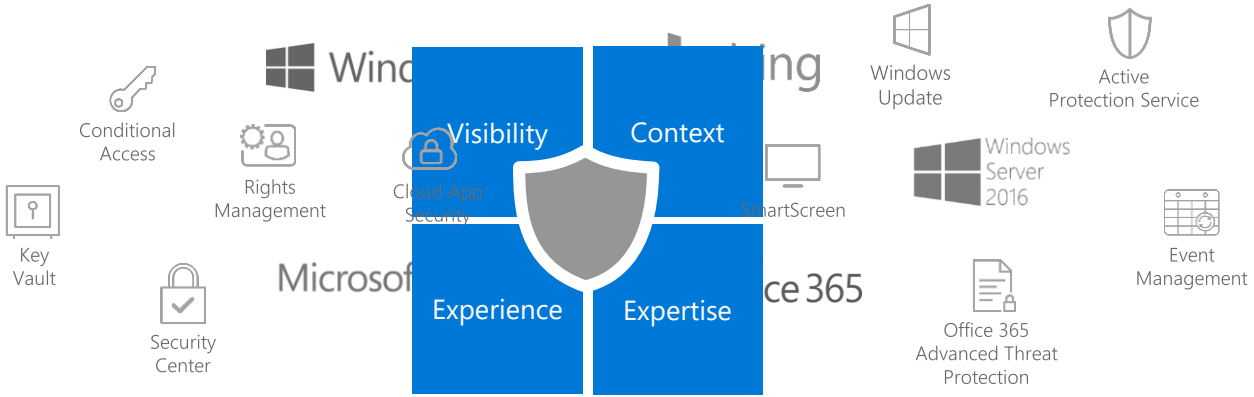
Topics

- Microsoft and Security
- Shared Responsibility
- How does Microsoft Secure the Platform
- Azure Regions – Azure Gov Cloud
- Securing Customer environment
  - Data Security
    - Encryption
  - Identity
  - Network Security
    - Network isolation
    - First party and third party controls
    - Hybrid Cloud - VPN and Express Route Connectivity
- Logging, Monitoring, and Operations
  - Azure Security Center and OMS
- Partner Security Solutions

Microsoft industry leading security capabilities



VISIBILITY

- **Malware** largest anti-virus and antimalware service
- **Clients** Windows Updates, Error Reports
- **Email** Outlook.com, Office 365
- **Web content** Bing, Azure AD
- **Cloud platform** Azure IaaS and PaaS, Azure Security Center

CONTEXT

- **Trillions** of URLs indexed
- **Hundreds of Billions** of authentications, monthly emails analyzed
- **Billions** of daily web pages scans, Windows devices reporting
- **Hundreds of Millions** of reputation look ups
- **Millions** of daily suspicious files detonations

EXPERIENCE

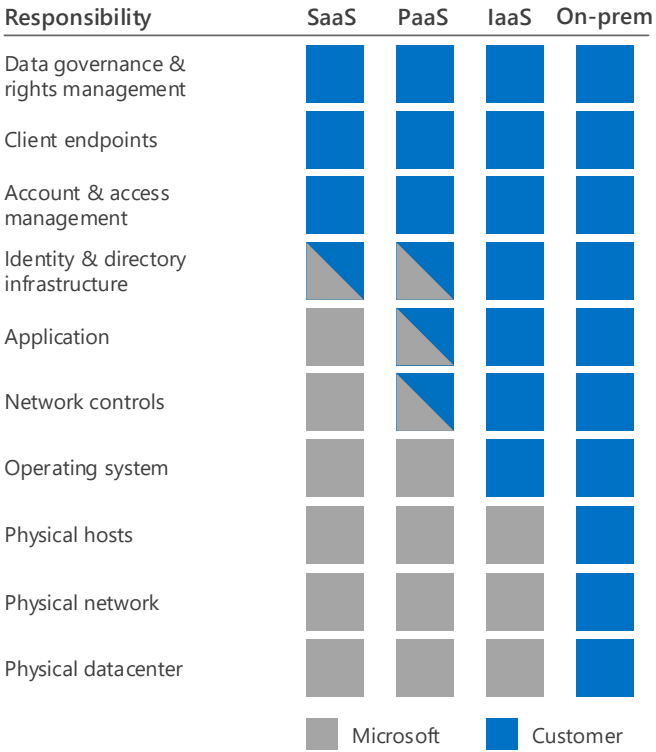
- **1M+** Corporate Machines protected by enterprise IT security
- **Multi-platform** cloud-first hybrid enterprise
- **Decades of experience** as a global enterprise
- **Runs on multi-tenant Azure environment**, same as you

EXPERTISE

- **Development Security** established Security Development Lifecycle (SDL) - ISO/IEC 27034-1
- **Operational Security** for Hyper-scale cloud services
- **Combatting Cybercrime** in the cloud & partnering with law enforcement to disrupt malware
- **Incident Investigation** and recovery for customers

Microsoft spends $1B+ on security R&D every year

Shared Security Model



Security threats targeting all layers

Attacks ultimately target data

Everything else required to secure the data

Security responsibilities shift

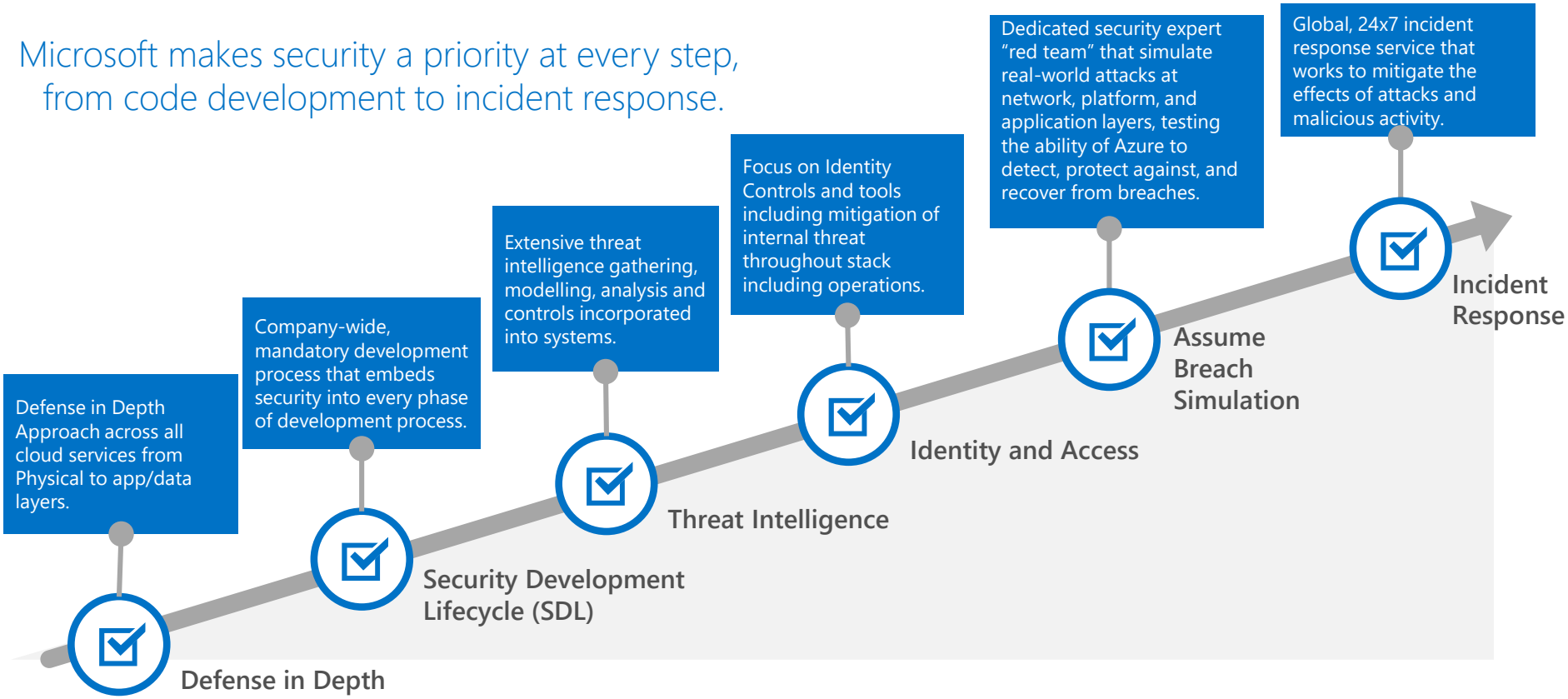
Per workload

Cloud service provider responsibility

Tenant responsibility

Microsoft Cloud Security Practices

Microsoft makes security a priority at every step, from code development to incident response.



Achieve global scale, in local regions

Trust

42

Azure regions

RECENTLY LAUNCHED:

US Gov: US Gov Texas and US Gov Arizona

NEWLY ANNOUNCED:

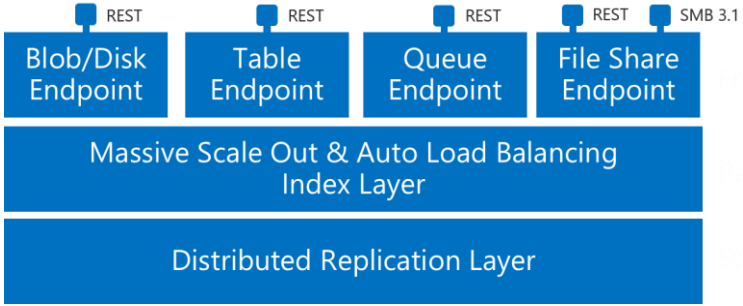
France: France Central and France South

Africa: South Africa North and South Africa West

Data in Azure

Azure Cloud Storage:

- Object based, durable, massively scalable storage subsystem
- Designed from ground up by Microsoft
- Presents as Blobs, Disks, Tables, Queues and Files
- Accessed via REST APIs, Client Libraries and Tools
- Access control:
  - Leverage Symmetric Shared Key Authentication
    - Trusted service that owns the storage accounts
  - Shared Access Signature (SAS)



Scale:

- More than 25 trillion stored objects
- 2.5+ Million requests/sec on average

Storage System Design and Architecture:

- Architecture and design details published and available “Windows Azure Storage – A Highly Available Cloud Storage Service with Strong Consistency

Azure Data Encryption - Data at Rest

Application Layer

- **BYO Encryption** - <.NET Librabries, Leverage on-prem HSM, etc.>

PaaS Services

- **SQL Database** - *<Transparent Data Encryption, Always Encrypted>*
- **HDInsight** - *<SQL Database>*
- **Azure Backup Service** - *<Leverages Azure Disk Encryption>*

Virtual Machine/OS Layer – Windows, Linux

- **Azure Disk Encryption** - *<BitLocker [Windows], DM-Crypt [Linux]>*
- **Partner Volume Encryption** – <CloudLink® SecureVM>
- **BYO Encryption** – <Customer provided>

Storage System

- **Azure Storage Service Encryption** – *<AES-256, Block, Append, and page Blobs>*

Keys Management

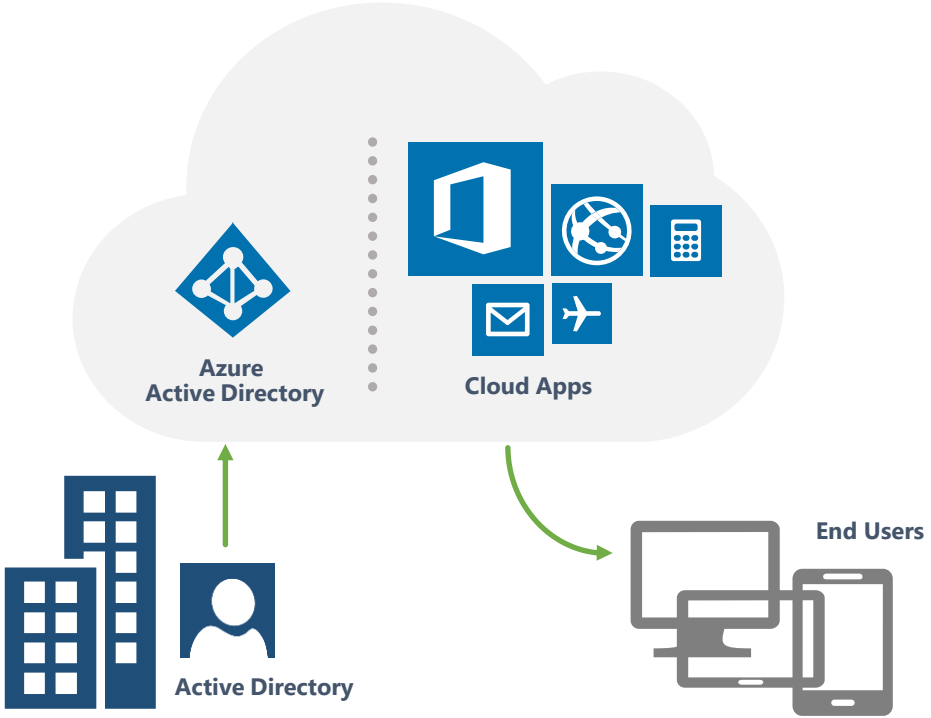
Azure Key Vault

<Keys and Secrets controlled by customers in their key vault>

Authentication to Key Vault

<Authentication to Key Vault is using Azure AD>

Enterprise cloud identity – Azure AD



AZURE:

- Provides enterprise cloud identity and access management
- Enables single sign-on across cloud applications
- Offers Multi-Factor Authentication for enhanced security

CUSTOMER:

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

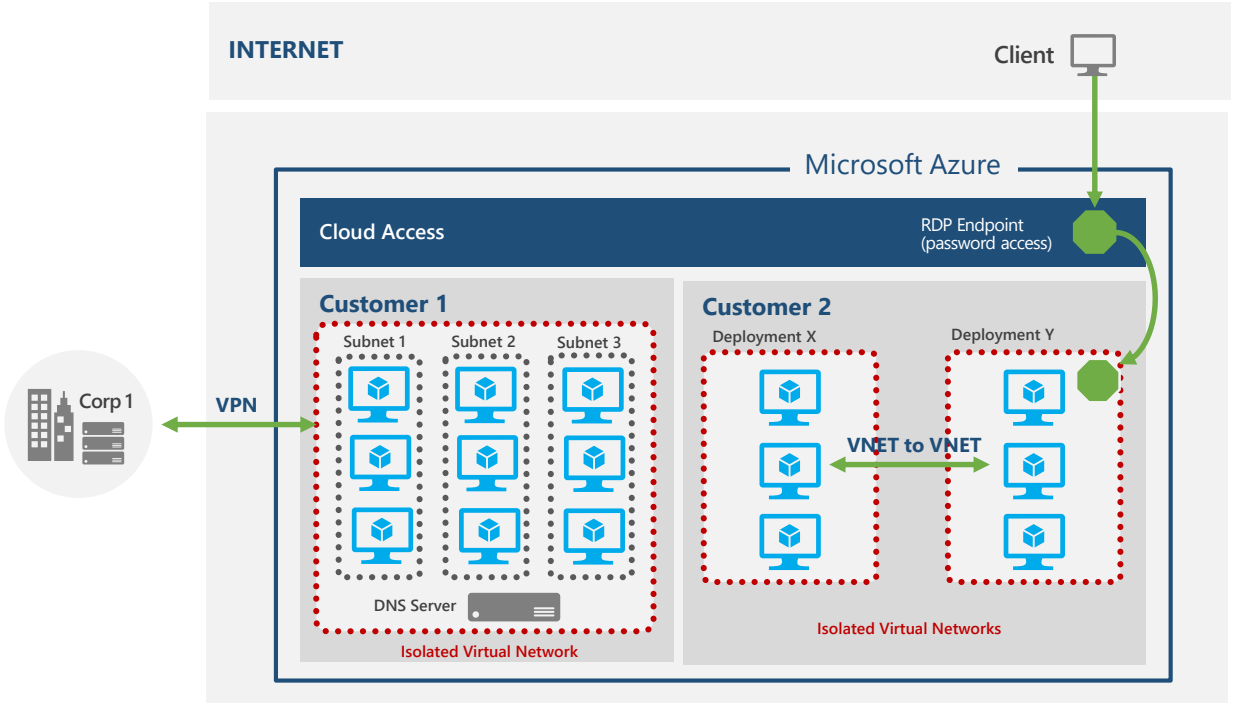
Azure Virtual Networking

AZURE:

- Allows customers to create isolated virtual private networks

CUSTOMER:

- Creates Virtual Networks with Subnets and Private IP addresses
- Enables communications between their Virtual Networks
- Can apply security controls
- Can connect to “corpnet” via VPN or Express Route



Platform Network Control – Network Security Groups (NSG)

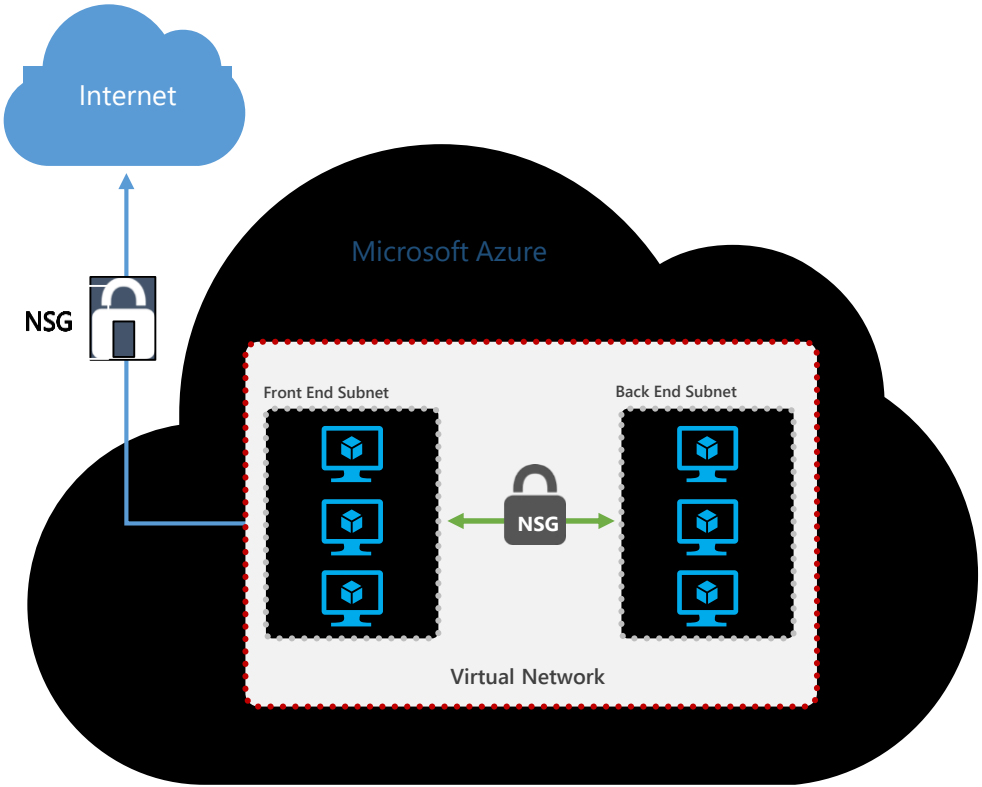
Grouping of network traffic rules as security group

Security groups associated with virtual machines or virtual subnets

Controlled access between machines in subnets

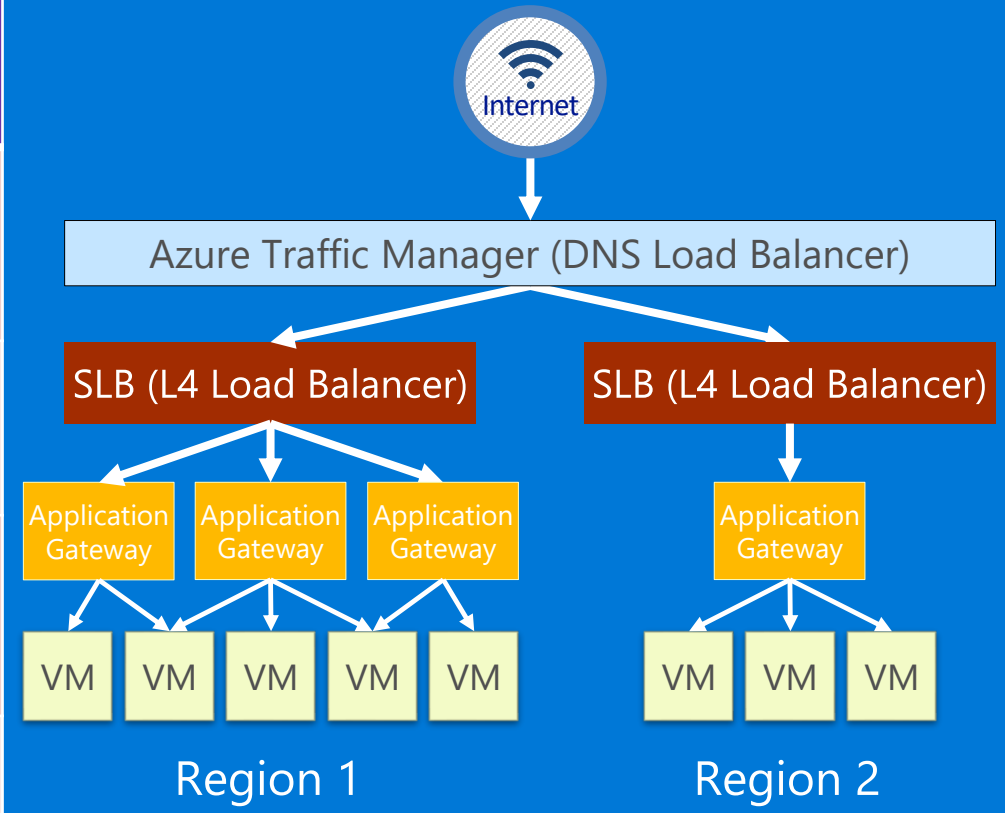
Controlled access to and from the Internet

Network traffic rules updated independent of virtual machines



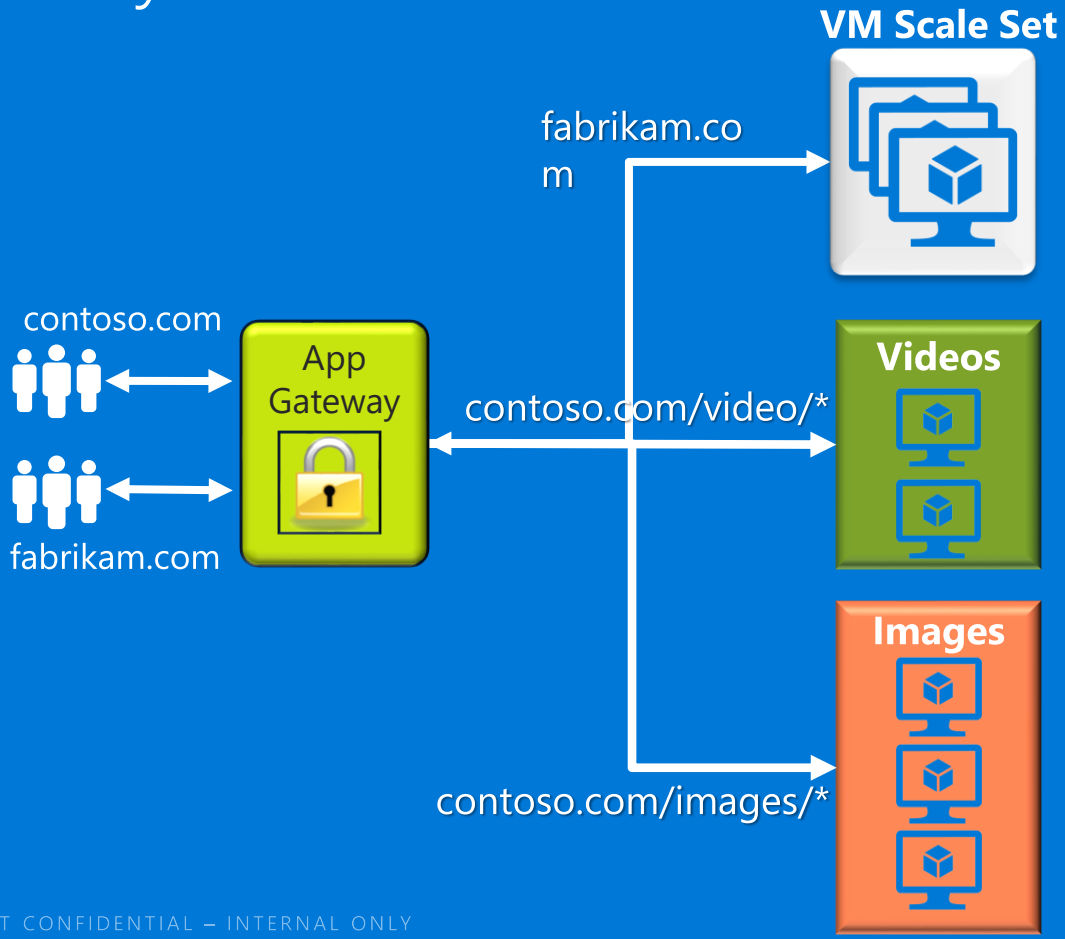
Platform Load Balancers

Azure Service	What	Example
Traffic Manager	Cross-region redirection & availability	http://news.com ➔ apac.news.com ➔ emea.news.com ➔ us.news.com
Azure Load Balancer	In-region scalability & availability	emea.news.com ➔ AppGw1 ➔ AppGw2 ➔ AppGw2
Azure Application Gateway	URL/content-based routing & load balancing	news.com/topnews news.com/sports news.com/images
VMs	Web Servers	

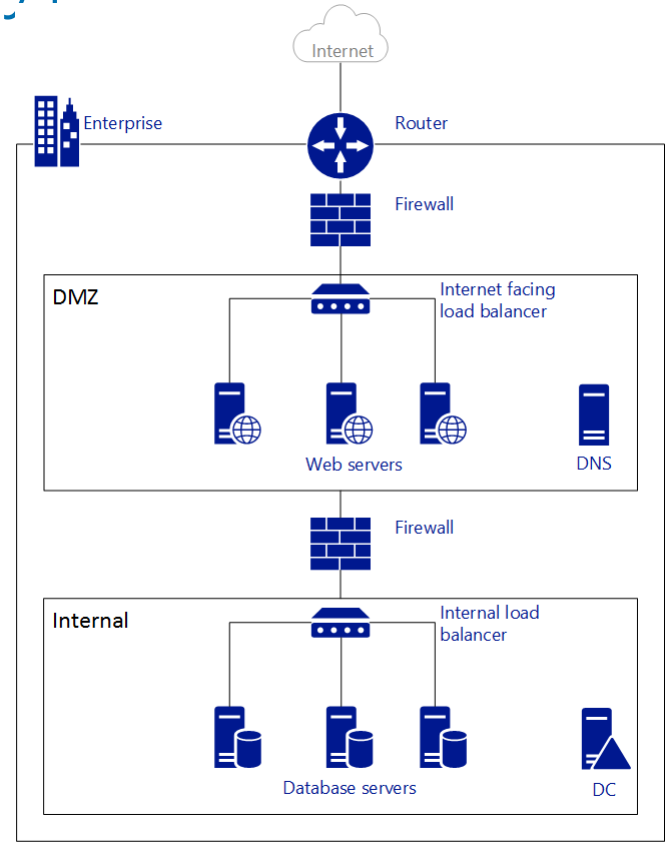


Application Gateway: Layer 7 ADC Features

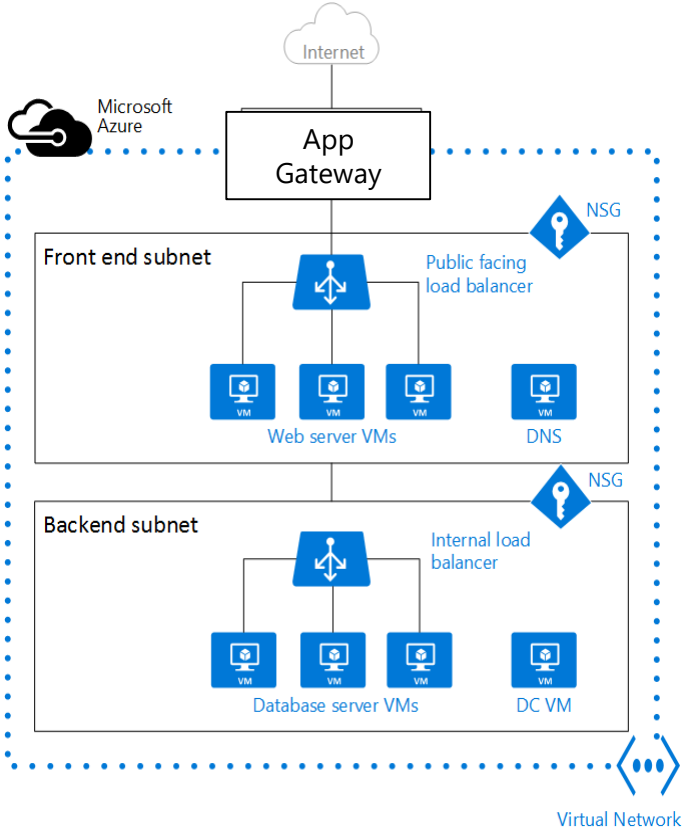
- Security
  - SSL termination
  - Allow/block SSL protocols
  - WAF – OWASP ModSecurity Core Rule Set
- Session & site management
  - Cookie based session affinity
  - Multi-site hosting – up to 20 web applications or sites
- Content management
  - URL based routing
- Backend management
  - Rich diagnostics including Access and Performance logs
  - VM Scale Set support
  - Custom health probes



Typical Tiered Architecture

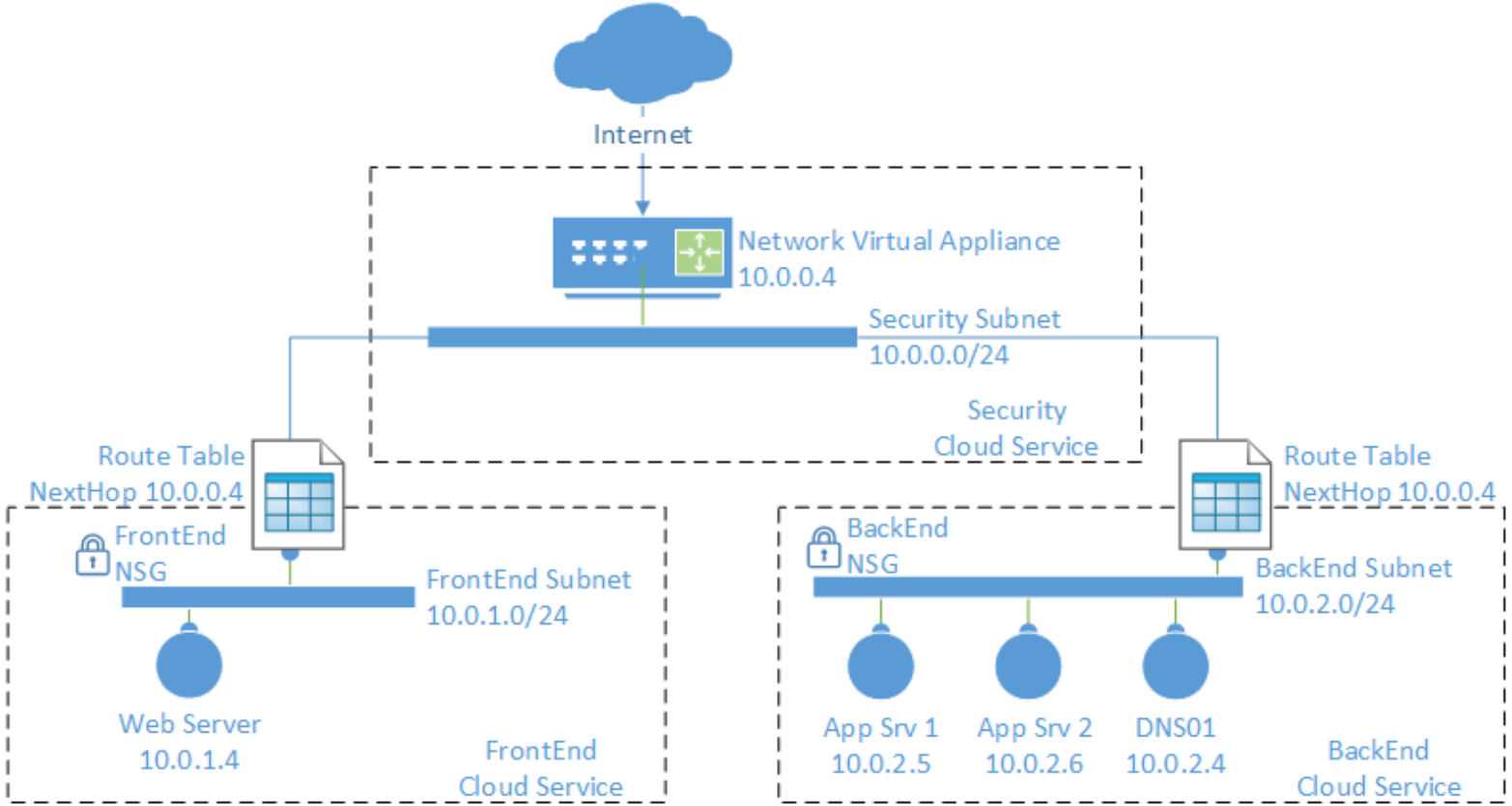


Simplified On-Prem Network

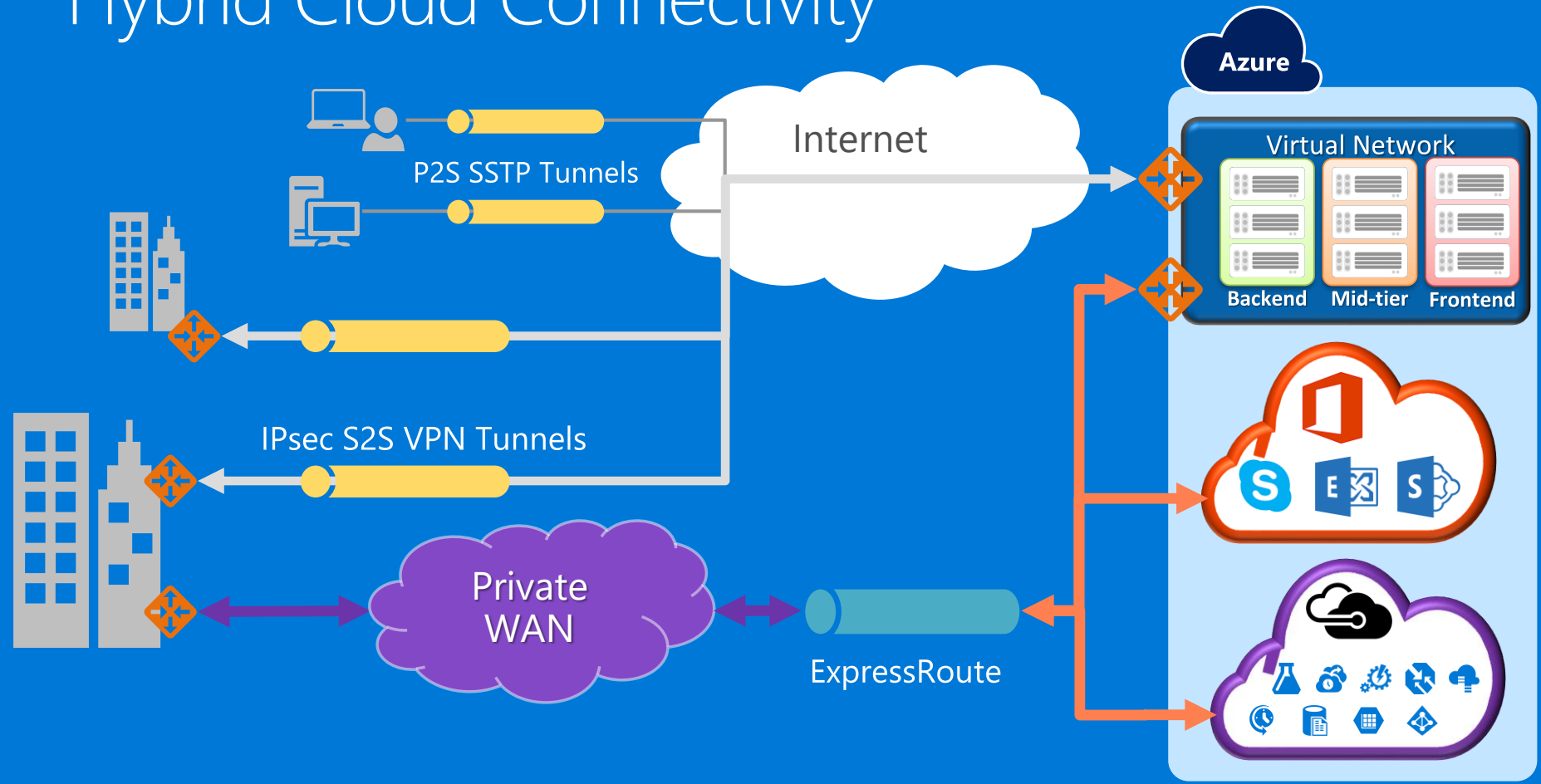


As deployed in Azure

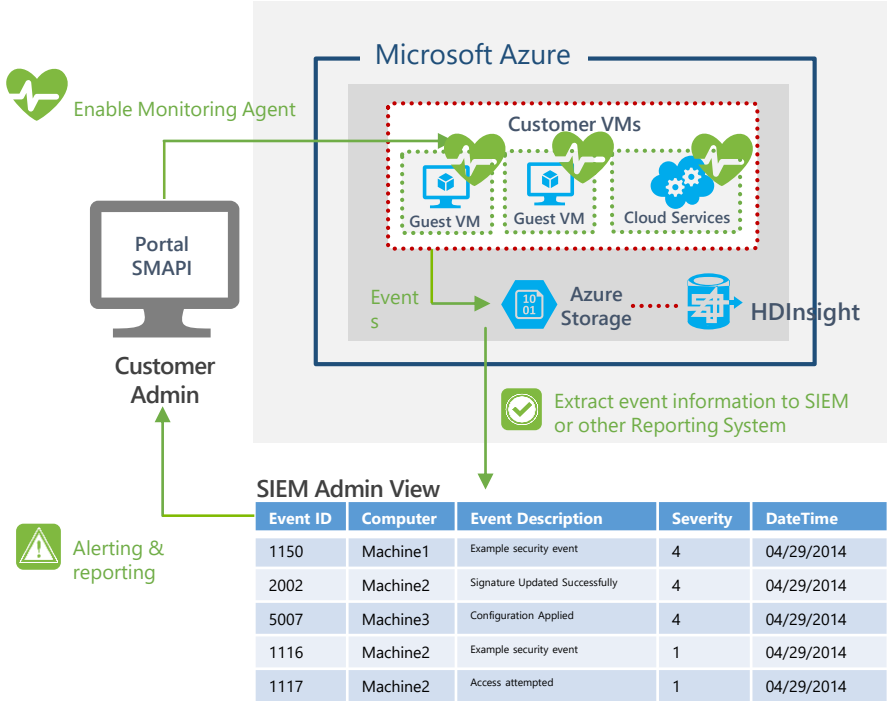
User Defined Routing and Virtual Appliances



Hybrid Cloud Connectivity



Monitoring & logging



Event ID	Computer	Event Description	Severity	DateTime
1150	Machine1	Example security event	4	04/29/2014
2002	Machine2	Signature Updated Successfully	4	04/29/2014
5007	Machine3	Configuration Applied	4	04/29/2014
1116	Machine2	Example security event	1	04/29/2014
1117	Machine2	Access attempted	1	04/29/2014

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

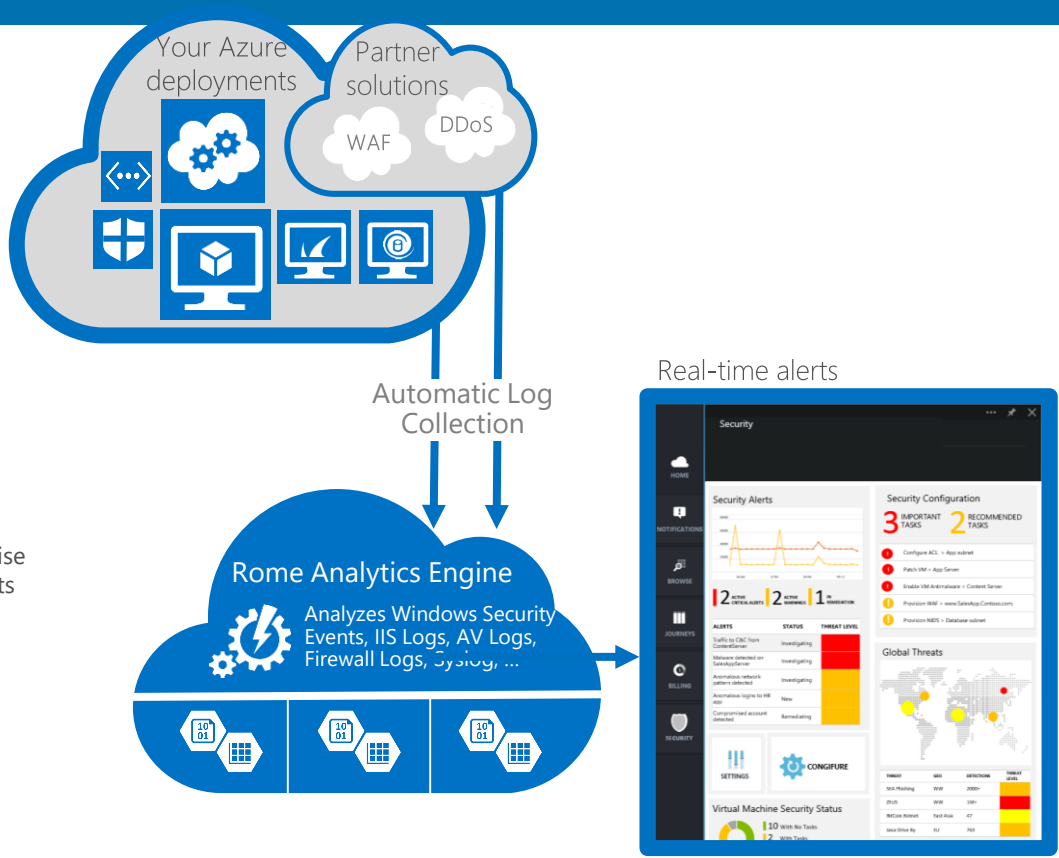
Azure Security Center

What is the feature?

Prevent, detect and respond to threats with increased visibility and control over the security of your Azure resources and advanced analytics, which identify attacks that might otherwise go unnoticed

Benefits

- Understand the security state of Azure resources
- Take control of cloud security with policies that enable you to recommend and monitor security configurations
- Make it easy for DevOps to deploy integrated Microsoft and partner security solutions
- Find threats with advanced analysis of your security-related events developed using Microsoft's vast global intelligence assets and expertise
- Respond and recover from incidents faster with real-time security alerts
- Export security events to a SIEM for further analysis



Operations Management Suite

Log analytics

- Near real time perf. data collection/monitoring
- Linux agents including monitoring integrations
- Mobile Apps in Windows, Android and iOS
- Custom fields
- SOC1 and SOC2 Type 1 Compliant

Backup & disaster recovery

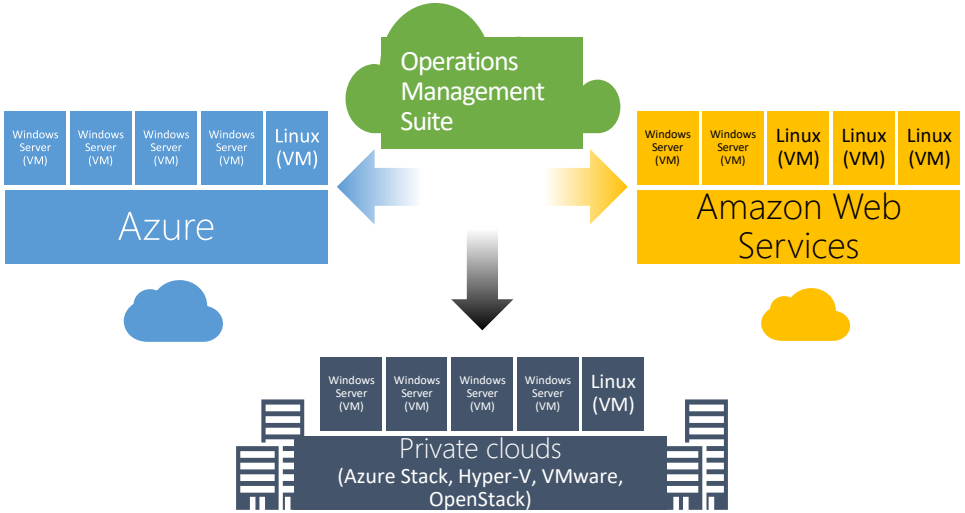
- Backup >1.6TB support
- ASR integration with SQL Always-On public preview
- ASR CSP and IaaS V2 support
- IaaS v1 & v2 VMs backup
- Azure backup server for application workload backups

IT automation

- Automation DSC
- Source Control support through GitHub for runbooks
- Hybrid support for schedules / test jobs
- PowerShell script support on hybrid workers
- Linux DSC support

Security & compliance

- Wire data solution
- Azure network analytics solution
- Malicious IP detection



Partner Security Solutions

Microsoft is dedicated to working with partners across the ecosystem enabling customers to augment their security posture

Network Virtual Appliances

Hosted Network Controls – Firewalls,WAF, Ddos, IDS/IPS, DLP

Operations/Management – Monitoring, logging, correlation

Penetration Testing

Vulnerability assessments/Threat Modeling