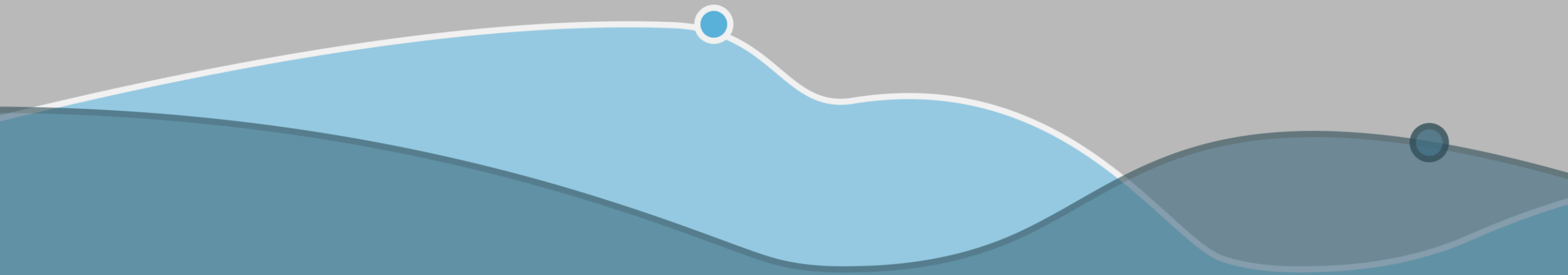
Microsoft

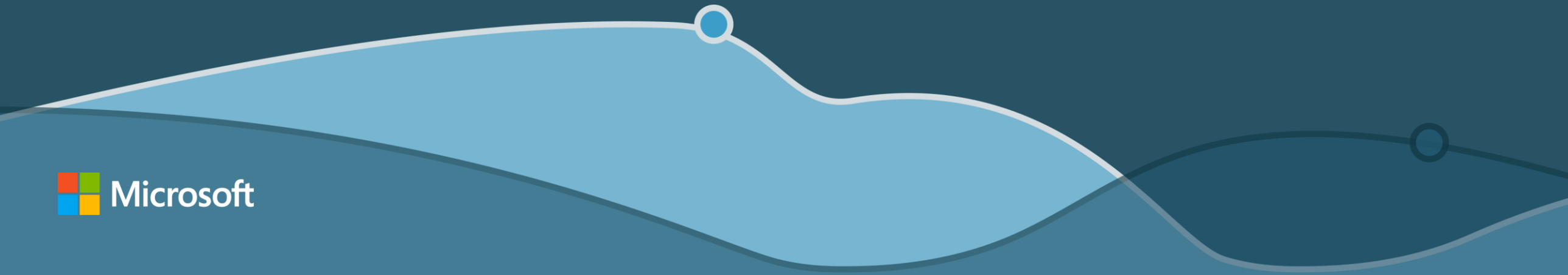
# Cortana Analytics Workshop

## Sept 10 – 11, 2015 • MSCC



# Cortana Analytics
# Security, Privacy & Compliance

Eric Golpe
Senior Program Manager, AzureCAT



Microsoft

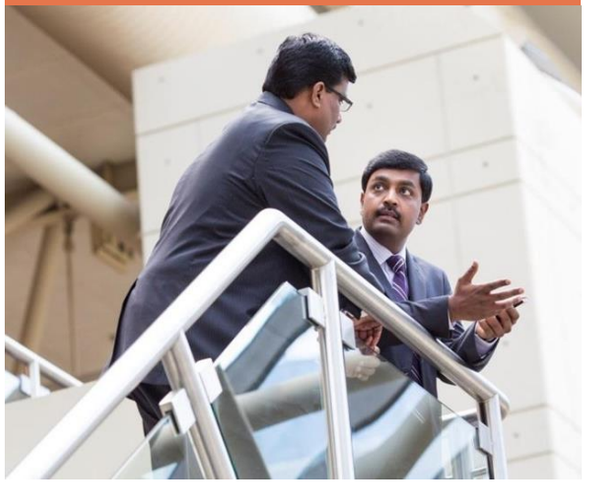
# Microsoft Cloud principles

## Security

## Privacy and Control

## Transparency

## Compliance



# Security with Cortana Analytics

## Microsoft delivers enterprise cloud services customers can trust

- Industry-leading best practices in the design and management of online services
- Enhanced security, operational management, and threat mitigation practices
- Trustworthy enterprise cloud services
- Centers of excellence

# Cloud services – shared responsibility

| On-Premises | Infrastructure (as a Service) | Platform (as a Service) | Software (as a Service) |
|---|---|---|---|
| Applications | Applications | Applications | Applications |
| Data | Data | Data | Data |
| Runtime | Runtime | Runtime | Runtime |
| Middleware | Middleware | Middleware | Middleware |
| O/S | O/S | O/S | O/S |
| Virtualization | Virtualization | Virtualization | Virtualization |
| Servers | Servers | Servers | Servers |
| Storage | Storage | Storage | Storage |
| Networking | Networking | Networking | Networking |

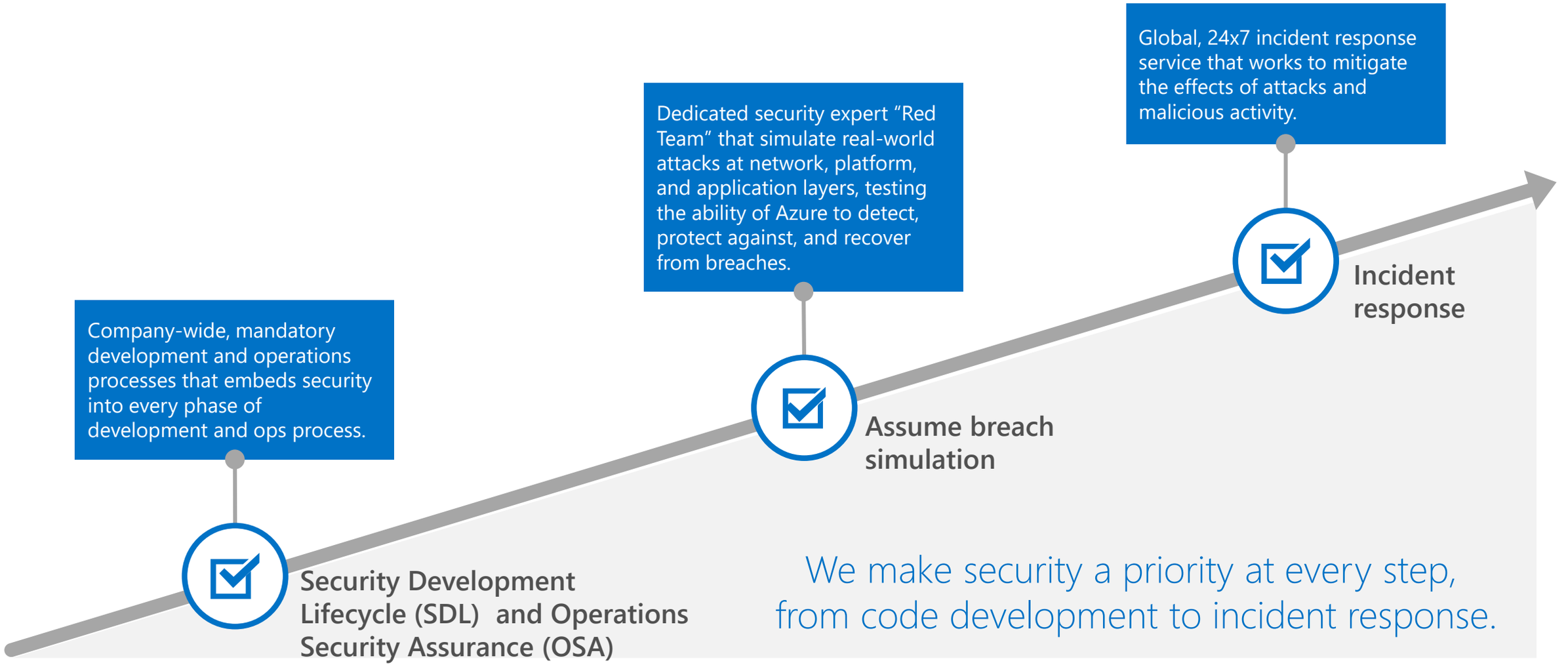
Microsoft Azure

Each customer environment is isolated on top of Azure's Infrastructure

Shared Physical Environment

Managed by:
**customer**
**Vendor**

# Azure Security Design and Operations




We make security a priority at every step, from code development to incident response.

# Prevent and assume breach

## Prevent and assume breach

**Security monitoring and response**

**Prevent breach**

- Secure Development Lifecycle
- Operational Security

**Assume breach**

- Bug Bounty Program
- War game exercises
- Live site penetration testing

**Threat intelligence**

**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

# Infrastructure protection

Azure infrastructure includes hardware, software, networks, administrative and operations staff, policies and procedures, and the physical datacenters that house it all

24-hour monitored
**PHYSICAL SECURITY**

Centralized
**MONITORING AND ALERTS**

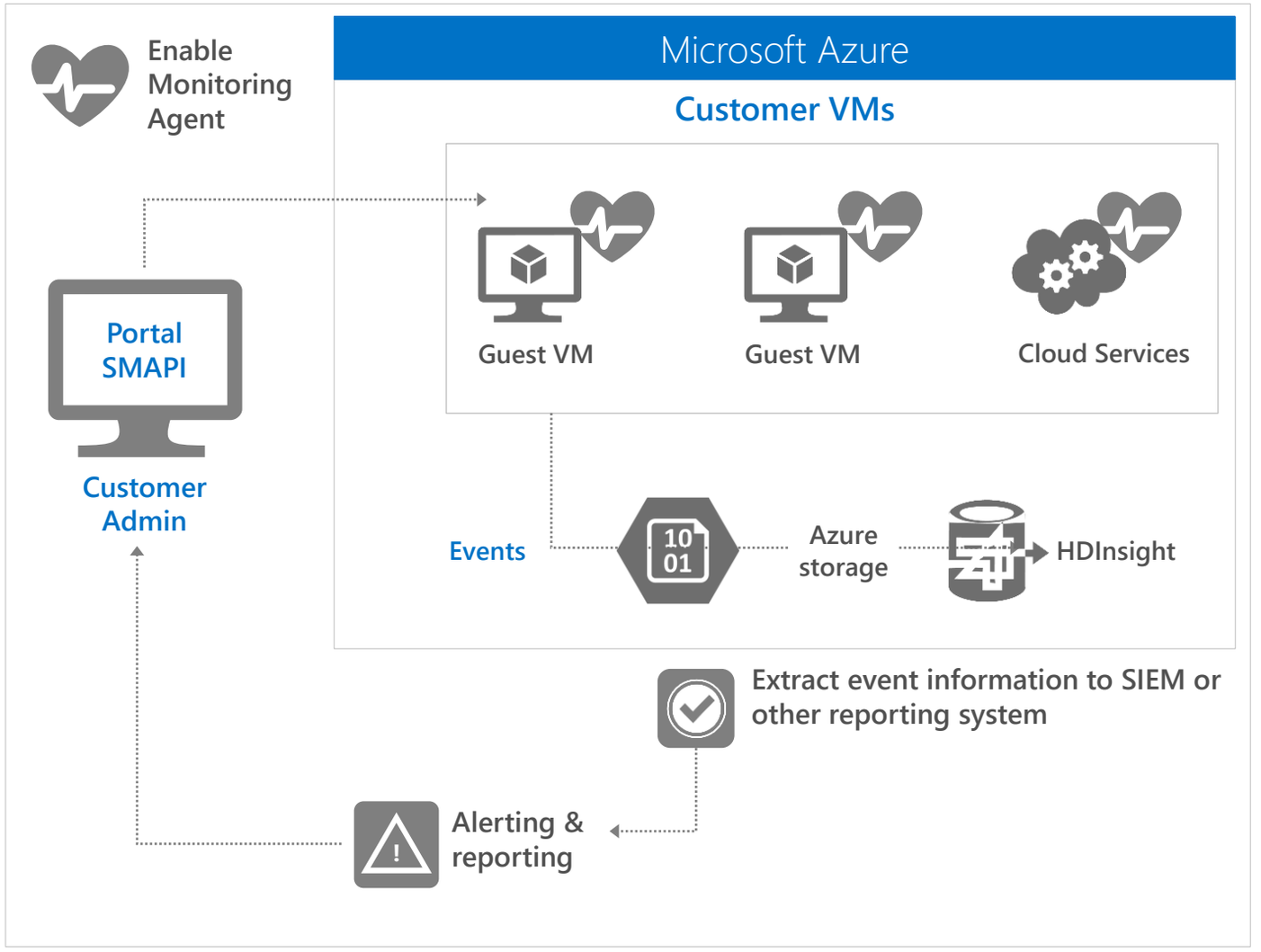
Update
**MANAGEMENT**

Antivirus/Antimalware
**PROTECTION**

Red Teaming
**PENETRATION TESTING**

**FIREWALLS**

# 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

# Update management

## Azure

- Applies regularly scheduled updates to the platform
- Releases critical patches immediately
- Rigorously reviews & tests all changes
- Uses a combination of third-party scanning tools for Azure environment
- Utilizes integrated deployment systems to manage the distribution and installation of security updates

## Customer

- Applies similar patch management strategies for their Virtual Machines

### MONTHLY MSRC PATCH REVIEW

- Monitor 100,000+ vulnerability reports
- Sourced from customers & worldwide network of security researchers

### PATCHING ROLLOUT

- Prioritize critical updates
- Monthly OS releases with patches

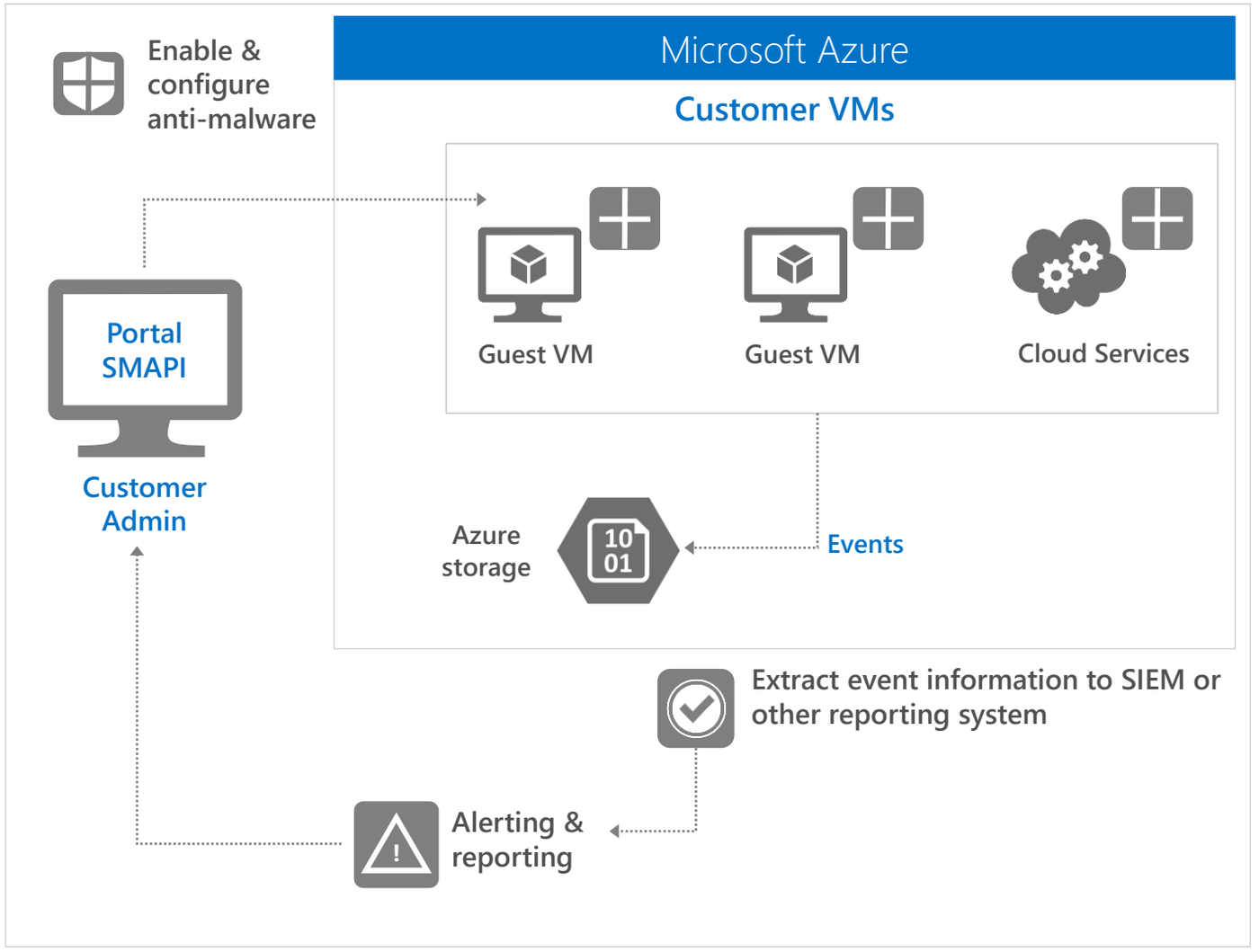
### SCANNING

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

### AUDIT VALIDATION

- Reconciliation report
- Resolution summary

# Antivirus/antimalware protection




## AZURE

- Performs monitoring & alerting of antimalware events for the platform
- Enables real time protection, on-demand scanning, and monitoring via Microsoft Antimalware for Cloud Services and Virtual Machines

## CUSTOMER

- Configures Microsoft Antimalware or an AV/AM solution from a partner
- Extracts events to SIEM
- Monitors alerts & reports
- Responds to alerts

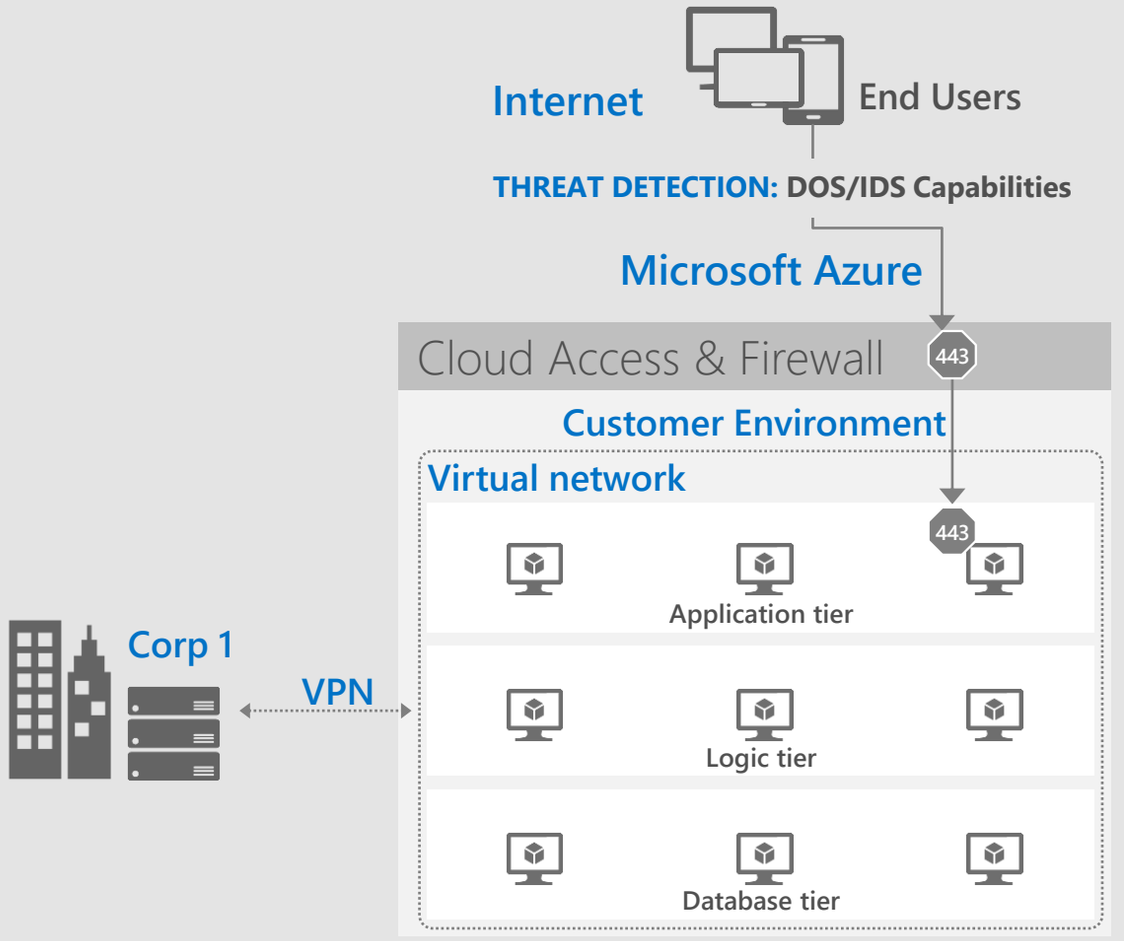
# Threat protection

## Azure

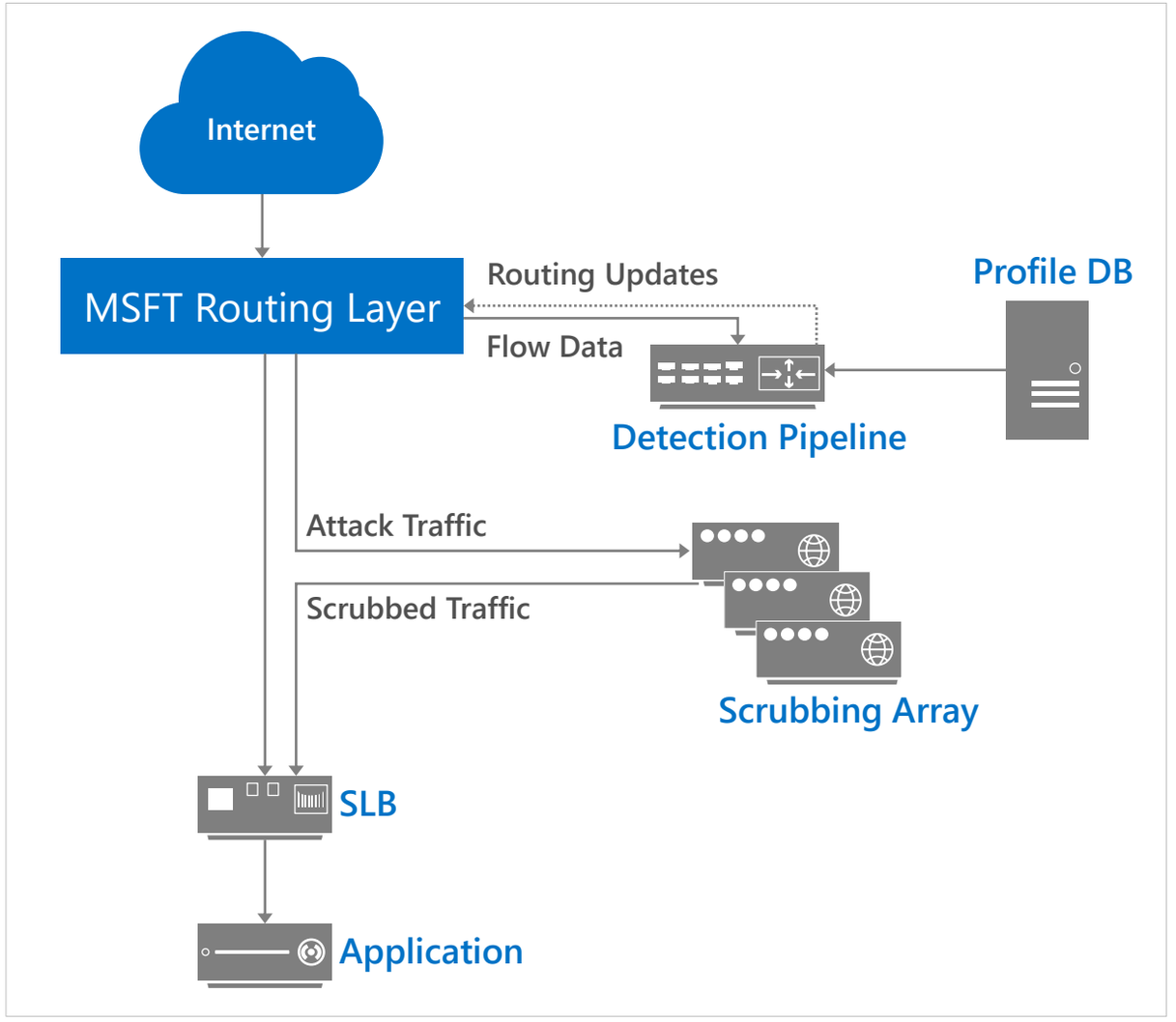
- Performs big data analysis of logs for intrusion detection & prevention for the platform
- Employs denial of service attack prevention measures for the platform
- Regularly performs penetration testing

## 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

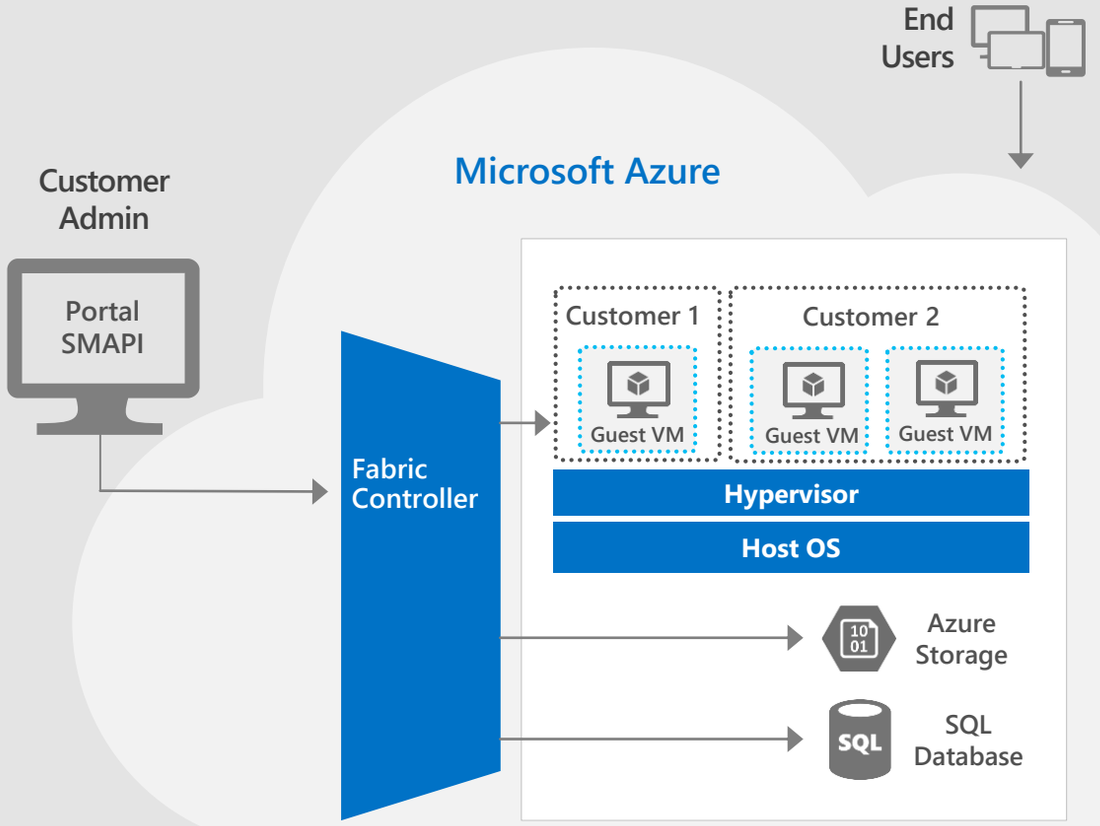
# Architected for more secure multi-tenancy

## Azure

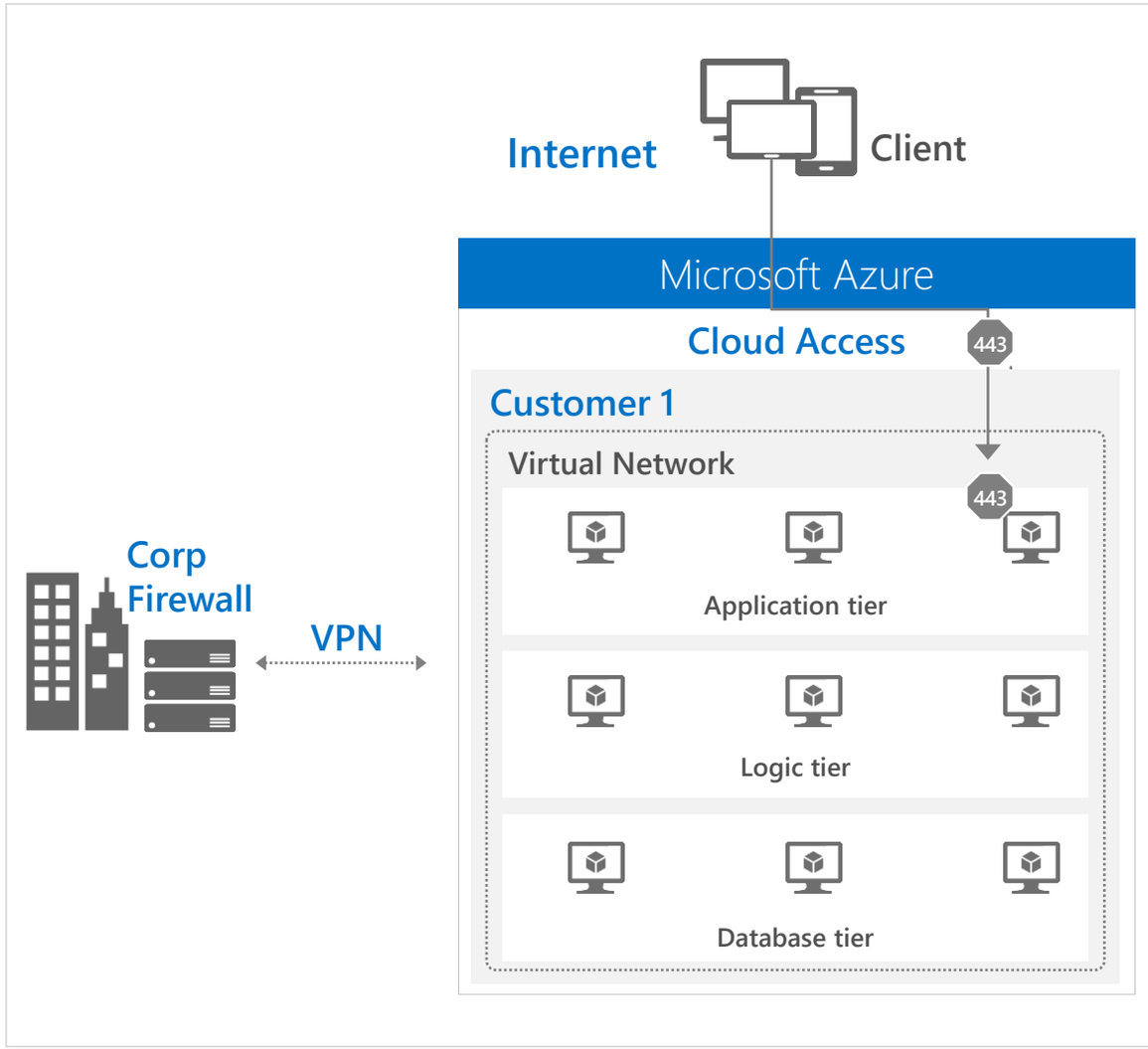
- Centrally manages the platform and helps isolate customer environments using the Fabric Controller
- Runs a configuration-hardened version of Windows Server as the Host OS
- Uses Hyper-V, a battle tested and enterprise proven hypervisor
- Runs Windows Server and Linux on Guest VMs for platform services

## Customer

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



# 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

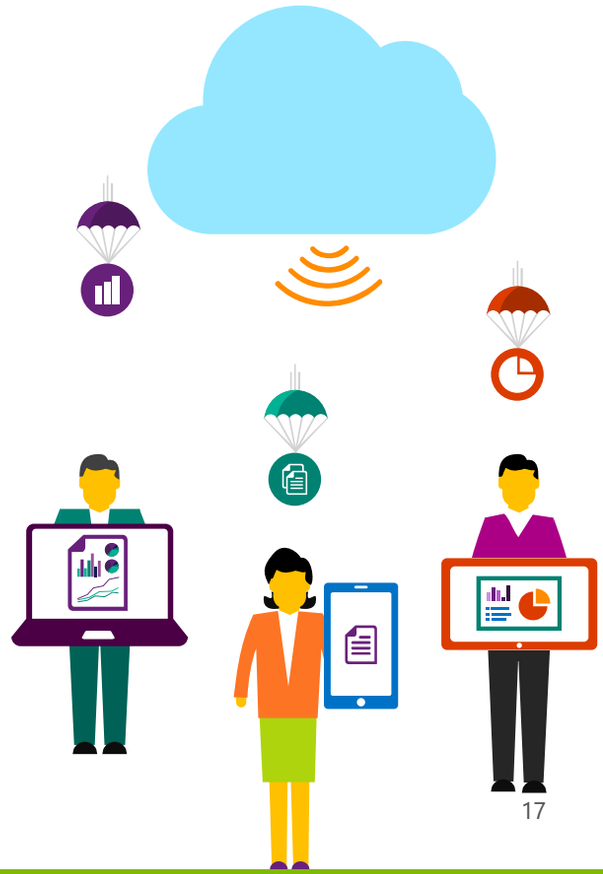
- Applies corporate firewall using site-to-site VPN
- Configures endpoints
- Defines access controls between tiers and provides additional protection via the OS firewall

# Identity & access

Azure enables customers to better control access in a multi-tenant environment

| Enterprise cloud directory | Multi-Factor Authentication (MFA) | Access monitoring and logging |
| --- | --- | --- |
| Azure Active Directory (AAD) offers enterprise identity and access management in the cloud. | Strong authentication adds an extra layer of security for user logins. | Security reports monitor access patterns that help identify potential threats. |

| Single sign-on | Integration with customer applications |
| --- | --- |
| Users get a single sign-on option across multiple applications and services. | Developers can integrate their app with Azure AD for single sign-on functionality for their users. |



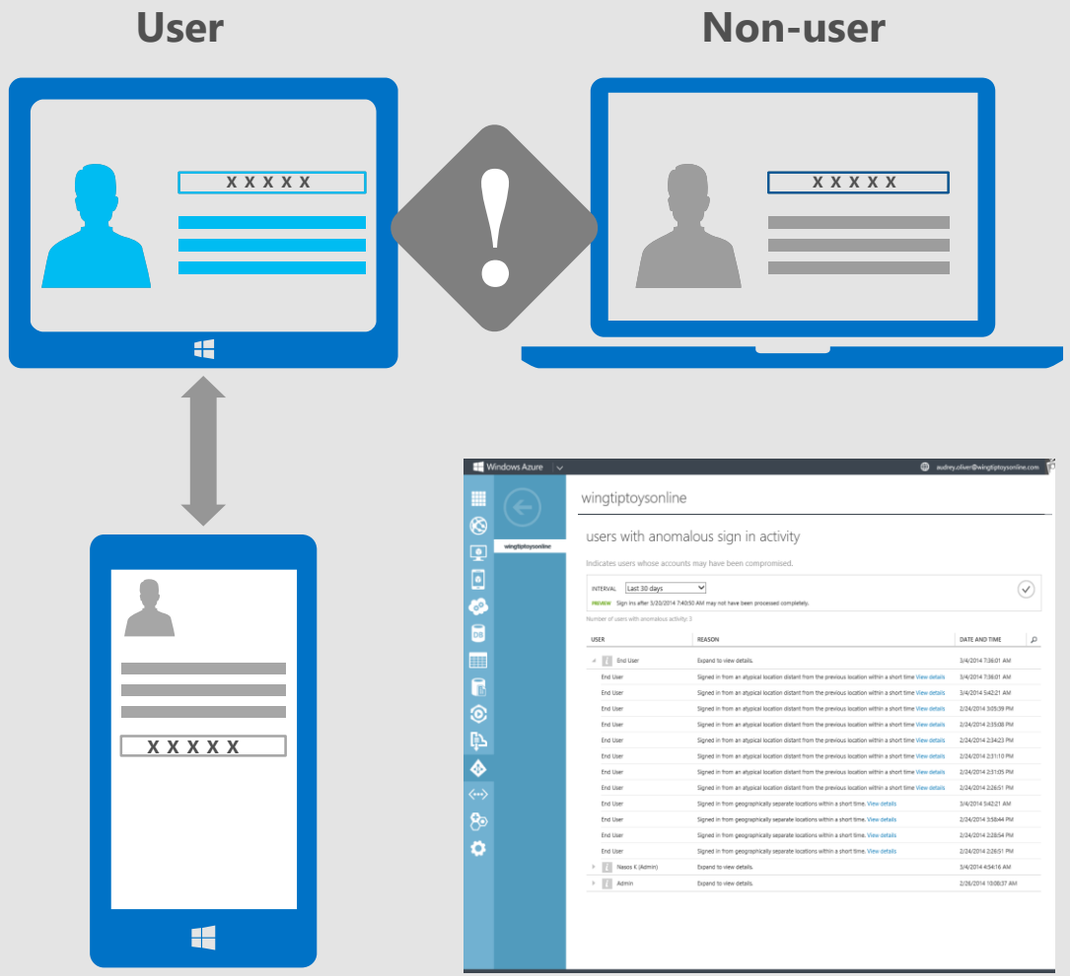
# Access monitoring and logging

## Azure

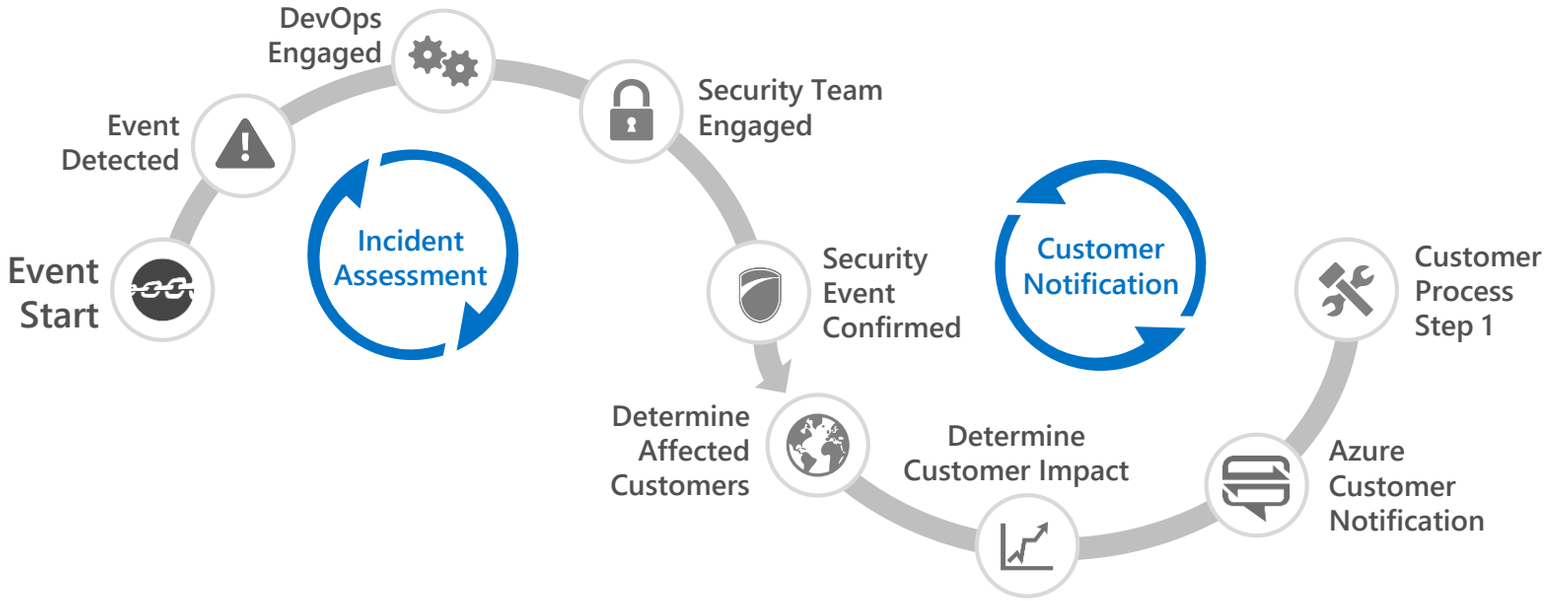
- Uses password hashes for synchronization
- Offers security reporting that tracks inconsistent traffic patterns, including:
  - Sign-ins from unknown sources
  - Multiple failed sign-ins
  - Sign-ins from multiple geographies in short timeframes
  - Sign-ins from suspicious IP addresses and suspicious devices

## Customer

- Reviews reports and mitigates potential threats
- Can enable Multi-Factor Authentication



# 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

# Privacy & Control

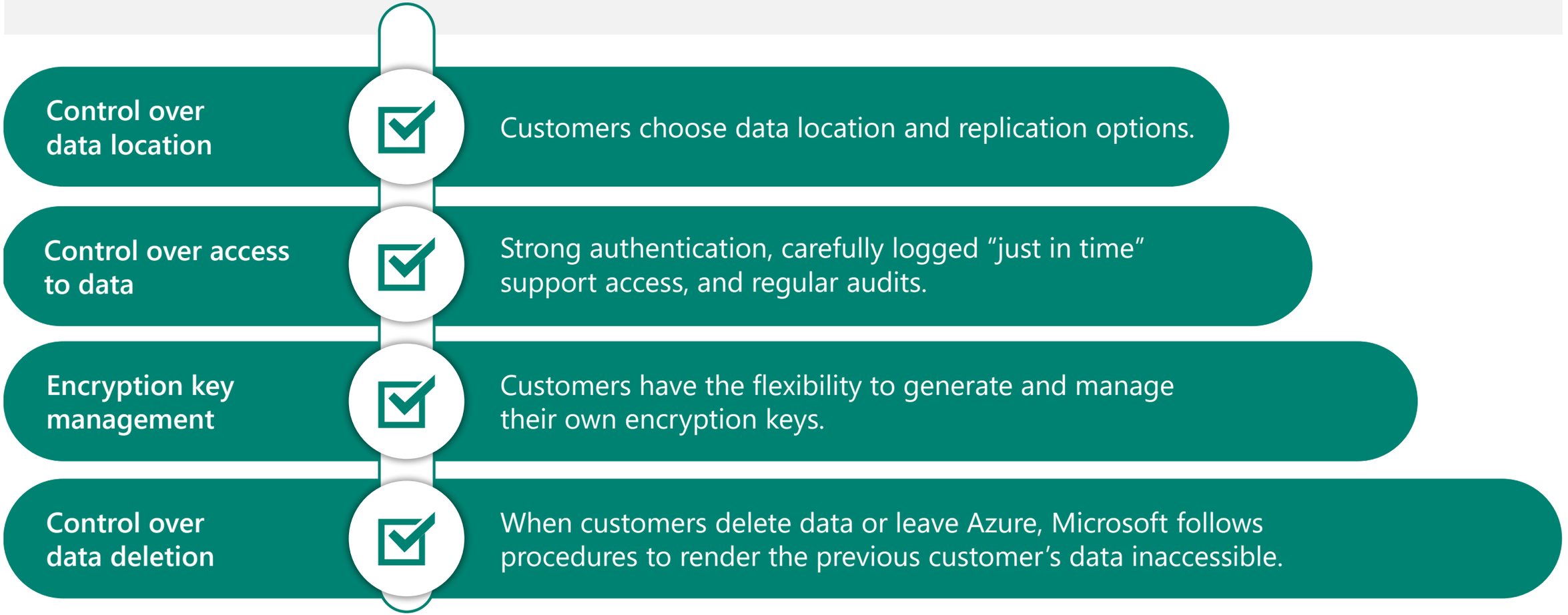
Microsoft makes our commitment to the privacy of our customers a priority with independently audited policies and practices that include restricting the mining of customer data for advertising or similar commercial purposes.

# Trustworthy foundation

| | |
|---|---|
| Privacy by design | Microsoft privacy principles are designed to facilitate the responsible use of customer data, be transparent about practices, and offer meaningful privacy choices. |
| Microsoft privacy standard | Guidelines that help ensure privacy is applied in the development and deployment of products and services. |
| Data segregation | Azure uses logical isolation to segregate each customer's data from that of others. |

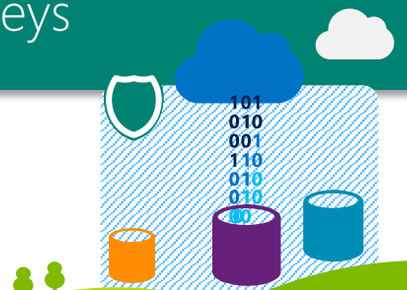
# Customer data

When a customer utilizes Cortana Analytics, they own their data.



# Data control

| | |
|---|---|
| Data location | For many services, customers can specify the geographic areas where their customer data is stored |
| Data access | Access to customer data by Microsoft personnel is restricted; Microsoft provides cloud-service-specific privacy statements and strong contractual commitments to safeguard customer data |
| Data protection | Technical safeguards help keep customer data secure; Customers have the flexibility to implement additional encryption and manage their own keys |



# Data location and replication

*Microsoft Azure datacenters*

## AZURE

- Microsoft will not store customer data outside the customer-specified geography except for global services and certain regional services
- Azure replicates data both locally and to different physical locations
- Every blob is replicated across three computers in a Microsoft Azure datacenter
- Geo-replicated storage in a datacenter hundreds of miles away
- Microsoft may transfer customer data within a geo (e.g., within Europe) for data redundancy or other purposes

## CUSTOMER

- Chooses where data resides
- Configures data replication options

# Data access

## Restricted data access

Customer data is only accessed when necessary to support customer's use of Azure, or when required by law

## Role-based access control

Customer data is only used to provide the service, including purposes compatible with providing those service and is never used for advertising

## Microsoft employee access management

Microsoft controls employee access to Azure customer environment

# Restricted data access

- Customer data is only accessed when necessary to support customer's use of Azure (e.g. troubleshooting or feature improvement), or when required by law.
- When granted, access is controlled and logged.
- Strong authentication, including MFA, helps limit access to authorized personnel only.
- Access is revoked as soon as it's no longer needed.

Access controls are verified by independent audit and certifications

# 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.

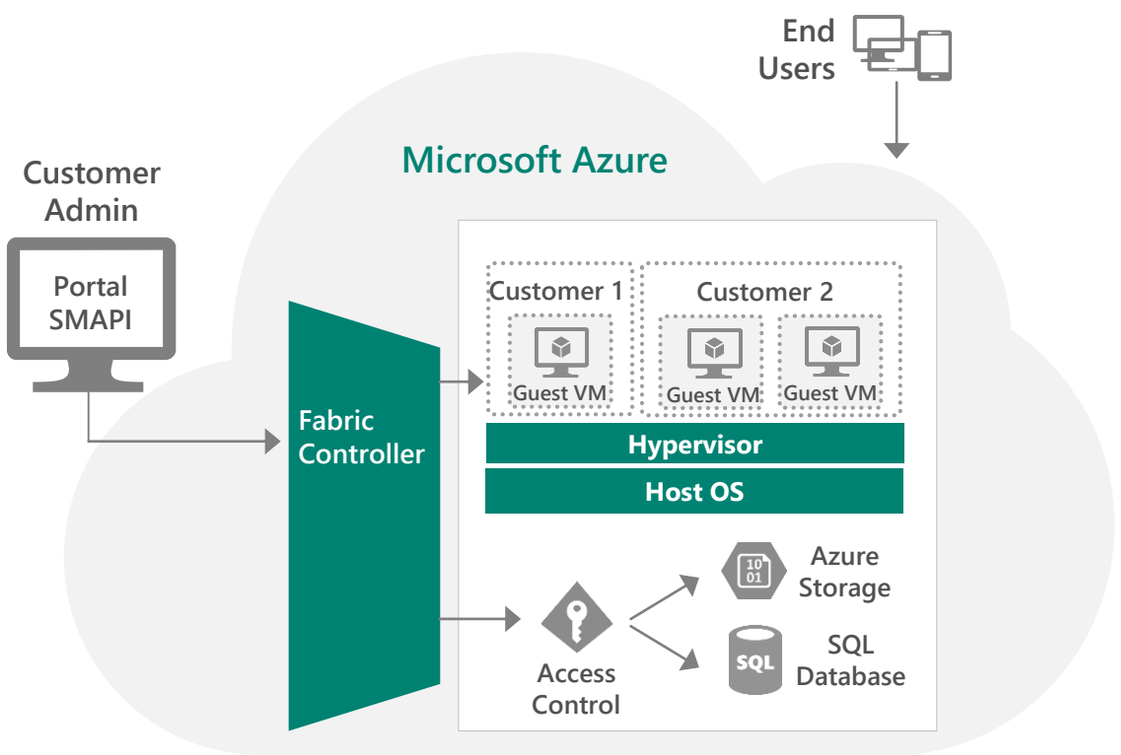
## Data redundancy

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

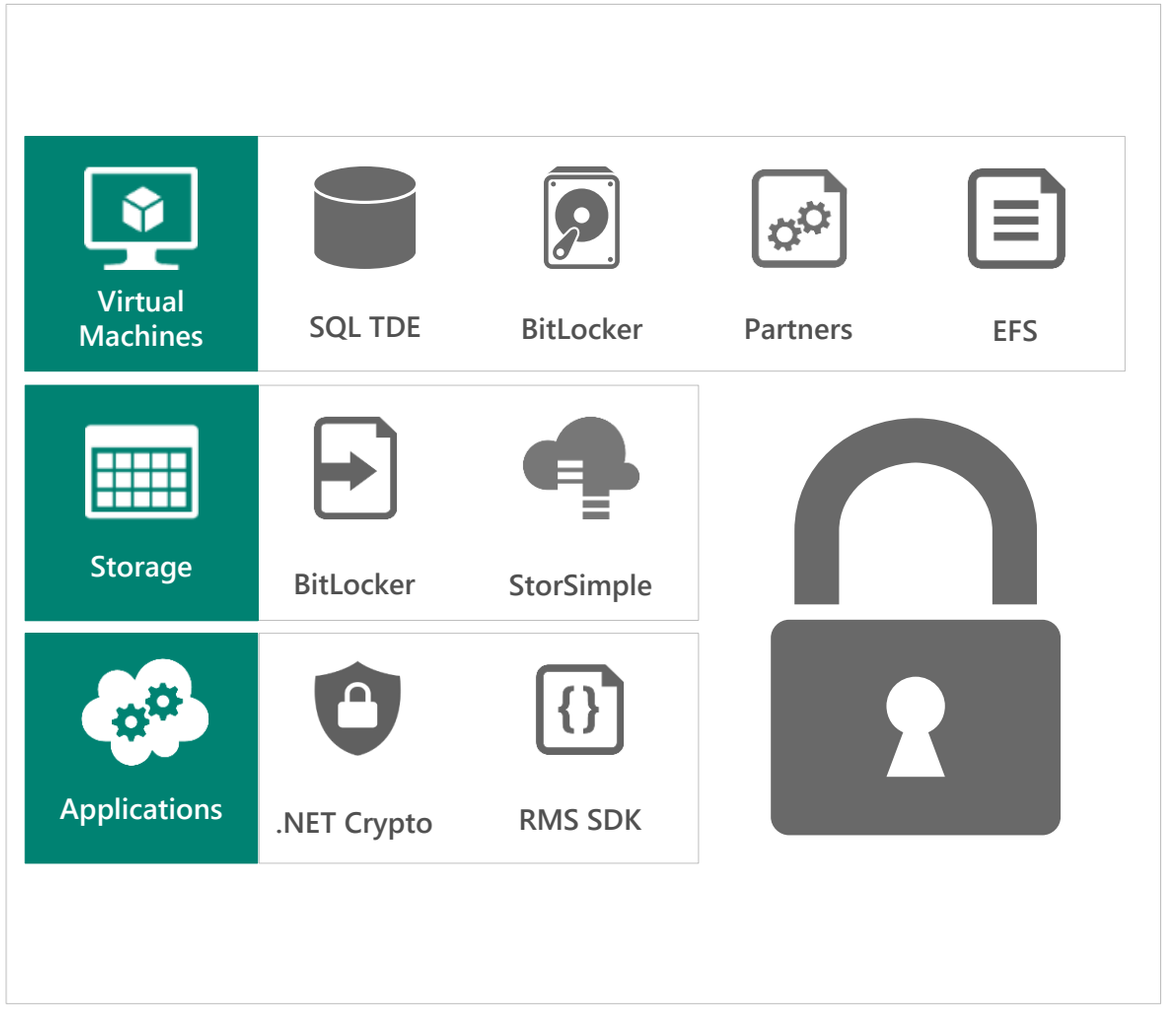
## Azure

- 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

## Applications

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

# Azure Key Vault Service

## What is the feature?

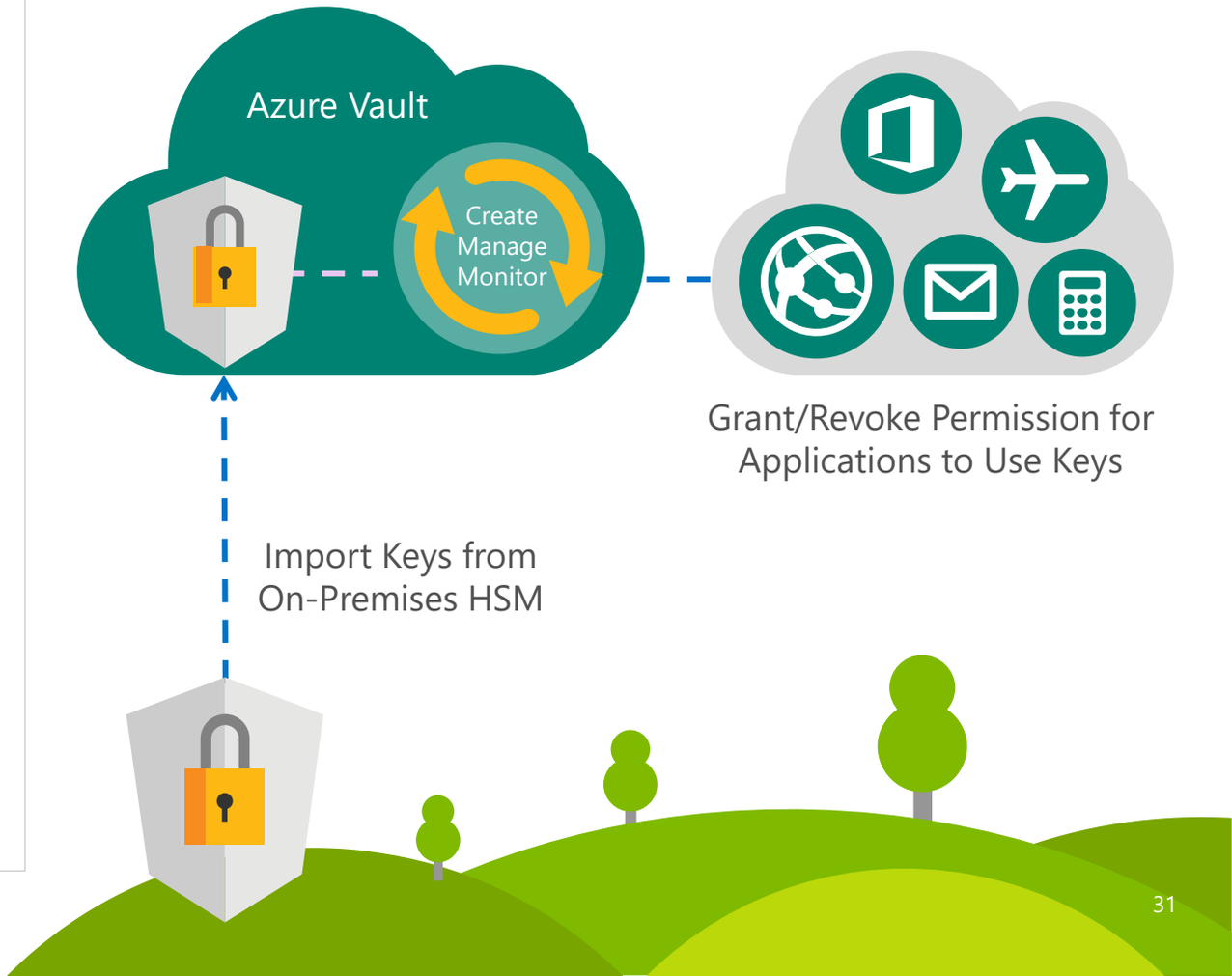
Microsoft Azure Key Vault offers encryption key management in the cloud, enabling customers to safeguard keys for use in applications they develop as well as SaaS applications that encrypt data on their behalf. In Azure, customers can:

- Create/import, store, and manage cryptographic keys
- Secure those keys in FIPS 140-2 Level 2 Hardware Security Modules (HSMs)

Benefits:

- Scale to meet the encryption needs of cloud applications
- Improve performance of cloud applications by storing keys in the cloud
- Reduce the time and cost required to maintain dedicated HSM hardware
- Maintain control over keys - grant and revoke use by applications as needed
- Gain visibility into key use through Azure logging

Customer keys stay locked in very tightly monitored HSMs. Rogue operators and software cannot see customer keys.



# Demo – Key Rollover

Eric Golpe

# 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 Microsoft in first release and by customers in next release | |
| | • StorSimple – provides primary, backup, archival | Managed by customers | Supports AES-256 to encrypt data in StorSimple<br>StorSimple link and documentation |
| System | • BitLocker support for data volumes<br>• Partner solutions for system volume encryption<br>• BitLocker support | Managed by customers | BitLocker for fixed or removable volumes<br>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 |

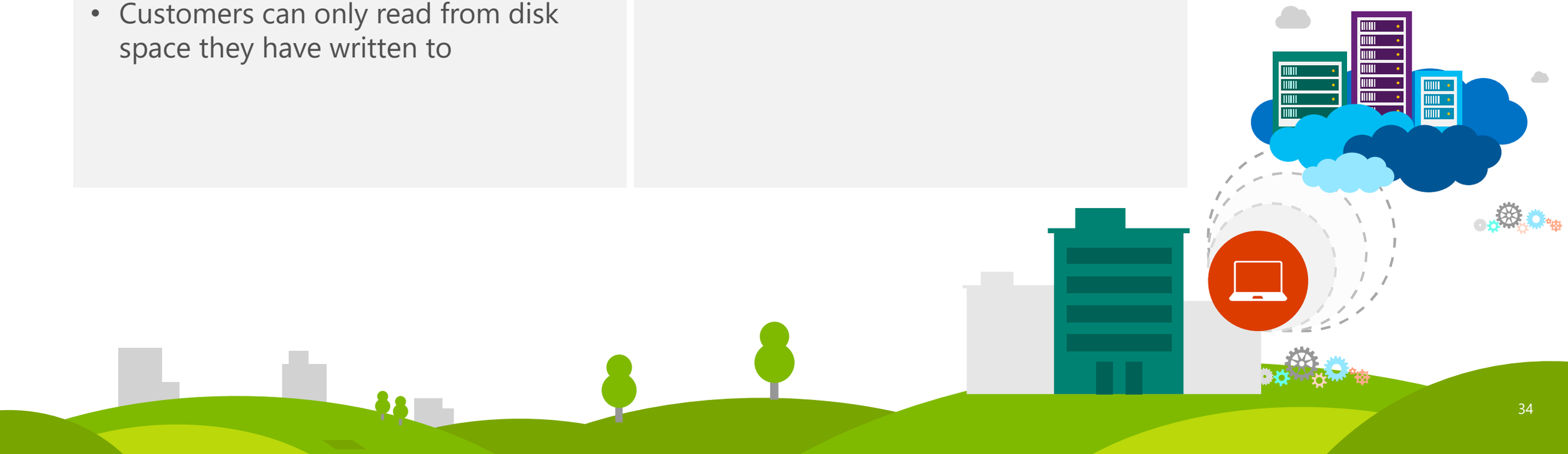
# Data Destruction

## 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



# Cortana Analytics Transparency on Azure

Azure helps enable customer control over customer data by providing transparency into where it is stored, who can access it, and how Microsoft helps secure it, with accessible tools and straightforward language.

# Data storage and use

Customers know where and how their data is stored and used

- Customers control where customer data is stored
- Microsoft doesn't use customer data for advertising
- Microsoft doesn't share customer data with our advertiser-supported services or mine it for marketing
- Microsoft uses customer data only to provide the services, including purposes compatible with providing the services
- Customers may delete customer data or leave the service at any time

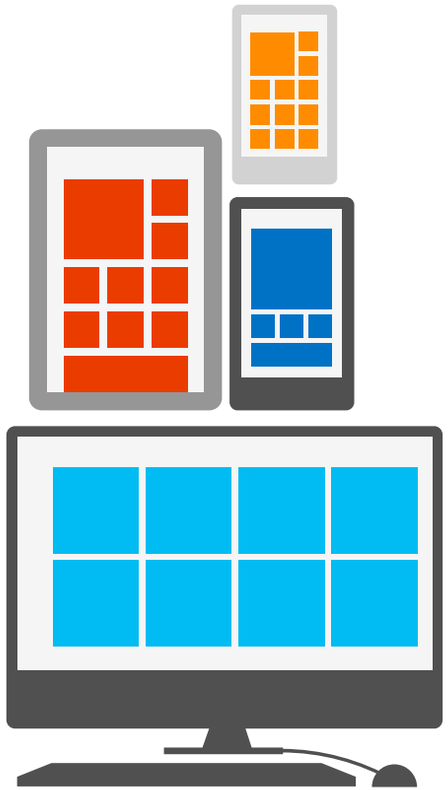

# Data access

Customer knows who can access their data and under what conditions

Customer controls who has access to customer data

Microsoft may hire other companies to provide limited services, such as customer support, on its behalf

Subcontractors are prohibited from using customer data for any other purpose



# Microsoft and compliance

Microsoft invests heavily in the development of innovative compliance technology, processes and integration in Azure. The Microsoft compliance framework for online services maps controls to multiple regulatory standards, which helps drive the design and building of services that meet today's high level of security and privacy needs.

# Microsoft and Compliance

Azure meets a broad set of international, regional, and industry-specific compliance and regulatory standards.

| Compliance certifications | Continual evaluation, benchmarking, adoption, test & audit | Independent verification | Access to audit reports | Proven 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. |

Microsoft