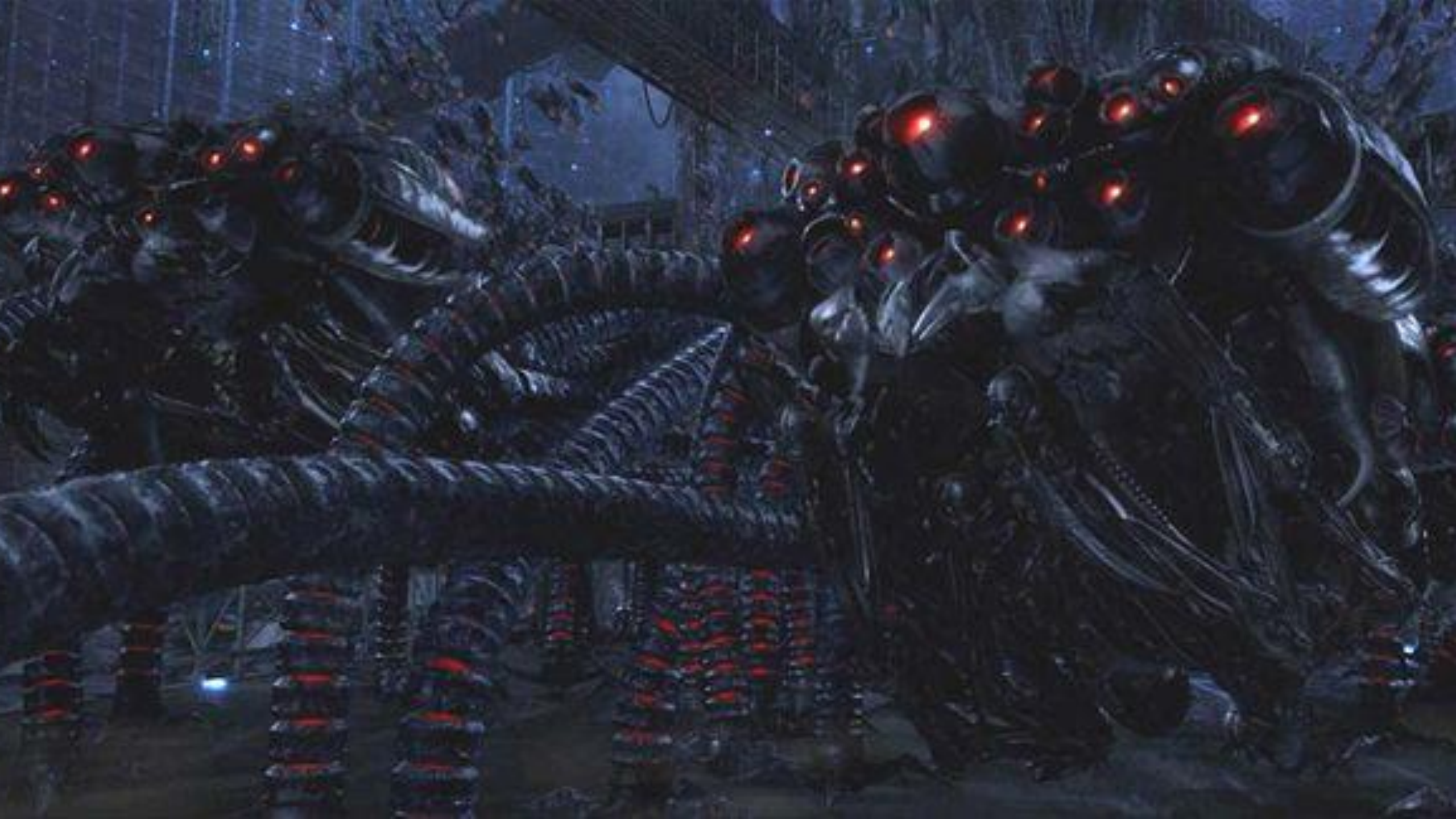
Enter the Matrix.

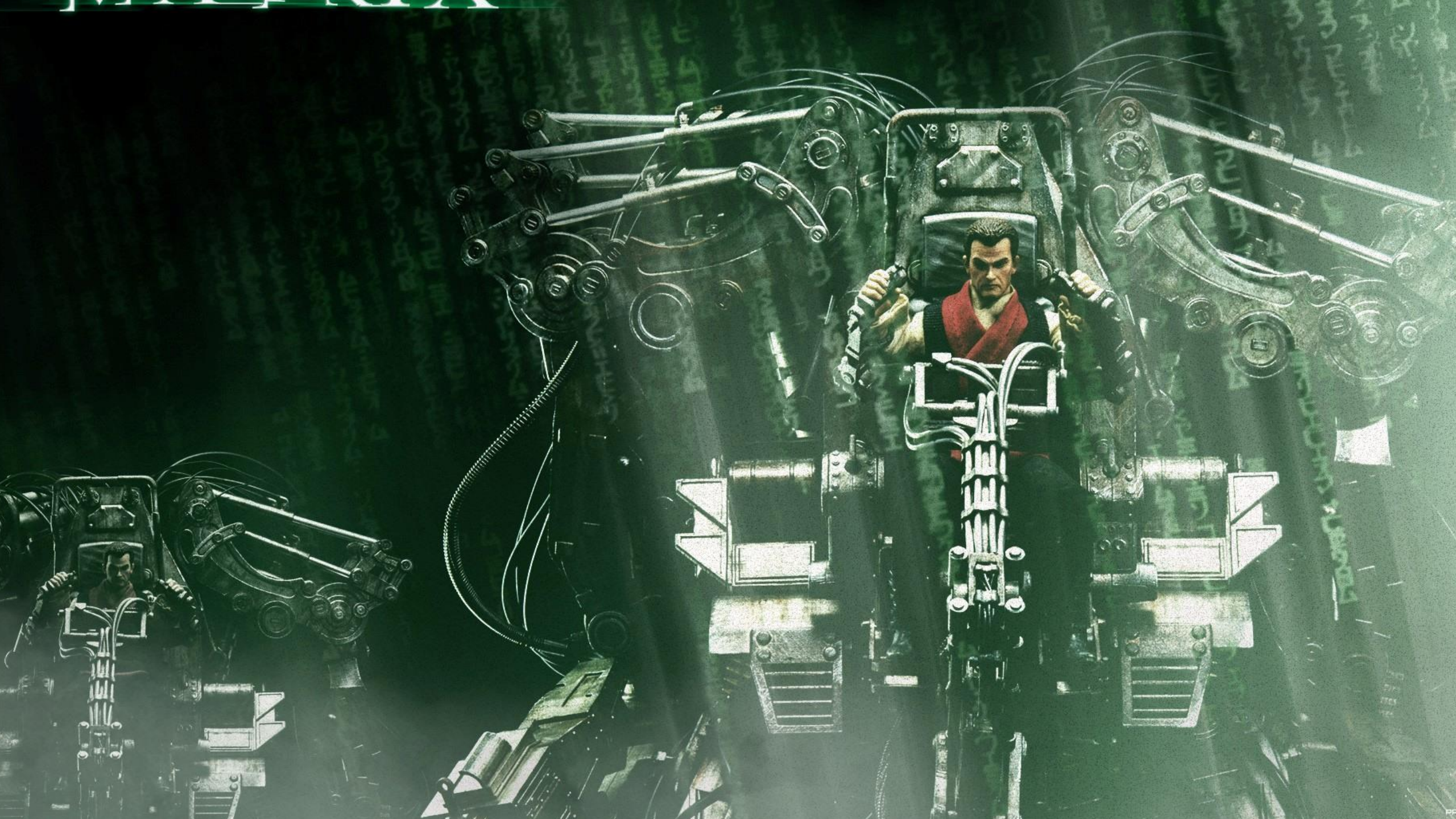
Securing Azure's Assets

Mike MARTIN, Technical Evangelist

Microsoft

STEELGOHST@HOTMAIL.COM






SYSTEM FAILURE

Microsoft Azure

Search resources, services and docs

mike.martin.1977@ou...
MIKE MARTIN

- New
- Dashboard
- Service Health
- Subscriptions
- What's new
- Recent
- Help + support
- All resources
- Resource groups
- Resource Explorer
- Activity log
- Cost Management + Billing
- Tags
- Templates
- Monitor
- Metrics
- Security Center
- Advisor
- Users and groups
- Portal settings

More services >

Who Am I | New dashboard | Edit dashboard | Share | Fullscreen | Clone | Delete

Quickstart tutorials

- Windows Virtual Machines
  Provision Windows Server, SQL Server, SharePoint VMs
- Linux Virtual Machines
  Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs
- App Service
  Create Web Apps using .NET, Java, Node.js, Python, PHP
- Functions
  Process events with a serverless code architecture
- SQL Database
  Managed relational SQL Database as a Service

Brussels Edit

16:02

Friday, March 28, 2019

Audit Logs

View activity

Microsoft

Marketplace

Service Health

Help + support

Audit Logs

View activity

Mike Martin

Technical Evangelist

#Azure

Ex-MVP, Advisor, User group

azug.be

MVP Microsoft Most Valuable Professional

Social

- @techmike2kx
- mimar@microsoft.com

//what

- Flexible
- Passionate about tech
- Family
- Global reach
- Knowledge sharing

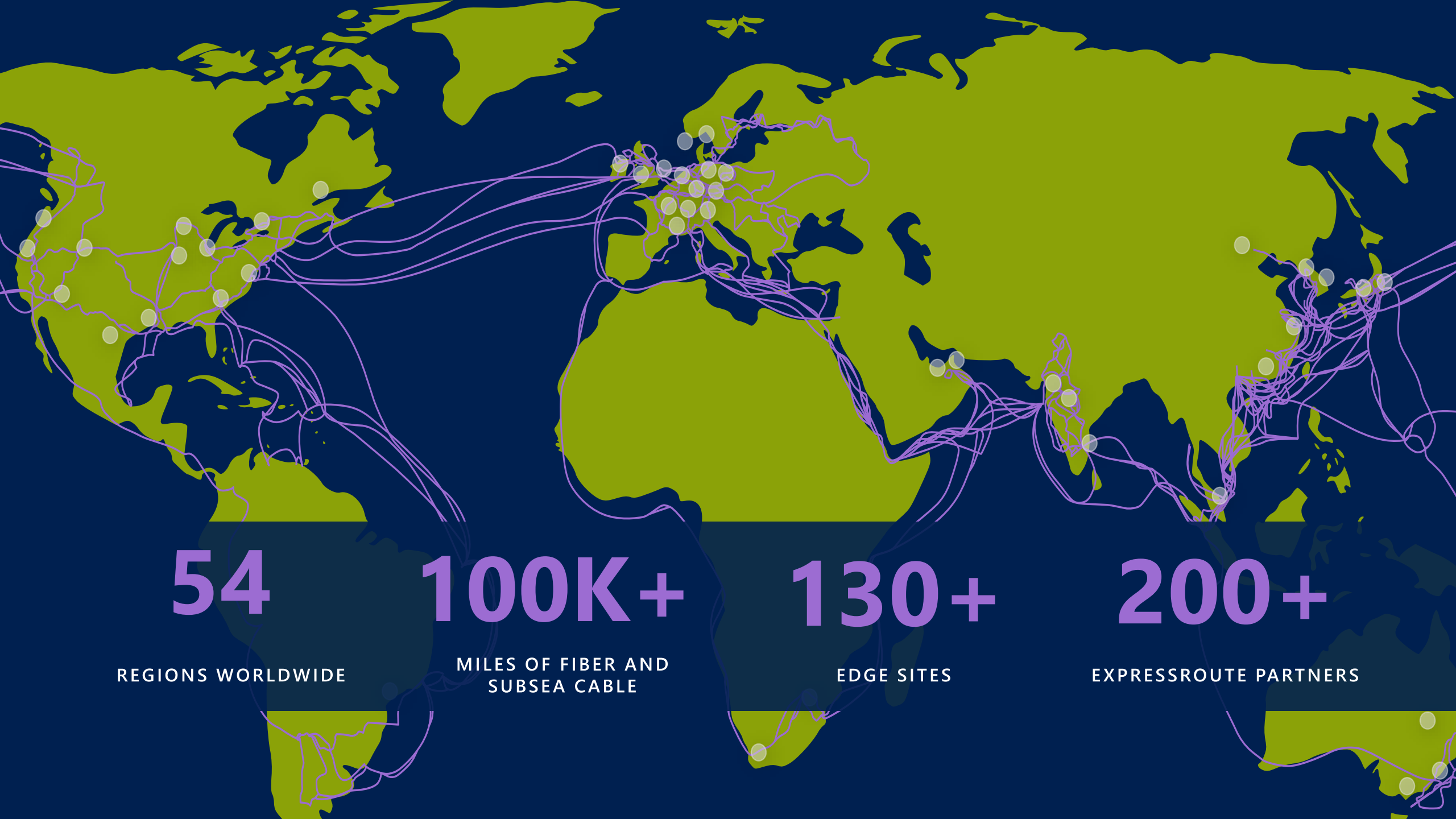
//also

- curious
- Straightforward
- Feedback eager!

Gold sponsors

Silver sponsors

Azure


54
REGIONS WORLDWIDE
100K+
MILES OF FIBER AND SUBSEA CABLE
130+
EDGE SITES
200+
EXPRESSROUTE PARTNERS

Security & Management

- Security Center
- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/ Marketplace
- VM Image Gallery & VM Depot

Platform Services

Media & CDN

- Media Services
- Media Analytics
- Content Delivery Network

Integration

- API Management
- BizTalk Services
- Logic Apps
- Service Bus

Compute Services

- Container Service
- VM Scale Sets
- Batch
- RemoteApp
- Dev/Test Lab

Application Platform

- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Notification Hubs
- Functions

Developer Services

- Visual Studio
- Mobile Engagement
- VS Team Services
- Xamarin
- Application Insights
- HockeyApp

Data

- SQL Database
- SQL Data Warehouse
- DocumentDB
- SQL Server Stretch Database
- Redis Cache
- Storage Tables
- Azure Search

Intelligence

- Cognitive Services
- Bot Framework
- Cortana

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Store
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- Blob
- Queues
- Files
- Disks

Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure (42 Regions, and growing)

Microsoft Security Advantage

$1B annual investment in cybersecurity

3500+ global security experts

Trillions of diverse signals for unparalleled intelligence

?


Identity
Authentication
Authorization
Auditing
Segmentation
Data protection
Application security
Health management
Compliance assessment
Business continuity/ disaster recovery
Incident response & communication
Key management
Anomaly detection/ monitoring
Physical security
Policy, laws & operations


The Matrix
Physical Defenses
Azure Edge Defenses
Your defenses
Your App / code


WARNING:
Even Batman used Shark Repellent
OCEANIC REPELLENT
BAT SPRAYS
BARRACUDA REPELLENT
WHALE REPELLENT
MANTA-RAY REPELLENT
SHARK REPELLENT


MATRIX

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

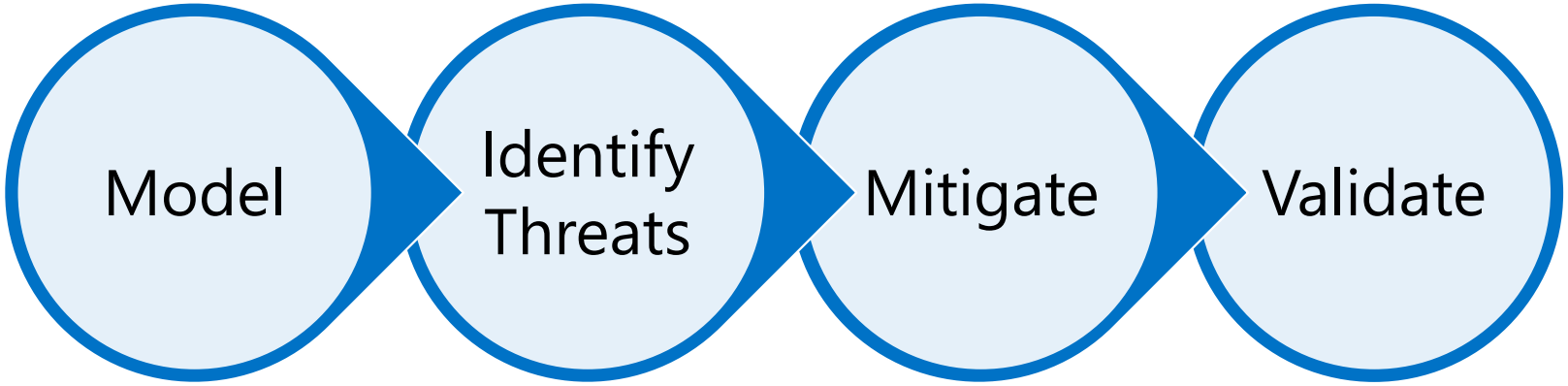
STRIDE

Spoofing	• Authentication
Tampering	• Integrity
Repudiation	• Non-repudiation
Information disclosure	• Confidentiality
Denial of Service	• Availability
Elevation of Privilege	• Authorization

Threat Modeling : Simplified

From "Threat Modeling for Security", Shostack 2014
http://www.threatmodelingbook.com/

1. What are you building?
2. What can go wrong?
3. What are you going to do about it?
4. Did you do an acceptable job at 1-3?



Know Your Code (from a security perspective)

"Knowledge is power only if a [person] knows what facts not to bother about." – R.W. Lynd

- Identify flow of untrusted and sensitive data in your system
  - ...in the code!
- Document all security sensitive code paths in source. Write once. Read many.
- Document your security intent and decisions in code.
- Create security-focused models/diagrams
  - Better mental models == better ongoing maintenance
- Watch out for dependencies. Keep an eye on rotting legacy components.

http://aka.ms/TMTPreview

Threat Modeling Tool vNext / 2017

https://blogs.msdn.microsoft.com/secdevblog/2017/04/21/whats-new-with-microsoft-threat-modeling-tool-preview/

Keyvault Configuration Package

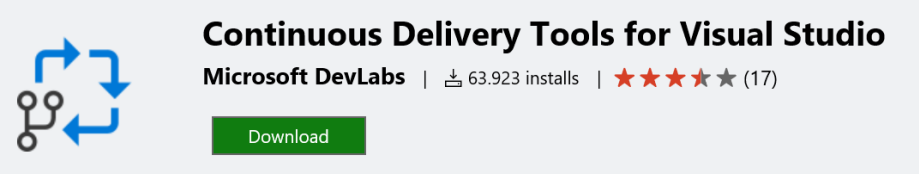
To use the provider, add a reference to the Microsoft.Extensions.Configuration.AzureKeyVault package.

Secret Manager

The Secret Manager tool stores sensitive data for development work outside of your project tree. The Secret Manager tool is a project tool that can be used to store secrets for a .NET Core project during development. With the Secret Manager tool, you can associate app secrets with a specific project and share them across multiple projects.

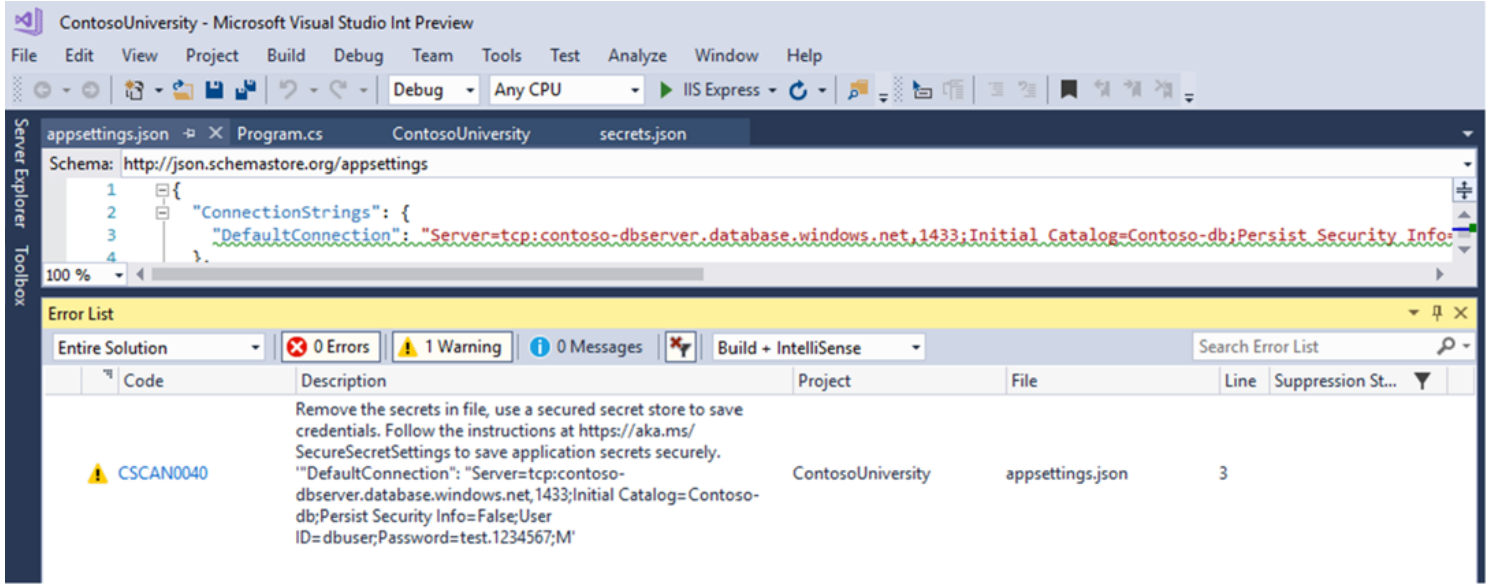
Add to .csproj following and save to restore the associated NuGet package

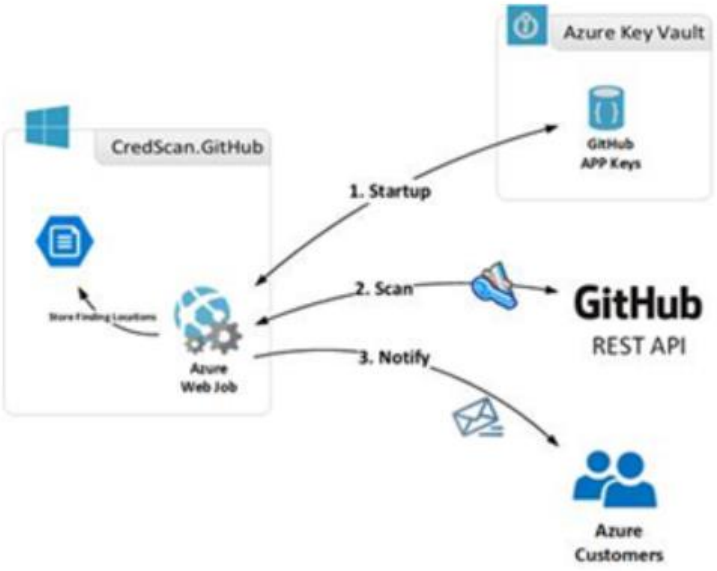
```
<DotNetCliToolReference Include="Microsoft.Extensions.SecretManager.Tools"
Version="2.0.0" />
```



Microsoft Azure

https://aka.ms/SecCode



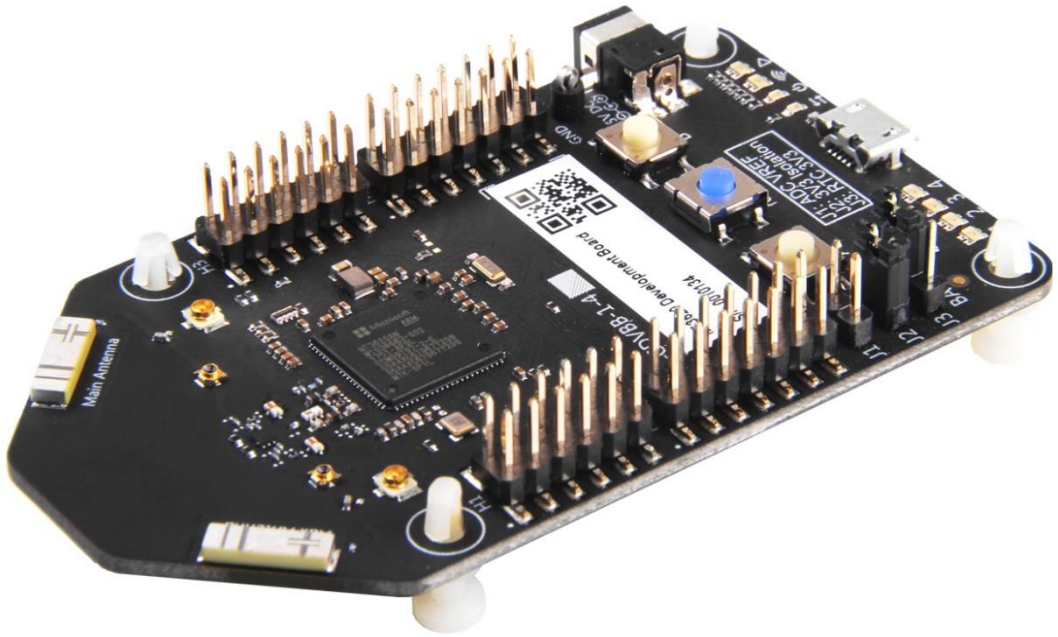


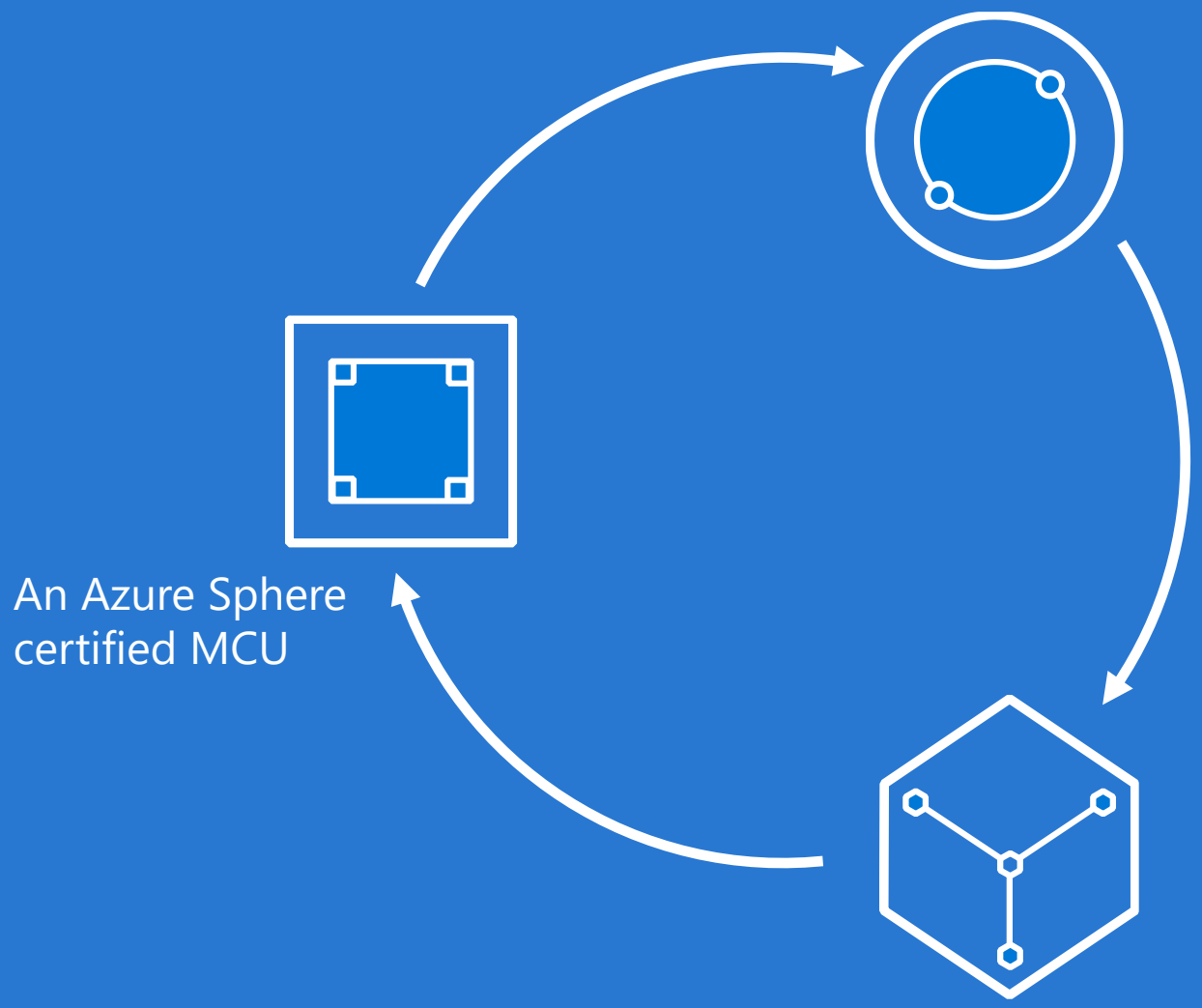
CredScan + GitHub

Microsoft

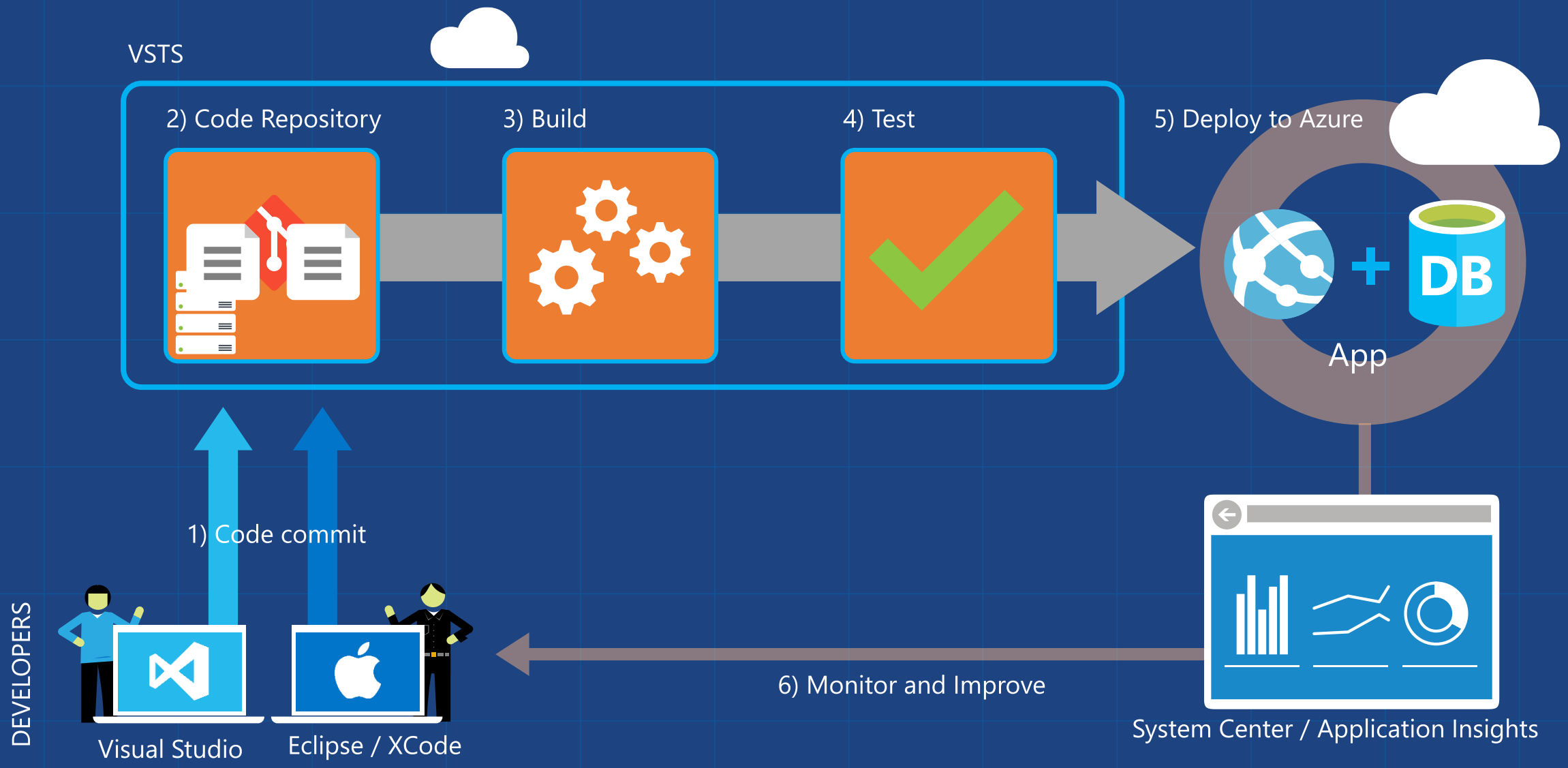
TMT – vNext

Three components.
One low price.
No subscription required.

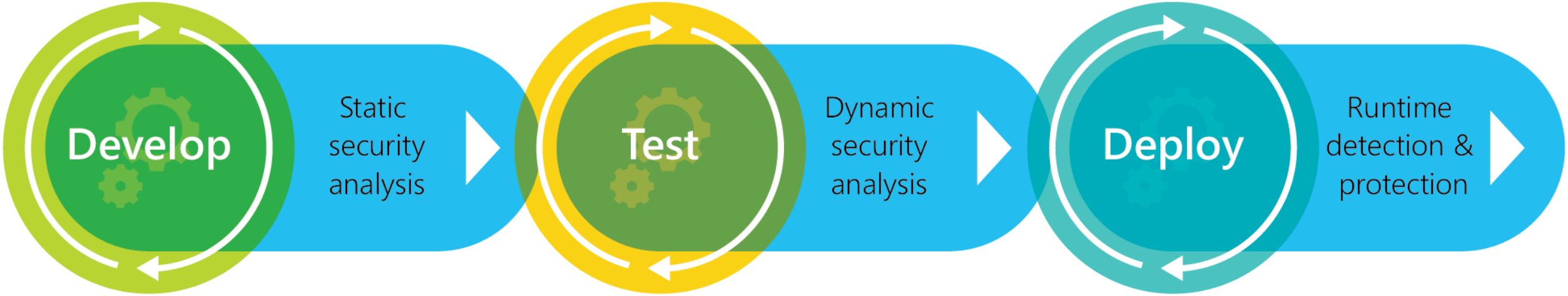




DevOps


VSTS
2) Code Repository
3) Build
4) Test
5) Deploy to Azure
DB
App
1) Code commit
DEVELOPERS
Visual Studio
Eclipse / XCode
6) Monitor and Improve
System Center / Application Insights

SecOps

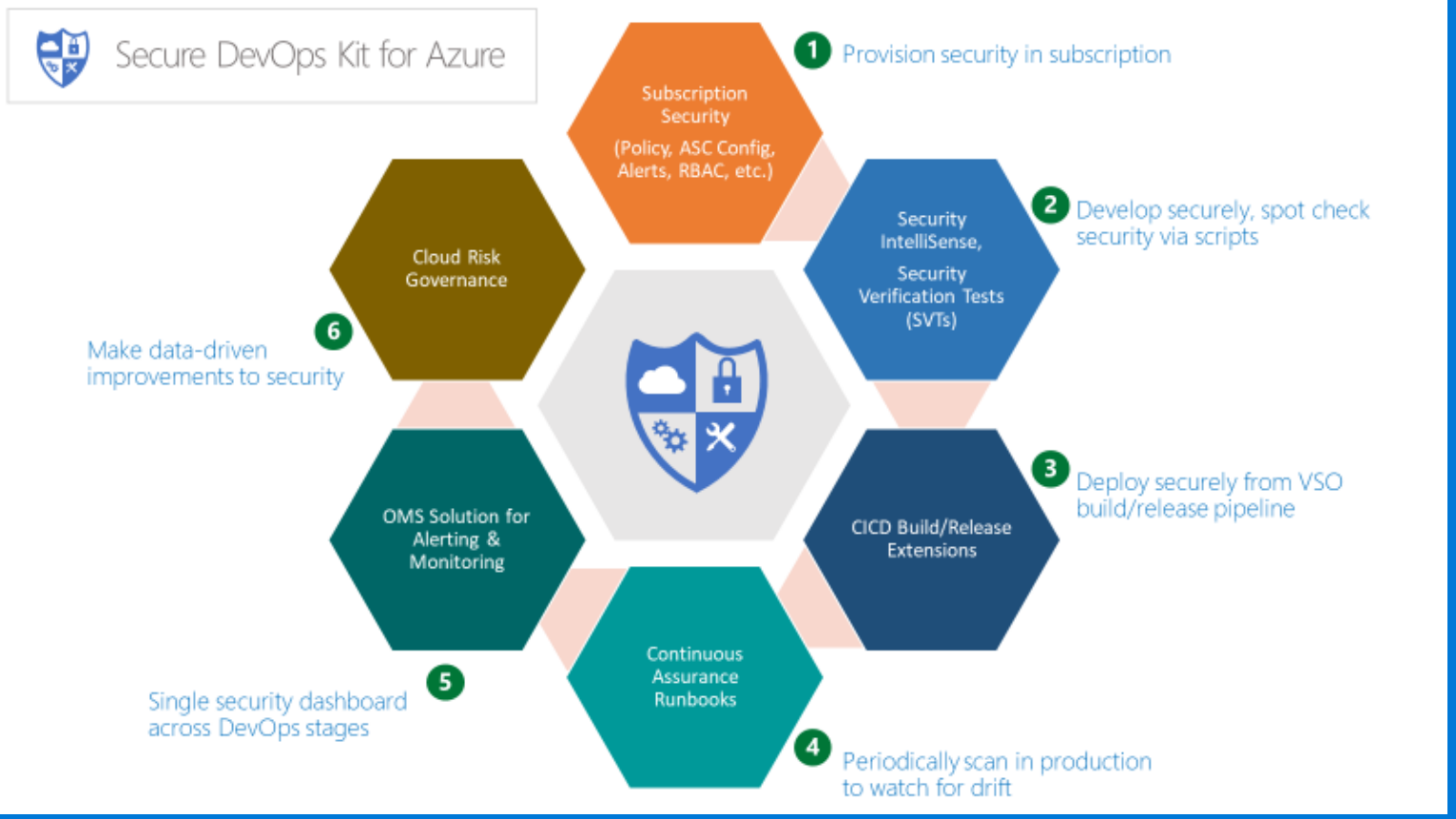

Develop
Static security analysis
Test
Dynamic security analysis
Deploy
Runtime detection & protection

DevOps – Secure - Practices

Task	Automated tool
Code scanning and quality verification	Static and dynamic analysis tooling
Deployment	Azure Resource Manager (ARM)–based deployment tooling and scripts, templates, and PowerShell scripts
Infrastructure on demand	Scripted provisioning and de-provisioning
Configured operational standards	Process definitions for tasks that DevOps teams manage, such as configuration management, security monitoring, incident response, forensic investigation, backup, and recovery

DevOps – Secure - Tooling

Deployment strategy	For
Use ARM templates	Deploying hardened IaaS virtual machines, securing Key Vault access credentials
Use Forensic scripts (Azure PowerShell)	Extracting data for incident response
Use Hardening scripts (Azure PowerShell)	Evaluating compliance, automatically hardening infrastructure
Develop administrative accelerators	Creating runbooks for Azure Storage account key rotations
Develop guidance and control procedures	Providing step-by-step instructions, with validation for each step
Develop admin SQL scripts	Providing helper scripts for SQL Azure



http://aka.ms/azskdevops
http://aka.ms/azsecops
http://aka.ms/azsecopsinfo
http://aka.ms/azskkarlots

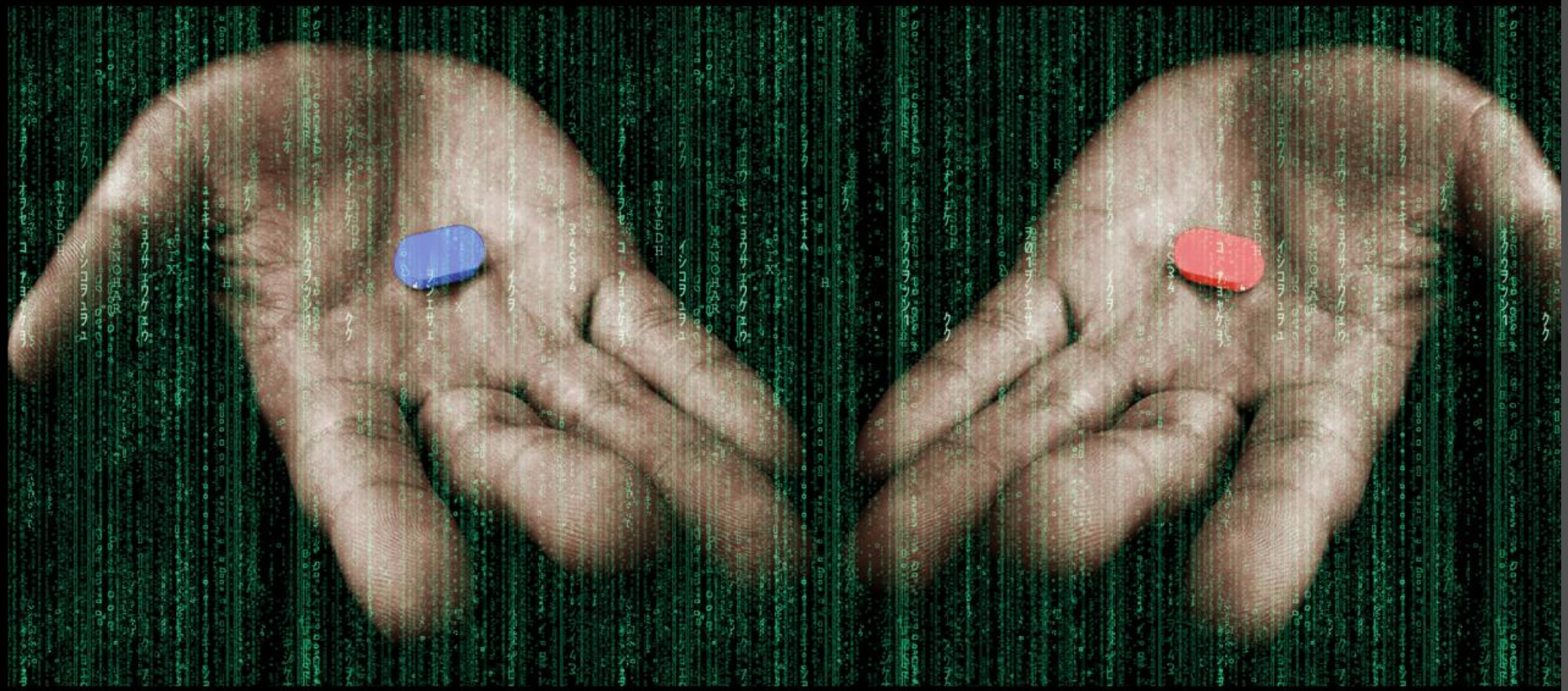
Trust

Cloud security is a shared responsibility

Shared responsibility model for cloud security

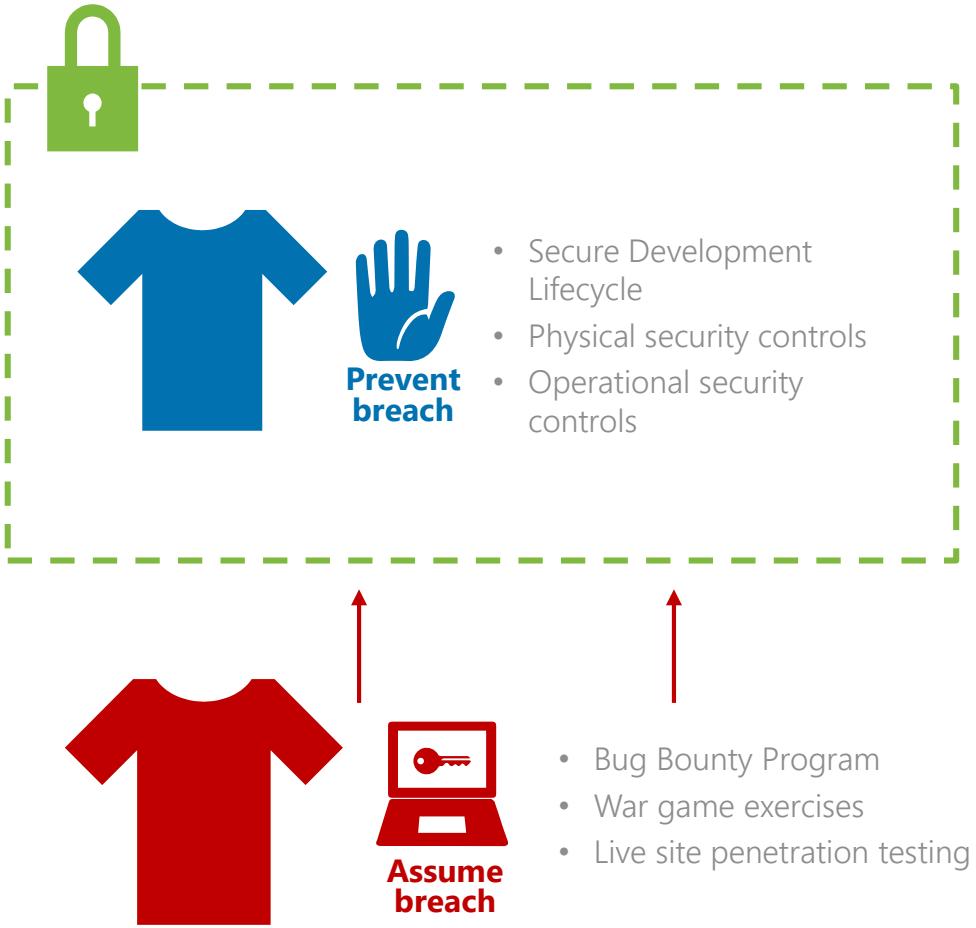
Microsoft's commitment	Joint responsibility
Secure foundation	**Microsoft provides built-in controls**
Physical assets	Virtual machines and networks
Datacenter operations	Apps and workloads
Cloud infrastructure	Data

After this there is not turning back



You can take the red pill, wake up in your bed and believe what ever you want to believe or you can take the blue pill, stay in wonder-land and I will show you how deep the holerabbit goes

Prevent & Assume Breach



- ✓ **Prevent Breach** is a defensive strategy aimed at predicting and preventing a security breach
- ✓ The **Assume Breach** strategy, unique to Microsoft, is a key operational practice that hardens cloud services
  - ✓ Leverages Microsoft's vast threat intelligence
  - ✓ Includes state of the art security monitoring and response

Model Realworld Attacks

- Model Emerging Threats, Use Blended Threats
- Exfiltrate & Leverage Compromised Data
- Escape And Evade / Persistence

Identify Gaps In Security Story

- Measure Time To Compromise (Mttc) / Pwnage (Mttp)
- Highlight Security Monitoring & Recovery Gaps
- Improve Incident Response

Demonstrable Impact

- Prove Need For Assume Breach
- Enumerate Business Risks
- Justify Resources, Priorities & Investment Needs

Exercises Ability To Detect & Respond

- Detect Attack & Penetration (MTTD)
- Respond & Recover To Attack & Penetration (MTT)
- Practiced Incident Response

Microsoft

Enhances Situational Awareness

- Produces Actionable Intelligence
- Full Visibility Into Actual Conditions Within Environment
- Data Analysis & Forensics For Attack & Breach Indicators

Measure Readiness & Impact

- Accurately Assesses Real-world Attacks
- Identifies Gaps & Investment Needs
- Focus On Slowing Down Attackers & Speeding Recovery
- Hardening That Prevents Future Attacks

Trusted Cloud Principles

Commitment to principles worthy of your organization's trust

Security

We will implement strong security measures to safeguard your data.

Privacy & Control

We will provide you with control over your data to help keep it private.

Compliance

We will help you meet your specific compliance needs.

Transparency

We will explain what we do with your data in clear, plain language.

Main Philosophy: 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 and 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**

Physical data center security

- Cameras
- 24X7 security staff
- Barriers
- Fencing
- Alarms
- Two-factor access control: Biometric readers & card readers
- Security operations center
- Seismic bracing
- Days of backup power

Perimeter

Building

Computer room

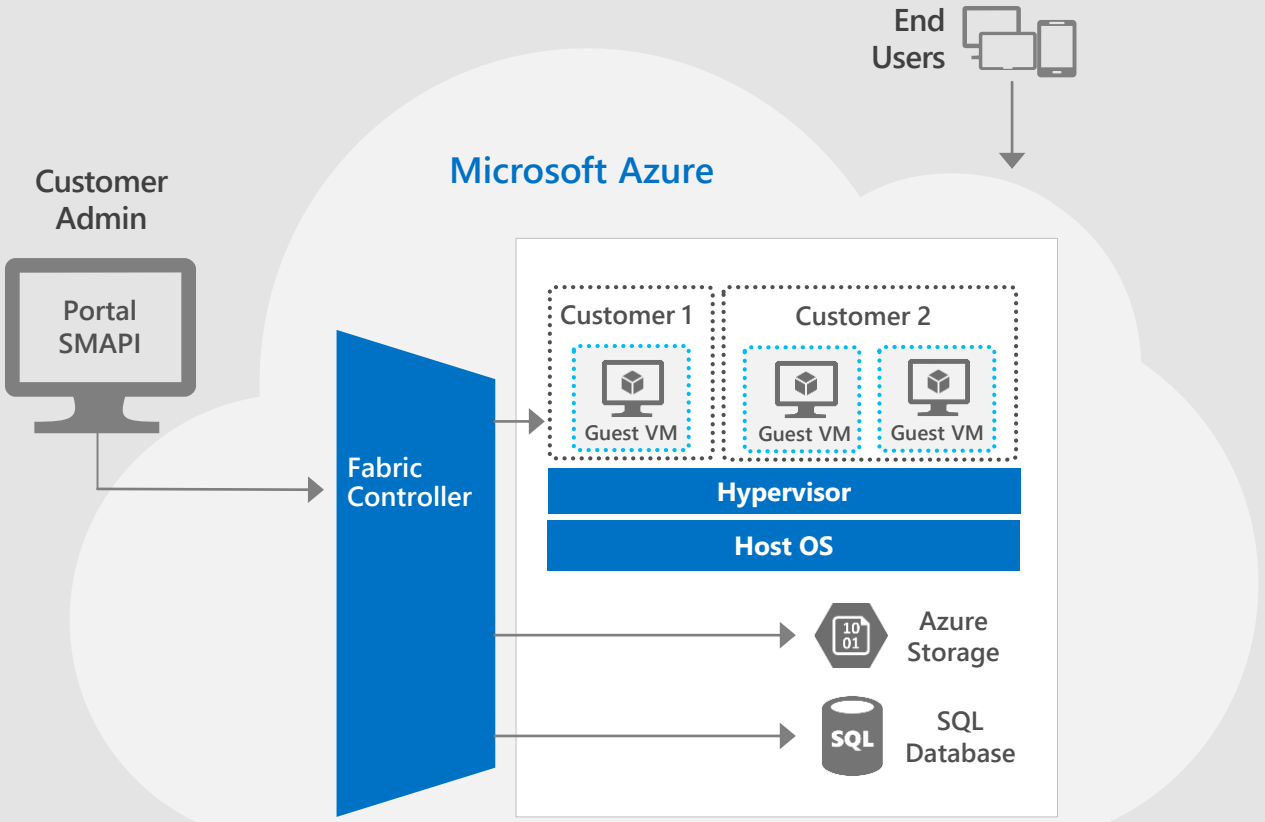
Secure Multi-Tenancy Architecture

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



Data Segregation

Azure

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:

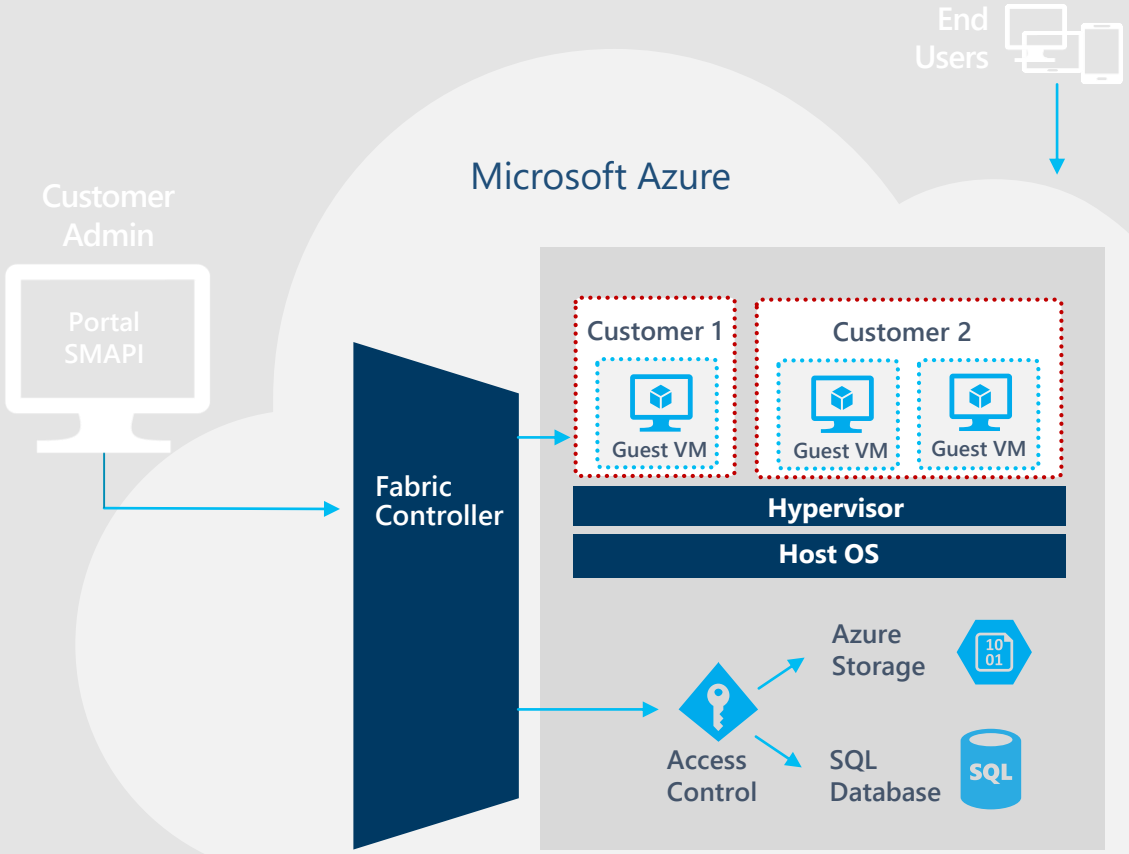
- SQL Database isolates separate databases using SQL accounts

Network isolation:

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

Customer

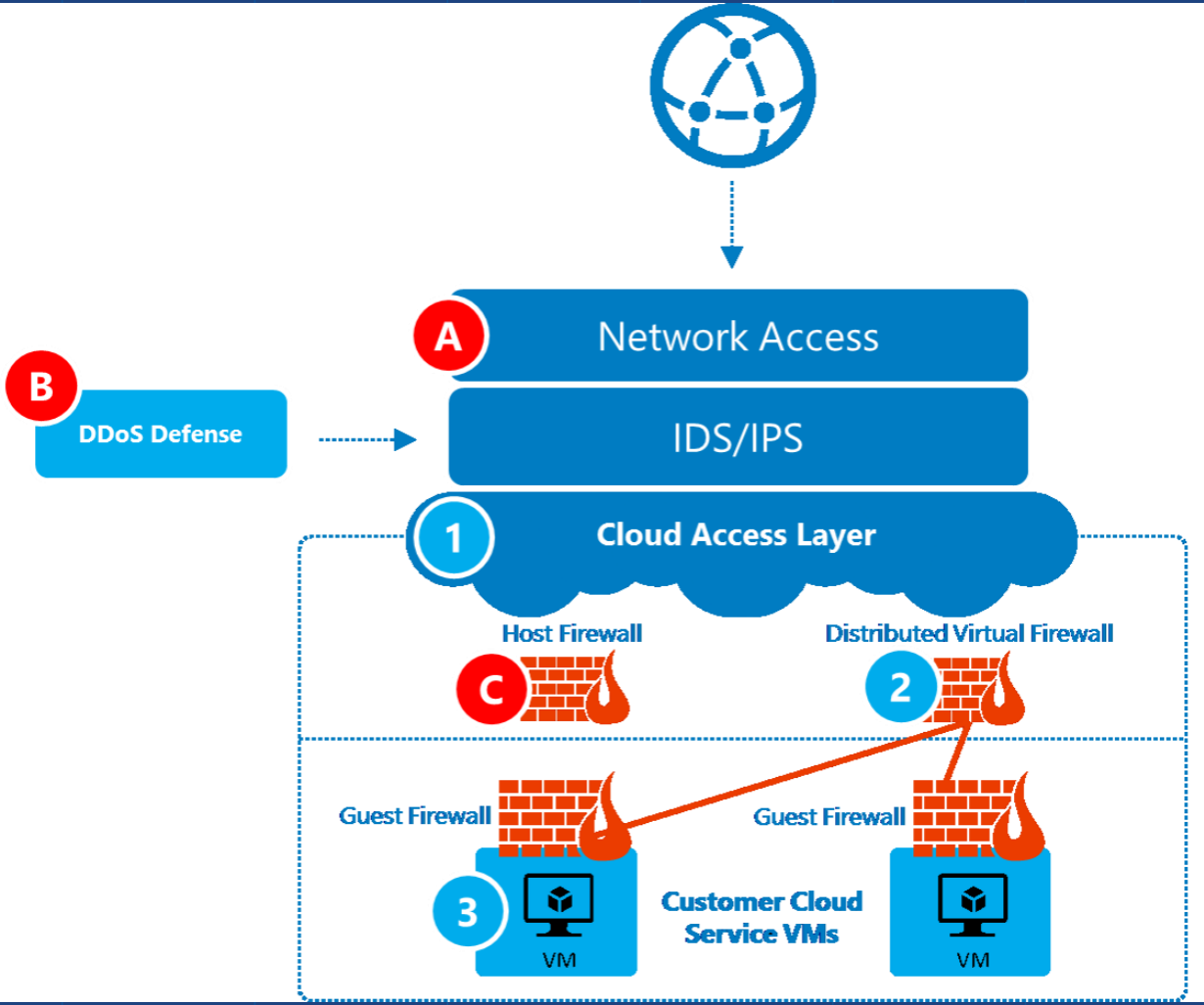
- Design same principles for multi-tenancy



Secure operations

Azure platform services infrastructure protection

1. Azure Protection
Layer A: The Network Access Layer
Layer B: Azure's DDoS/DOS/IDS Layer
Layer C: Host firewalls protect all the hosts, and the VLANs
Layer D: Conformance with security and privacy requirements includes two-factor authentication for operators.



2. Customer protection:
Layers 1-2: The distributed firewall isolates customer's
Layer 3: The virtual network can be managed similar to an on-premises private network.
i. Inside the VM: Firewalls, IDS, and DoS solutions.
ii. Virtual network appliances

Patching and Update Management

Azure

- Applies regularly scheduled updates to the platform
- Releases critical patches immediately
- Rigorously reviews and tests all changes
- Uses a combination of third-party scanning tools for Azure environment

Customer

- Applies similar patch management strategies for their Virtual Machines

MONTHLY MSRC PATCH REVIEW

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

PATCHING ROLLOUT

- Prioritize critical updates
- Monthly OS releases with patches

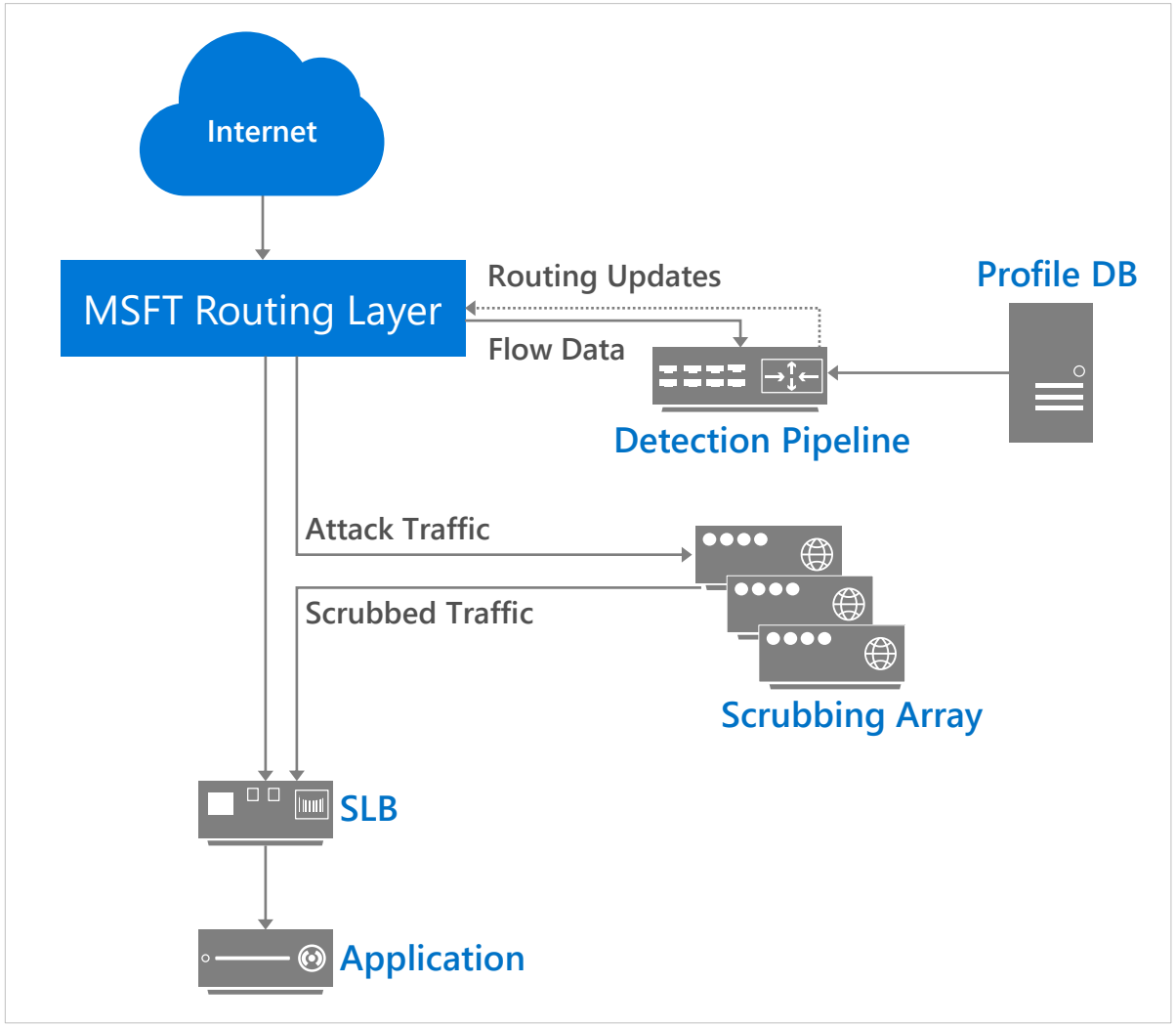
SCANNING

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

AUDIT VALIDATION

- Reconciliation report
- Resolution summary

DDoS System Protection Overview



SUPPORTED DDOS ATTACK PROFILES

- TCP SYN
- UDP/ICMP/TCP Flood

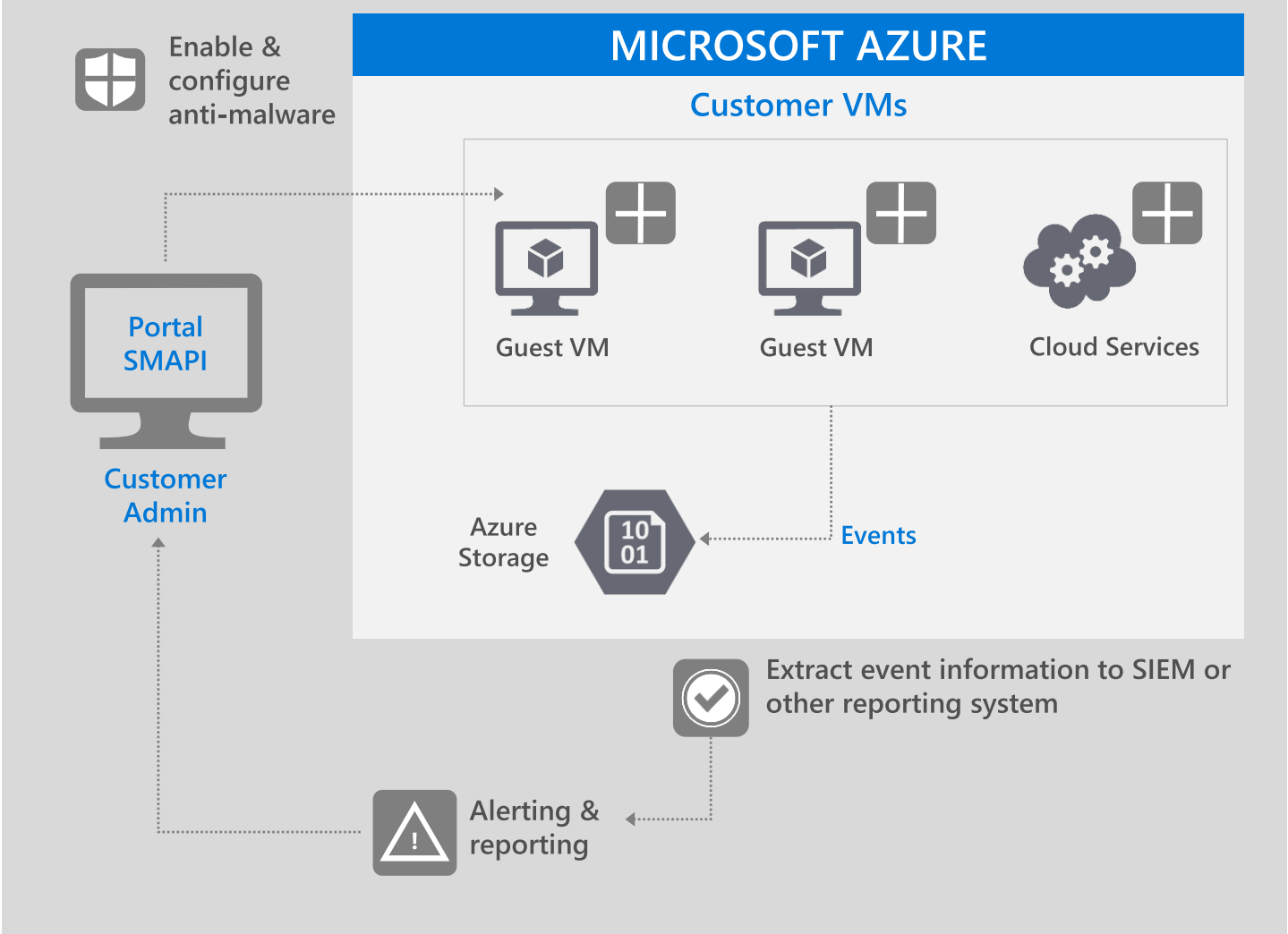
DETECTION PROCESS

- 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

Antivirus/Antimalware Protection



AZURE

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

CUSTOMER

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

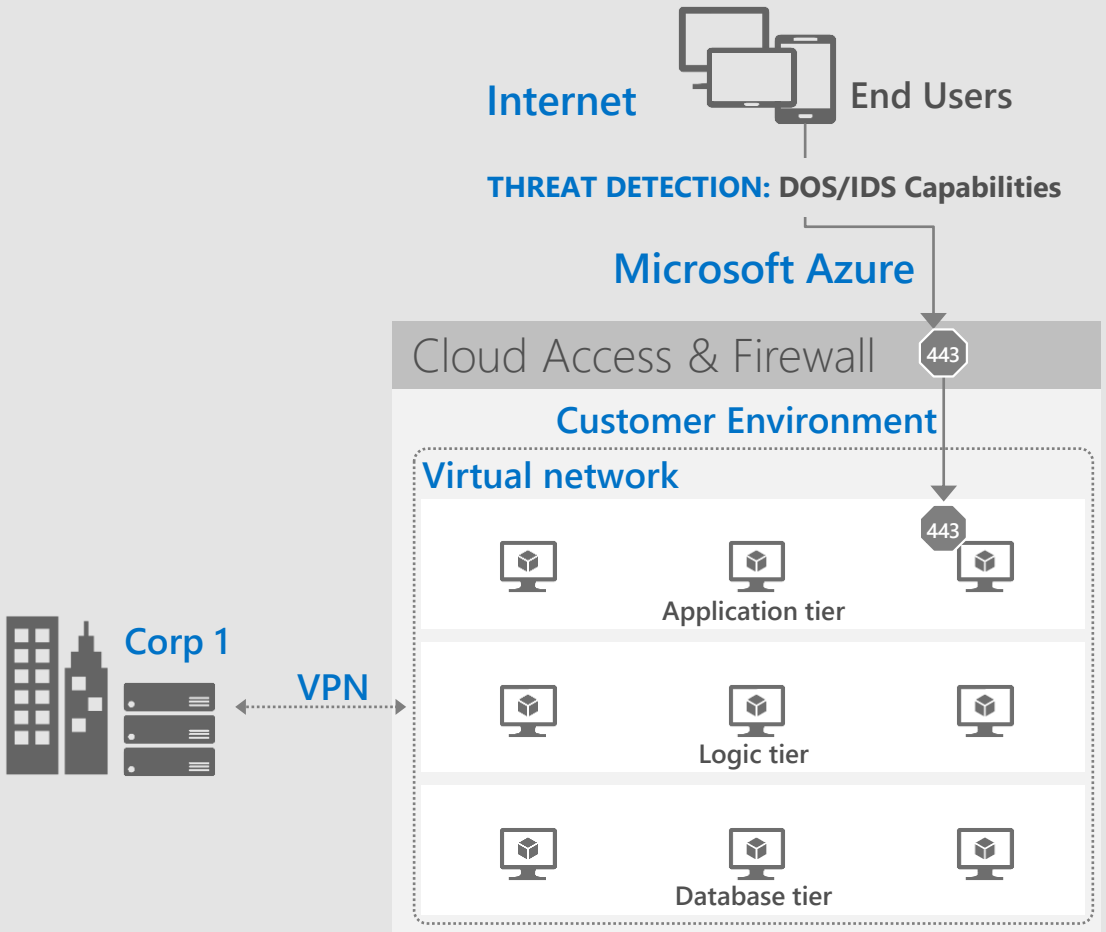
Threat Protection

Azure

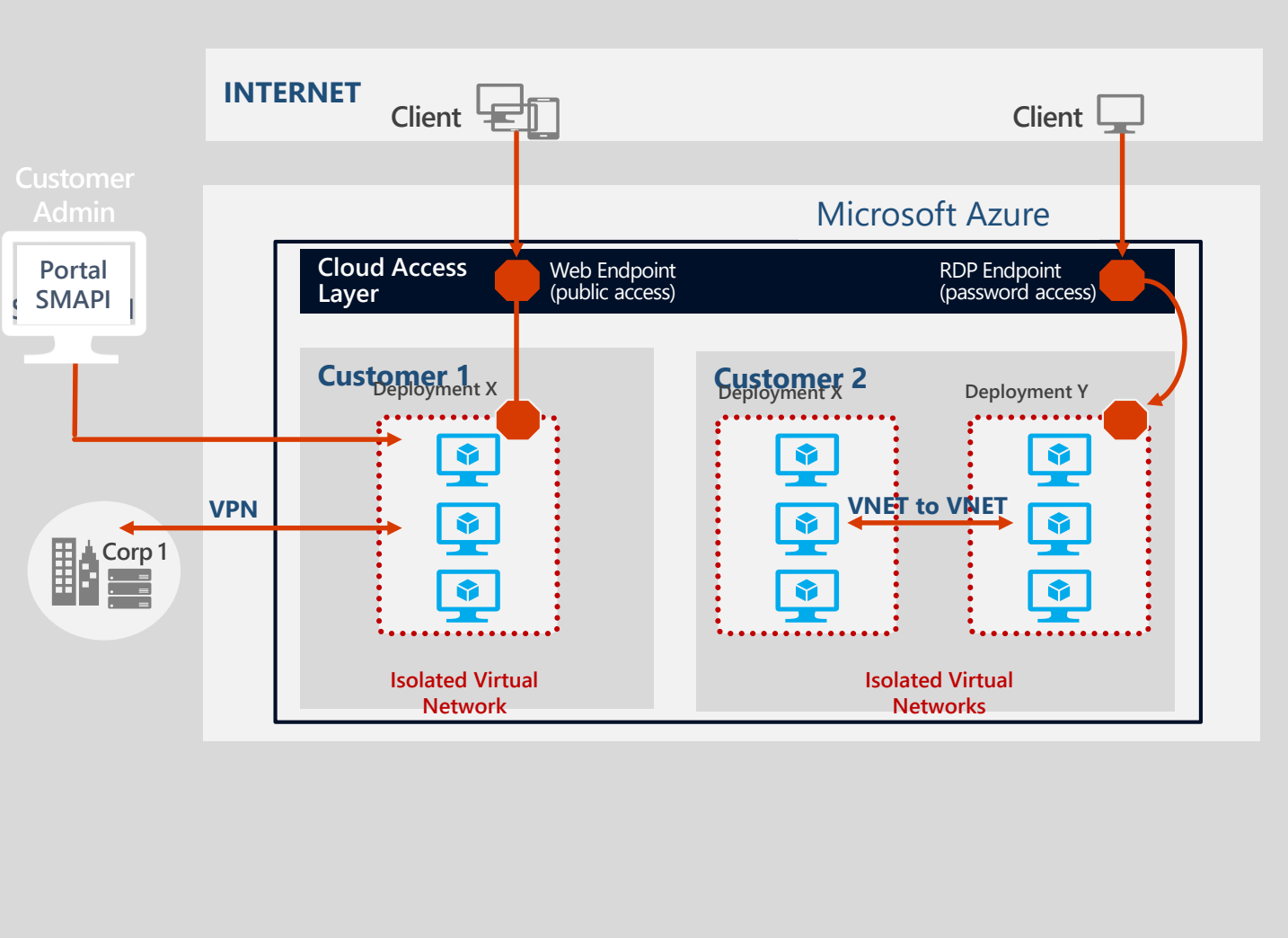
- Performs big data analysis of logs for intrusion detection & prevention for the platform
- Employs denial of service attack prevention measures for the platform
- Regularly performs penetration testing

Customer

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



Network Isolation



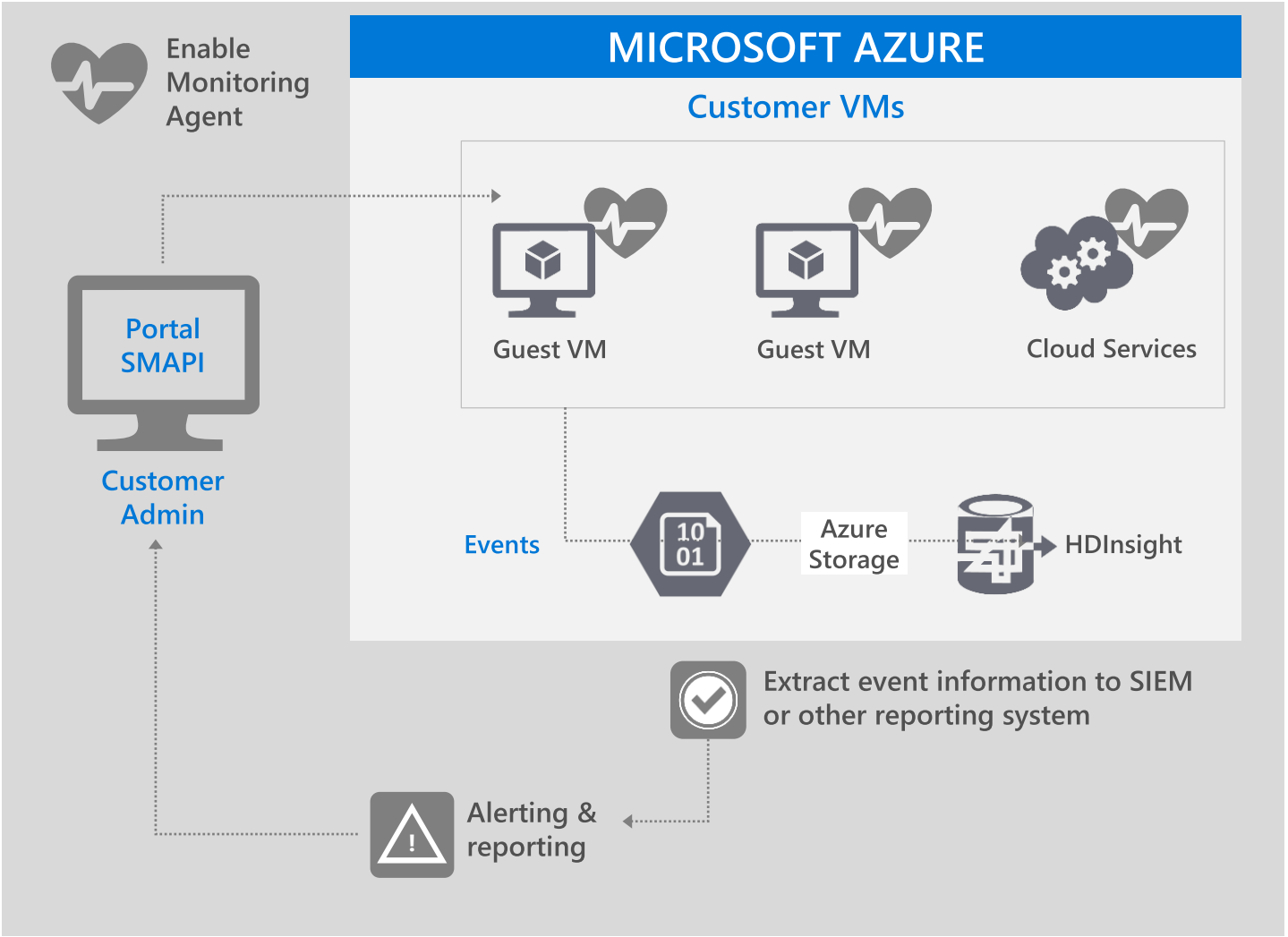
AZURE

- Does not enable general internet access by default, except remote administration endpoints configured when Virtual Machines are created in the Portal

CUSTOMER

- Configure endpoints for required access
- Creates connections to other cloud and on-premises resources

Monitoring and Alerts



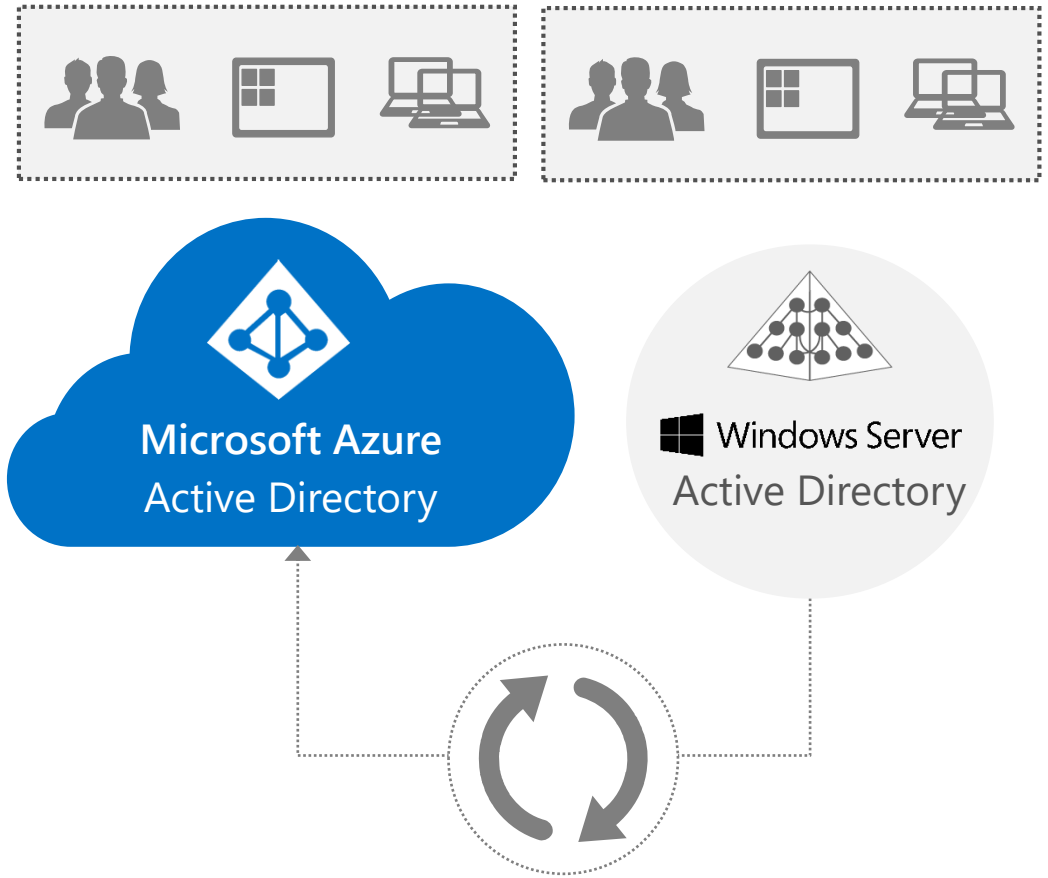
AZURE

- Performs monitoring and 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

Azure Active Directory 2FA Mandatory



Azure Active Directory (AAD) integration

- Secure access management requires strong, centralized, identity management.
- Active Directory (AD) helps you with that on-premises.
- Azure Active Directory (AAD) helps you in Azure…and in Office 365, and in 1200+ apps.
- AD and AAD are tightly integrated, to enable single sign-on, a single directory, and centralized management.
- AD and AAD help address your compliance requirements.

Use Two Factor Authentication or DevOPs to access your production services

- Two Factor Authentication can be implemented with Phone Factor or with AD on-premises.

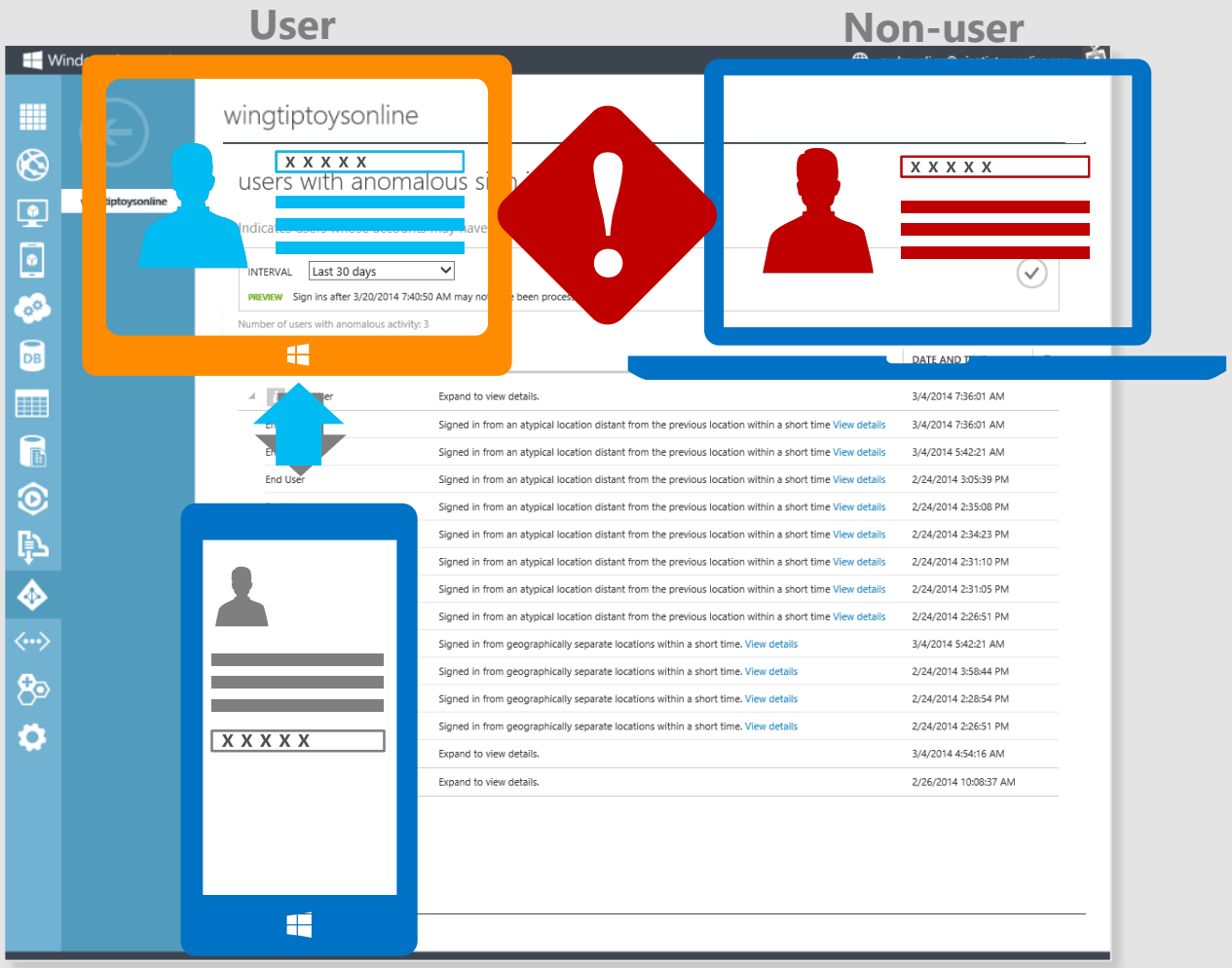
Threat Protection

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



Transparency

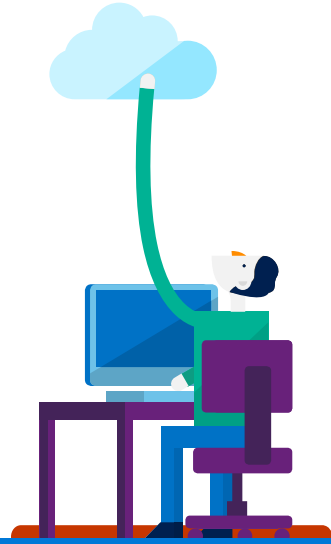
Transparency & independent verification

AIDS CUSTOMERS IN MEETING SECURITY & COMPLIANCE OBLIGATIONS

Third-party verification	Access to audit reports	Compliance packages	Best practices and guidance
Trust Center	Cloud Security Alliance	Security Response Center progress report	Security Intelligence report

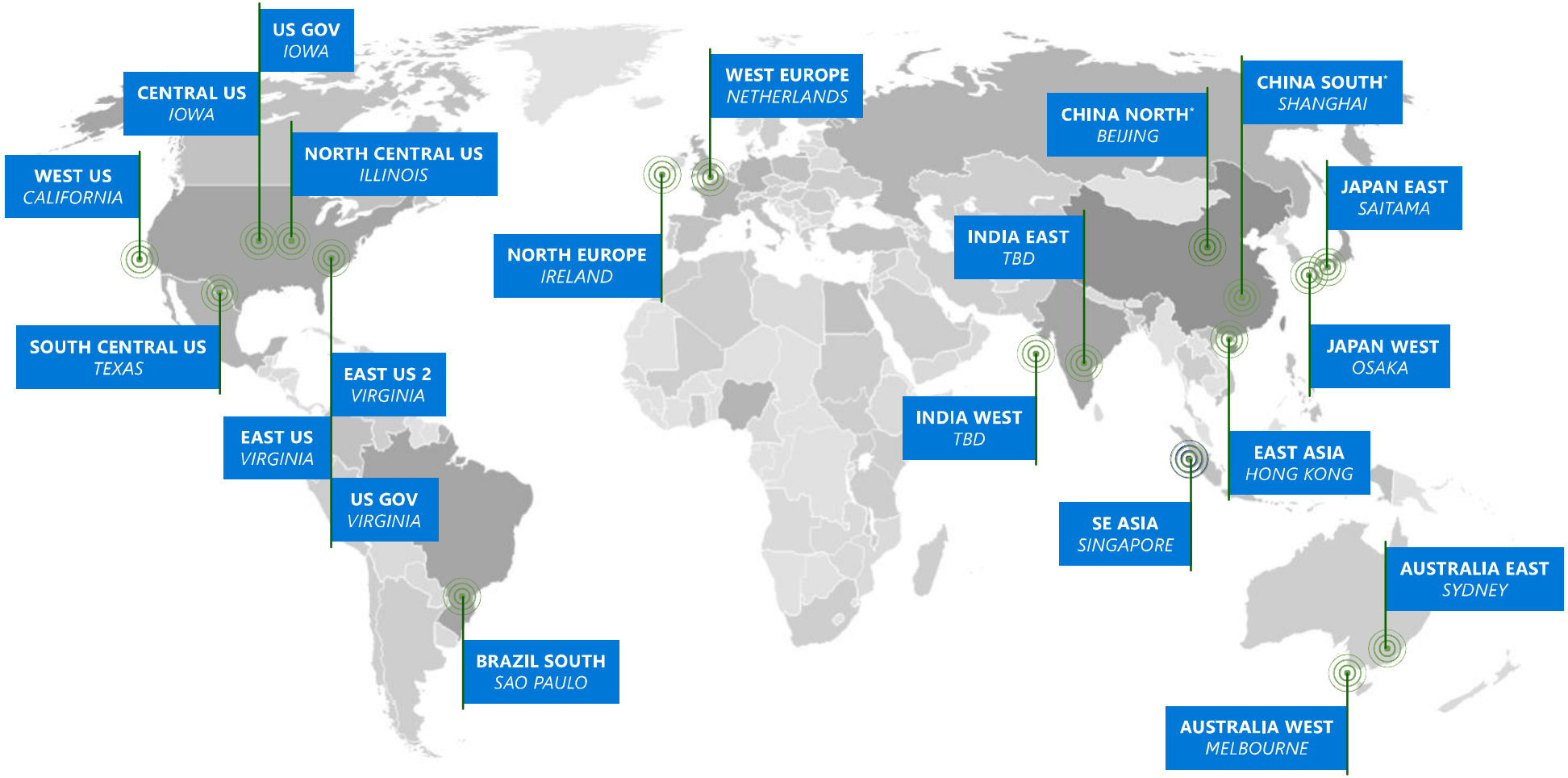
Data storage and use

- Customers control where customer data is stored
- Microsoft doesn’t use customer data for advertising, marketing or share your data
- Customers may delete their data or leave the service at any time



Customers know where and how their data is stored and used

Data Location and Replication



100+ Datacenters in over 40 countries

AZURE

- Microsoft will not store customer data outside the customer-specified geography
- Microsoft may only transfer customer data within a geo for redundancy of a geo

CUSTOMER

- Chooses where data resides
- Configures data replication options

Privacy and Control

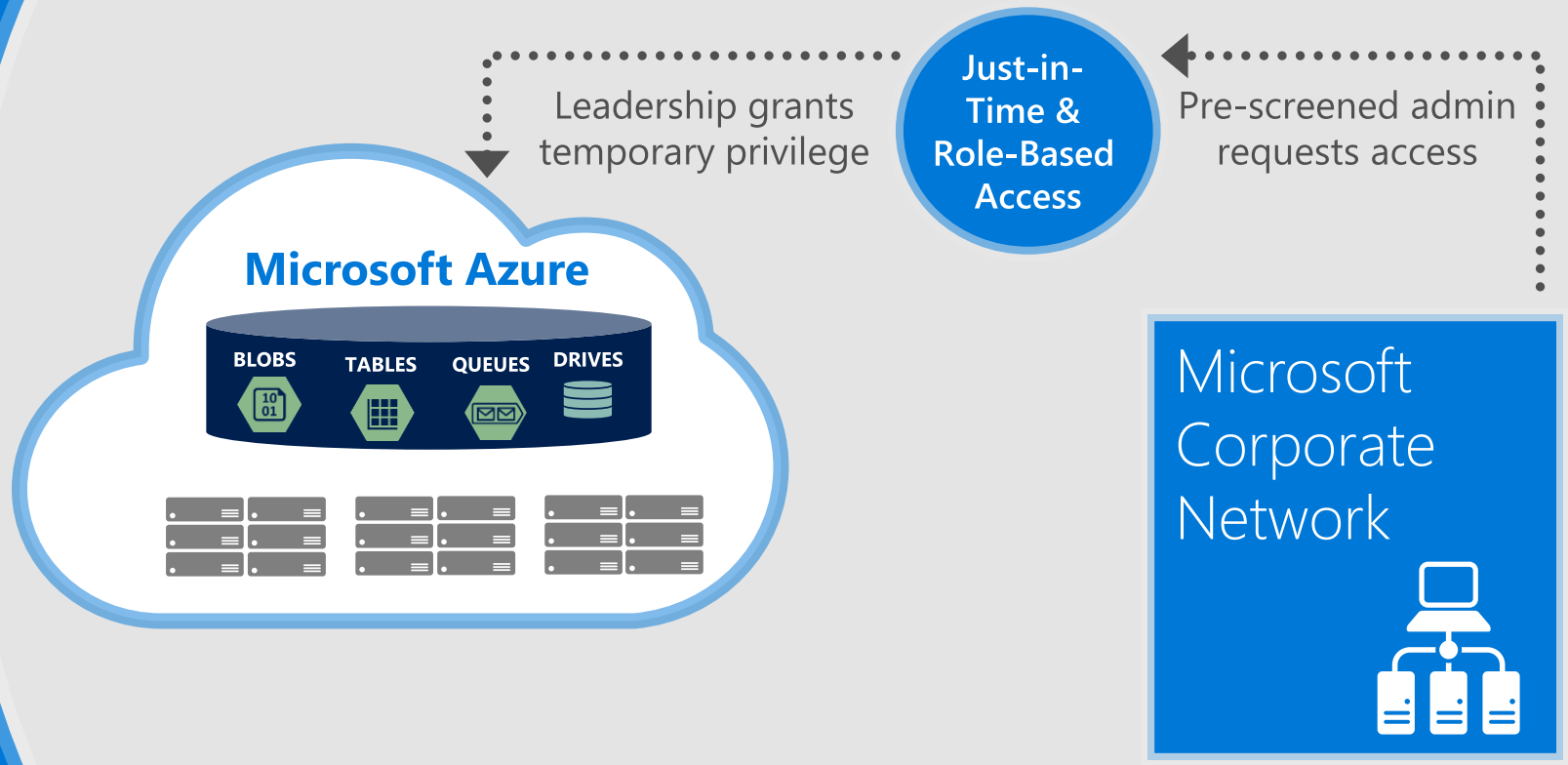
Microsoft Employee Access Management

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



Encryption in Transit

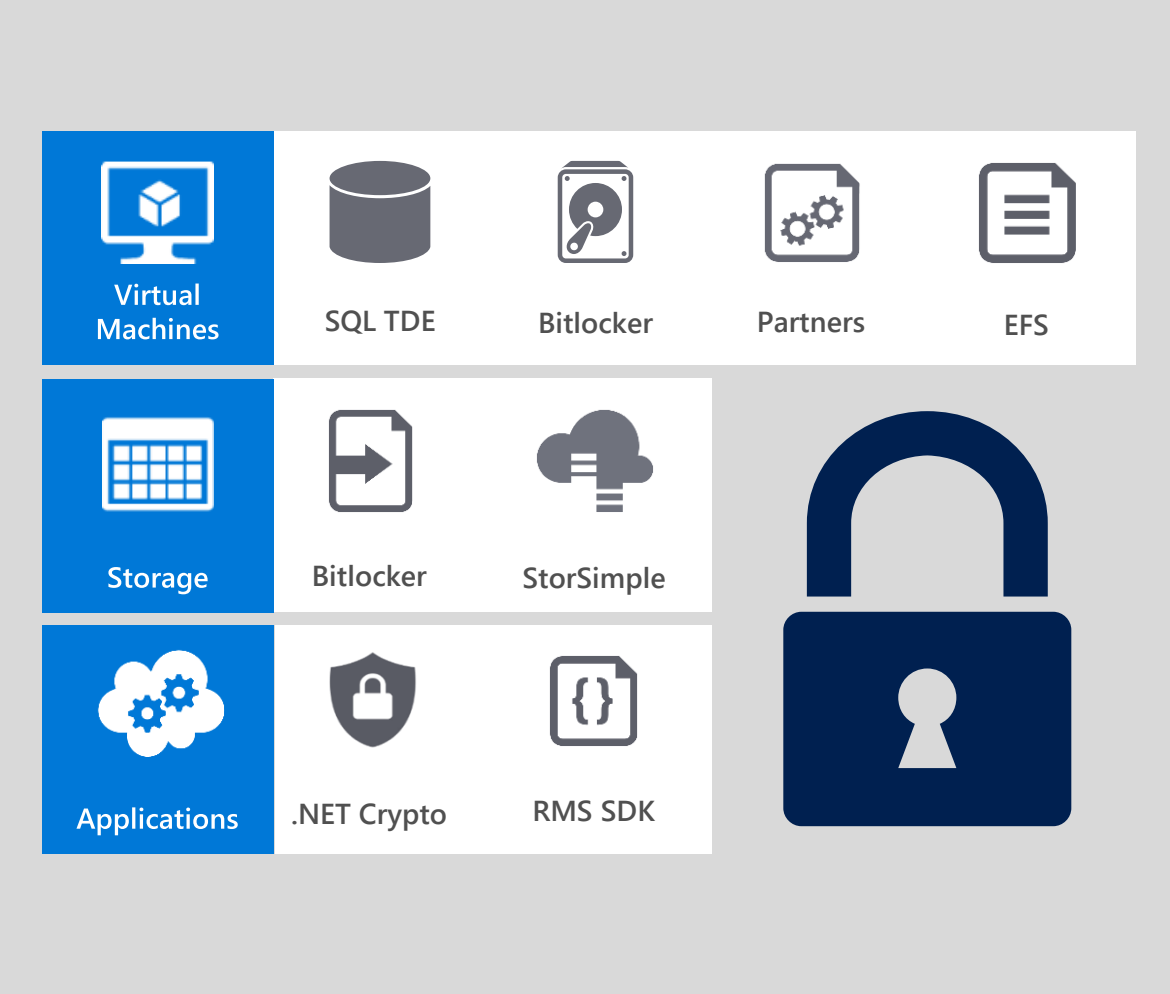
Azure

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

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

- Boot **and** Data drives—full disk encryption using BitLocker
- 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

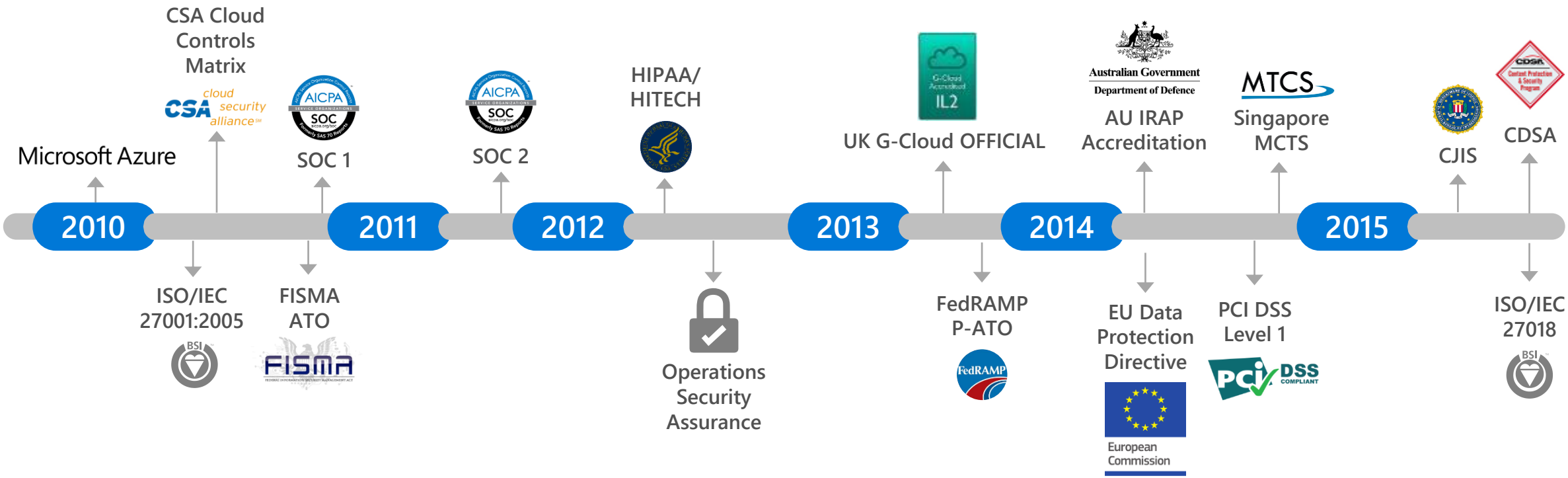
- Client Side encryption through .NET Crypto API
- RMS Service and SDK for file encryption by your applications

Compliance

Azure Compliance Framework

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

Extensive and growing experience



Data destruction

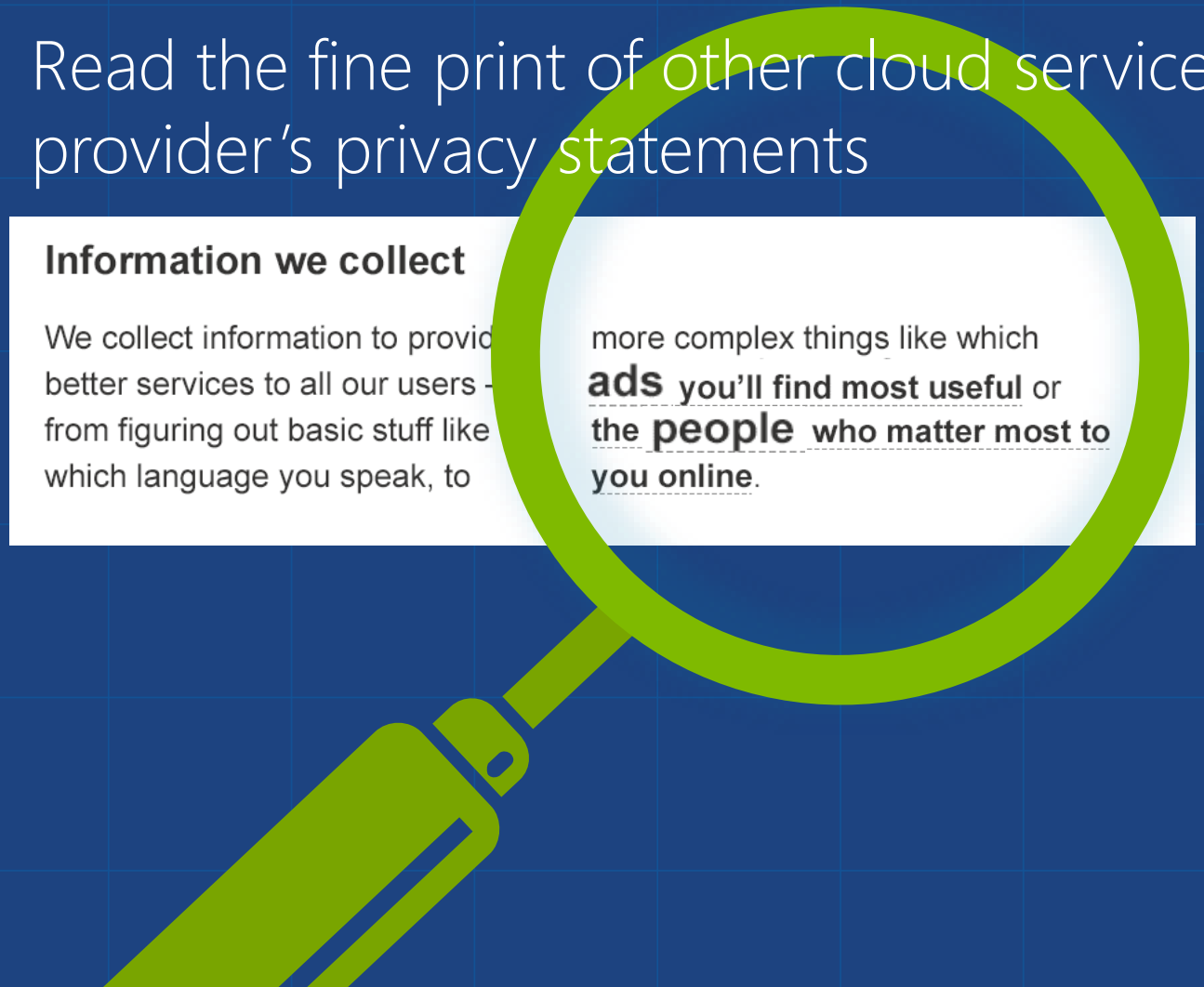
Data Deletion	• Index immediately removed from primary location • Geo-replicated copy of the data (index) removed asynchronously • Customers can only read from disk space they have written to
Disk Handling	• Wiping is NIST 800-88 compliant • Defective disks are destroyed

Data use policies

Azure does not share data with its advertiser-supported services

Azure does not mine Customer Data for advertising

Read the fine print of other cloud service provider's privacy statements



Mechanisms 4 u

Authentication and Access (4x)

- Portal access
  - Uses **Live ID** (Microsoft Account)
  - Go to http://manage.windowsazure.com
    - Role: Service Administrator or Co-Administrator
  - Uses special REST API without providing certificate
- Management certificate
  - **Certificate** can be self-signed
  - Does not check certificate expiration
  - Used by PowerShell
  - Used by REST API
- Storage access
  - Uses **secret** key
  - Or **anonymous** share access
- RDP VM access
  - Uses **username/password**

Authentication and Access … BUT…!

- Portal access
  - Uses **Live ID** (Microsoft Account) –> Better have **AAD / Org ID + MFA**
  - Implement **RBAC → JEA principle**
- Management certificate
  - ARE EVIL !!!!!
  - Only Use them in a management solution when that is the ONLY option!
- Storage access
  - I'v got the key … I've got ALL your Secrets
  - If needed? **IMPLEMENT KEY VAULT!**
- RDP VM access
  - Harden from the outside , and **access through GW / S2S / ER**
  - Better implement **SSH / PoSh Remoting over SSL**

Authentication and Access … BUT…!

- Automation
  - Use Service Principals

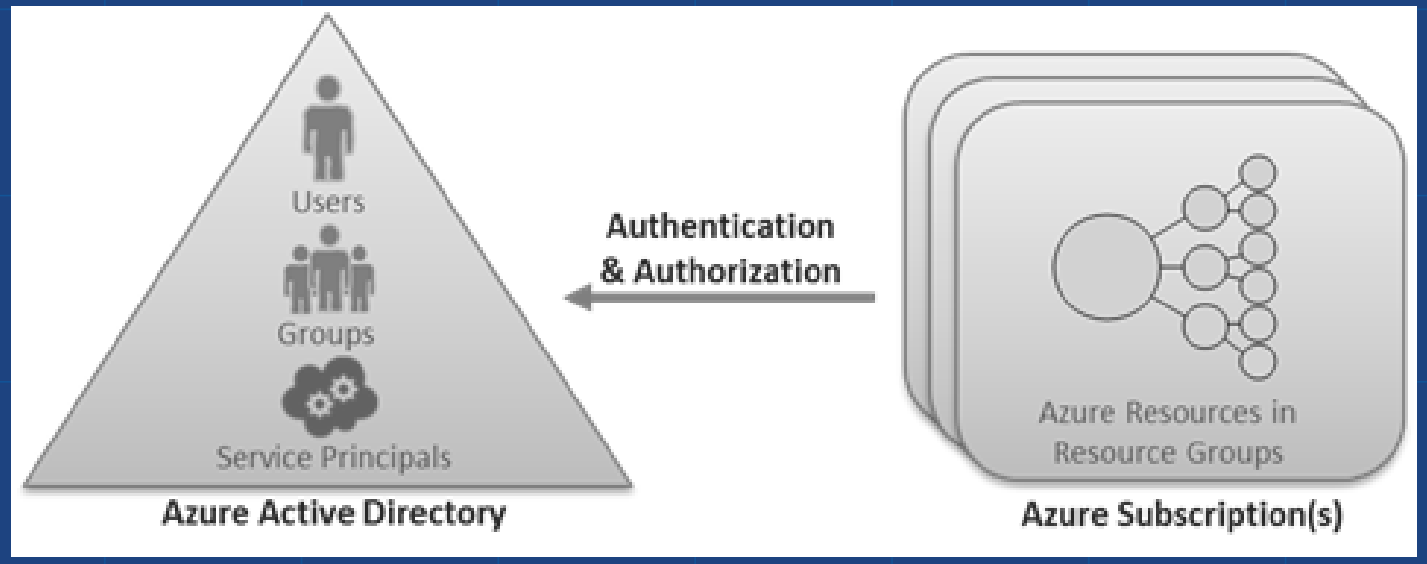
```
az login
az account set --subscription <Subscription ID>
az ad sp create-for-rbac
```

  - Use Managed Service Identity (MSI)
    - Per service authentication through AAD

https://docs.microsoft.com/en-us/azure/active-directory/managed-service-identity/overview

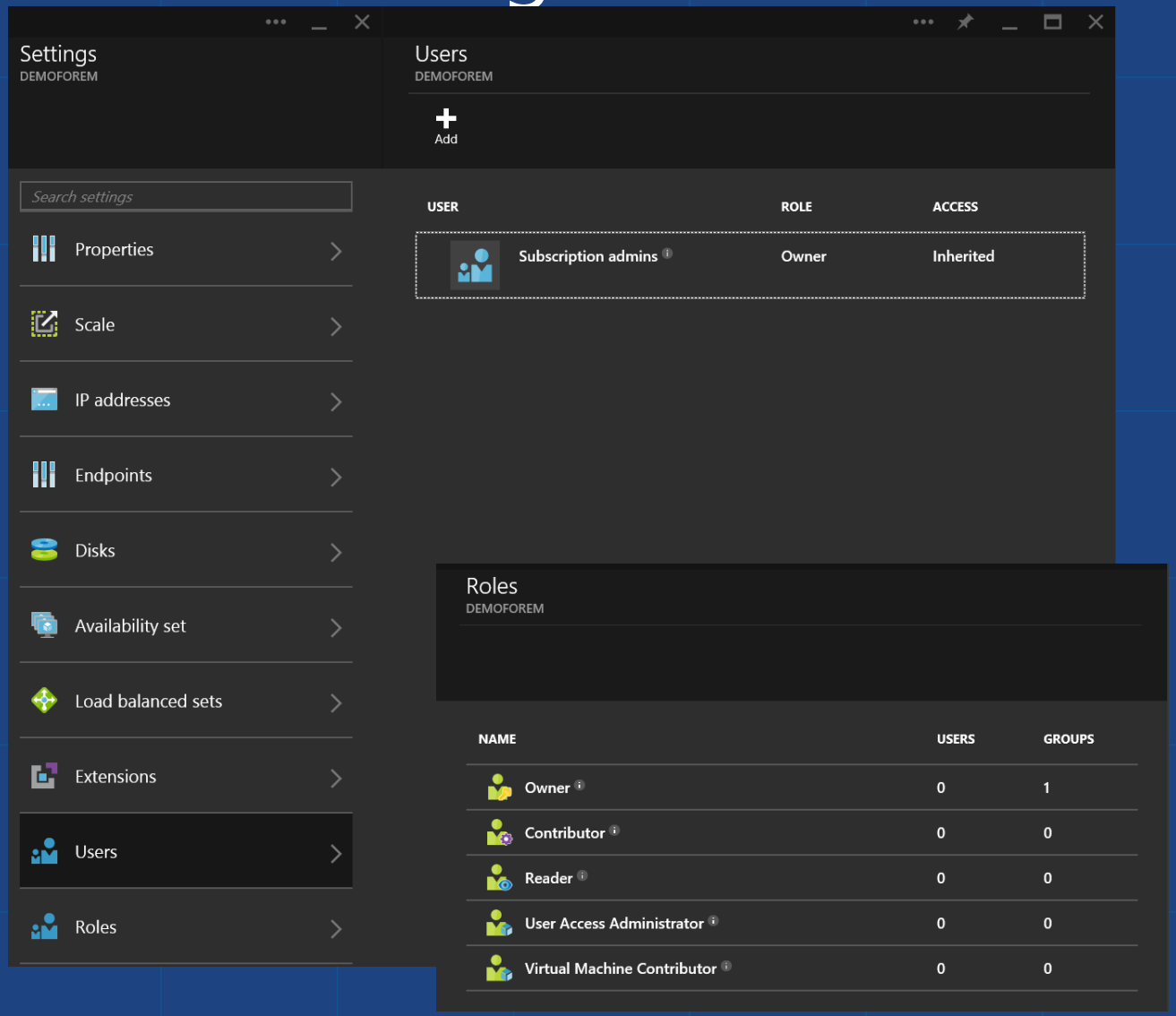
Role Based Access in Azure – aka RBAC

- **Role**
- Collection of actions
- **Role Assignment**
- Access is granted to AAD users and services role assignment on the resources.
- **Azure AD Security Principals**
  - Roles can be assigned to the following types of Azure AD security principals:
    - **Users**
    - **Groups**
    - **Service principals**



RBAC in Azure

- Portal Management

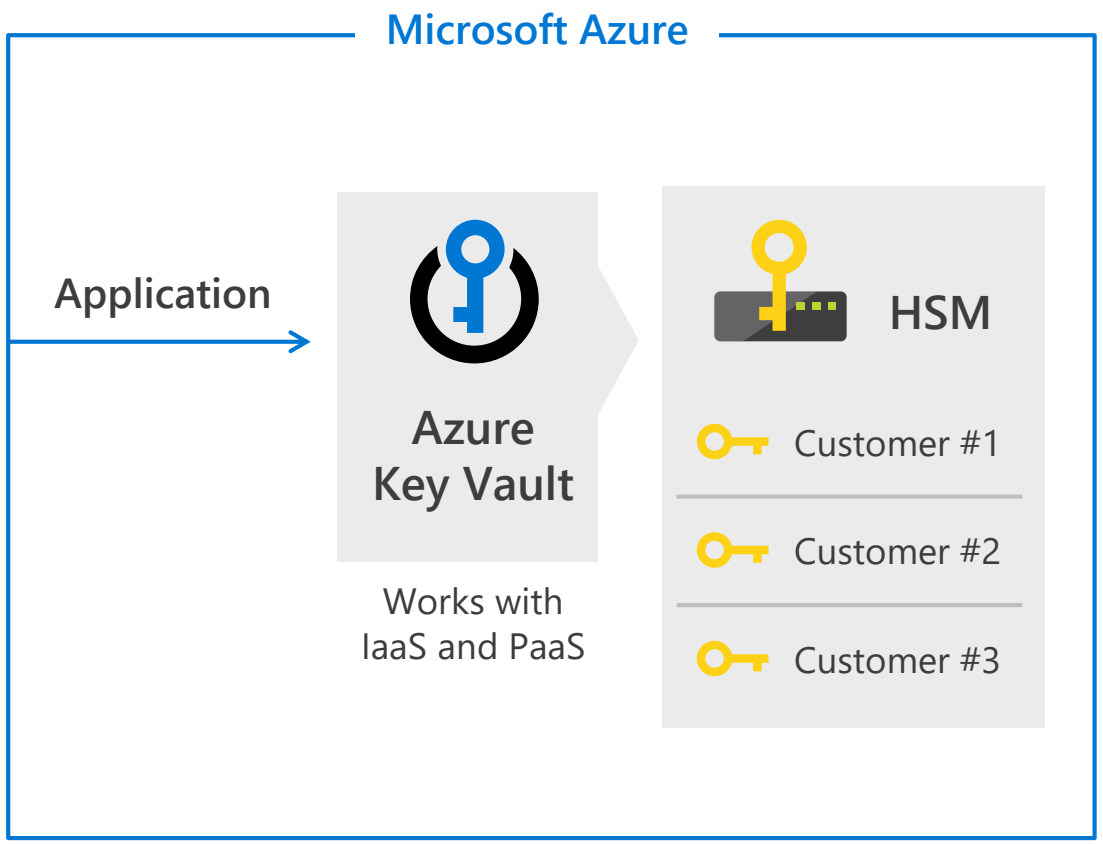


- Powershell

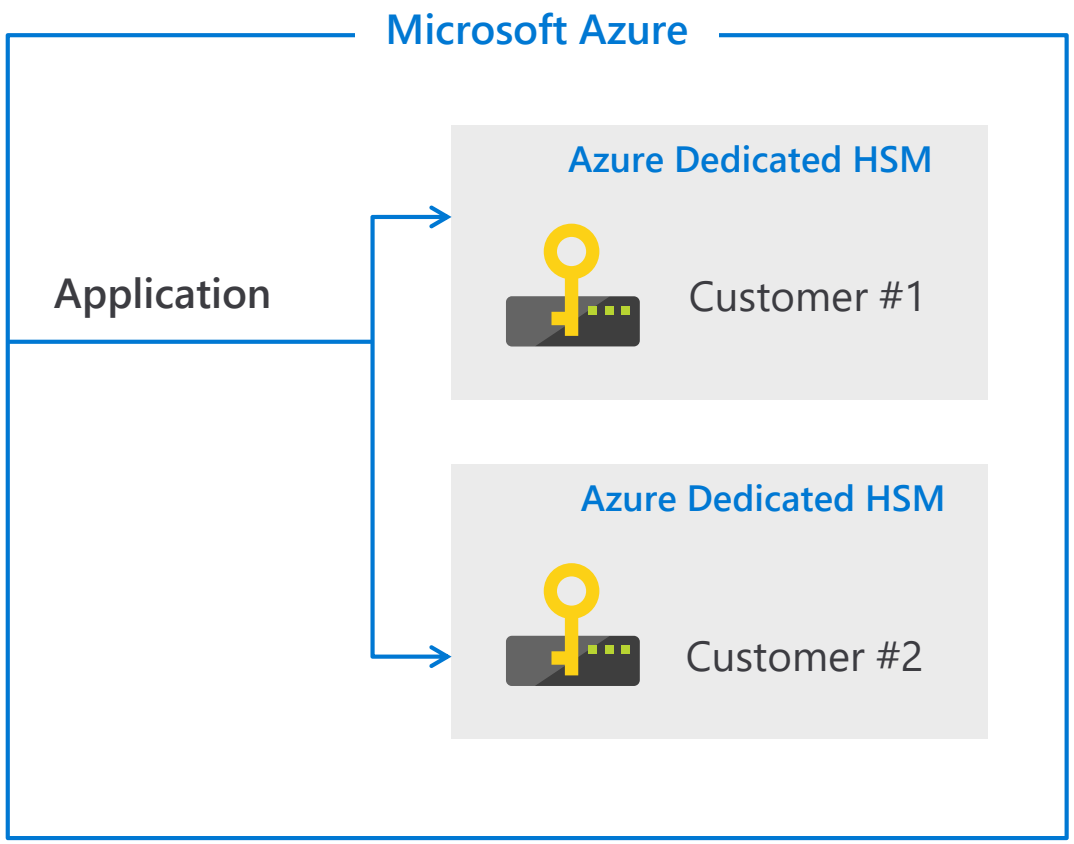
```
foreach ($roledef in Get-AzureRMRoleDefinition) {
    Write-Host 'Role: '$roledef.Name
    Write-Host 'Actions'
    (Get-AzureRMRoleDefinition -Name $roledef.Name).Actions
    Write-Host 'NoActions'
    (Get-AzureRoleRMDefinition -Name $roledef.Name).NoActions
    Write-Host ([Environment]::NewLine)
}
```

Key management offers

Existing public offer



New offer to address industry needs



When to use Azure Key Vault or Azure Dedicated HSM?

Azure Key Vault:

Scenario 1: Industry customers that need key management that is FIPS 140-2 Level 2 validated

Scenario 2: Applications that are running in the cloud, and need its keys need to be in an HSM

Scenario 3: Store keys that work with first-party or third-party PaaS and SaaS services running in Azure

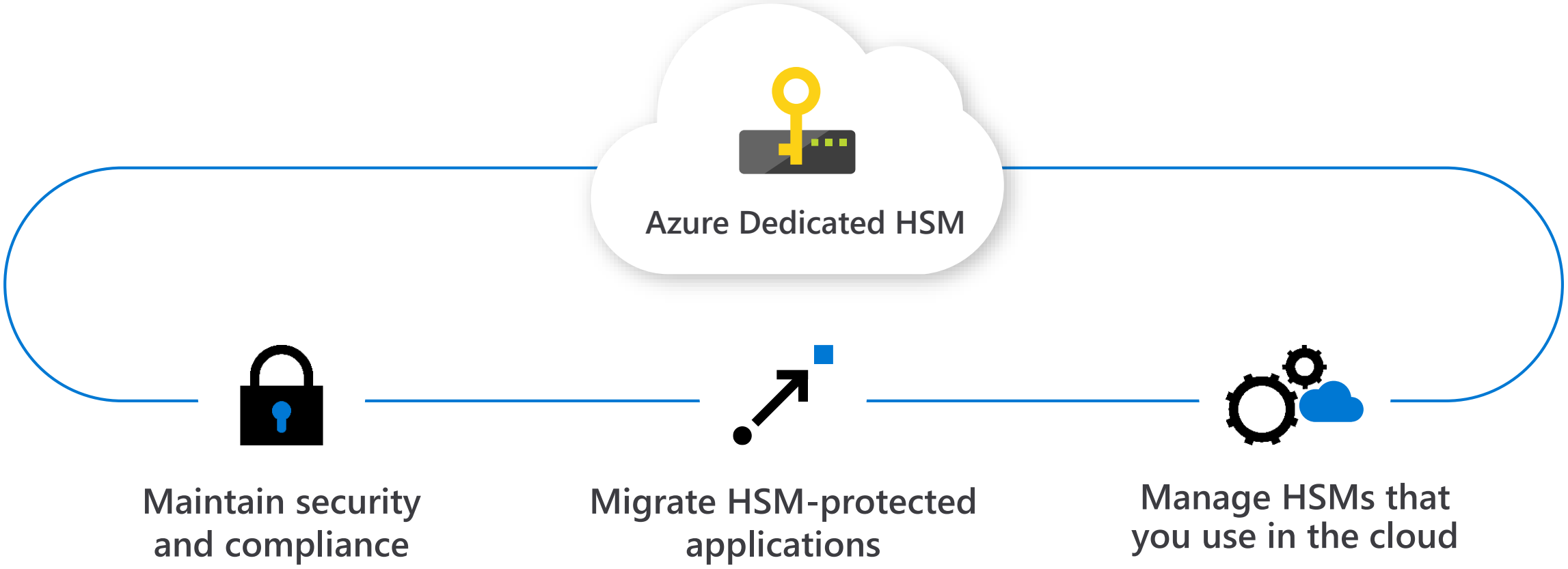
Azure Dedicated HSM:

Scenario 1: Customers in highly-regulated industries that need key management that is FIPS 140-2 Level 3 validated

Scenario 2: Migrating applications from on-premises or from other clouds to Azure

Scenario 3: Store keys for homegrown or legacy applications that are running in Azure

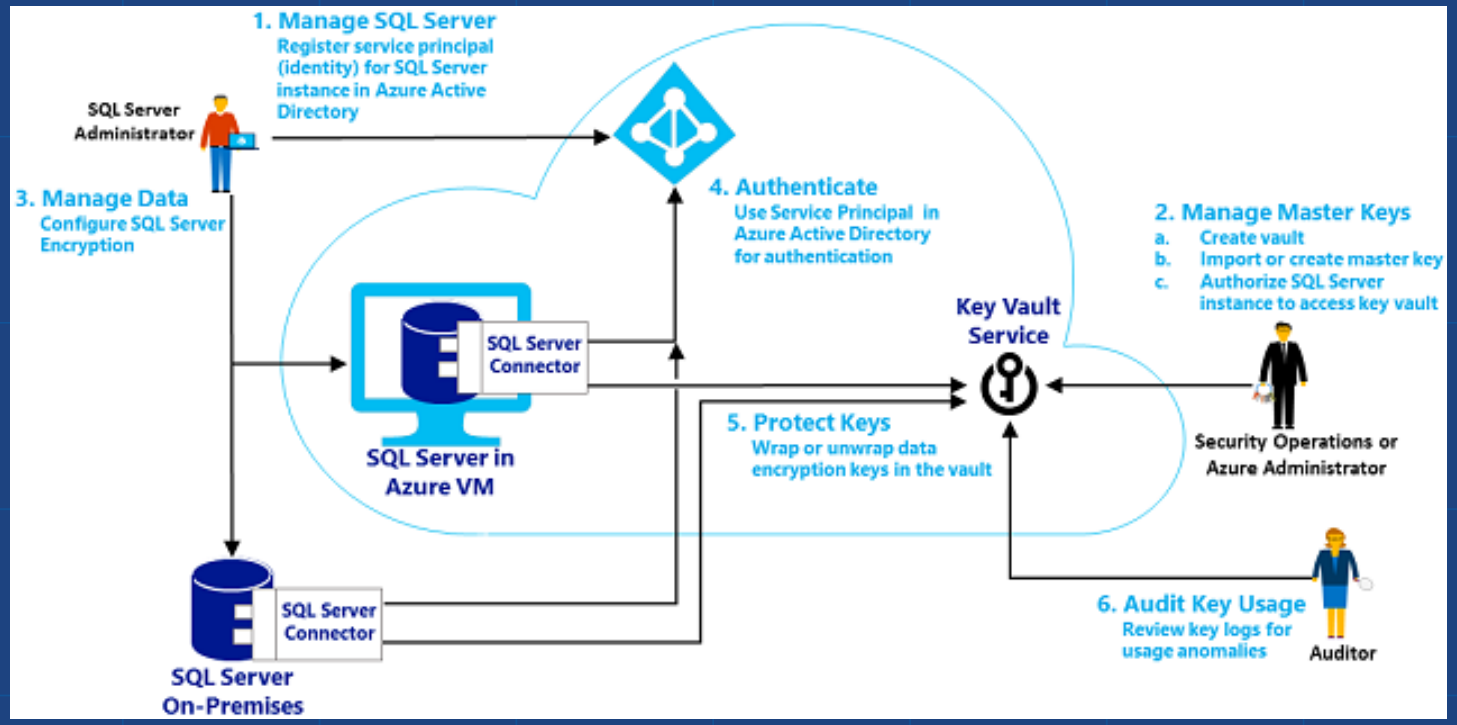
A hardware security module in the cloud that you manage



Microsoft Azure Key Vault

Safeguard cryptographic keys and other secrets used by cloud apps and services

- Increase security and control over keys and passwords
- Create and import encryption keys in minutes
- Applications have no direct access to keys
- Use FIPS 140-2 Level 2 certified HSMs
- Reduce latency with cloud scale and global redundancy



SQL Server Scenario

Applying to Azure - Infrastructure

- Port scanning: the only open ports are those defined by us!
- Denial of service:
  - External: depends on our settings, but the Fabric Controller tries to identify the attacks
  - Internal: all DOS attacks initiated from internal VMs will result in removing those VMs from the network
- Spoofing: compromised machines cannot impersonate VMs from the Fabric Controller (broadcast and multicast are blocked, https between VMs and FC)
- Sniffing: the Hyper-V switch prevents sniffing from a VM to another VM on the same host; racks switches block it to other VMs
- VMs are untrusted by the Root OS Hypervisor

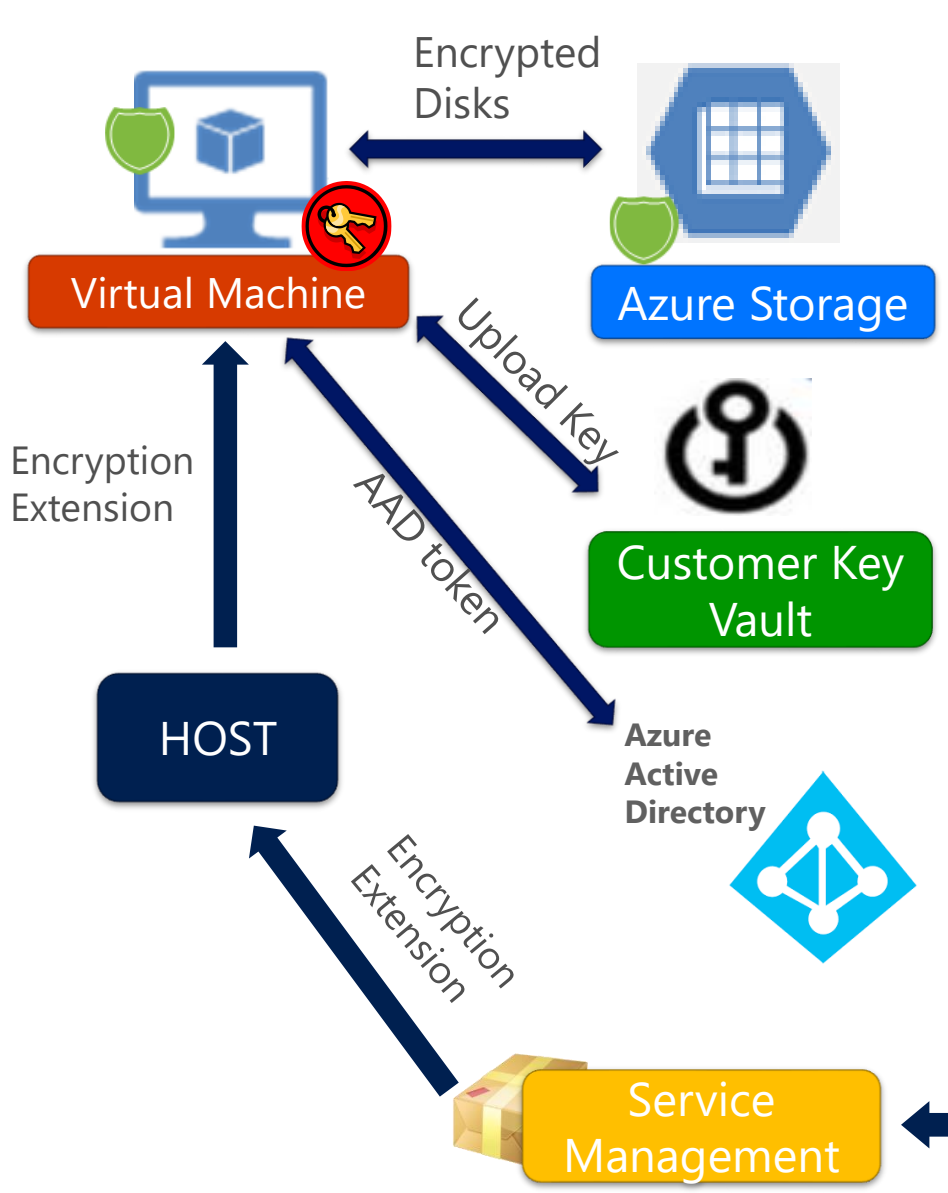
VM Security

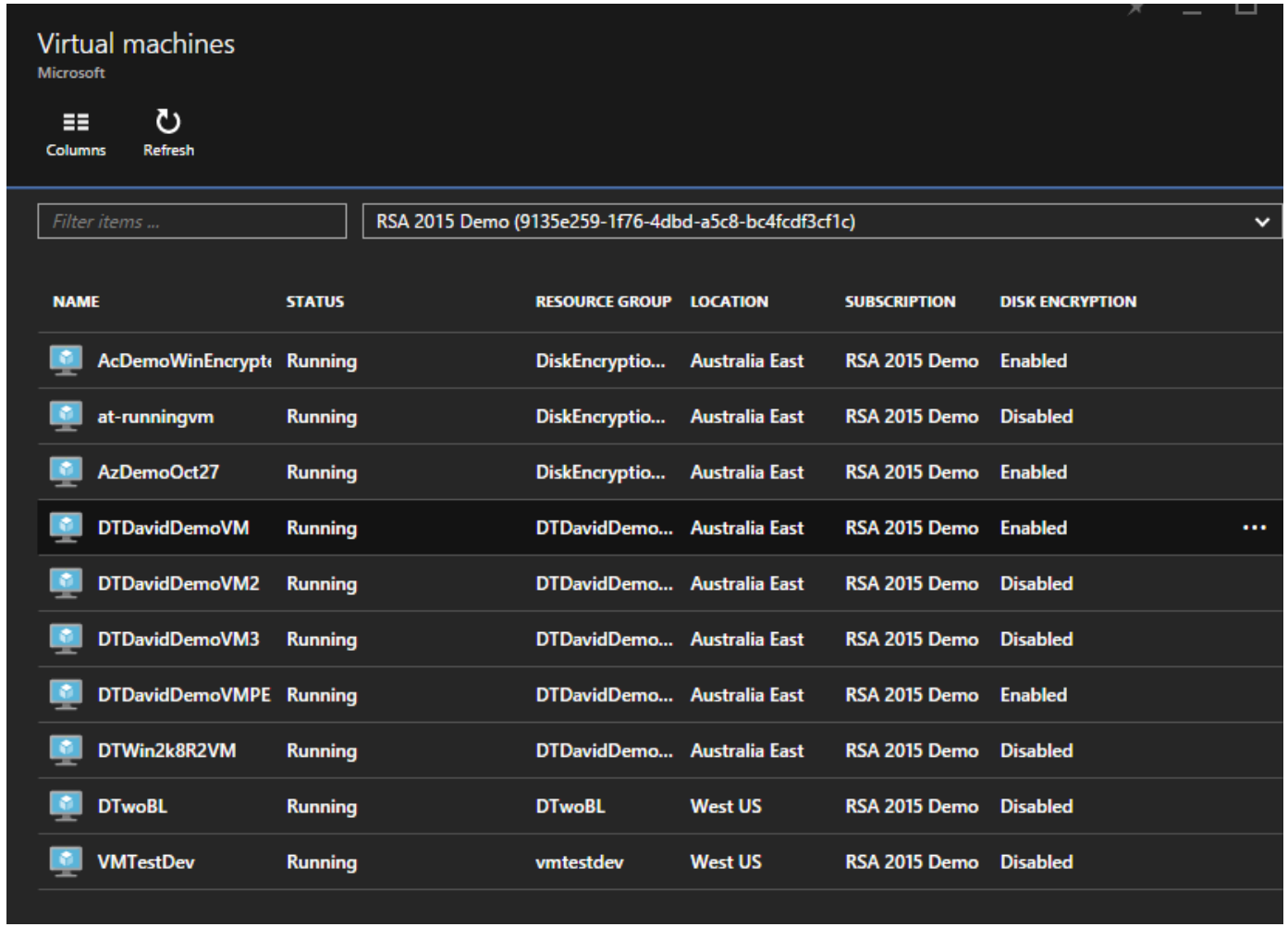
- Endpoints
- Antimalwae extensions
- Storage access
- Bitlocker Support on Disks
- Managed Identity Extension

Configuring Virtual Machine Security

- Firewall rules
  - Leveraging public/private/domain profiles
- Access control lists (ACL)
  - Controls port access through at subnet level
  - IP address blacklisting
  - VM endpoint rules (up to 50 per endpoint)
  - Rule ordering
- Encryption
  - DPAPI not supported for cloud service
  - Secure key data with encryption keys
  - CloudLink

Azure Disk Encryption – New VM or Running VM Workflow





NAME	STATUS	RESOURCE GROUP	LOCATION	SUBSCRIPTION	DISK ENCRYPTION
AcDemoWinEncrypt	Running	DiskEncryptio...	Australia East	RSA 2015 Demo	Enabled
at-runningvm	Running	DiskEncryptio...	Australia East	RSA 2015 Demo	Disabled
AzDemoOct27	Running	DiskEncryptio...	Australia East	RSA 2015 Demo	Enabled
DTDavidDemoVM	Running	DTDavidDemo...	Australia East	RSA 2015 Demo	Enabled
DTDavidDemoVM2	Running	DTDavidDemo...	Australia East	RSA 2015 Demo	Disabled
DTDavidDemoVM3	Running	DTDavidDemo...	Australia East	RSA 2015 Demo	Disabled
DTDavidDemoVMPE	Running	DTDavidDemo...	Australia East	RSA 2015 Demo	Enabled
DTWin2k8R2VM	Running	DTDavidDemo...	Australia East	RSA 2015 Demo	Disabled
DTwoBL	Running	DTwoBL	West US	RSA 2015 Demo	Disabled
VMTestDev	Running	vmtestdev	West US	RSA 2015 Demo	Disabled

Azure networking services

Virtual Network
Virtual WAN
ExpressRoute
VPN
DNS

DDoS Protection
Firewall
Network Security Groups
Web Application Firewall
Virtual Network Service Endpoints

Network Watcher
ExpressRoute Monitor
Azure Monitor
Virtual Network TAP
Azure Security Center
Azure Sentinel

CDN
Front Door
Traffic Manager
Application Gateway
Load Balancer

Endpoint ACL's

Using Network ACLs, you can do the following:

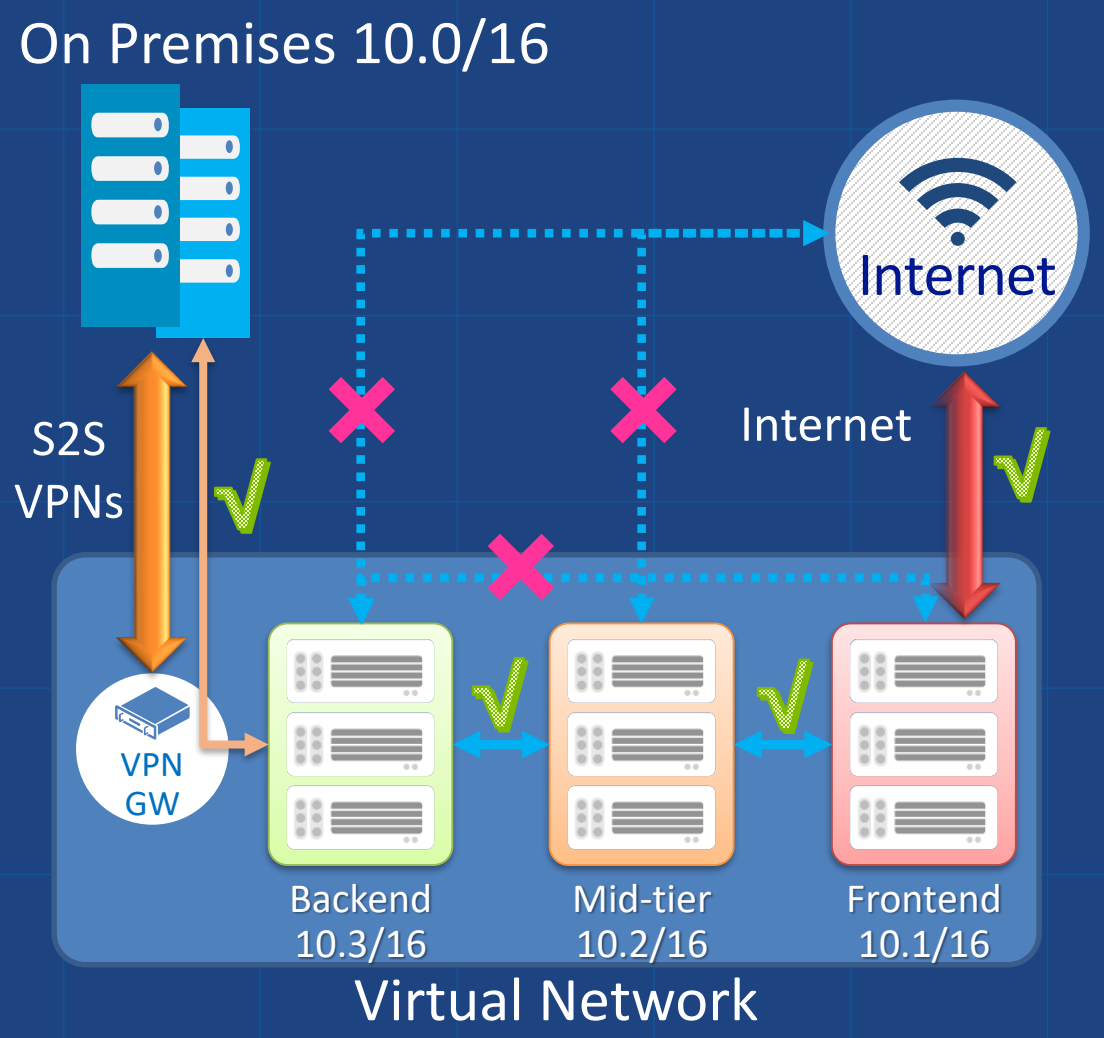
- Selectively permit or deny incoming traffic based on remote subnet IPv4 address range to a virtual machine input endpoint.
- Blacklist IP addresses
- Create multiple rules per virtual machine endpoint
- Specify up to 50 ACL rules per virtual machine endpoint
- Use rule ordering to ensure the correct set of rules are applied on a given virtual machine endpoint (lowest to highest)
- Specify an ACL for a specific remote subnet IPv4 address.

Network Security Groups (NSG)

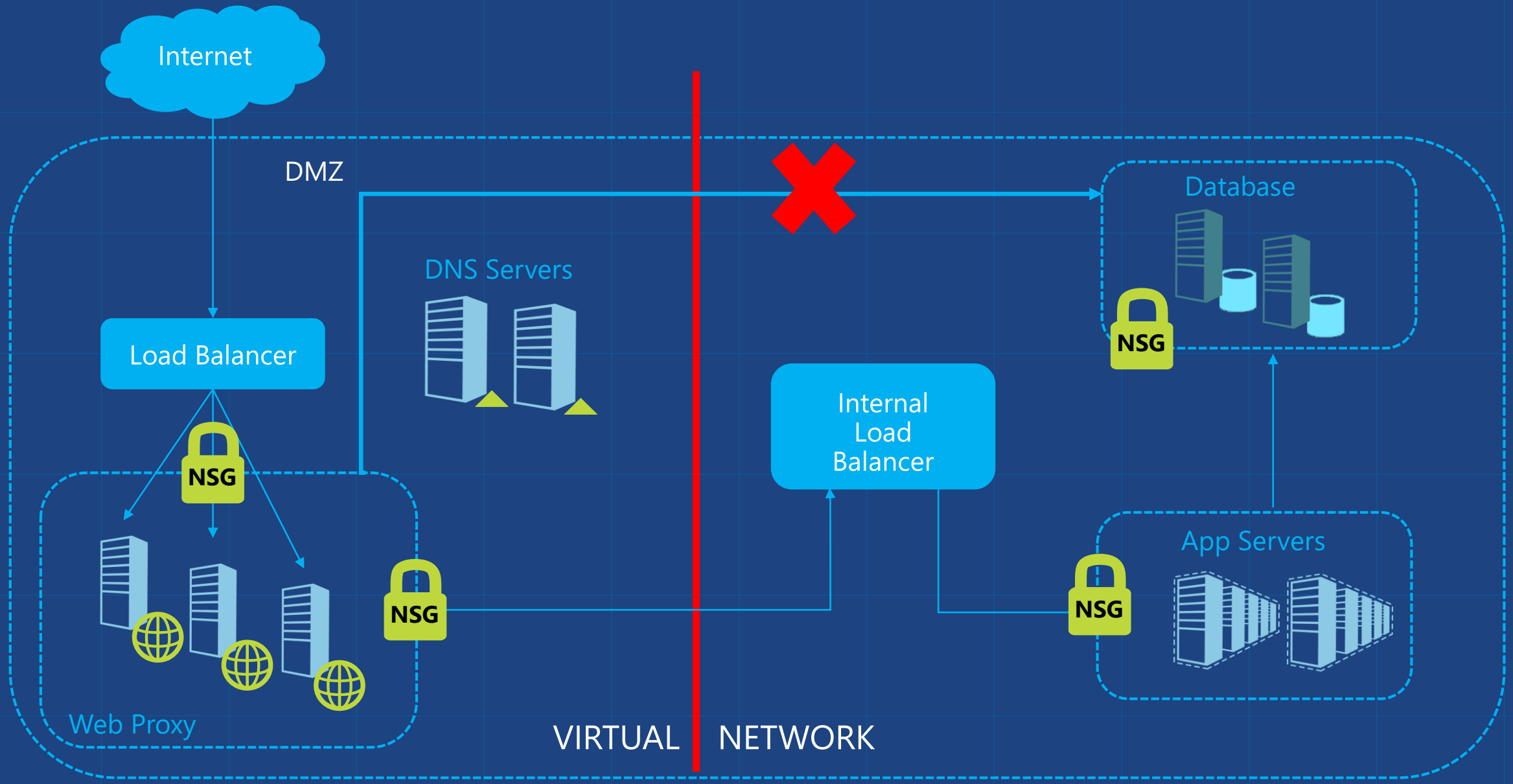
- Enables network segmentation & DMZ scenarios
- Access Control List
  - Filter conditions with allow/deny
  - Individual addresses, address prefixes, wildcards
- Associate with VMs or subnets
- ACLs can be updated independent of VMs

- Network Security Groups (NSGs) for Layer 3 and Layer 4 filtering
- Eases IP management for VNet firewall rules

- VIRTUAL_NETWORK tag includes IPs for:
  - Virtual network
  - All connected, peered networks
  - On-premises



DMZ in a Virtual Network

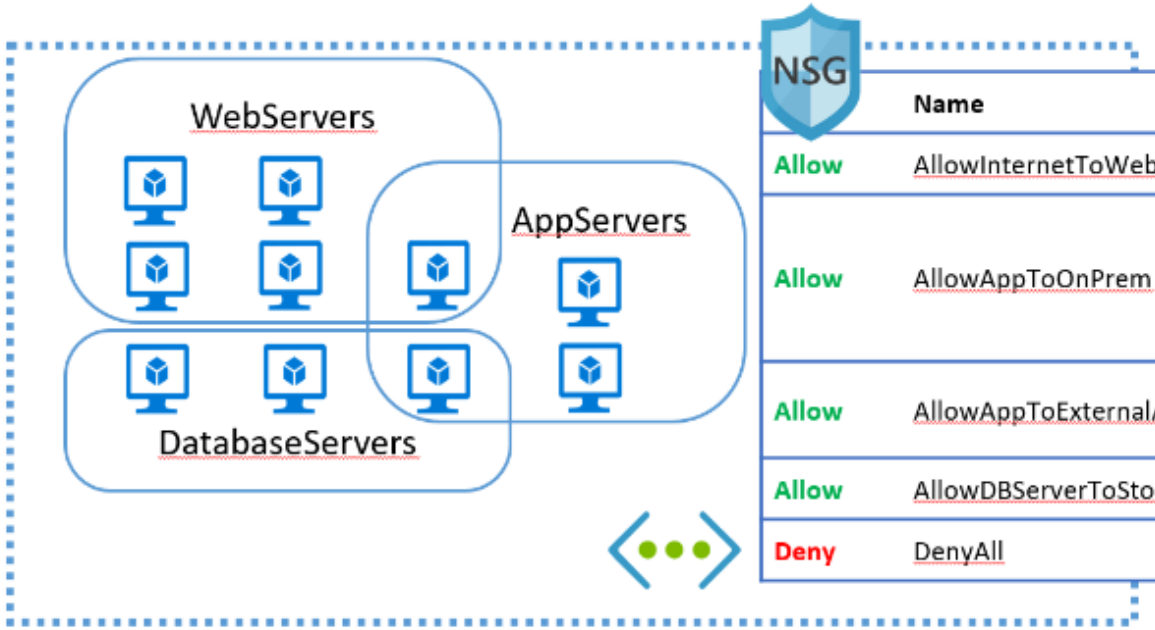


Security considerations when using NSG

- Endpoint ACLs and Network Security Groups don't work together
- Multi-NIC : for now the Network Security Group rules apply only to the traffic in primary NIC
- For RDP endpoints for VM's and Network Security Group : NSG does not allow access to any port from Internet, you have to create a specific rule to allow RDP traffic.

Simplified NSG Management

- Application Security Groups: User-defined VM groups for NSG rules
- Augmented NSG Rules: Multiple IP addresses, ports in a single NSG rule



	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,8080 (HTTP)
Allow	AllowAppToOnPrem	AppServers	10.10.128.0/22, 10.20.36.0/20, 192.168.65.0/20, 192.168.10.0/24	22, (SSH) 21, (FTP) 3389, (RDP) 3306 (MySQL)
Allow	AllowAppToExternalAPI	AppServers	148.234.0.0/16, 190.22.33.8/30	443 (HTTPS)
Allow	AllowDBServerToStorage	DatabaseServers	Storage	Any
Deny	DenyAll	Any	Any	Any

Application Gateway

Level 7 routing

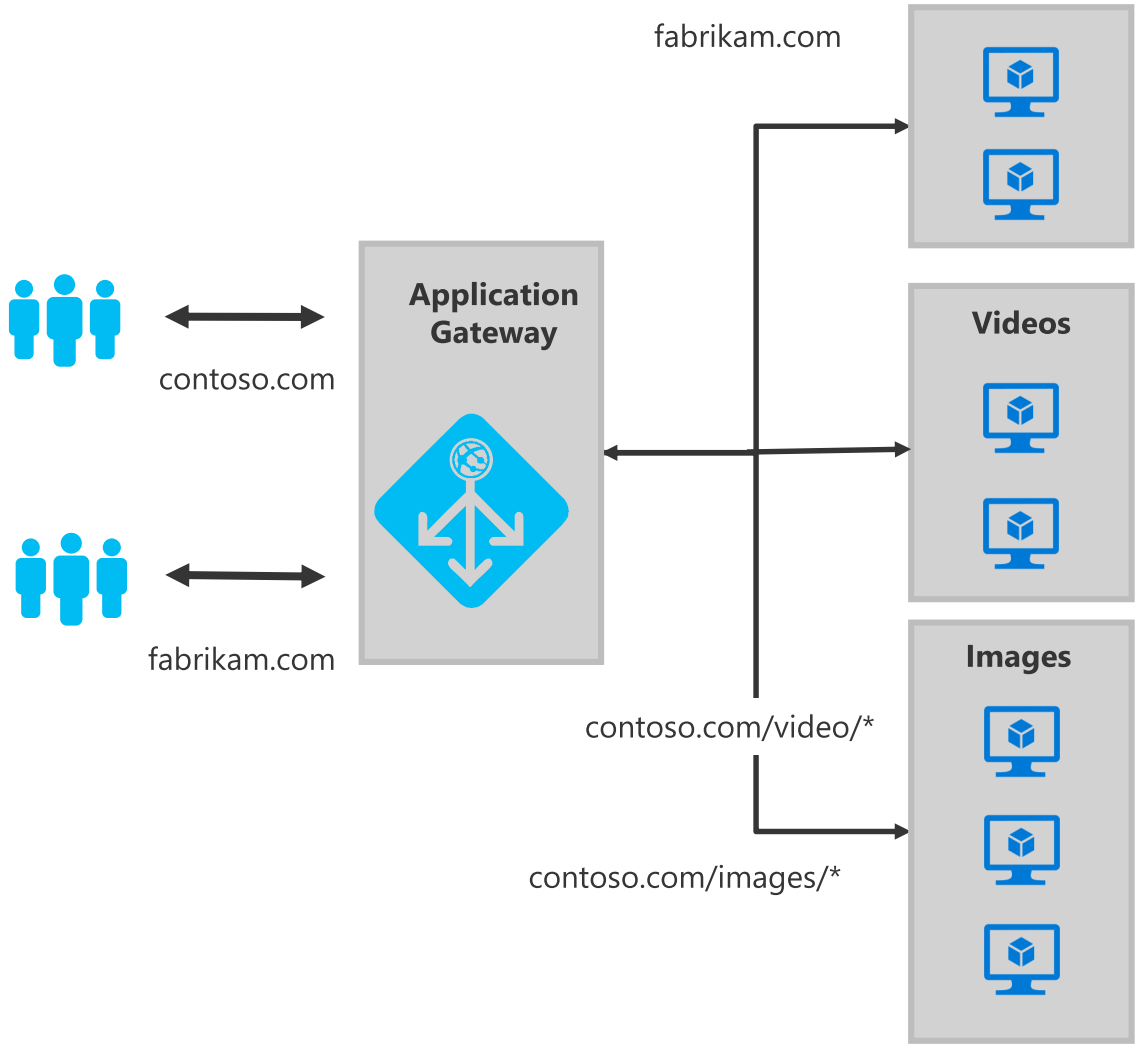
- HTTP round robin
- Cookie based session affinity
- Multi-site hosting
- URL based routing

Security

- SSL termination
- SSL Policy (protocol version and cipher)
- End to end SSL
- Web Application Firewall

Diagnostics and probes

- Rich diagnostics including access and performance logs, WAF logs, backend health log
- Custom health probes



Web Application Firewall (WAF)

Protect applications from web based intrusions

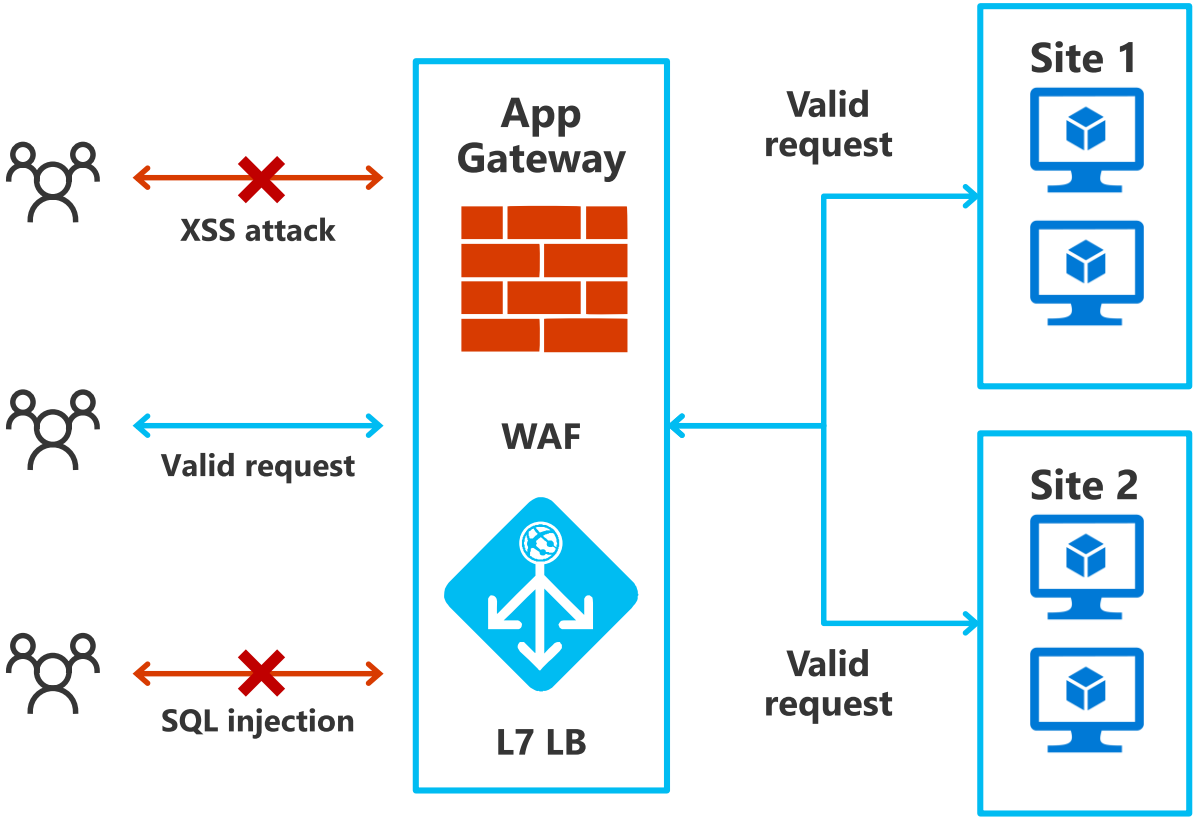
Highly available, scalable, fully platform managed

Built using popular ModSecurity Core Rule Set

- CRS 2.2.9
- CRS 3.0

Preconfigured rule set for baseline protection from OWASP top 10 vulnerabilities

- SQL Injection
- XSS attacks



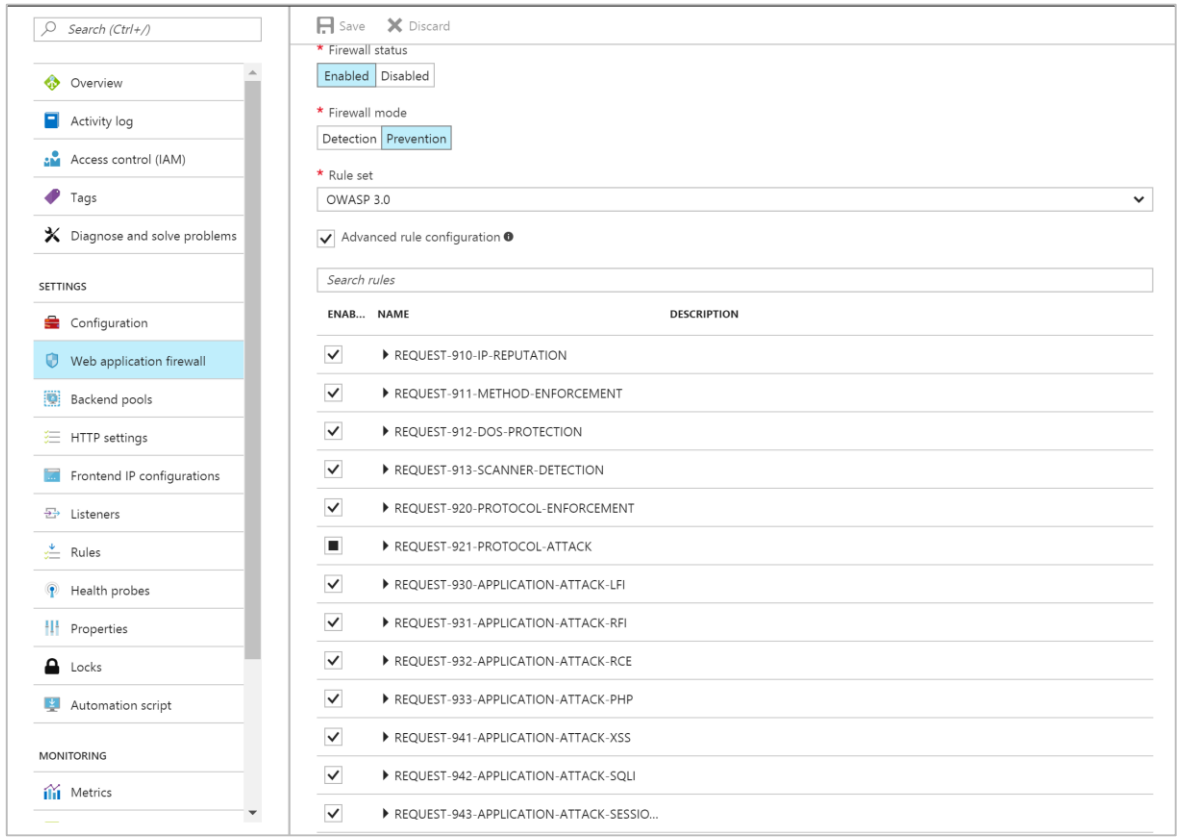
WAF preconfigured rules

RuleSet offered:

- CRS 2.2.9
- CRS 3.0

Protect from:

- SQL Injection
- Cross site scripting
- Protocol violations
- Generic attacks
- HTTP rate limiting
- Scanner detection
- Session fixation
- LFI/RFI



Monitor intrusions

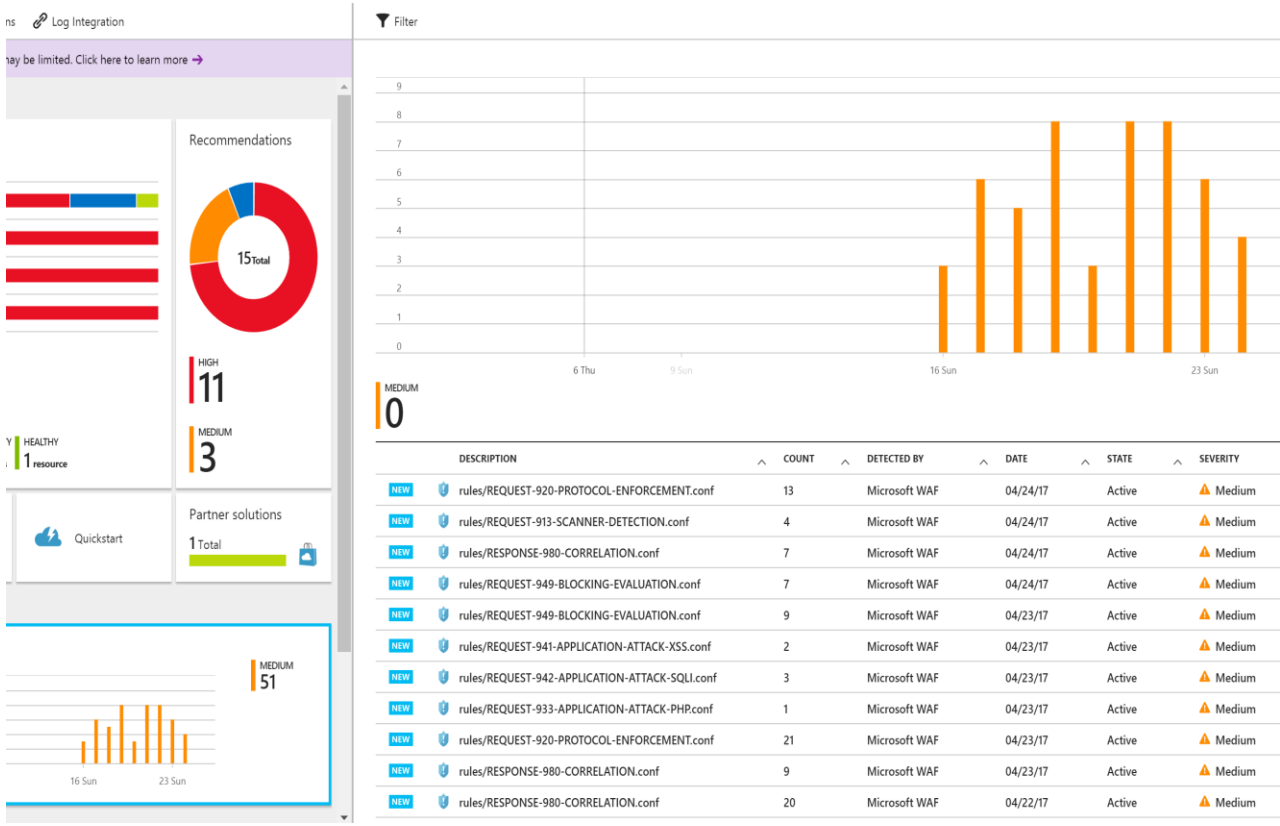
Enable WAF log via Azure Monitor

Real time logs to monitor attacks

WAF logs integrated with:

- Customer storage account in JSON format
- Event Hub
- OMS Log Analytics enabling search

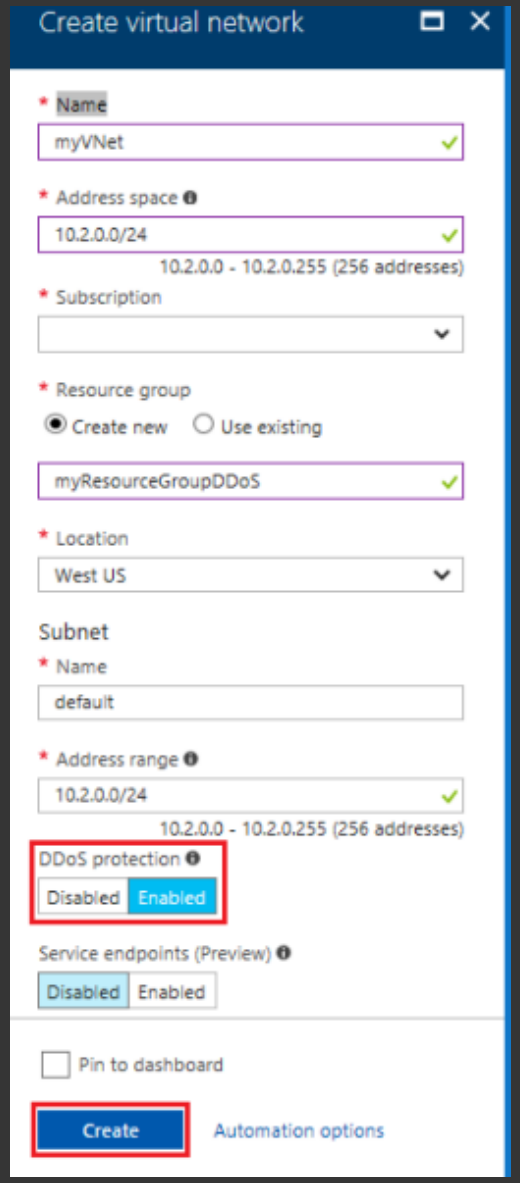
Azure Security Center Integration



Azure DDoS Protection Standard

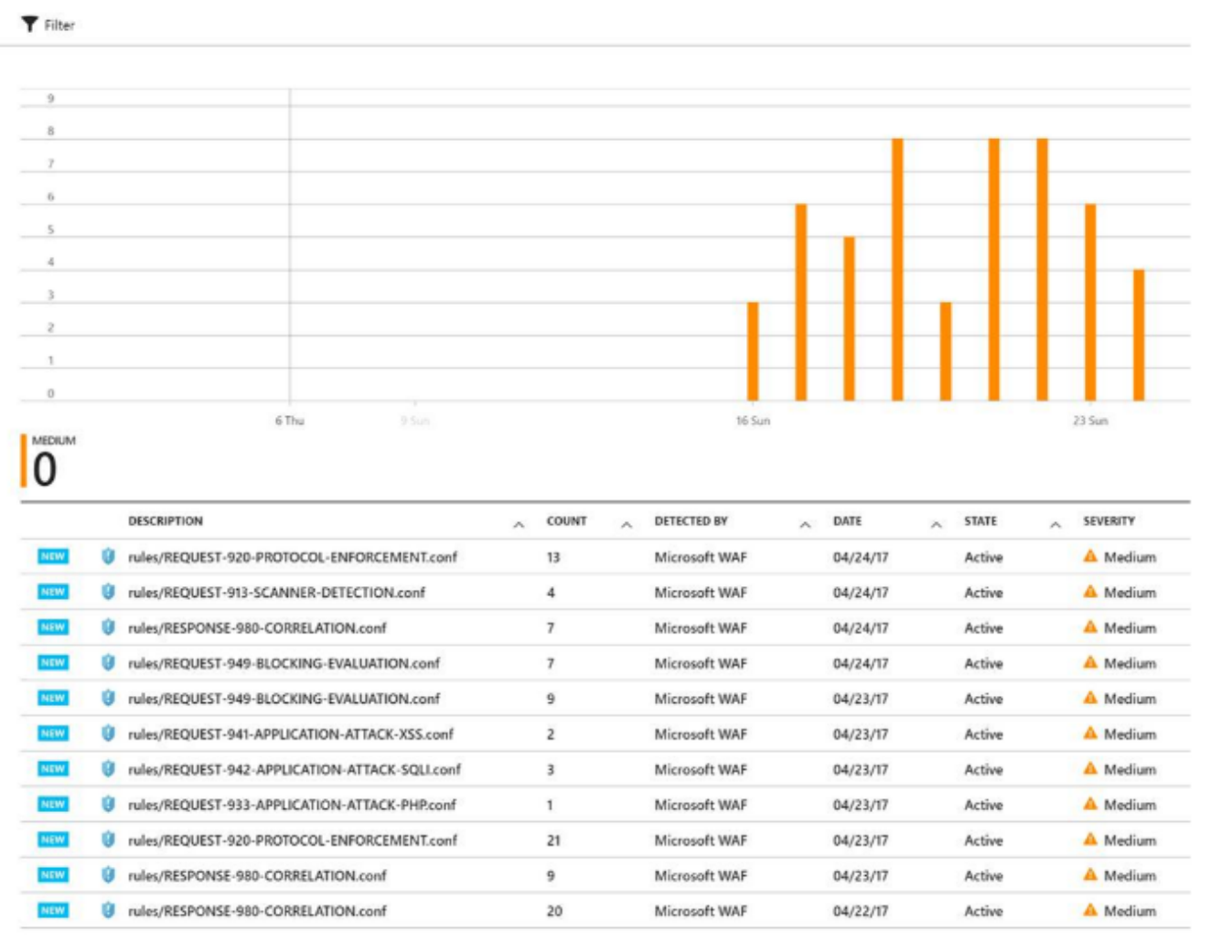
- Advanced protection for your virtual networks
- Automatic mitigation for attacks

Basic	Feature	Standard
✓	Always on monitoring	✓
✓	Automatic mitigation for Layer 3/4 attacks	✓
✓	L7 Protection with AppGW WAF	✓
	Protection policies tuned to your VNet	✓
	Logging, alerting, and telemetry	✓
	Resource cost scale protection	✓



Improved Auditing & Metrics

- ✓ NSG Data plane logs
- ✓ NSG Data plane analytics
- ✓ DDoS metrics and logs
- ✓ WAF Diagnostics logs



	DESCRIPTION	COUNT	DETECTED BY	DATE	STATE	SEVERITY
NEW	rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf	13	Microsoft WAF	04/24/17	Active	Medium
NEW	rules/REQUEST-913-SCANNER-DETECTION.conf	4	Microsoft WAF	04/24/17	Active	Medium
NEW	rules/RESPONSE-980-CORRELATION.conf	7	Microsoft WAF	04/24/17	Active	Medium
NEW	rules/REQUEST-949-BLOCKING-EVALUATION.conf	7	Microsoft WAF	04/24/17	Active	Medium
NEW	rules/REQUEST-949-BLOCKING-EVALUATION.conf	9	Microsoft WAF	04/23/17	Active	Medium
NEW	rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf	2	Microsoft WAF	04/23/17	Active	Medium
NEW	rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf	3	Microsoft WAF	04/23/17	Active	Medium
NEW	rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf	1	Microsoft WAF	04/23/17	Active	Medium
NEW	rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf	21	Microsoft WAF	04/23/17	Active	Medium
NEW	rules/RESPONSE-980-CORRELATION.conf	9	Microsoft WAF	04/23/17	Active	Medium
NEW	rules/RESPONSE-980-CORRELATION.conf	20	Microsoft WAF	04/22/17	Active	Medium

Services in a Virtual Network

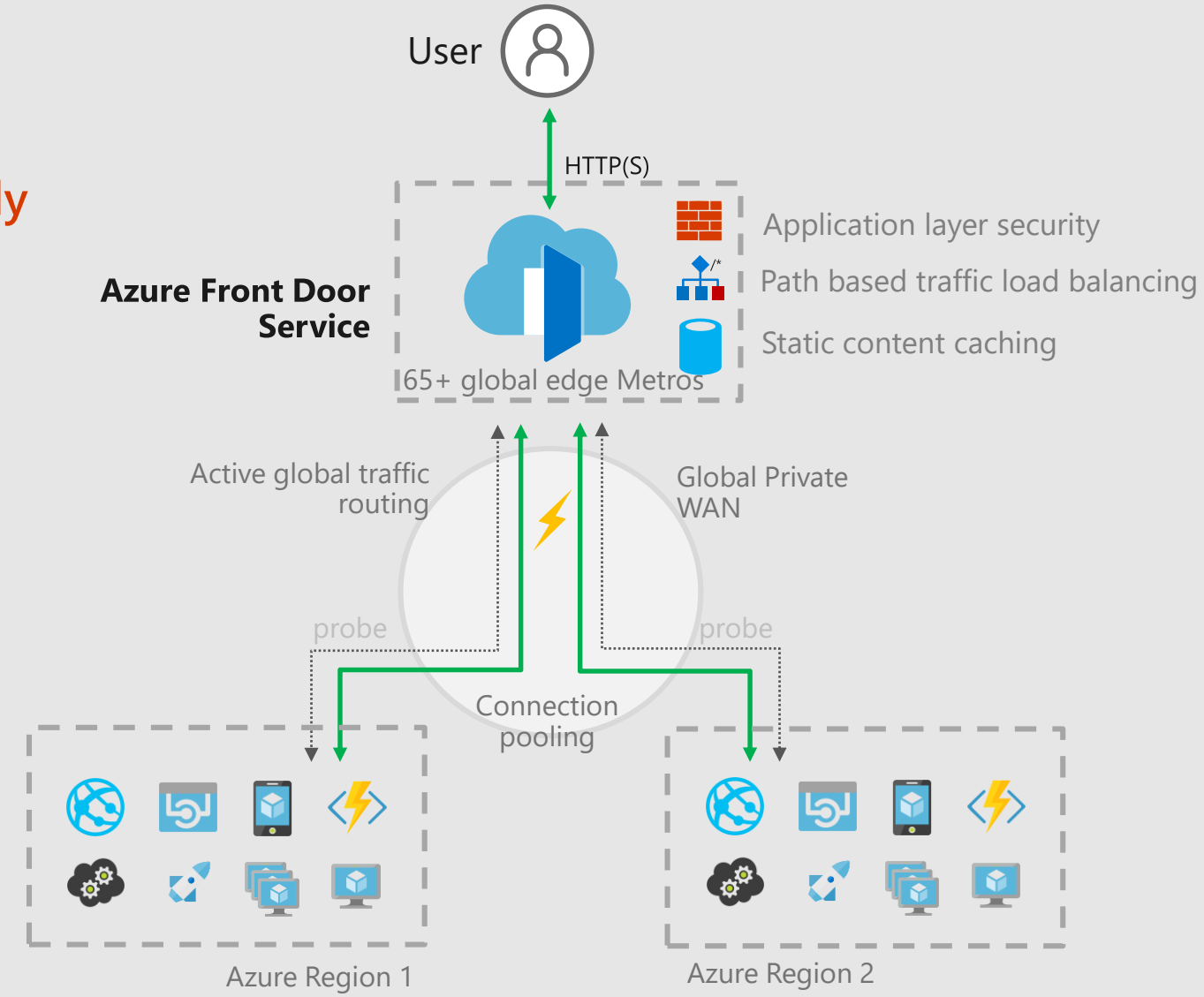
Deploy into Virtual Network	VNet Service Endpoints
SQL DB Managed Instance Azure Active Directory Domain Services for ARM Azure Batch for ARM Azure App Service V2 Azure API Management Azure Batch for ASM VNets HDInsight Azure App Service V1 RedisCache	Azure Storage Azure SQL Database

And more services where that came from…

Azure Front Door Service

Your secure entry point for delivering globally performant hyperscale apps.

- ✓ Global HTTP load balancing with instant failover
- ✓ Application acceleration at Microsoft's edge
- ✓ L4 DDoS protection + WAF @ Edge
- ✓ Massive SSL offload
- ✓ Integrated static content caching
- ✓ Domain and certificate management
- ✓ Integration with various Azure resources
- ✓ Central application traffic dashboard
- ✓ Traffic insights



DATA PLATFORM - LAYERS OF PROTECTION

Azure Active Directory

Centrally manage and control identity and user access

Encryption

Encrypt a database, associated backups, and log files at rest—without changing your app

Data protection

Protect data at rest, in motion, or in use

Row-Level Security

Control which users can access specific row-level data

Auditing and threat detection

Get notified of potential threats with auditing tools and anomalous activity alerting

Regulatory compliance

Leverage ISO/IEC 27001/27002, Fed RAMP/FISMA, SOC, HIPPA, and PCI DSS compliance

AZURE ACTIVE DIRECTORY AUTHENTICATION

Overview

Manage user identities in one location

Enable access to Azure SQL Database and other Microsoft services with Azure Active Directory user identities and groups

Benefits

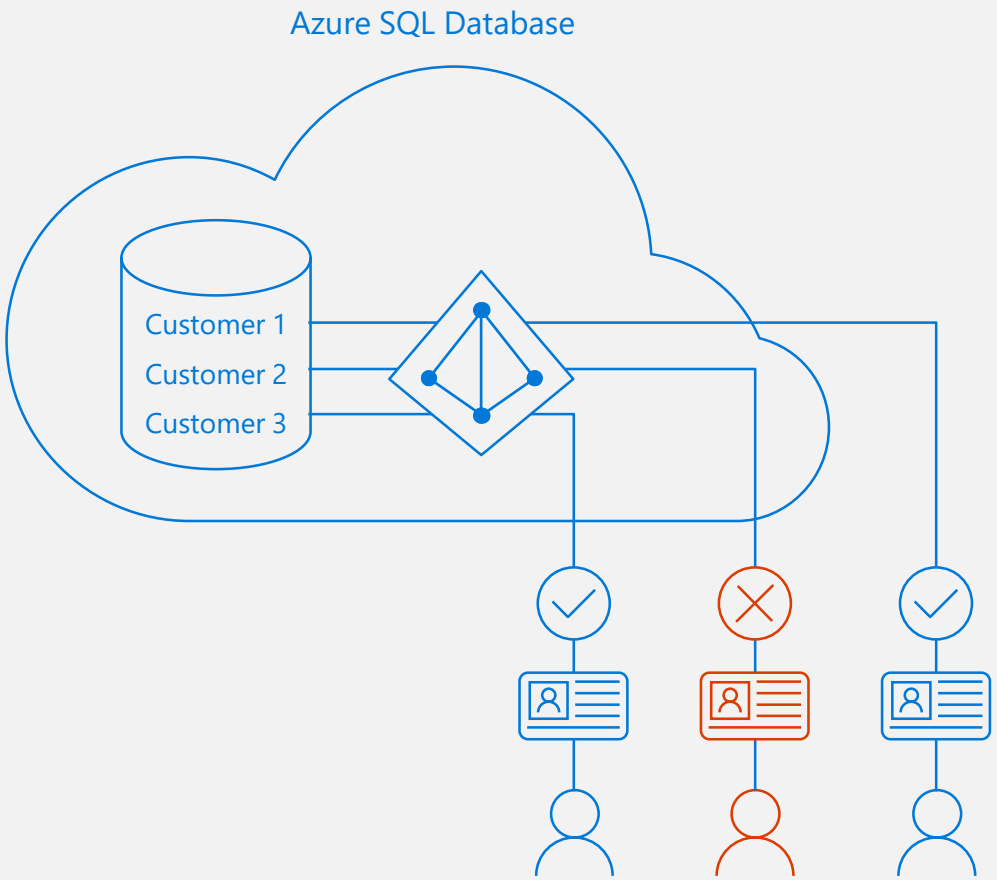
Alternative to SQL Server authentication

Limits proliferation of user identities across databases

Allows password rotation in a single place

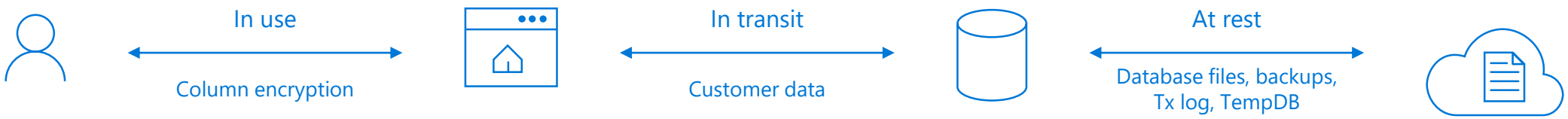
Enables management of database permissions by using external Azure Active Directory groups

Eliminates the need to store passwords



TYPES OF DATA ENCRYPTION

Data encryption	Encryption technology	Customer value
In transit	Transport Layer Security (TLS) from the client to the server	Protects data between client and server against snooping and man-in-the-middle attacks *Azure SQL Database is phasing out Secure Sockets Layer (SSL) 3.0 and TLS 1.0 in favor of TLS 1.2
At rest	Transparent Data Encryption (TDE) for Azure SQL Database	Protects data on the disk Key management is done by Azure, which makes it easier to obtain compliance
In use (end-to-end)	Always Encrypted for client-side column encryption	Data is protected end-to-end, but the application is aware of encrypted columns This is used in the absence of data masking and TDE for compliance-related scenarios



TRANSPARENT DATA ENCRYPTION

All customer data encrypted at rest

Encryption keys managed by Azure

Application changes kept to a minimum

Transparent encryption/decryption of data in a TCE-enabled client driver

Support for equality operations (including joins) on encrypted data

ALWAYS ENCRYPTED

Overview

Protect data at rest and in motion, on premises and in the cloud

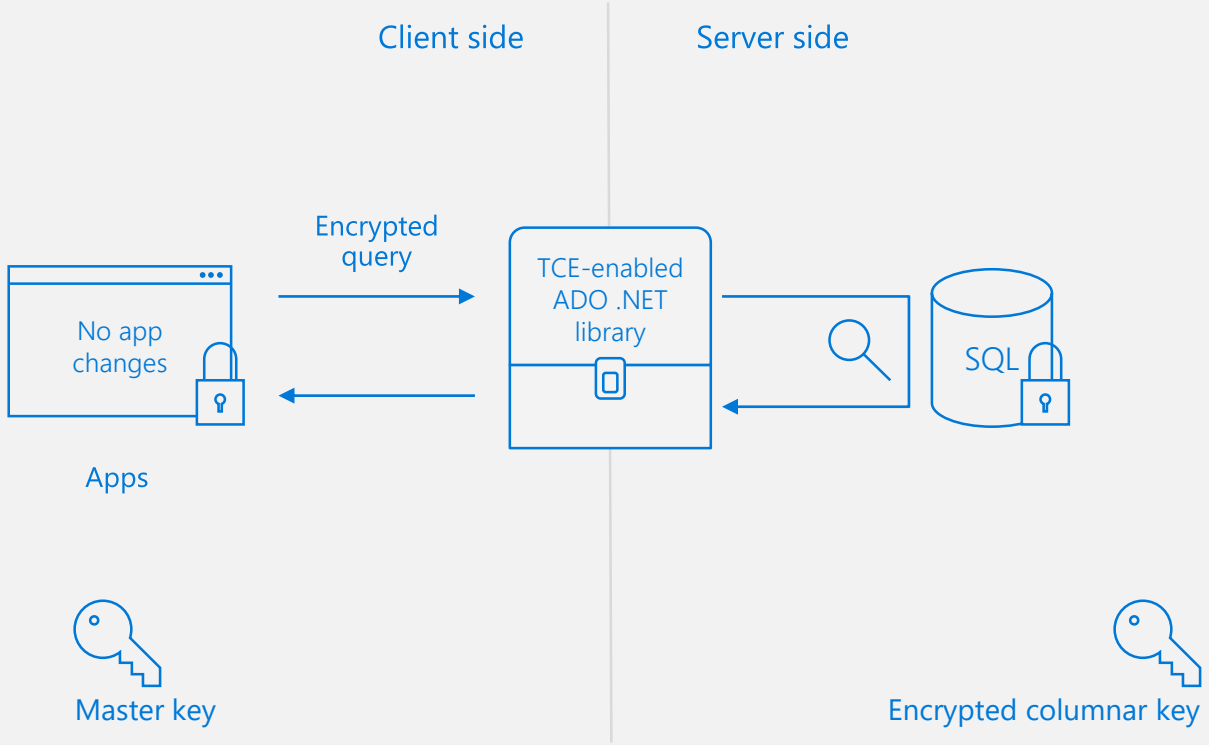
Transparent client-side encryption, while SQL Server executes T-SQL queries on encrypted data

Benefits

Sensitive data remains encrypted and queryable at all times on-premises and in the cloud

Unauthorized users never have access to data or keys

No application changes



CONFIDENTIAL COMPUTING

Overview

Confidential computing allows data to be protected inside a Trusted Execution Environment (TEE), also known as an enclave

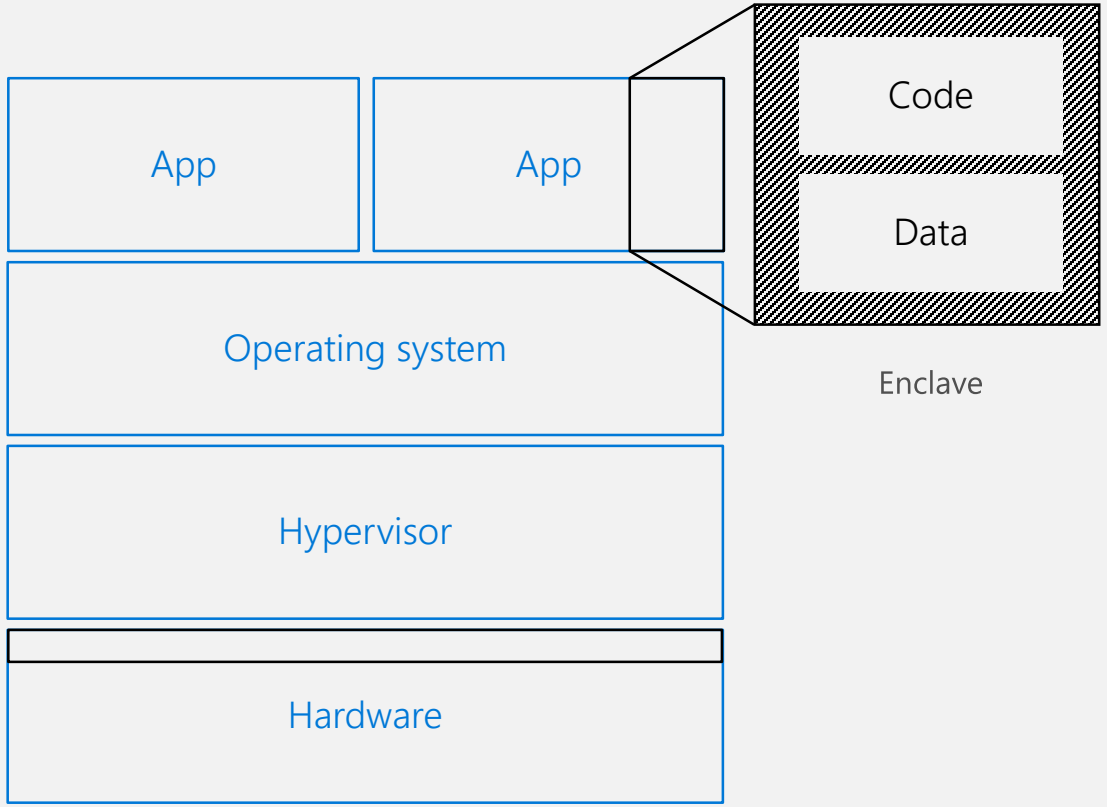
An enclave is a protected region of memory that appears as a black box to the containing process and the OS

Microsoft supports SGX and VSM TEEs

Benefits

Only authorized code is permitted to run inside an enclave

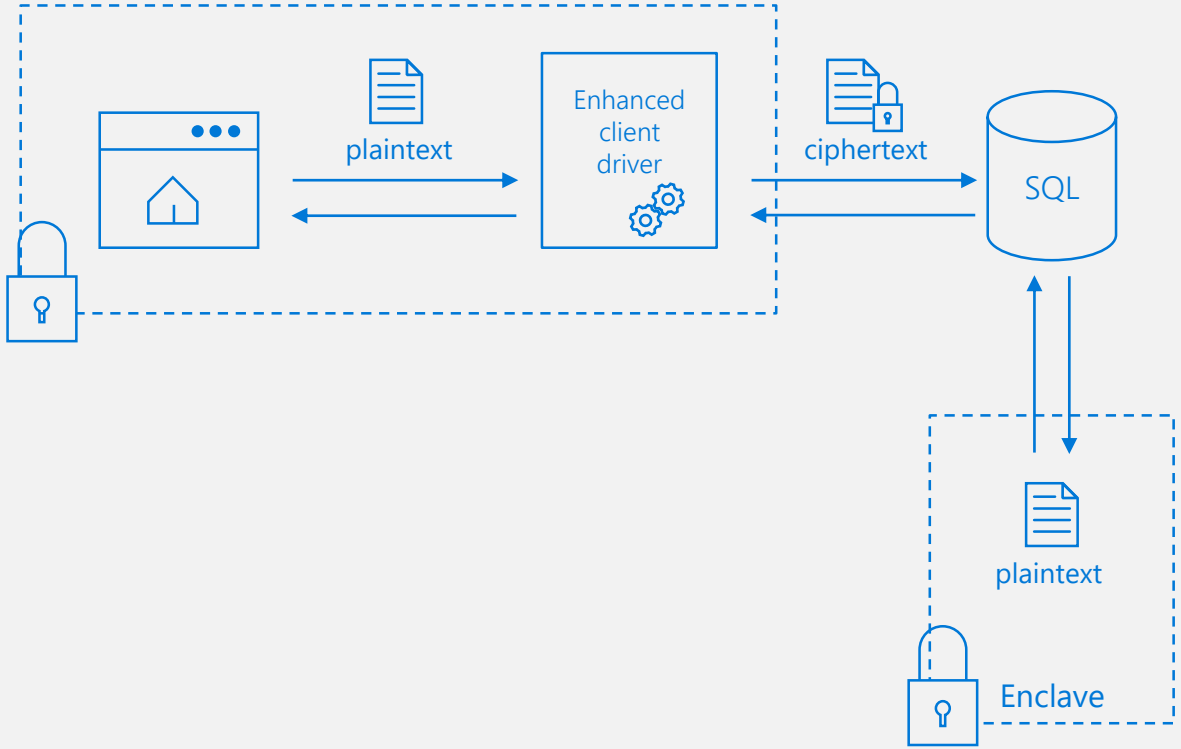
Both the data and the code inside the enclave are inaccessible from the outside and protected from malicious insiders, hackers, and malware



DATA PROTECTION INSIDE A TRUSTED EXECUTION ENVIRONMENT

Secure computations inside the enclave

When processing queries, the SQL Server database engine delegates rich computations and cryptographic operations on encrypted columns to the enclave, where the data is safely decrypted and processed



VULNERABILITY ASSESSMENT

Get visibility

Discover sensitive data and potential security holes

Remediate

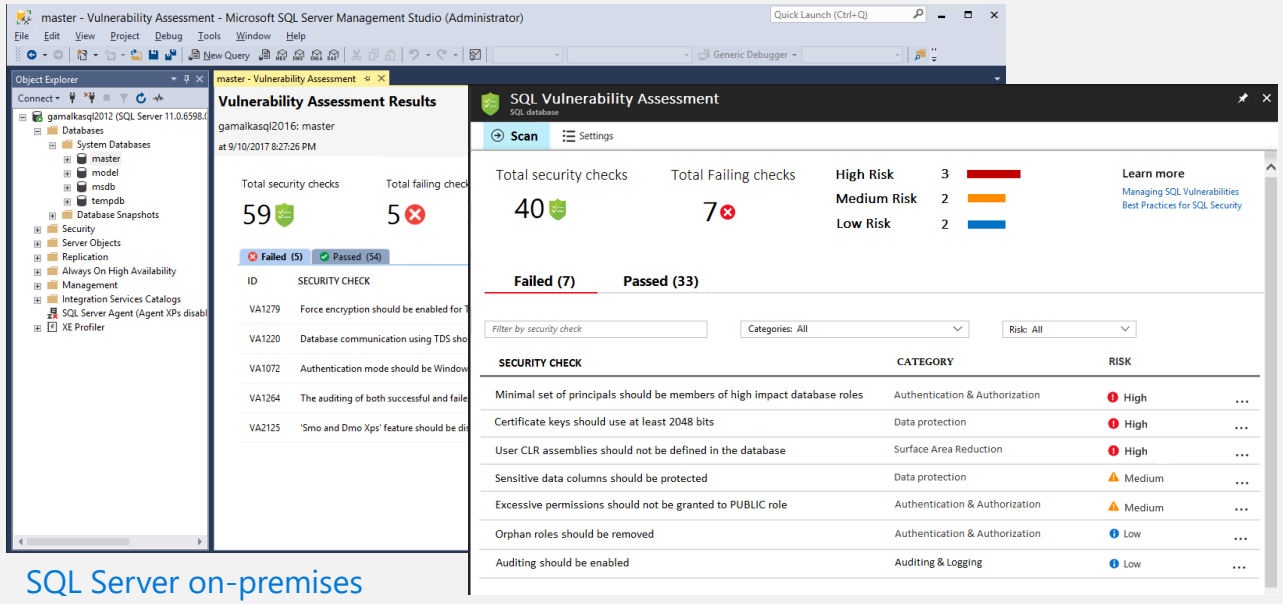
Actionable remediation and security hardening steps

Customize

Baseline policy tuned to your environment, allowing you to focus on deviations

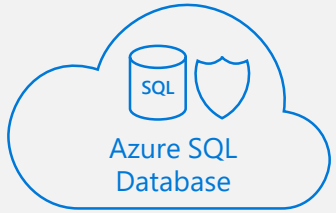
Report

Pass internal or external audits to facilitate compliance



SQL Server on-premises

Azure SQL Database

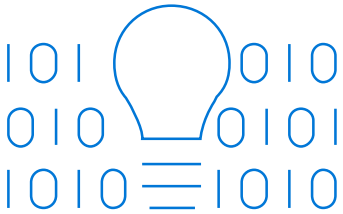


Vulnerability Assessment

Identifies, tracks, and resolves SQL security vulnerabilities

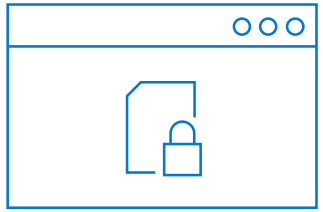
Developer/DBA

INFORMATION PROTECTION



Discover

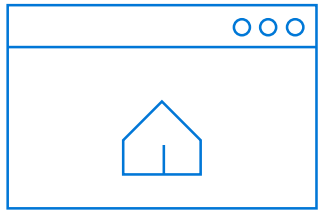
Will be integrated into the Microsoft Information Protection framework
Protects data and moves across database boundaries in your organization



Classify

Automatic Data Discovery and recommendations to classify sensitive data
Each column associated with a sensitivity label and label type
Manual classification on data can also be added

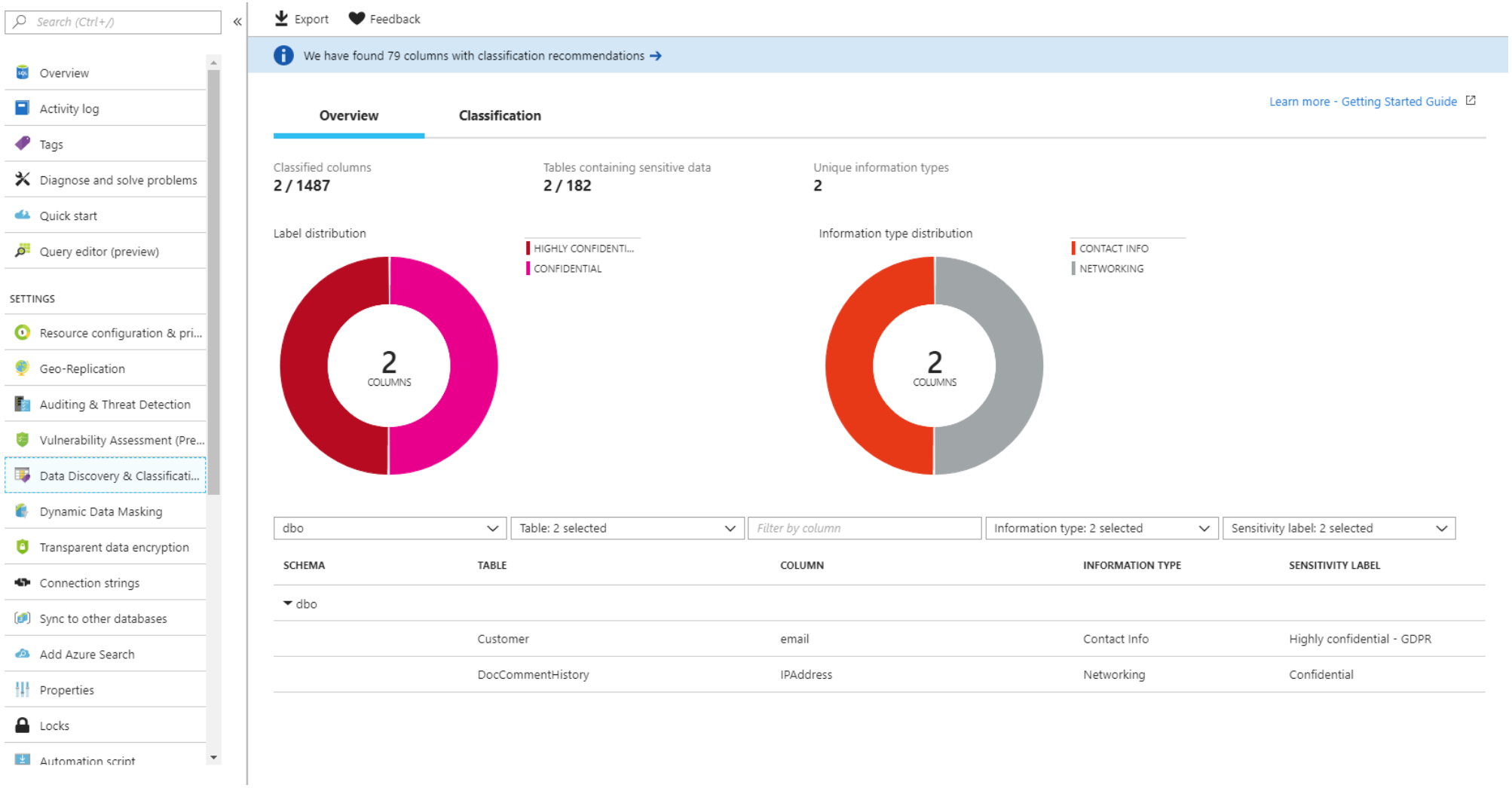
Column label persisted as column metadata as new classification attributes in SQL Engine
Export classification information to Excel report for internal or external auditing purposes



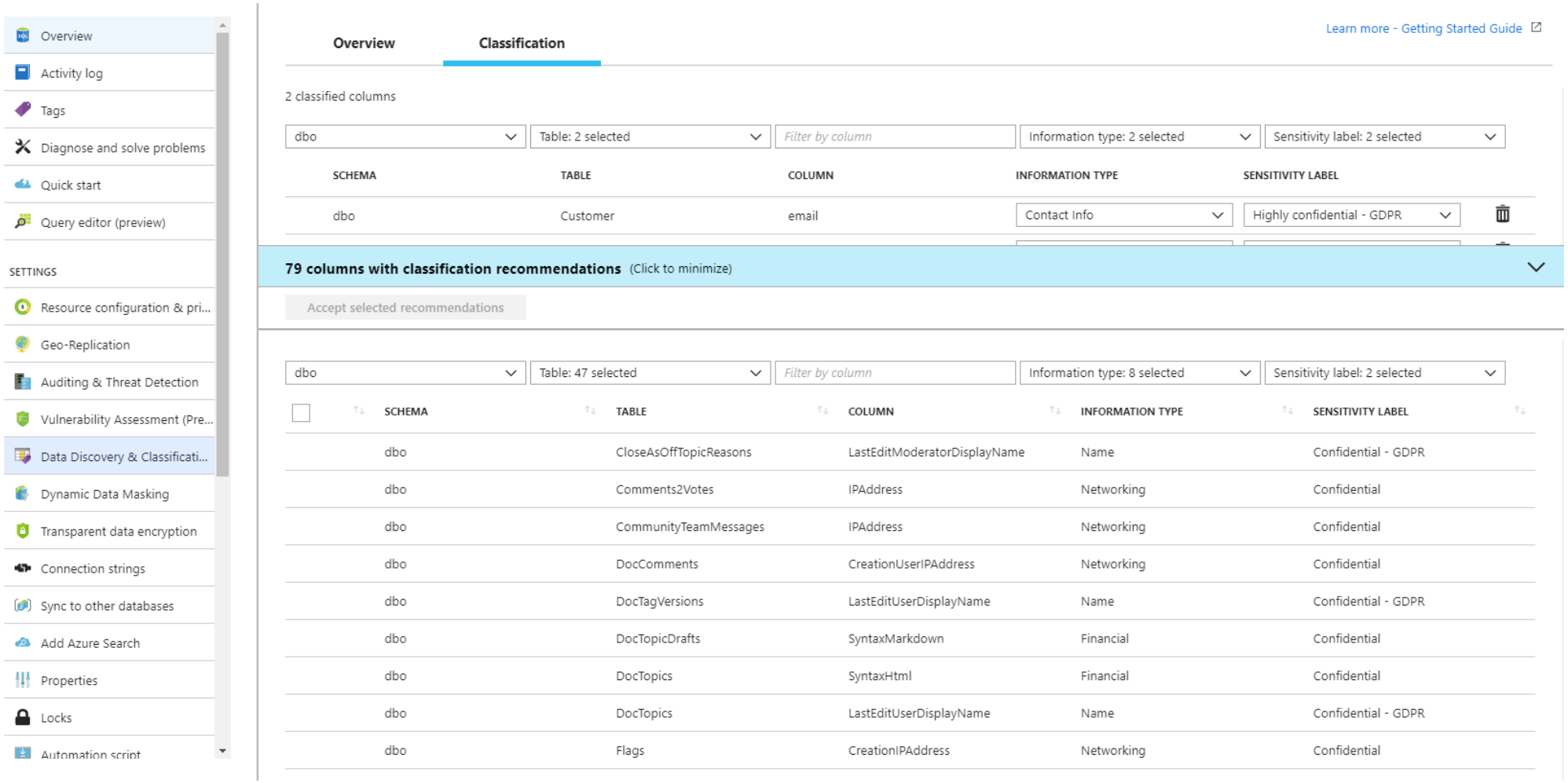
Label

Once a column is labeled it can be used for auditing and protection purposes
All labeled columns will be fully audited at run time for any queries that access them
Auditing will monitor which users access sensitive data and how much sensitive data they access

DATA DISCOVERY & CLASSIFICATION



DATA DISCOVERY & CLASSIFICATION



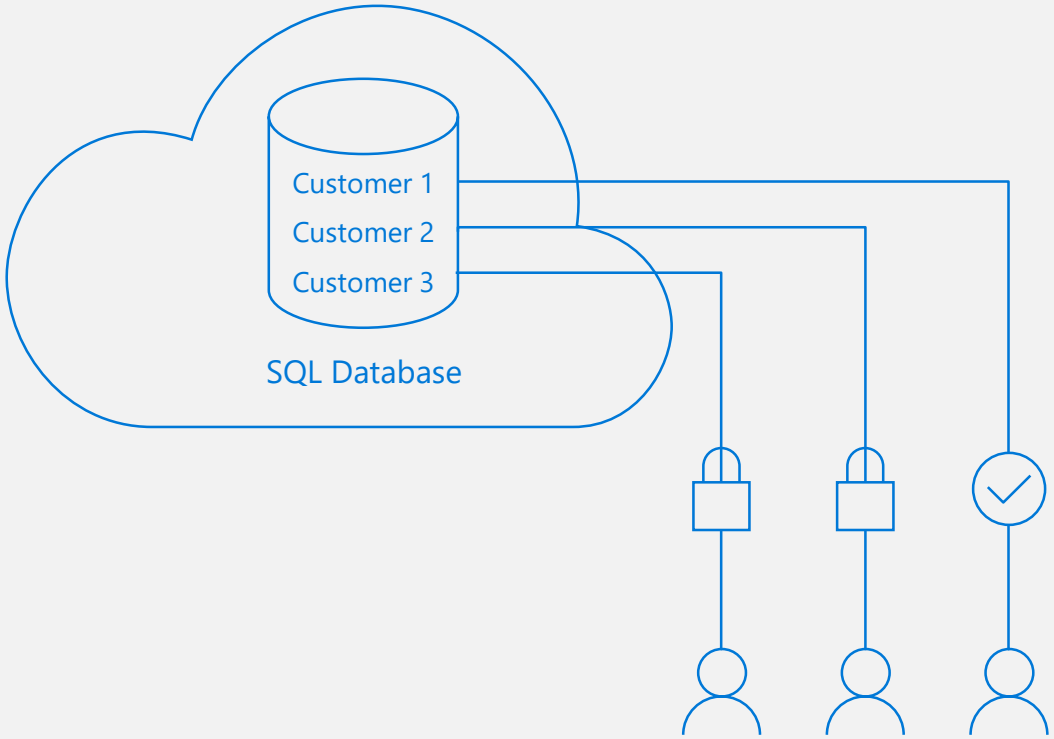
ROW-LEVEL SECURITY

Control access of specific rows in a database table

Help prevent unauthorized access when multiple users share the same tables, or implement connection filtering in multitenant applications

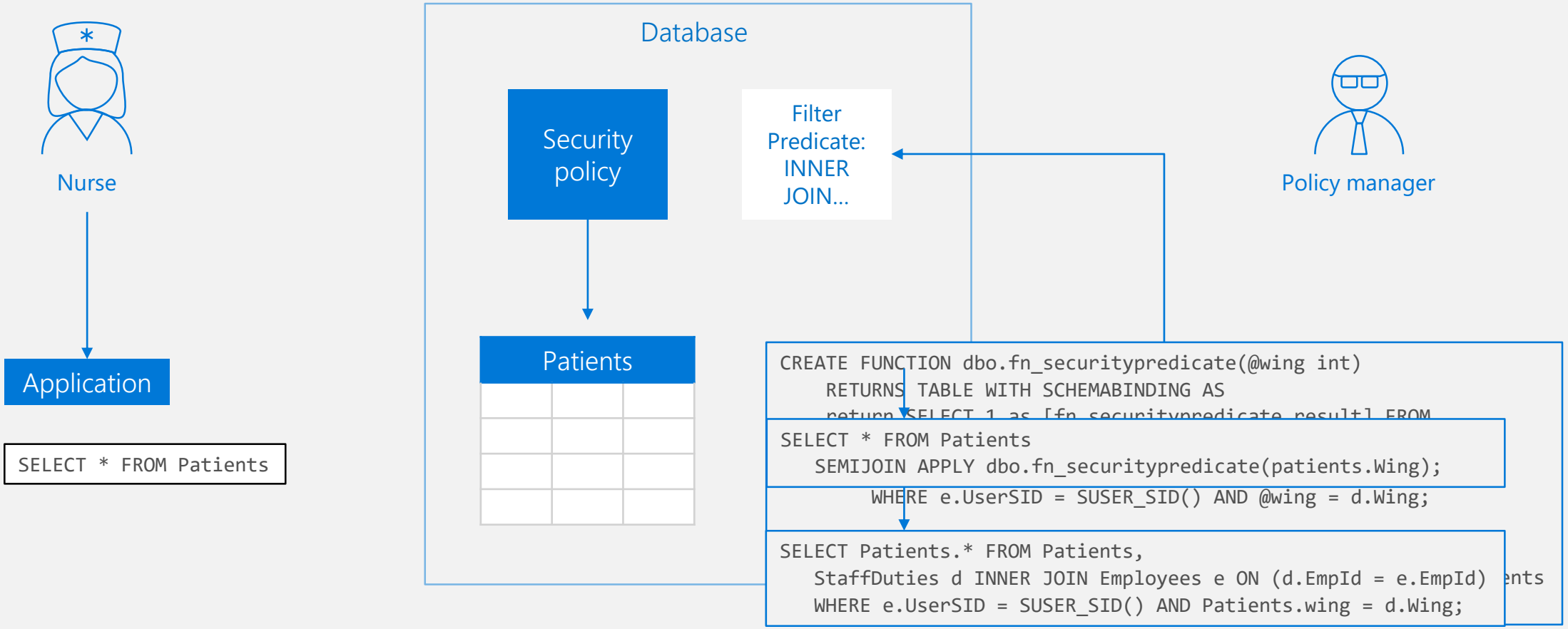
Administer via SQL Server Management Studio or SQL Server Data Tools

Easily locate enforcement logic inside the database and schema bound to the table



RLS IN THREE STEPS

1. Policy manager creates security policy in T-SQL, binding the predicate to the Patients table
2. Application (e.g., nurse) selects from Patients table
3. Security policy adds filter predicate to Patients table



DYNAMIC DATA MASKING

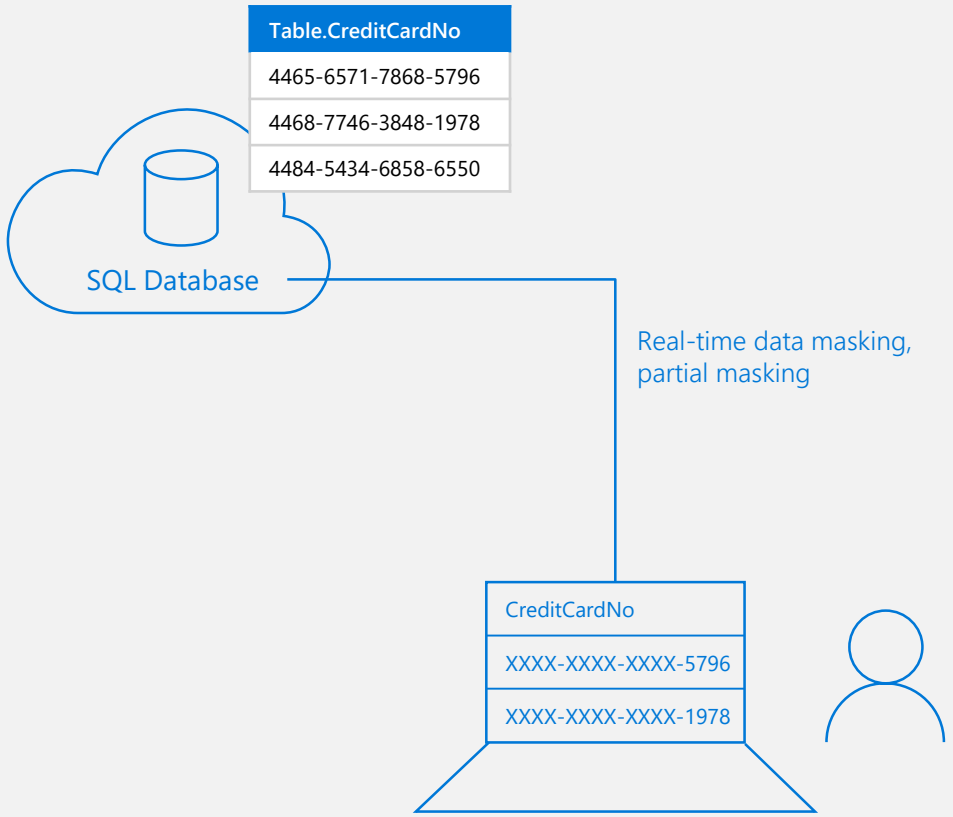
Prevent abuse of sensitive data by hiding it from users

Easy configuration in new Azure Portal

Policy-driven at table and column level, for a defined set of users

Data masking applied in real-time to query results based on policy

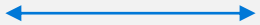
Multiple masking functions available, such as full or partial, for various sensitive data categories (credit card numbers, SSN, etc.)

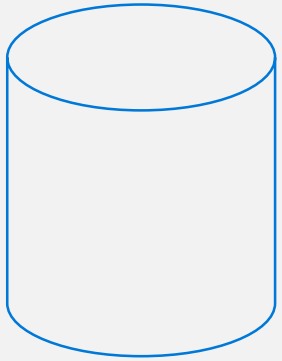


DYNAMIC DATA MASKING

1. The app offers data masking capabilities to the Employee table
2. The app uses data masking to protect sensitive data in the Employee table
3. The app uses data masking to protect sensitive data in the Employee table

Business app





```
ALTER TABLE [Employee] ALTER COLUMN [SocialSecurityNumber]
ADD MASKED WITH (FUNCTION = ‘SSN()’

ALTER TABLE [Employee] ALTER COLUMN [Email]
ADD MASKED WITH (FUNCTION = ‘EMAIL()’)

ALTER TABLE [Employee] ALTER COLUMN [Salary]
ADD MASKED WITH (FUNCTION = ‘RANDOM(1,20000)’)

GRANT UNMASK to admin1
```

Security officer

```
SELECT [Name],
       [SocialSecurityNumber],
       [Email],
       [Salary]
FROM [Employee]
```

other logon

	First Name	Social Security Number	Email	Salary
1	LILA	XXX-XX-XX37	lXX@XXXX.net	8940
2	JAMIE	XXX-XX-XX14	jXX@XXXX.com	19582
3	SHELLEY	XXX-XX-XX28	sXX@XXXX.net	3713
4	MARCELLA	XXX-XX-XX65	mXX@XXXX.net	11572
5	GILBERT	XXX-XX-XX87	gXX@XXXX.net	4487

admin1 logon

	First Name	Social Security Num...	Email	Salary
1	LILA	758-10-9637	lila.barnett@comcast.net	1012794
2	JAMIE	113-29-4314	jamie.brown@ntlworld.com	1025713
3	SHELLEY	550-72-2028	shelley.lynn@charter.net	1040131
4	MARCELLA	903-94-5665	marcella.estrada@comcast.net	1040753
5	GILBERT	376-79-4787	gilbert.juarez@verizon.net	1041308

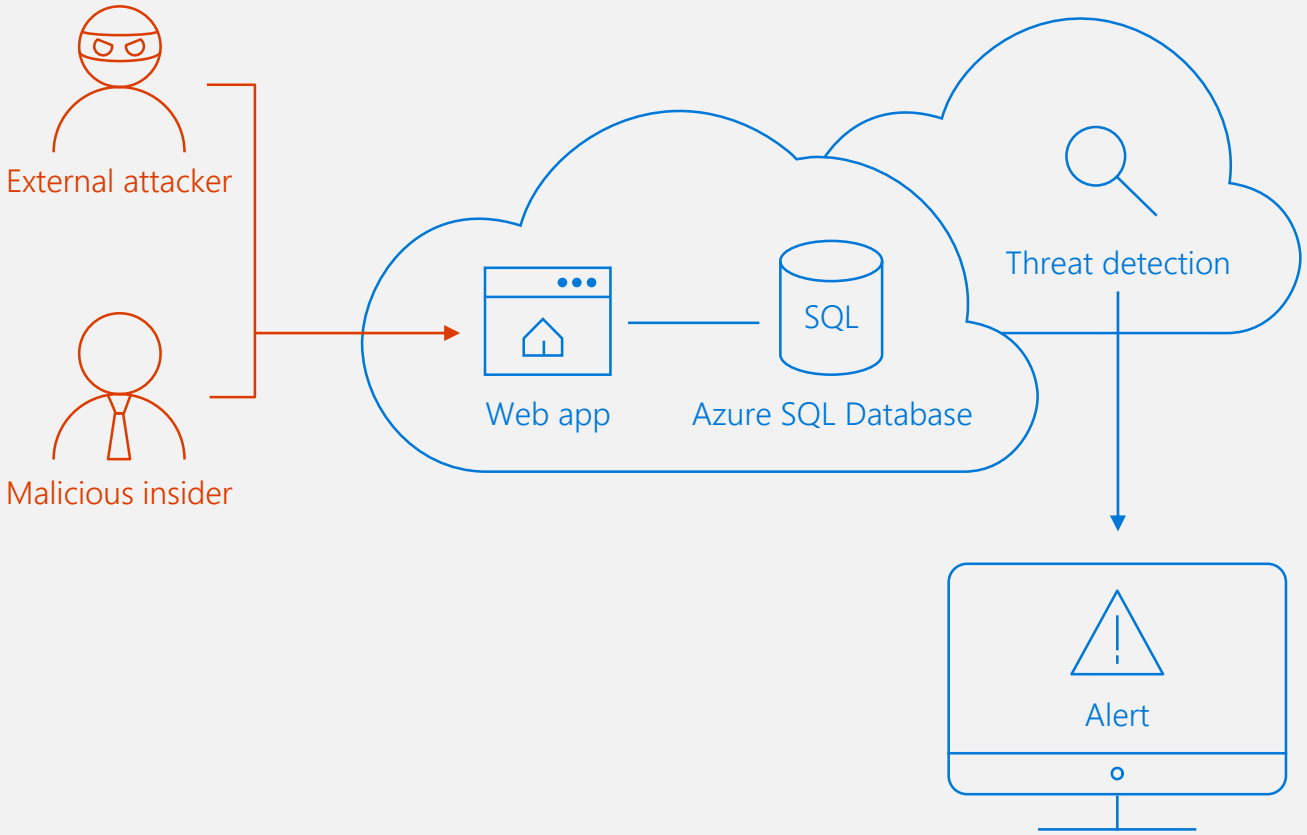
THREAT DETECTION

Detect anomalous database activities that could indicate a potential threat

Configure threat detection policy in Azure Portal

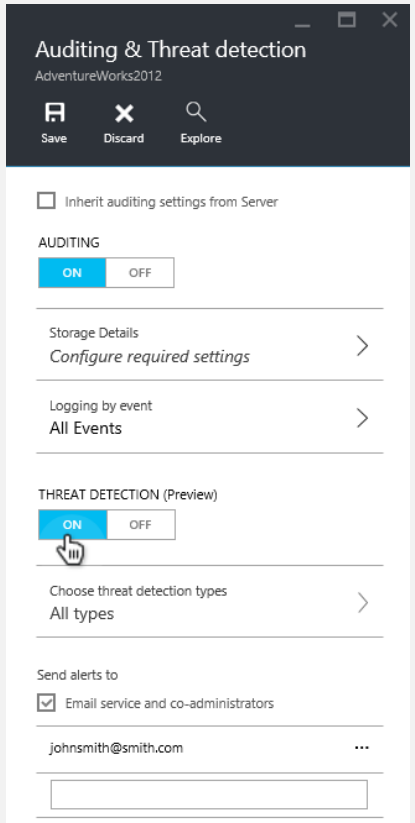
Receive alerts from multiple database threat detectors that identify anomalous activities

Explore audit log around the time of an event

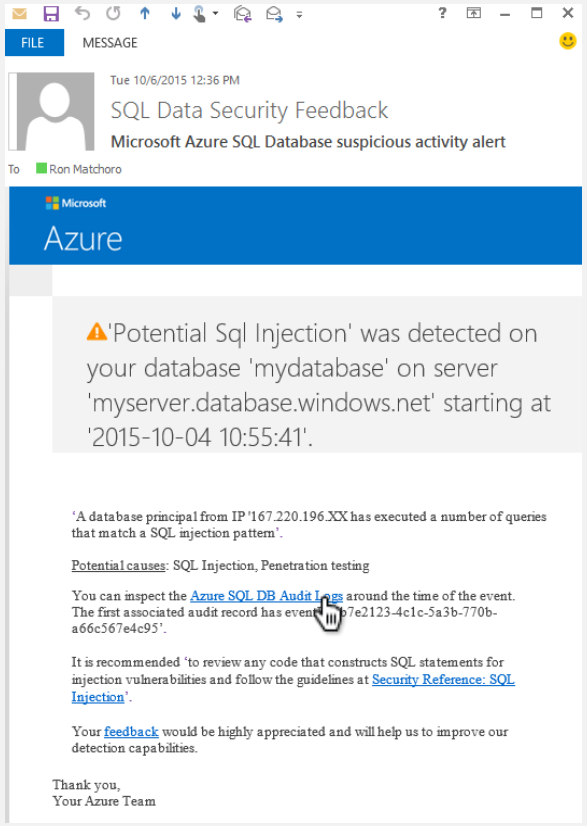


HOW THREAT DETECTION WORKS

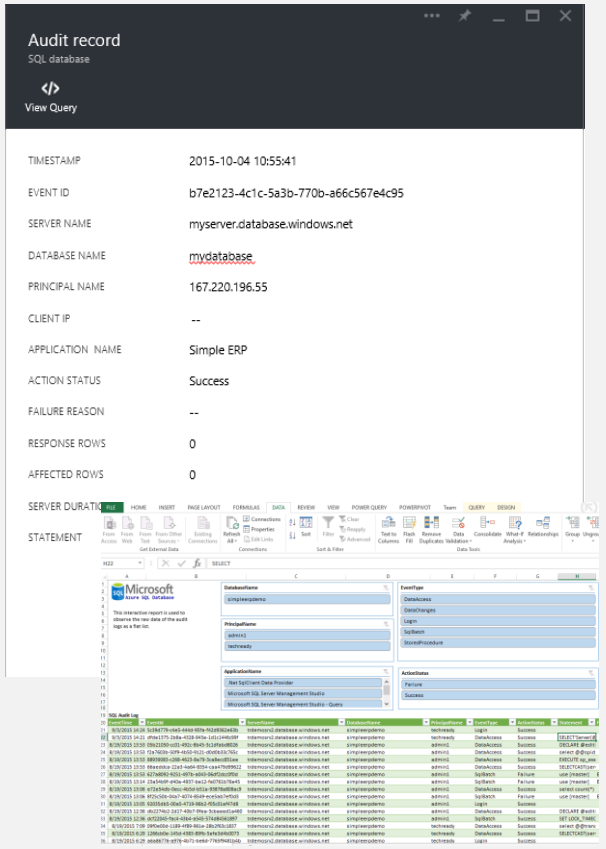
Set up



Alert



Explore



AZURE SQL DATABASE AUDITING

Gain insight into database events and streamline compliance-related tasks

Configurable to track and log database activity

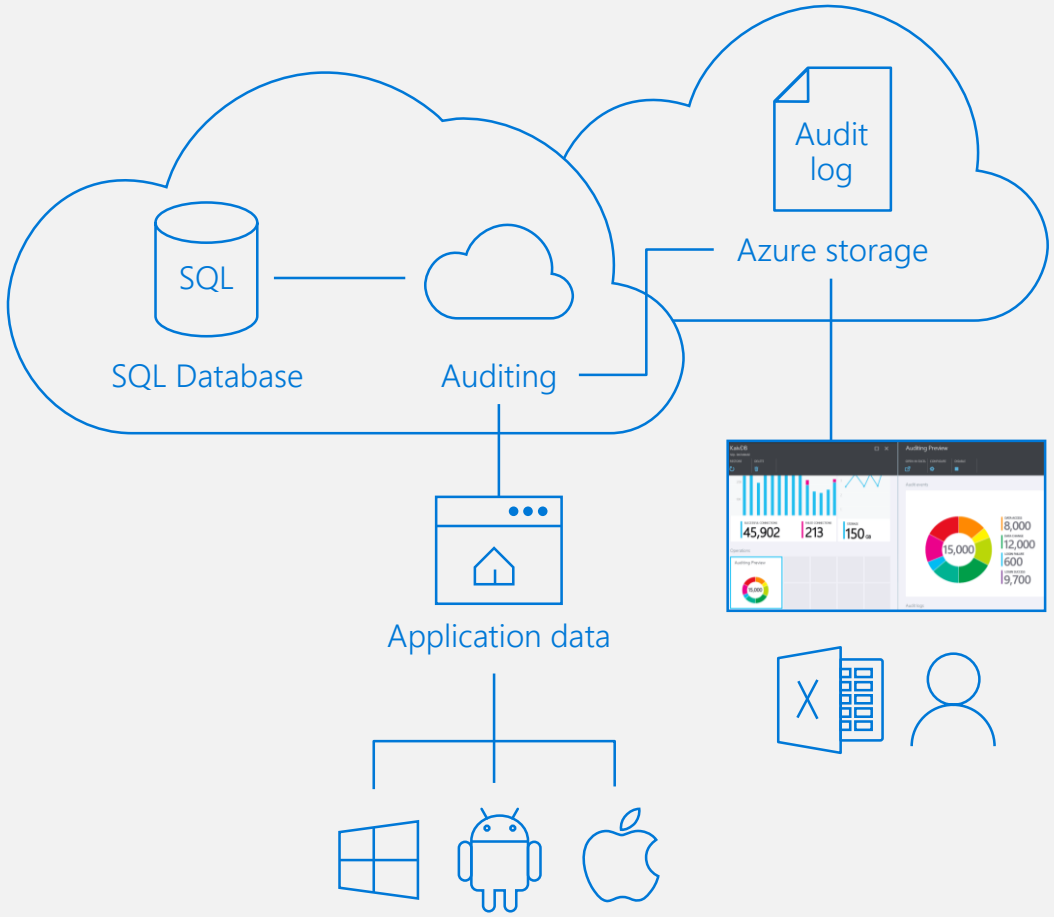
Dashboard views in portal for at-a-glance insights

Pre-defined Power View reports for deep visual analysis on audit log data

Audit logs reside in your Azure Storage account

Available in Basic, Standard, and Premium

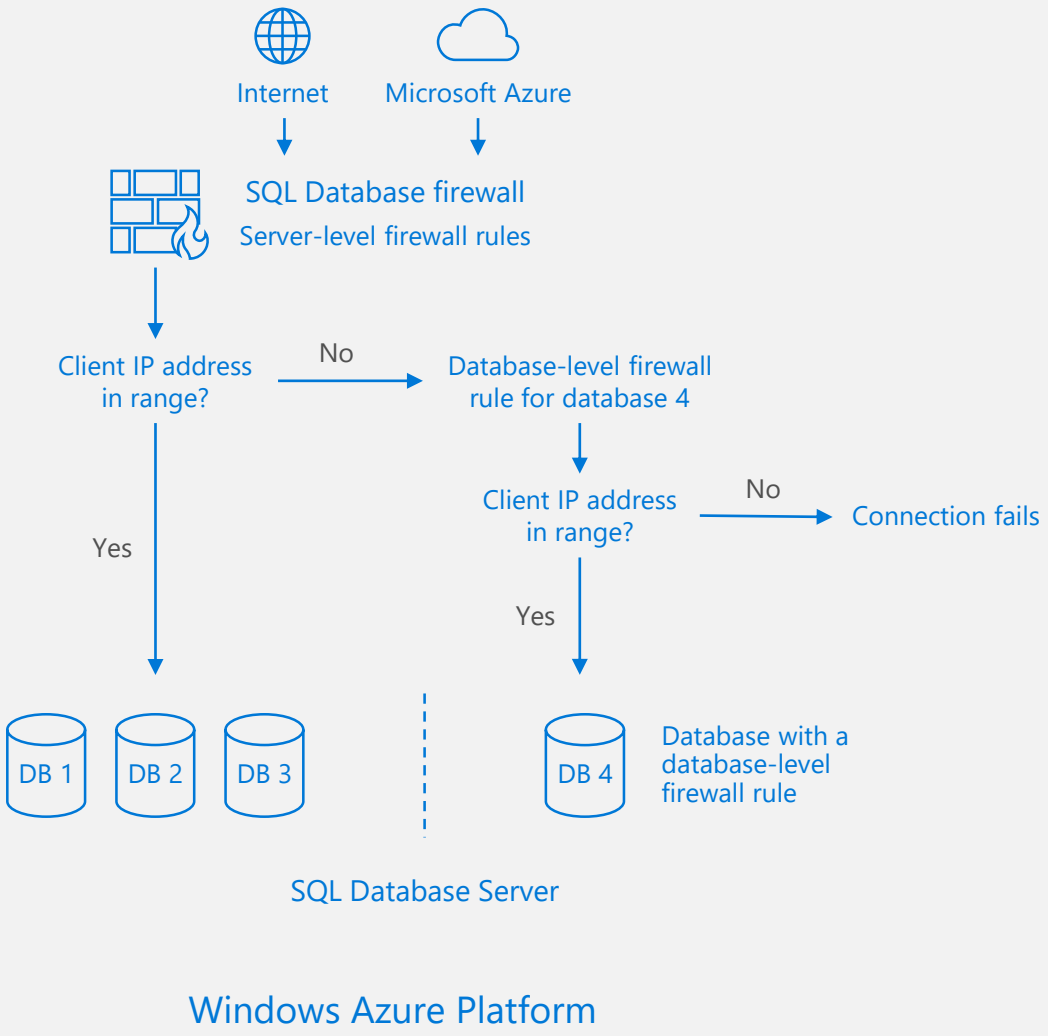
Access via Azure portal



SECURING YOUR DATABASE WITH FIREWALLS

Initially, all access to your Azure SQL Database server is blocked by the firewall

In order to begin using your Azure SQL Database server, you must go to the Management Portal



Azure Database for MySQL, PostgreSQL, and MariaDB

Azure Databases for MySQL, PostgreSQL, and MariaDB offer enterprise-ready and fully-managed community versions of the popular OSS databases.

Recently Released:

- Scaling across tiers for PostgreSQL and MySQL – GA June ’18
- 4 TB storage for PostgreSQL and MySQL – GA June ’18
- Virtual network service endpoints for PostgreSQL and MySQL – GA Aug ’18
- Intelligent Performance (Query Store, Performance Recommendation, and Query Insights) for PostgreSQL – Public Preview
- Advanced Threat Protection for PostgreSQL and MySQL – Public Preview
- Azure Database for MariaDB – Public Preview

Learn more about MySQL

Learn more about PostgreSQL

Learn more about MariaDB

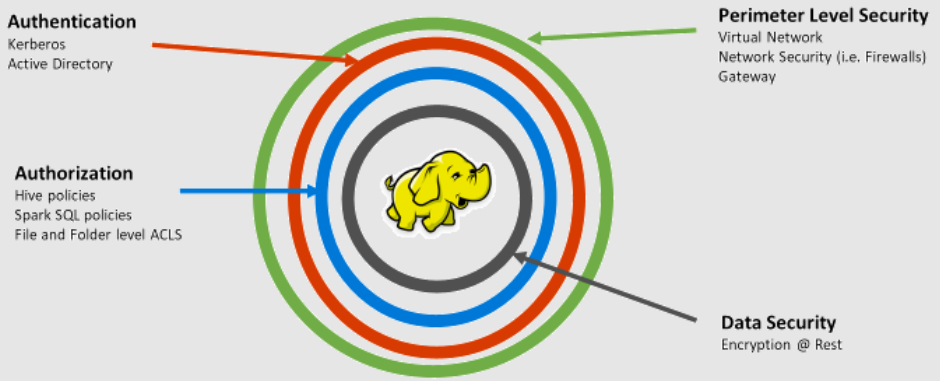
Enterprise Security Package for HDInsight

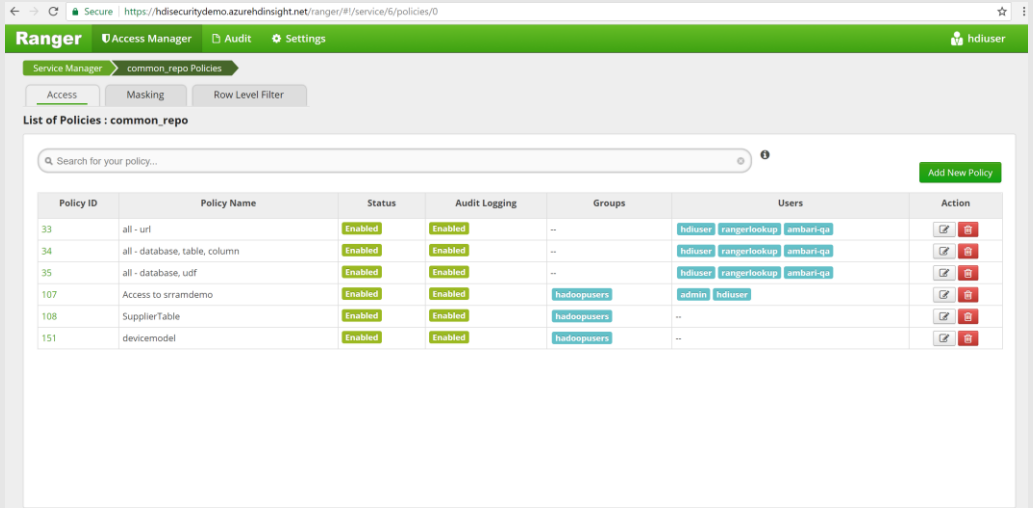
Enterprise grade security for Hadoop and Spark workloads

- Multi-user authentication using Active Directory or Azure Active Directory.
- Multi-user Zeppelin notebook with collaborative data science experience.
- Role based access control for Ambari operations.
- Fine grained role based access control for Hive SQL and Spark SQL using Apache Ranger.
- Data masking of sensitive data using Apache Ranger.
- Seamless integration with file and folder level ACLs in Azure Data Lake Store.
- Audit all access to sensitive data as well as changes to access policies.
- Transparent server side encryption at rest as well as encryption in transit.

[Learn more.]

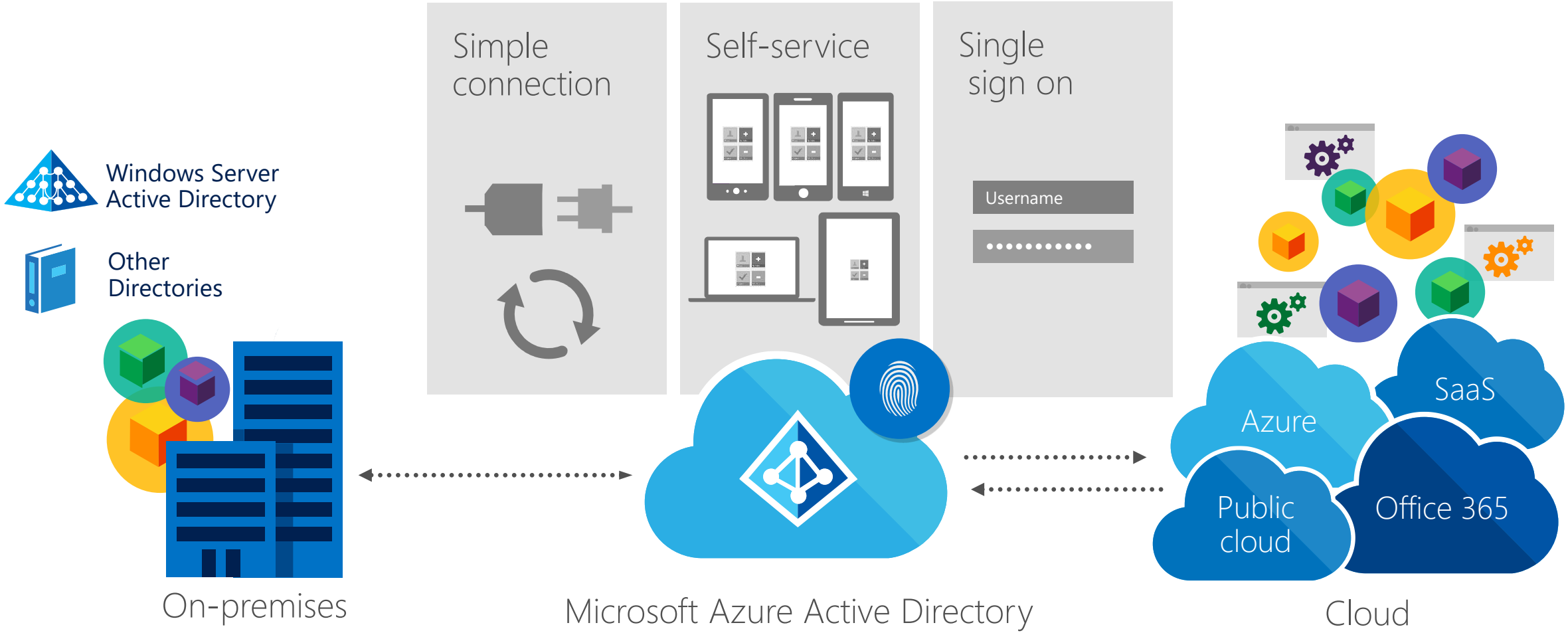
HDInsight security - Rings of defense





Azure Identity Management

Identity as the control plane



The Connected AD

Cloud Management

Secure the data

User Empowerment

Your Directory on the cloud

Centrally managed identities and access.

Monitor and protect access to cloud applications.

Empower Users

Your Directory on the cloud

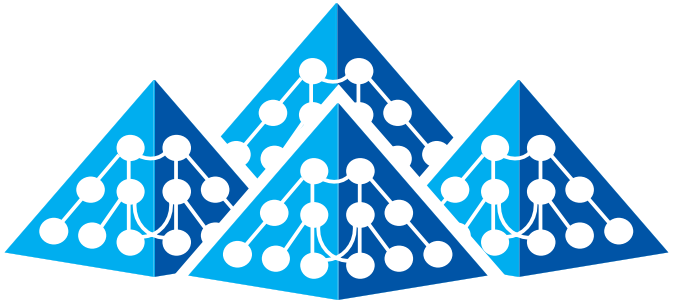
Centrally managed identities and access.

Monitor and protect access to cloud applications.

Empower Users

Your Directory on the cloud

Connect and Sync on-premises directories with Azure.



Windows Server
Active Directory

* Azure Active Directory Connect

Microsoft Azure
Active Directory

PowerShell

SQL (ODBC)

LDAP v3

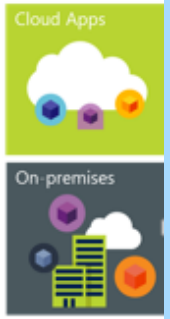
Web Services
(SOAP, JAVA, REST)

Other Directories

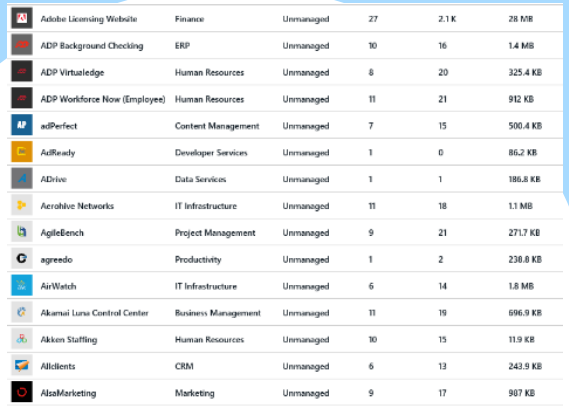
Azure AD : Identity driven security

SSO + MFA

Conditional access

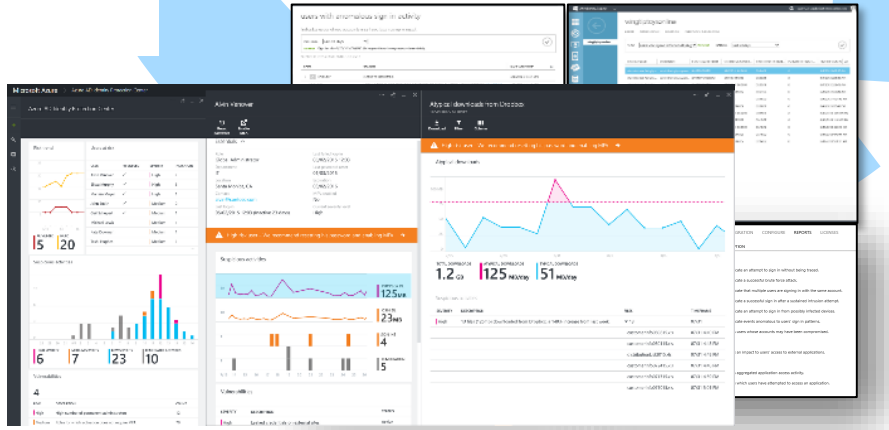


Cloud App Discovery

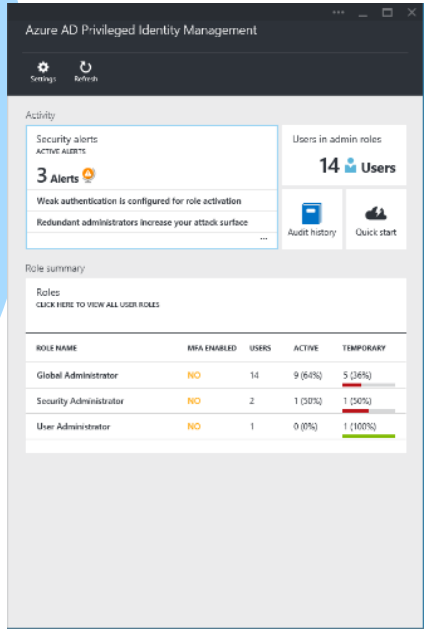


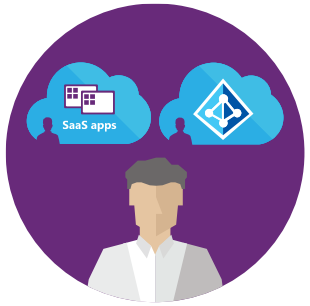
Adobe Licensing Website	Finance	Unmanaged	27	2.1 K	28 MB
ADP Background Checking	ERP	Unmanaged	10	16	1.4 MB
ADP Virtualedge	Human Resources	Unmanaged	8	20	325.4 KB
ADP Workforce Now (Employee)	Human Resources	Unmanaged	11	21	912 KB
adPerfect	Content Management	Unmanaged	7	15	500.4 KB
AdReady	Developer Services	Unmanaged	1	0	86.2 KB
ADrive	Data Services	Unmanaged	1	1	186.8 KB
Aerohive Networks	IT Infrastructure	Unmanaged	11	18	1.1 MB
AgileBench	Project Management	Unmanaged	9	21	271.7 KB
agreedo	Productivity	Unmanaged	1	2	238.8 KB
AirWatch	IT Infrastructure	Unmanaged	6	14	1.8 MB
Akamai Luna Control Center	Business Management	Unmanaged	11	19	696.9 KB
Akken Staffing	Human Resources	Unmanaged	10	15	11.9 KB
AllClients	CRM	Unmanaged	6	13	243.9 KB
AlsaMarketing	Marketing	Unmanaged	9	17	987 KB

Advanced security reporting



Privileged Identity Management



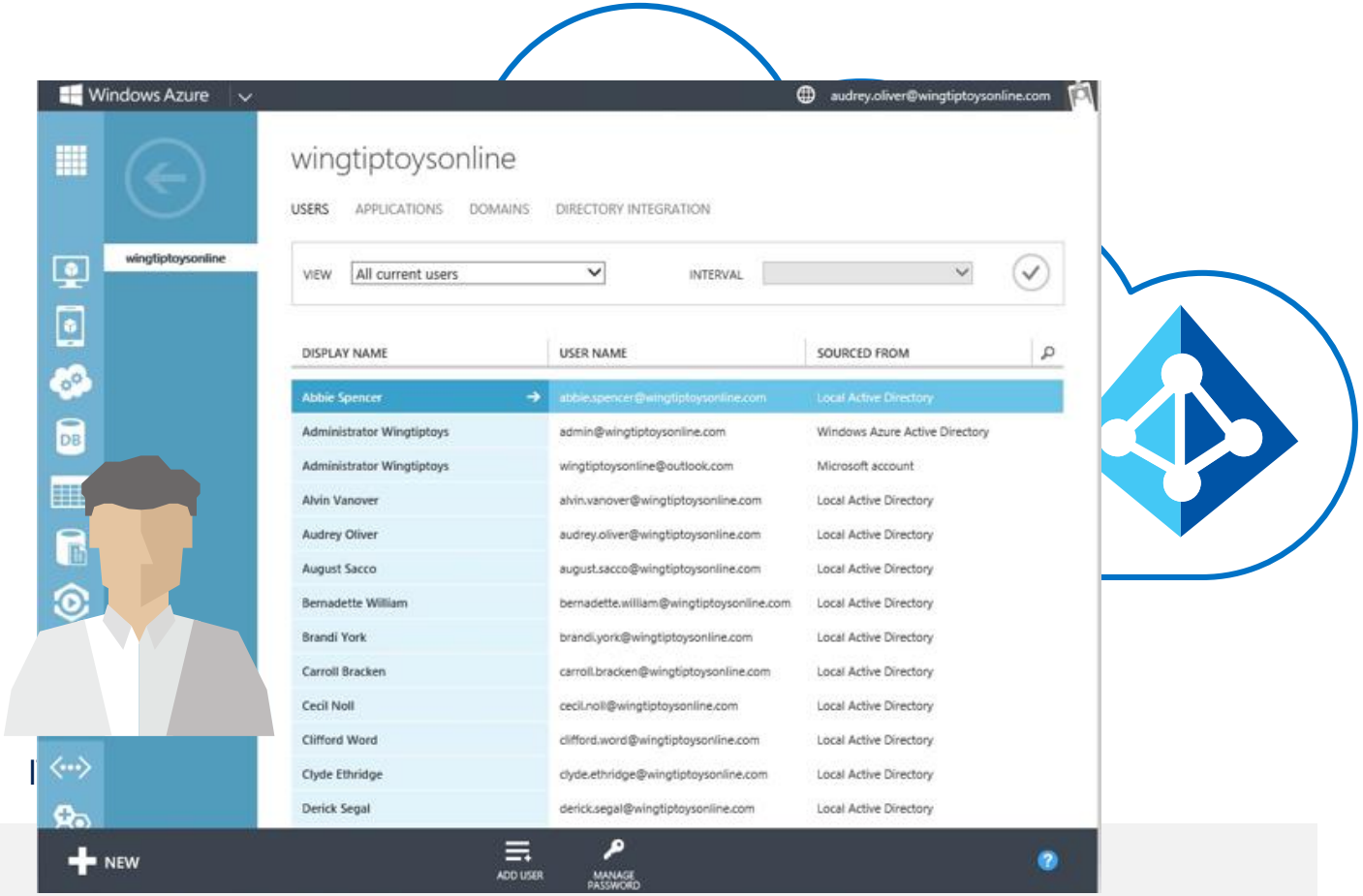


Centrally managed identities and access

Comprehensive identity and access management console.

Centralized access administration for preintegrated SaaS apps and other Cloud-based apps.

Secure business processes with advanced access management capabilities.

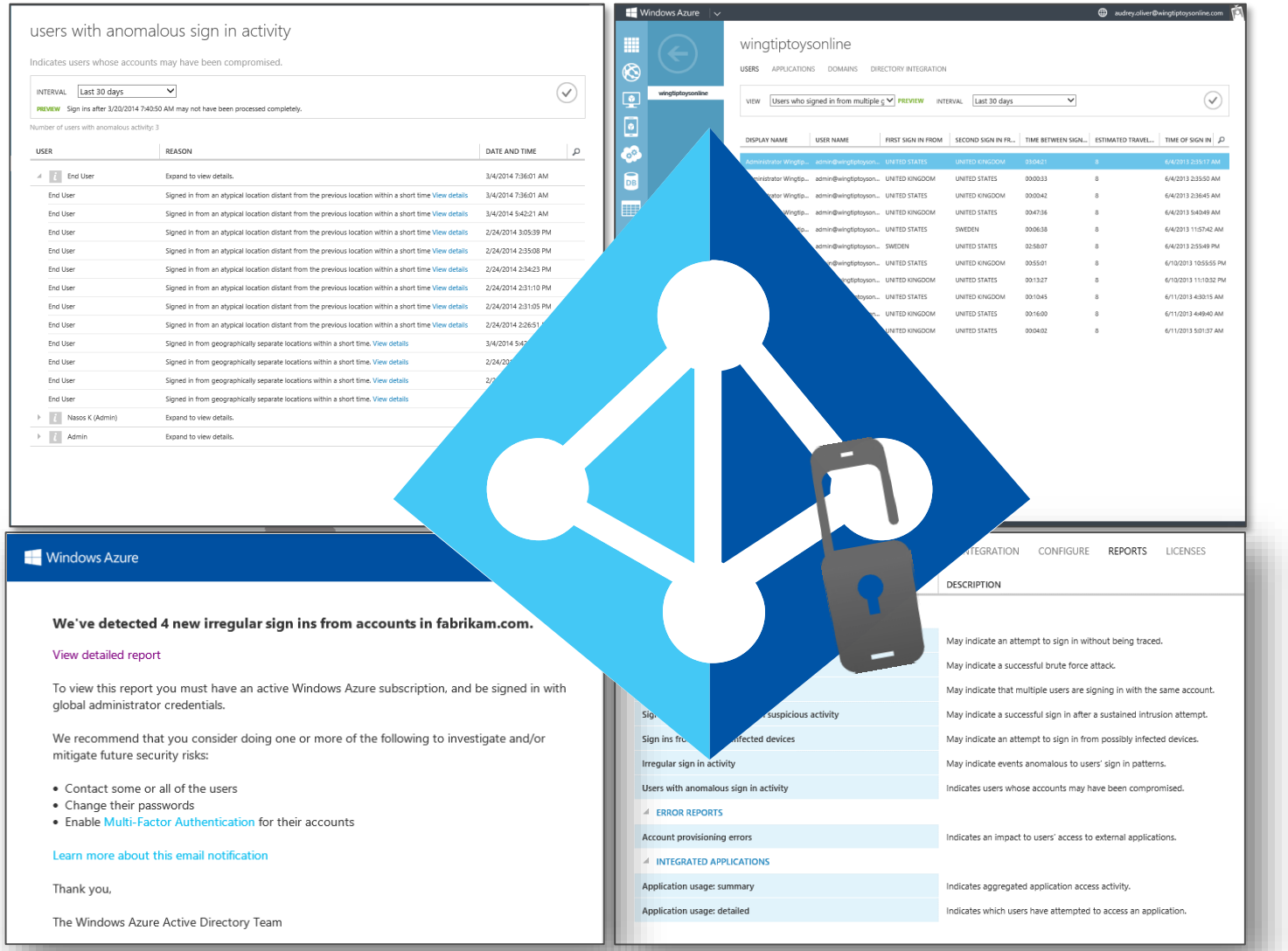


Your cloud apps ready when you are.

Monitor and protect access to enterprise apps

Built-in security features.

Security reporting that tracks inconsistent access patterns, analytics and **alerts.**



B2B: cross-organization collaboration

"I need to let my partners access my company's apps using their own credentials."

Share without complex configuration or duplicate users.

A user at a large partner may log into my company's apps with their Active Directory usernames and passwords.

A user at a smaller partner may log into my company's apps with their Office 365 usernames and passwords.

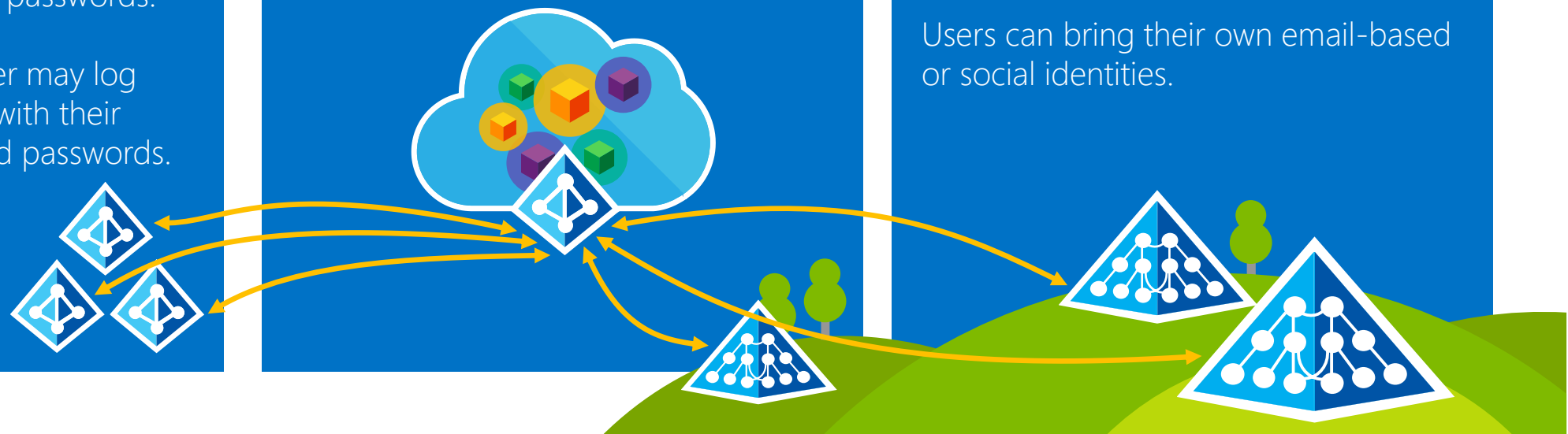
Admin configures sharing for cloud apps.

"I can't email my 25 MB file and need to share it with a partner using Box.com."

Seamlessly provide Azure Active Directory to customers & partners

For example, a user at a partner can set up everyone in their company.

Users can bring their own email-based or social identities.

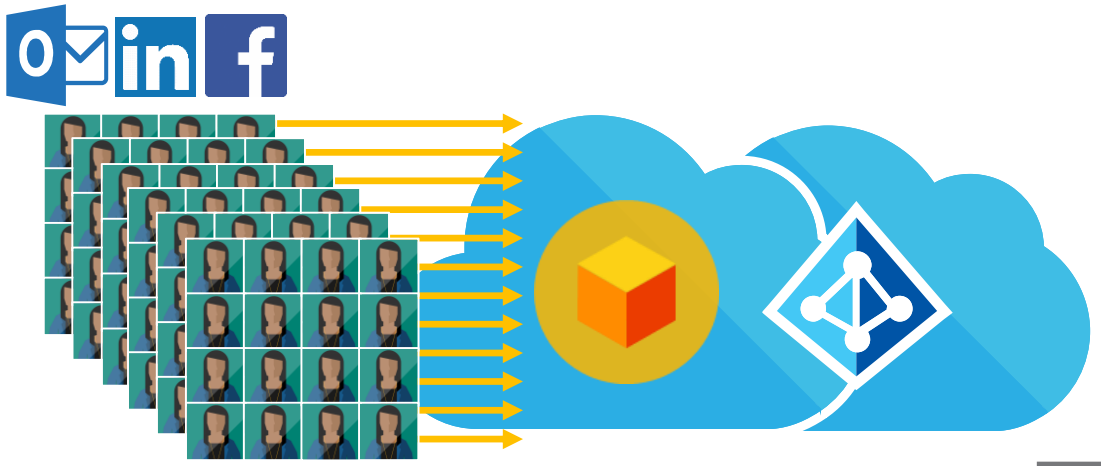


Azure Active Directory B2C(Business-to-Consumer)

Azure Active Directory B2C offering is tailored for enterprises who serve large populations (100's of thousands to millions) of individual customers, and whose business success depends upon consumer adoption of web applications for improving customer satisfaction and reducing operational costs.

Azure Active Directory B2C will include :

- Self-Service User registration
- Login with Social IdP or create your own credentials
- Optional MFA
- Bulk user import tools
- SSO to multiple web sites
- User interface customization



Cloud Domain Join

Cloud Domain Join makes it possible to connect work-owned Windows devices to your company's Azure Active Directory tenancy in the cloud. Users can sign-in to Windows with their cloud-hosted work credentials and enjoy modern Windows experiences.

Enterprise compliant Services

- Roaming Settings, Windows backup/Restore, Store access…
- Data stored in enterprise compliant backend services on Azure.
- No need to add a personal Microsoft account.

SSO from the desktop to org resources

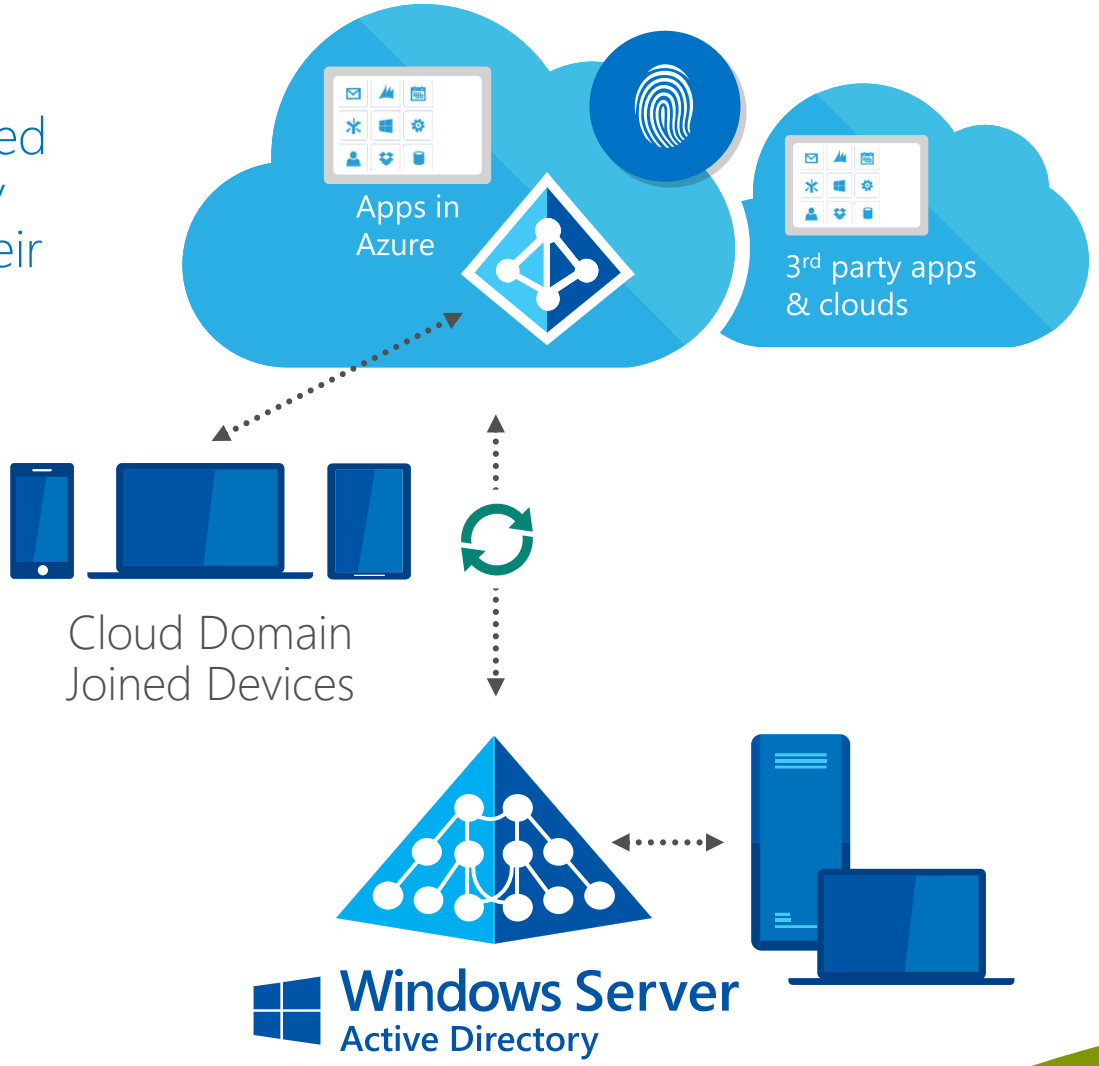
- SSO from desktop to Office 365 and 1,000's of enterprise apps, websites and resources.
- Access enterprise-curated Store and install apps using a work account.

Management

- Automatic MDM enrollment during first-run experience.

Support for hybrid environments

- Traditional Domain Joined PCs also benefit from Cloud Domain Join functionality when the on-prem Active Directory is connected with an Azure Active Directory in the cloud.



Azure Network Monitor

Azure Network Watcher

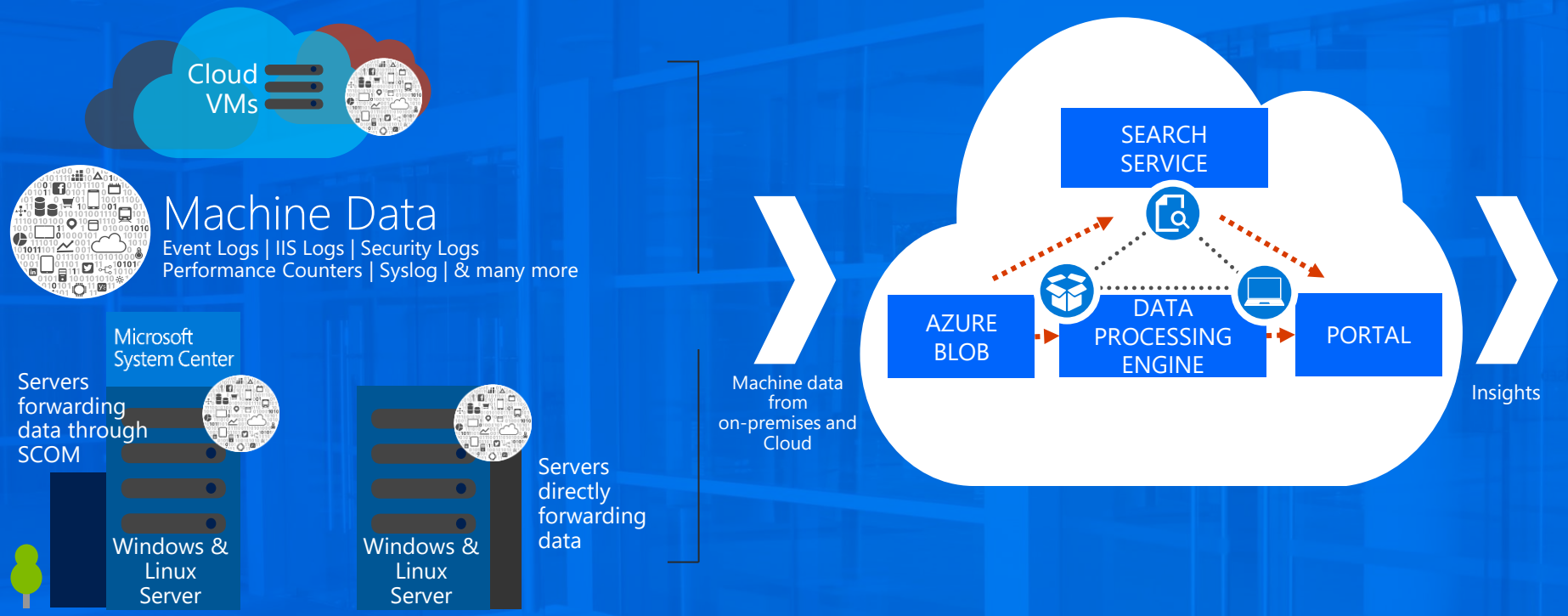
Topology	Network Diagnostics	Metric	Logs
Visualize your network topology	Diagnostic tools for networking related issues	Measure and view your network performance and health	Configure and view your logs
• Topology	• Variable Packet Capture • IP Flow Verify • Security Group View • Next Hop • VPN Diagnostics	• Network Subscription Limits	• Network Security Flow logs • Single place to configure all logs and Alerts

Azure Monitor

including / aka Azure Log Analytics
aka Azure Operational Insights
aka Operations Management Suite
aka System Center Advisor

Azure Monitor and Log Analytics

Log Management – Collect, correlate and visualize all your machine data



- Correlate & Search data from multiple sources
- Collect custom data types
- Build dashboards powered by search queries

Troubleshooting

- Forecast future capacity needs and pinpoint performance bottlenecks
- Check your update and malware protection status

Operation Insights

- Identify security breaches
- Meet compliance requirements for auditing
- Analyze security data

Security Intelligence

Key Benefits:

REAL TIME

SEARCH

READY MADE INTELLIGENCE

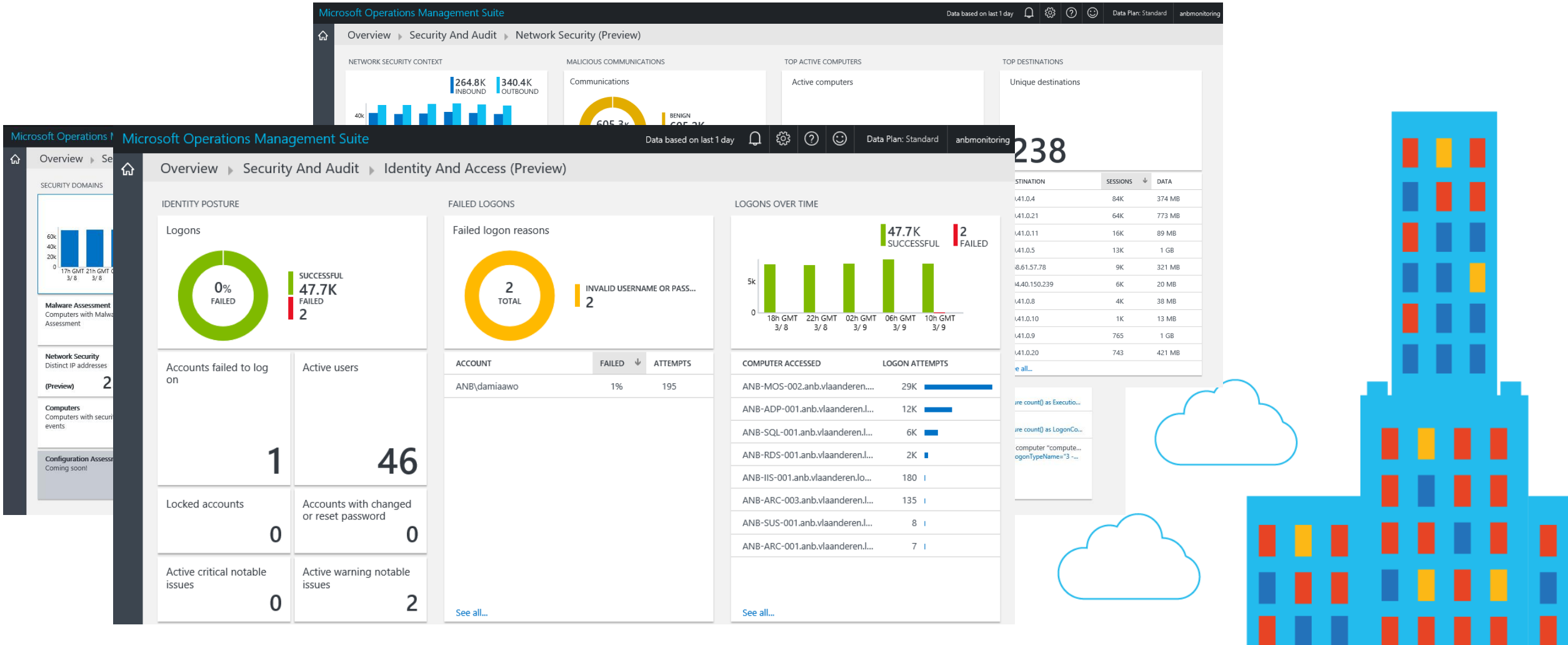
DASHBOARDS & REPORTING

SCALABLE

OMS Security related matters

- AD Assessment
- Malware Assessment
- System Update Assesment
- Change Tracking
- Wire Data
- Security and Audit

New : Security and Audit



Amazon Linux
- 2013.09 – 2015.09

CentOS
- 5 (x86/x64)
- 6 (x86/x64)
- 7 x64)

Debian GNU/Linux
- 6 (x86/x64)
- 7 (x86/x64)
- 8 (x86/x64)

Oracle Linux
- 5 (x86/x64)
- 6 (x86/x64)
- 7 x64)

Red Hat Ent. Linux
- 5 (x86/x64)
- 6 (x86/x64)
- 7 (x64)

SUSE Linux Enterprise Server
- 11 (x86/x64)
- 12 (x64)

Ubuntu Server
- 12.04 LTS (x86/x64)
- 14.04 LTS (x86/x64)

Microsoft ♥ Linux

OMS Agent For Linux

What sorts of data can I collect?

- **Syslog:** Collect your choice of syslog events from rsyslog and syslog-ng
- **Performance Metrics**: We can collect 70+ performance metrics at a 30 second granularity using our new. Get metrics from the following objects: System, Processor, Memory & Swap space, Process, Logical Disk (File System) and Physical Disk.
- **Docker container logs, metrics & inventory:** We show information about where your containers and container hosts are, which containers are running or failed, and Docker dameon and container logs sent to stdout and stderr. We also show performance metrics such as CPU, memory, network and storage for the container and hosts to help you troubleshoot and find noisy neighbor containers. We support Docker version 1.8+.
- **Alerts from Nagios + Zabbix:** The agent can collect alerts from your most popular monitoring tools. This allows you to view all your alerts from all your tools in a single pain of glass! Combine this with our existing support for collection of alerts from Operations Manager. We currently support Nagios 3+ and Zabbix 2.x.
- **Apache & MySQL performance metrics:** Collect performance metrics about your MySQL/MariaDB server performance and databases and Apache HTTP Servers and Virtual Hosts.

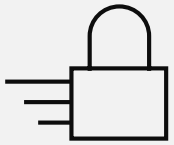
Azure Security Center

Improving security across hybrid cloud environments

Azure Security Center

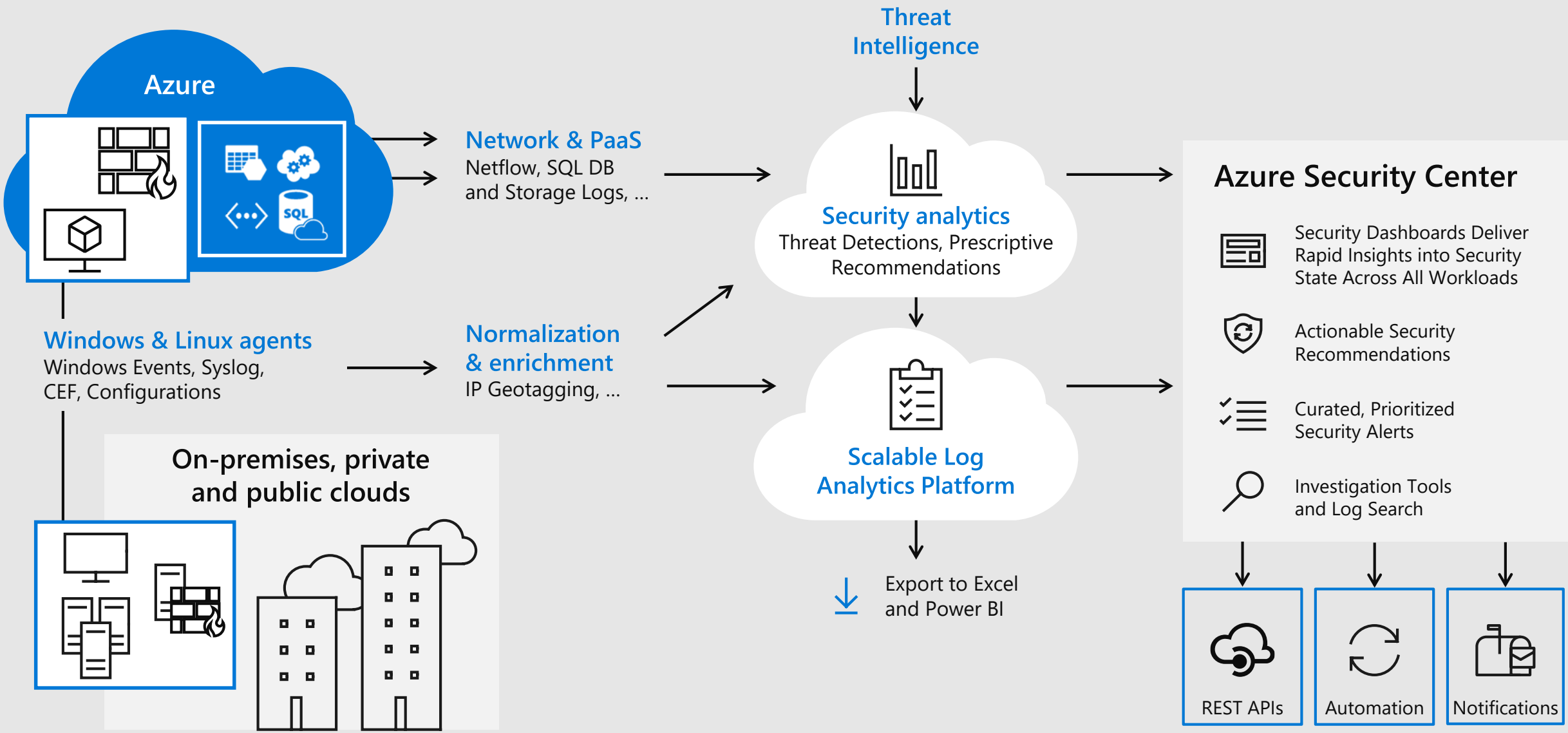
Strengthen security posture

Protect against threats



Get secure faster

Security Center Architecture



Azure Security Reporting

Introducing Microsoft Graph Security API

Unified gateway to security insights and actions across Microsoft products, services, and partners

Unify and standardize alert management

Unlock security context to drive investigation

Automate SecOps for greater efficiency

Security Providers

- Azure ATP
- Azure AD Identity Protection
- Windows Defender ATP
- Azure Security Center
- Office 365 ATP
- Cloud Application Security
- Azure Information Protection
- Intune
- Ecosystem Partners

Data and Actions

Microsoft Graph Security API

- Alerts
- Security Profiles
  Host | User | File | App | IP
- Actions
- Configurations

Other Microsoft Graph Services
Office 365 | Intune | Active Directory | More...

- Users
- Groups
- Mail
- Files
- Calendar

Insights and relationships

Authentication & Authorization

OAuth 2.0 and OpenID Connect 1.0

Supported SDKs and Sample Code

- ASP.NET MVC
- Xamarin
- UWP
- JavaScript
- Angular
- PHP
- Android
- iOS
- Ruby
- Python

Sensitive data is protected

Customers control access to their security data

App Access

Customer grants permission for the application to access their data via the Security API

Requests are brokered by the Security API, no data is stored

Access can be revoked by the customer at any time

+

User Access

User permissions can be managed in either of the following ways:

Delegated access

Customer assigns users to AAD role(s): Security Reader or Security Administrator

App only

Application implements role-based access for users

Resources

https://developer.microsoft.com/en-us/graph/docs/concepts/permissions_reference#security-permissions

https://techcommunity.microsoft.com/t5/Using-Microsoft-Graph-Security/Authorization-and-Microsoft-Graph-Security-API/m-p/184376#M2

Roadmap

Public Preview (available now)

Beta of Security API in Microsoft Graph

Client C# SDK available for integration

Code samples for C# and Python

Support for *Alerts* from Azure Security Center and Azure Active Directory Identity Protection with Intune and Azure Information Protection coming soon

Unified SIEM integration through Azure Monitor (QRadar, Splunk, SumoLogic)

Developer forums on Microsoft Tech Community & Stack Overflow

General Availability (H2 2018)

Onboarding additional Microsoft and ecosystem products

Unlock new security context through *Security Inventory*

Adding automation through *Actions* and *Configuration*

Provider SDK and documentation for broad ecosystem integration

Additional client SDKs and sample code through Microsoft Graph

Azure Sentinel

Introducing Microsoft Azure Sentinel

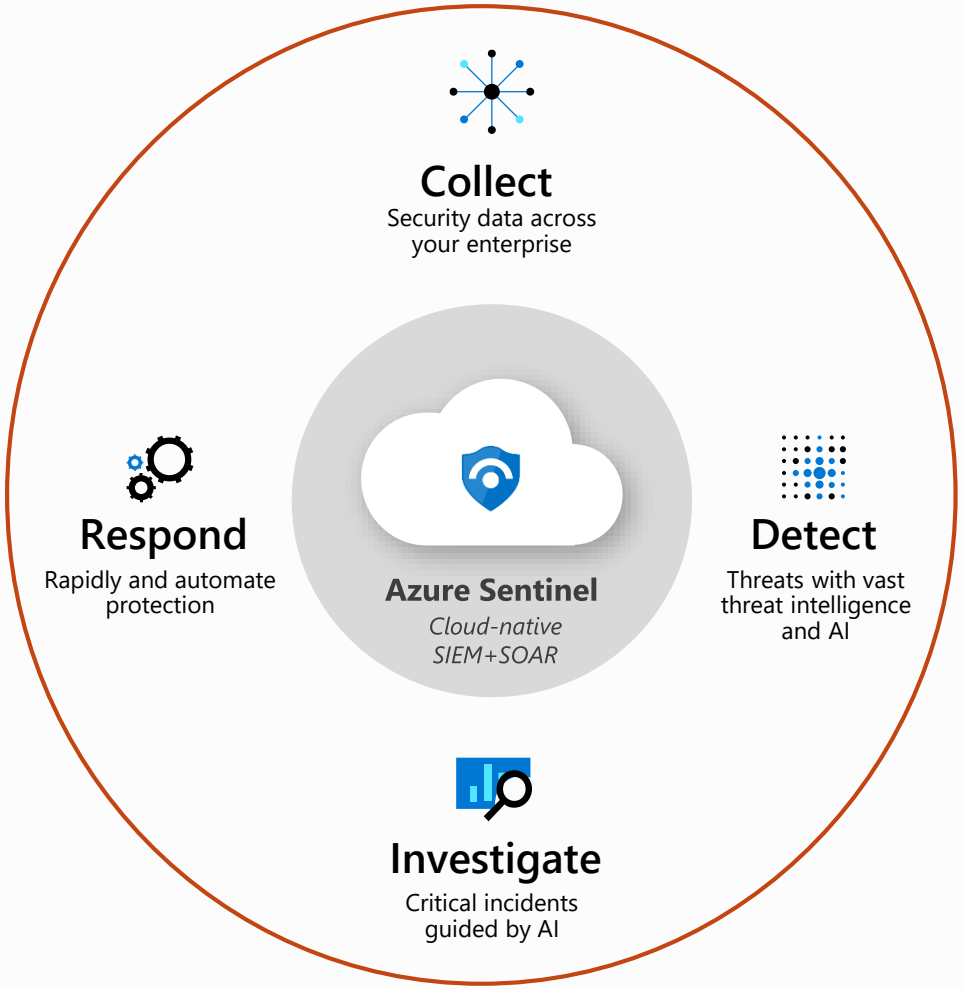
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**

Faster threat protection with **AI by your side**

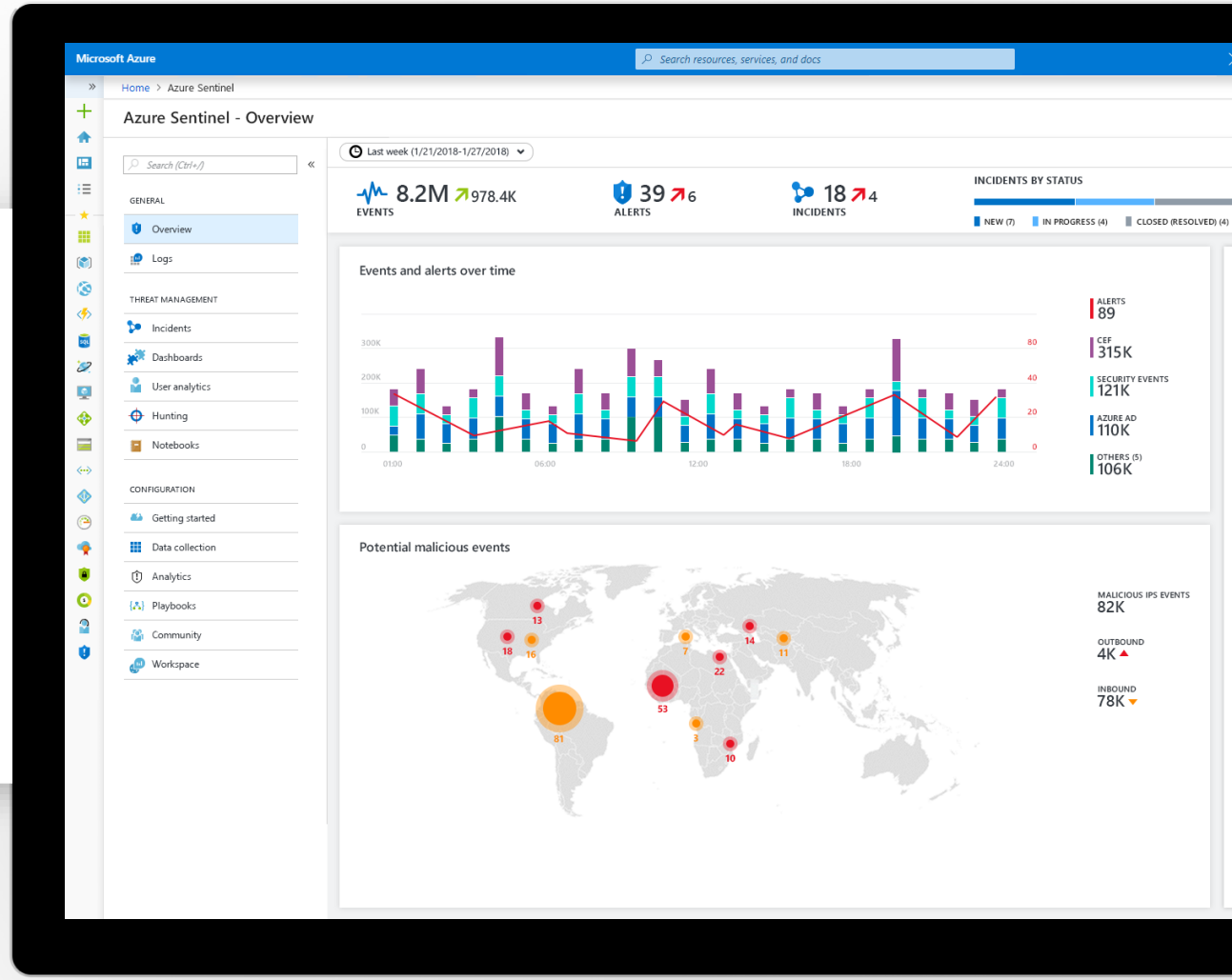


Focus on security, unburden SecOps from IT tasks

No infrastructure setup or maintenance

SIEM Service available in **Azure portal**

Scale automatically, put no limits
to compute or storage resources



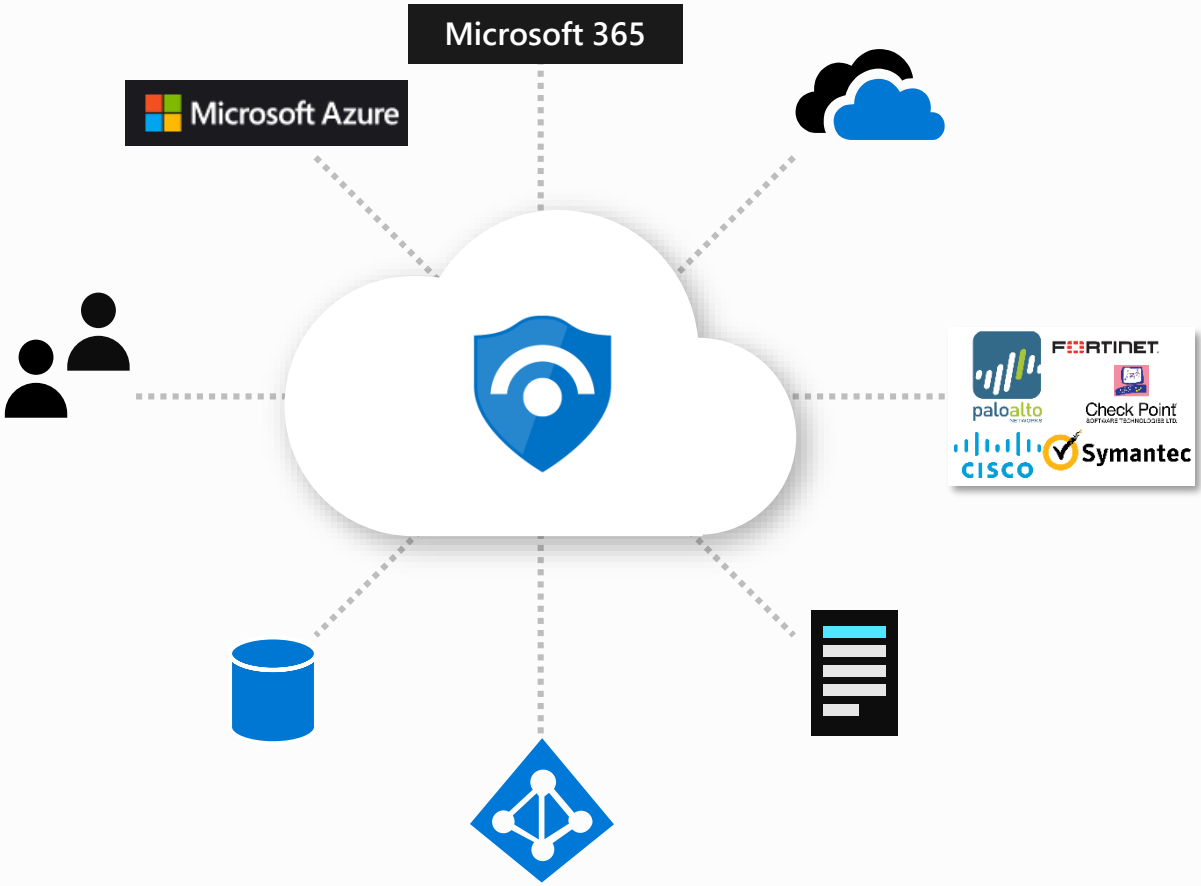
Collect security data at cloud scale from all sources across your enterprise

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

Proven log platform with **more than 10 petabytes** of daily ingestion



Resources

- Azure Security Documentation Center
  https://docs.microsoft.com/en-us/azure/security/
- https://docs.microsoft.com/en-us/azure/security/security-white-papers
- Azure Security Introduction
  https://docs.microsoft.com/en-us/azure/security/azure-security
- Azure Solutions Security Best Practices
  https://azure.microsoft.com/en-us/resources/security-best-practices-for-azure-solutions/
- Develop Secure Azure Solutions Whitepaper
  https://docs.microsoft.com/en-us/azure/security/abstract-develop-secure-apps

Resources

- Azure Trust Center
  http://azure.microsoft.com/en-us/support/trust-center/
- http://www.microsoft.com/trustcenter
- https://servicetrust.microsoft.com/
- Azure Security Blog
  http://blogs.msdn.com/b/azuresecurity/
- Azure Network Security Whitepaper
  https://azure.microsoft.com/en-us/blog/microsoft-azure-network-security-whitepaper-version-3-is-now-available/

Resources - PaaS

Azure Trust Center

- Securing PaaS deployments
- Securing PaaS web and mobile applications using SQL Database and SQL Data Warehouse
- Securing PaaS web and mobile applications using Azure App Services

Resources – Code Analysis

- Understanding SAL (source code annotation language)
  http://msdn.microsoft.com/en-us/library/hh916383.aspx
- Analyzing Application Quality by Using Code Analysis Tools
  http://msdn.microsoft.com/en-us/library/dd264897.aspx
- Visual Studio Static Code Analysis in depth: What? When and how?
  http://blogs.msdn.com/b/hkamel/archive/2013/10/24/visual-studio-2013-static-code-analysis-in-depth-what-when-and-how.aspx

Resources – Threath Modeling Azure

- Azure Security Docs on Threat Modeling
  https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool
- Article on the Importance of Threat Modeling
  https://msdn.microsoft.com/magazine/dd347831.aspx
- Microsoft Security Development Lifecycle Core Training
  https://www.microsoft.com/en-us/download/details.aspx?id=16420

Resources - SDL

- SDL Portal
  http://www.microsoft.com/sdl
- SDL Blog
  http://blogs.msdn.com/sdl/
- Simplified Implementation of the Microsoft SDL
  http://go.microsoft.com/?linkid=9708425
- Forrester Consulting Report "State of Application Security"
  http://go.microsoft.com/?linkid=9758989
- Aberdeen Group Report "Security and the Software Development Lifecycle: Secure at the Source"
  http://go.microsoft.com/?linkid=9769560