link and documentation
System	• BitLocker support for data volumes • Partner solutions for system volume encryption • BitLocker support	Managed by customers	BitLocker for fixed or removable volumes BitLocker commandline tool
Others	• Import/Export of xstore data onto drives can be protected by BitLocker	Managed by customers	Import/export step by step blog

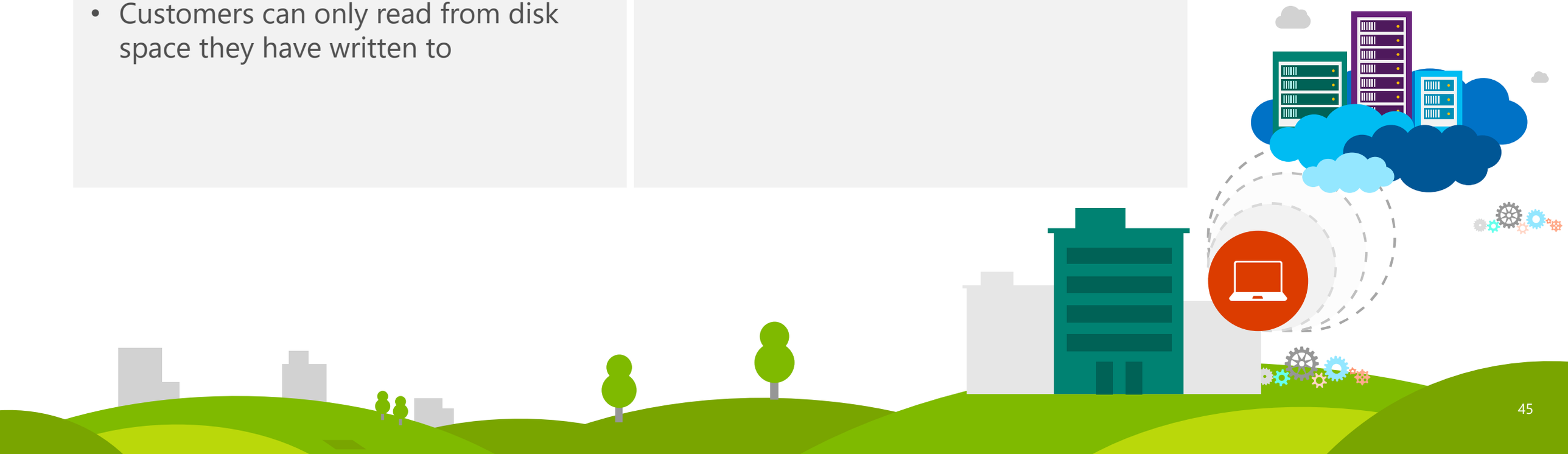
Data destruction

Data Deletion

- Index immediately removed from primary location
- Geo-replicated copy of the data (index) removed asynchronously
- Customers can only read from disk space they have written to

Disk Handling

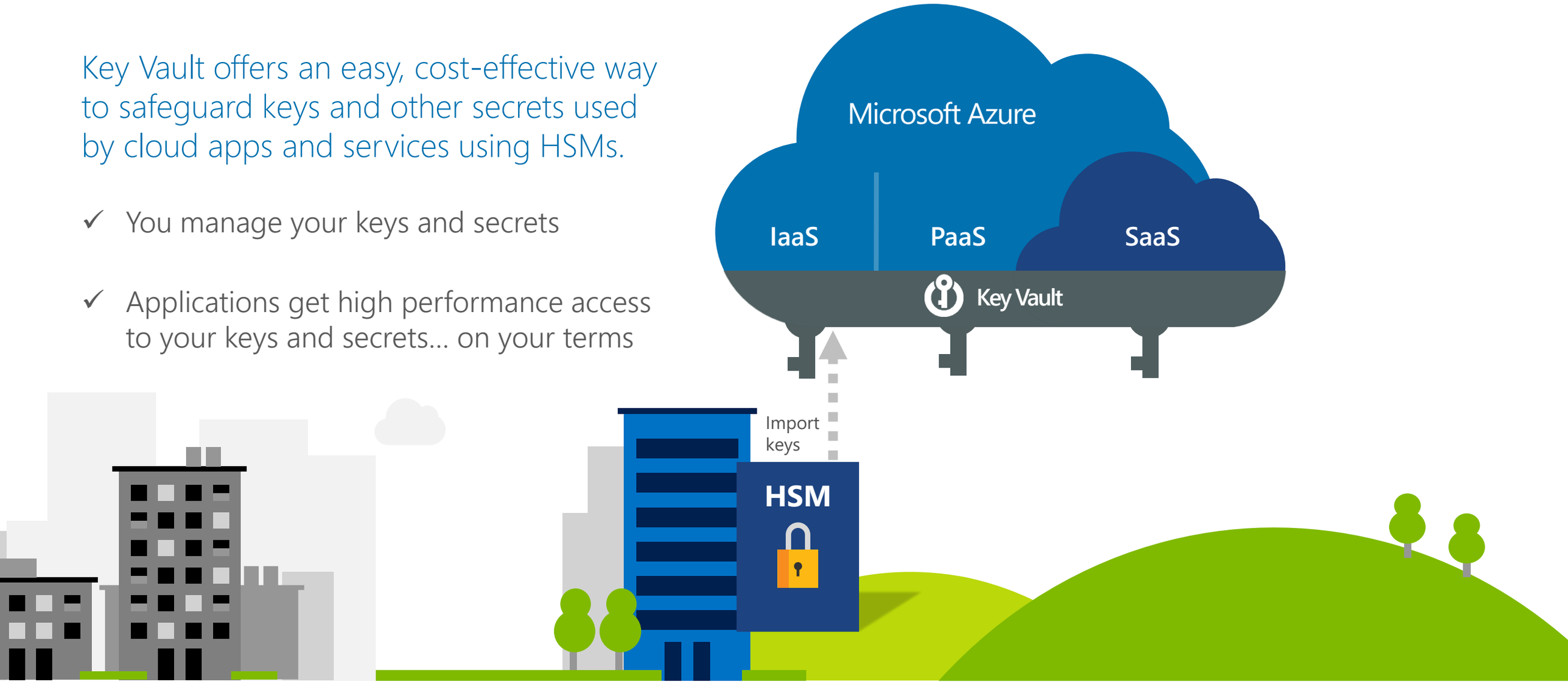
- NIST 800-88 compliant processes are used for destruction of defective disks



Microsoft Azure Key Vault

Key Vault offers an easy, cost-effective way to safeguard keys and other secrets used by cloud apps and services using HSMs.

- ✓ You manage your keys and secrets
- ✓ Applications get high performance access to your keys and secrets… on your terms

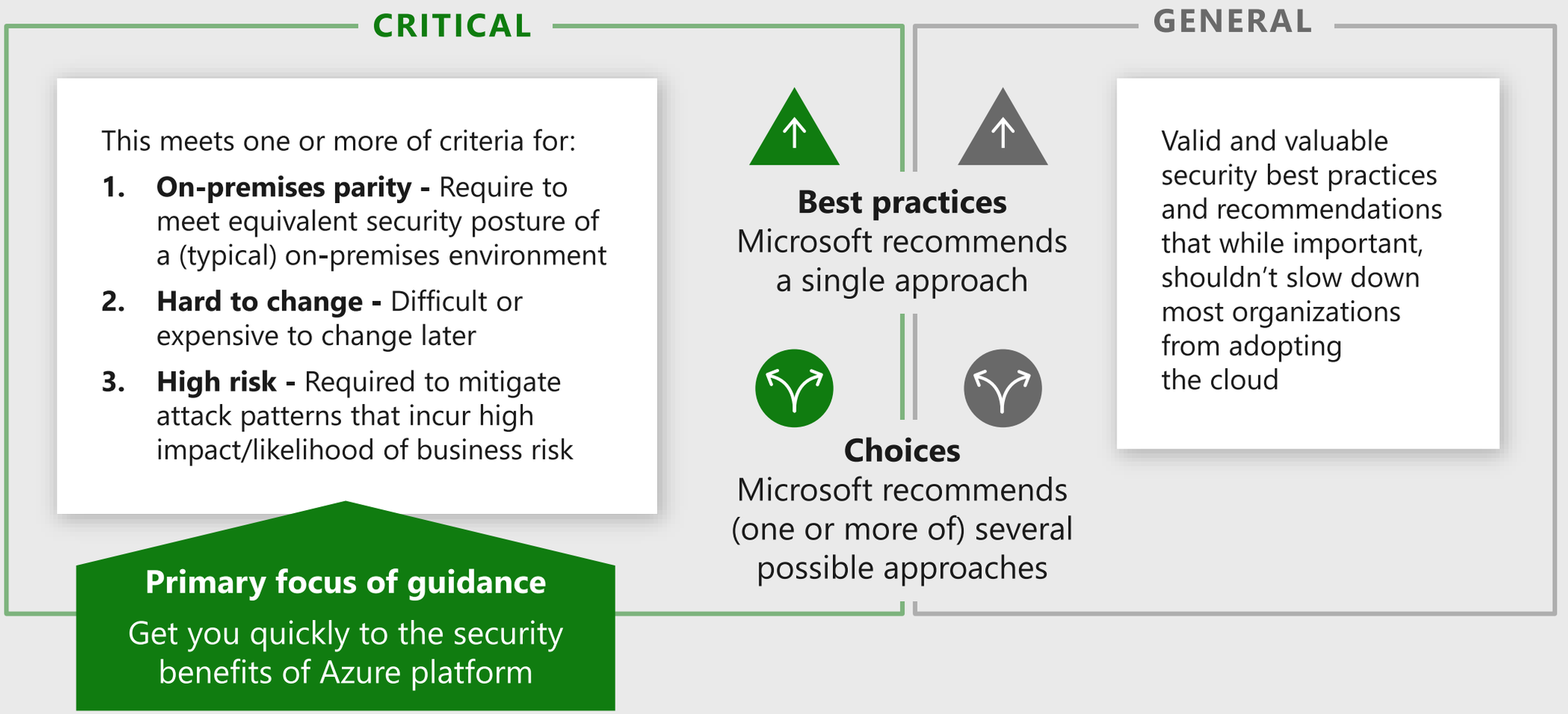


Compliance framework

Compliance certifications	Continual evaluation, benchmarking, adoption, test & audit	Independent verification	Access to audit reports	Best practices
Microsoft maintains a team of experts focused on ensuring that Azure meets its own compliance obligations, which helps customers meet their own compliance requirements.	Compliance strategy helps customers address business objectives and industry standards & regulations, including ongoing evaluation and adoption of emerging standards and practices.	Ongoing verification by third-party audit firms.	Microsoft shares audit report findings and compliance packages with customers.	Prescriptive guidance on securing data, apps, and infrastructure in Azure makes it easier for customers to achieve compliance.

Guidance Structure

Actionable and Prioritized



Note: *These represent Microsoft's default opinion based on our experience and knowledge. Your organization may prioritize risk and mitigations differently based on your unique business needs, business risks, or other factors.*

Executive Summary

OVERALL CRITICAL GUIDANCE

	Best Practices	Choices
Governance, Risk, and Compliance	13	4
Administration	8	4
Network Security & Containment	6	6
Storage, Data, & Encryption	3	0
Identity & Access Management	4	1
Security Operations	4	0
Total	**38**	**15**

TRACKING SPREADSHEET

Azure Security Compass
Status Summary

Critical Decisions/Implementation	74% / 73%
General Decisions/Implementation	82% / 45%

Critical Decisions	Decisions	Implementation
Governance, Risk, & Compliance	74%	68%
Administration	31%	92%
Network Security & Containment	84%	72%
Storage, Data, & Encryption	75%	37%
Identity & Access Management	100%	100%
Security Operations	81%	67%
Summary	**74%**	**73%**

General (non-critical) Decisions	Decisions	Implementation
Governance, Risk, & Compliance	50%	25%
Administration	100%	50%
Network Security & Containment	100%	67%
Storage, Data, & Encryption	100%	100%
Identity & Access Management	63%	25%

Security partners

In addition to the robust security capabilities built into Azure, the Azure Marketplace offers a rich array of additional security products built by our partners for Azure.

Antimalware

Virtual machines
- Kaspersky
- Trend Micro

Active Directory integrations
- Symantec
- McAfee

Networking security

- Alert Logic
- aiScaler
- Barracuda
- Check Point
- Riverbed
- Cohesive Networks

Encryption

- CloudLink
- Townsend Security

Monitoring and alerts

- Alert Logic
- Derdack
- Nagios

Messaging Security

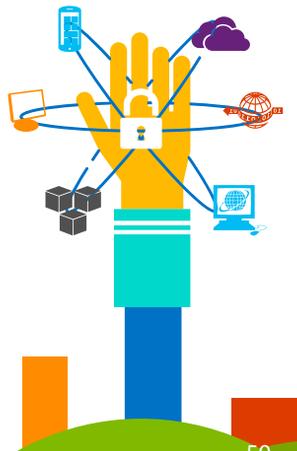
- Kaspersky
- Barracuda
- Trend Micro

Application Security

- Waratek

Authentication

- Login People




Microsoft