Mike Nelson

Technical Marketing Engineer @ Rubrik

@nelmedia
mike@geektweakers.com

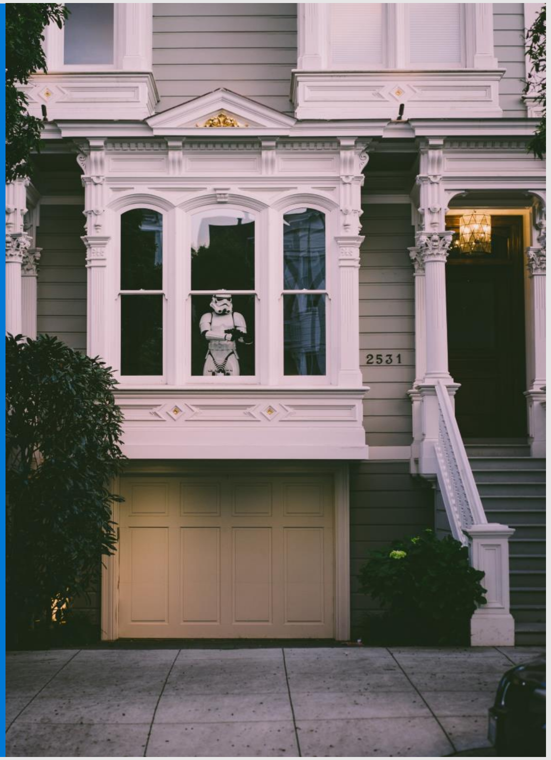
Microsoft MVP – C&DM
Microsoft Azure Advisor
Citrix CTP
VMware vExpert

#vBrownBag

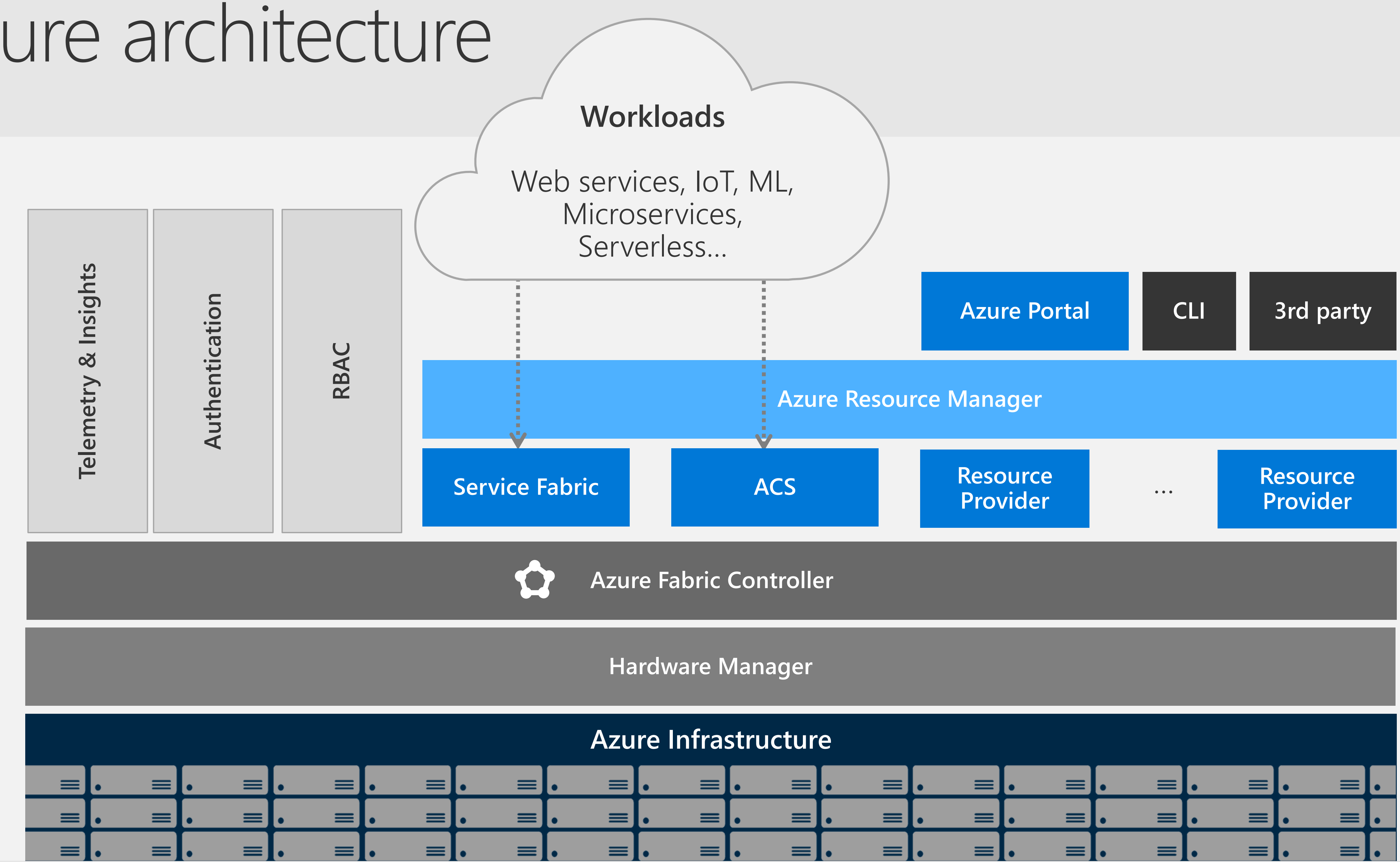
Is this your cloud security?

Interesting Security Info

- 2+ million breach attempts per day
- Three highest percentage of “encounters”:
  - Botnets
  - Phishing
  - Ransomware
- Over 1k brute force attacks every second
- Gamaru Botnet (aka Andromeda) tops all disruptions since Conficker with 1800+ CaCC’s, 464 distinct botnets, & 80+ malware variant families
- Botnet Kits widely available
- Ransomware-as-a-Service now available!



Azure architecture



Workloads

Web services, IoT, ML, Microservices, Serverless…

Alternatives to IaaS to consider

Containers	PaaS	SaaS	Minimal OS	Serverless
Not just for DevOps anymore Very secure and completely controllable security layers for standalone containers Container Services are more PaaS managed	Security layers controlled by provider Compliance and governance are more static than dynamic	Security layers controlled by provider “Buy it and forget it”	Security hardened OS Limited applications and drivers Linux and Windows flavors	Everything as a service, PaaS, SaaS, xaaS It’s really not “Serverless”

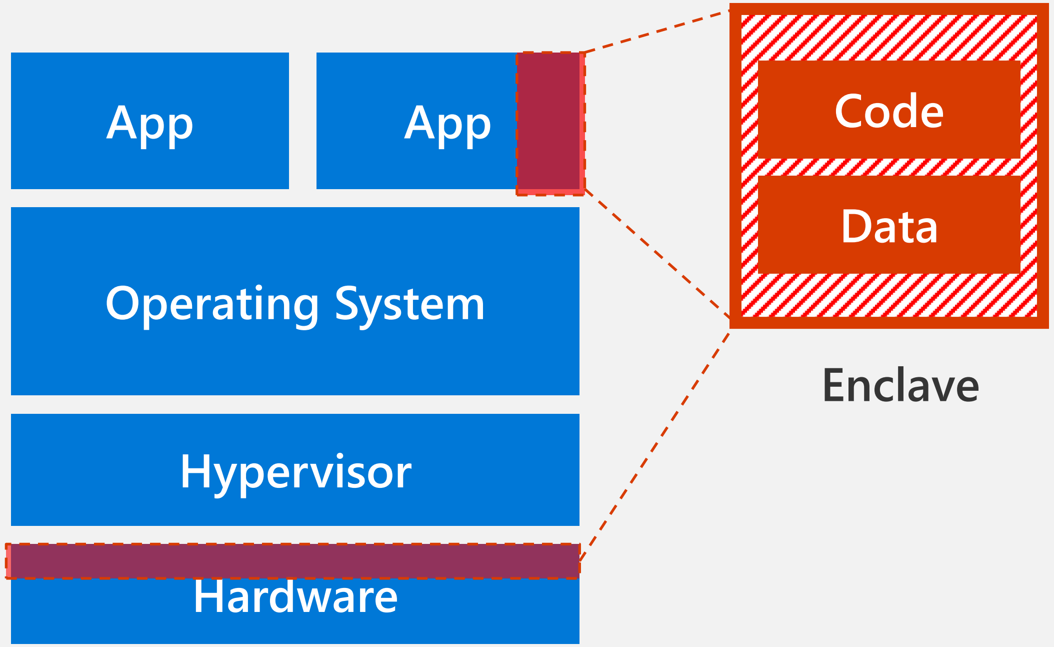
Confidential computing

Based on Trusted Execution Enclaves (TEEs)

- Windows Server Virtual Secure Mode
- Intel SGX

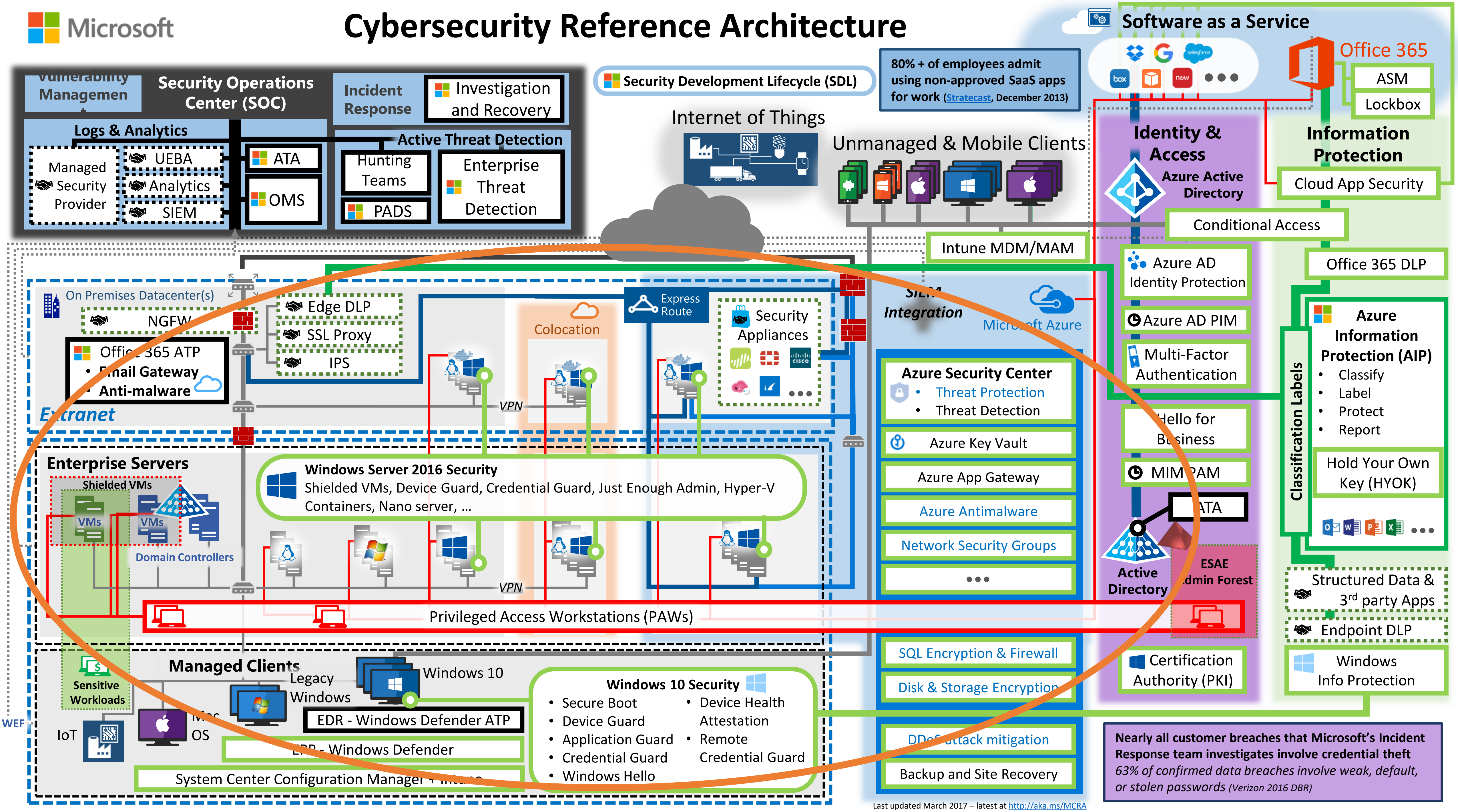
Protected Container

- Isolated portion of processor & memory
- Code or data cannot be viewed or modified from outside
- Supports attestation: proving of identity
- Supports sealing: persisting secrets
- Customer workloads are invisible to host fabric
- Customer data is always encrypted – during compute and storage



Microsoft

Cybersecurity Reference Architecture



80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)

Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft

63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

Last updated March 2017 – latest at http://aka.ms/MCRA

Security responsibility

MICROSOFT'S COMMITMENT

Securing and managing the cloud foundation

Physical assets

Datacenter operations

Cloud infrastructure

SHARED RESPONSIBILITY

Securing and managing your cloud resources

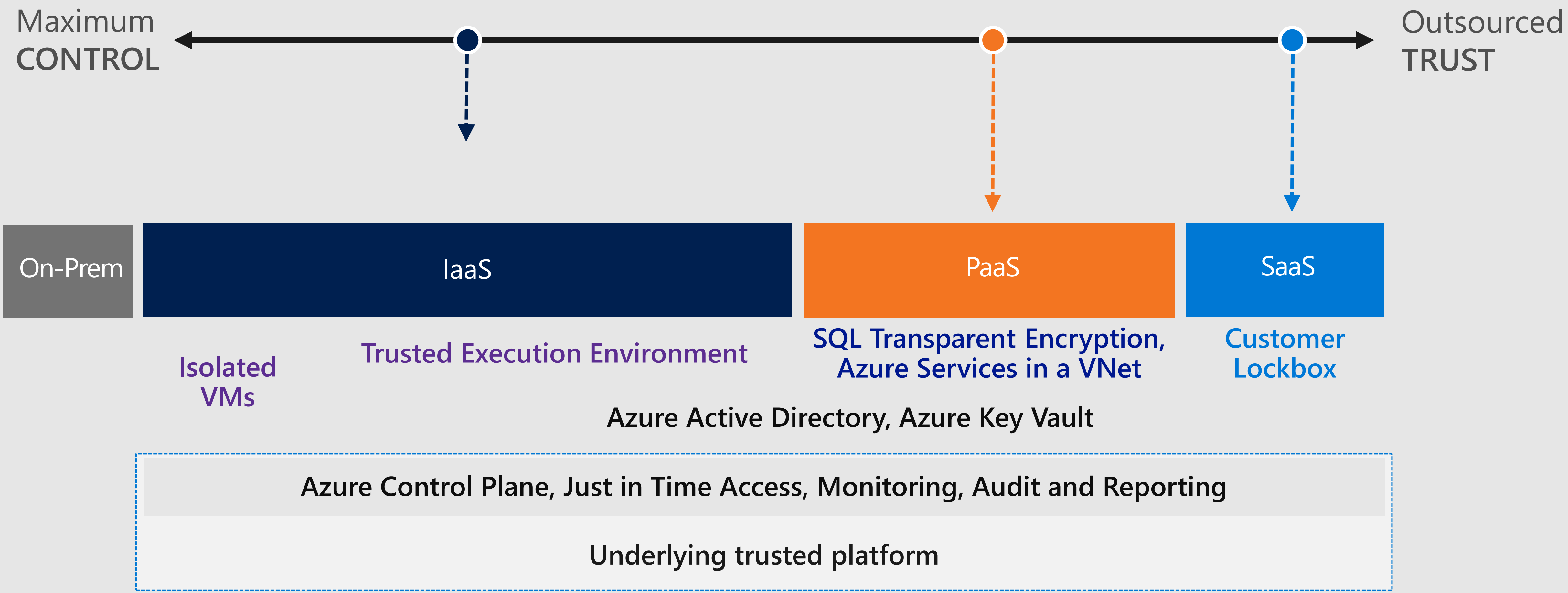
Virtual machines, networks & services

Applications

Data

VARIES ACROSS IAAS, PAAS, SAAS

Spectrum of control and trust



Maximum CONTROL

Outsourced TRUST

On-Prem

IaaS

PaaS

SaaS

Isolated VMs

Trusted Execution Environment

SQL Transparent Encryption, Azure Services in a VNet

Customer Lockbox

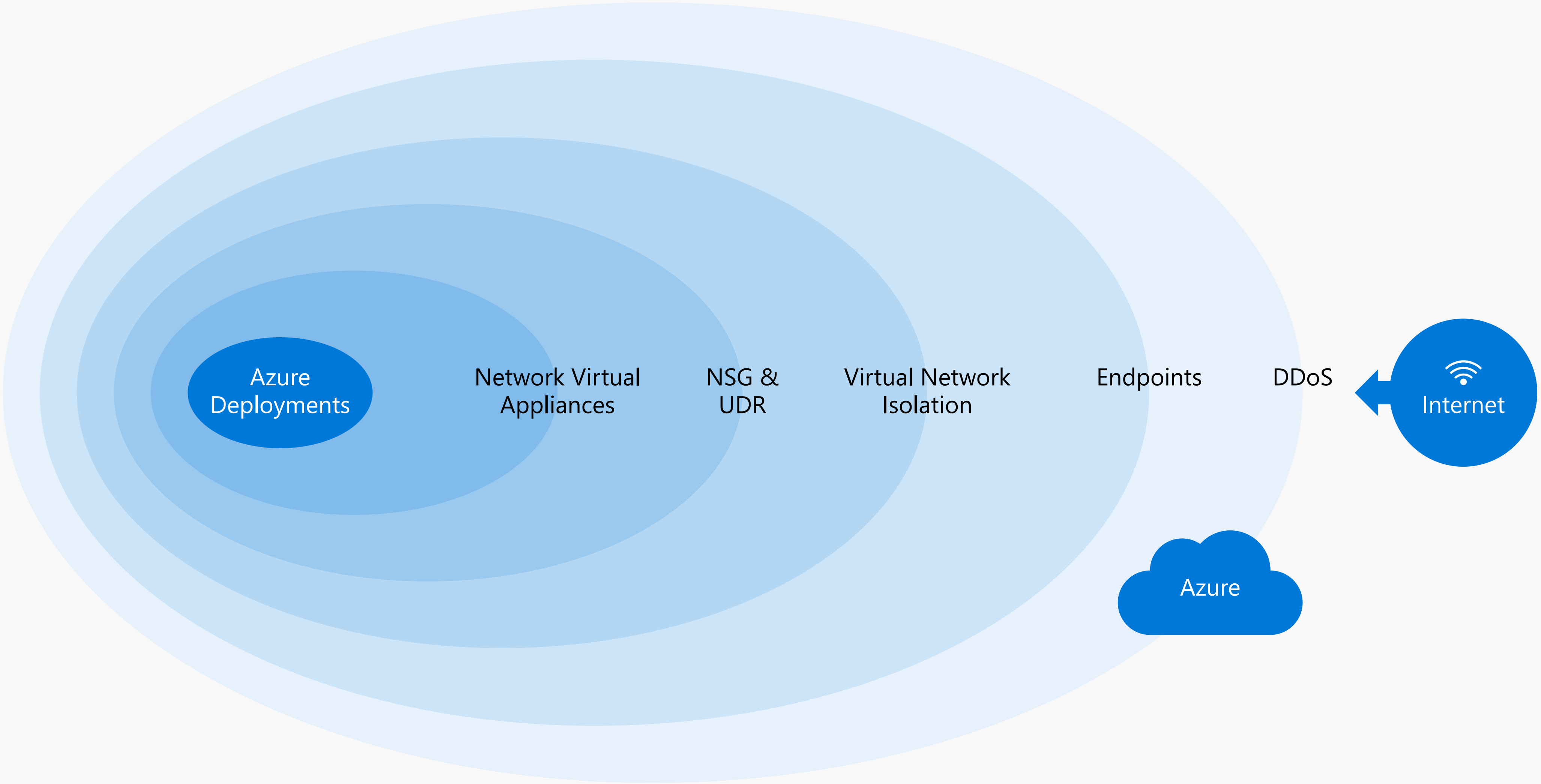
Azure Active Directory, Azure Key Vault

Azure Control Plane, Just in Time Access, Monitoring, Audit and Reporting

Underlying trusted platform

Where you land drives service model selection

Logical layered isolation



…is inherent in Azure design

Protecting IaaS means more than just virtual machines

VM protections are the focus, but the scope is increasing

Workloads contain VMs and servers, but also the supporting networks and services

Cloud is being used to describe modern workloads wherever they reside

IaaS Security POI

Identity

Azure Active Directory

Hybrid AD

Local users

MFA

Connectivity

Internet

Tunneling

Source IP

S2S VPN

ExpressRoute

Data Protection and Privacy

Storage Encryption

Disk encryption

VM encryption

RBAC

JiT access

Threat Defense

Security hardening

Advanced Threat Protection

Pen testing

Update management

Monitoring & alerting

Analytics

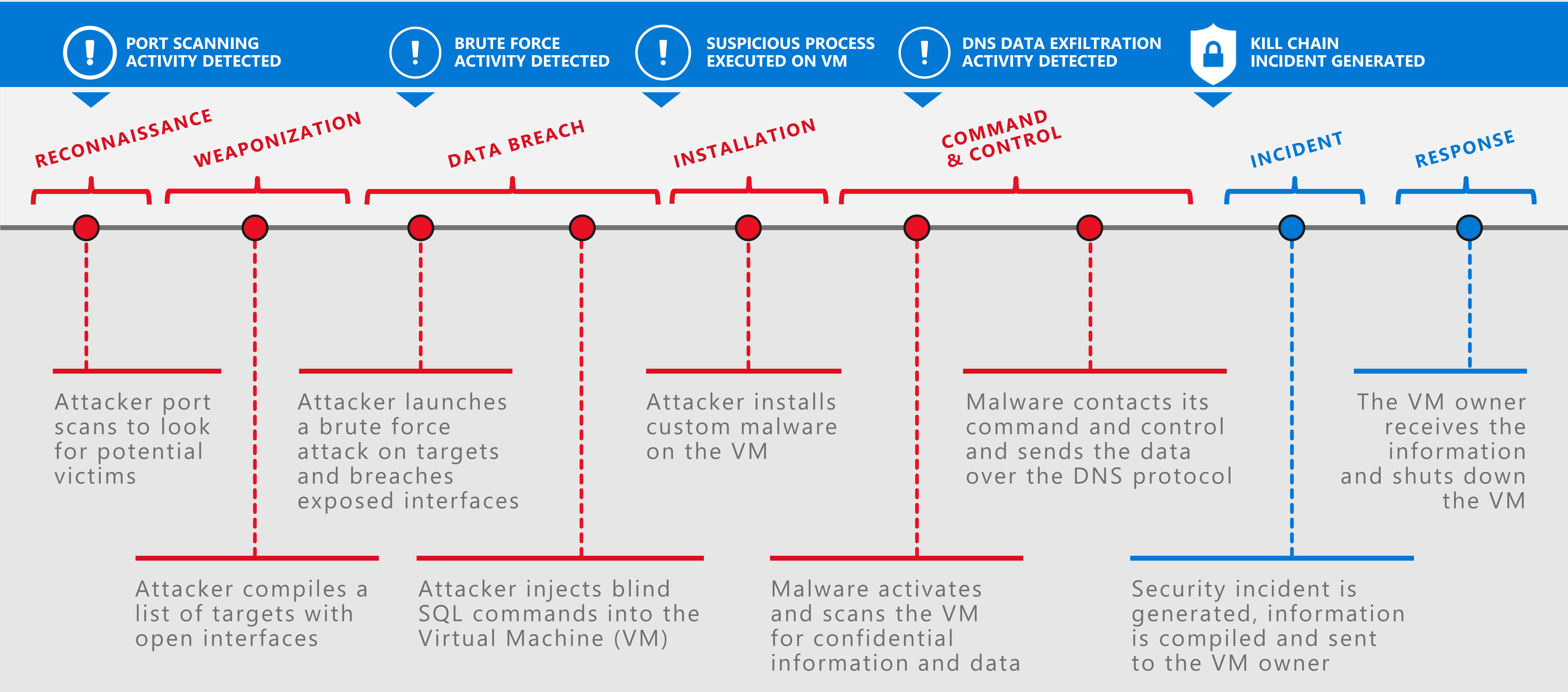
Compliance

Compliant services

Auditing

Policies

Anatomy of real attack in Azure



PORT SCANNING ACTIVITY DETECTED

BRUTE FORCE ACTIVITY DETECTED

SUSPICIOUS PROCESS EXECUTED ON VM

DNS DATA EXFILTRATION ACTIVITY DETECTED

KILL CHAIN INCIDENT GENERATED

RECONNAISSANCE

WEAPONIZATION

DATA BREACH

INSTALLATION

COMMAND & CONTROL

INCIDENT

RESPONSE

Attacker port scans to look for potential victims

Attacker compiles a list of targets with open interfaces

Attacker launches a brute force attack on targets and breaches exposed interfaces

Attacker injects blind SQL commands into the Virtual Machine (VM)

Attacker installs custom malware on the VM

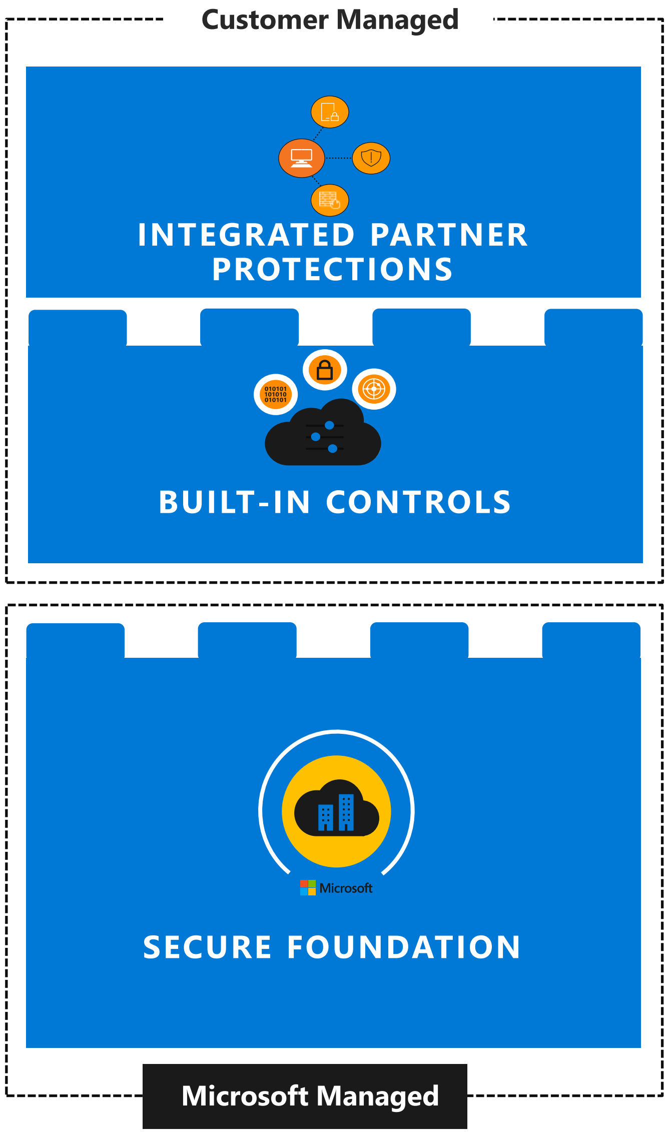
Malware activates and scans the VM for confidential information and data

Malware contacts its command and control and sends the data over the DNS protocol

Security incident is generated, information is compiled and sent to the VM owner

The VM owner receives the information and shuts down the VM

IaaS workload protection from Microsoft



Customer Managed

INTEGRATED PARTNER PROTECTIONS

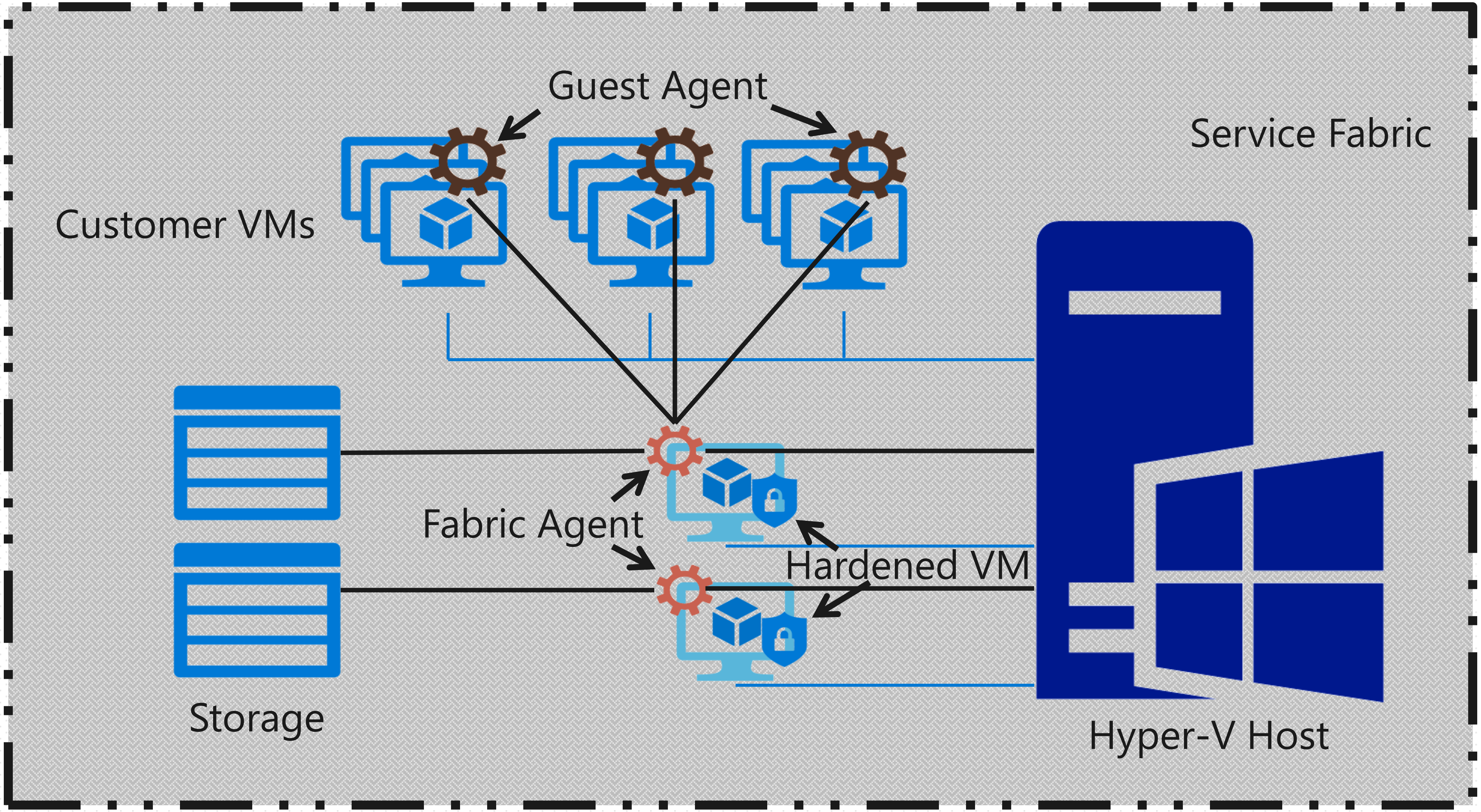
BUILT-IN CONTROLS

SECURE FOUNDATION

Microsoft Managed

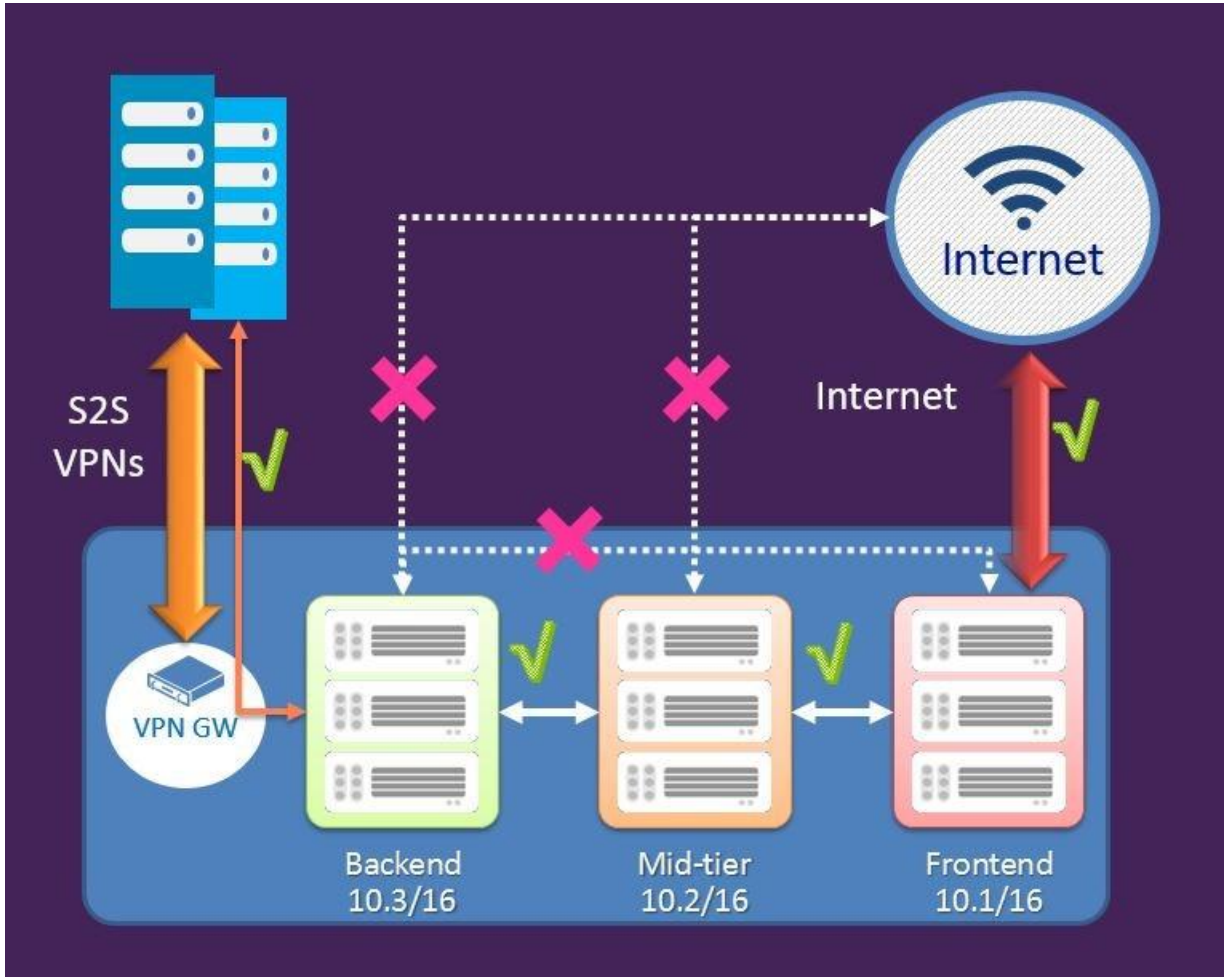
Azure Security Center

Compute Node Structure



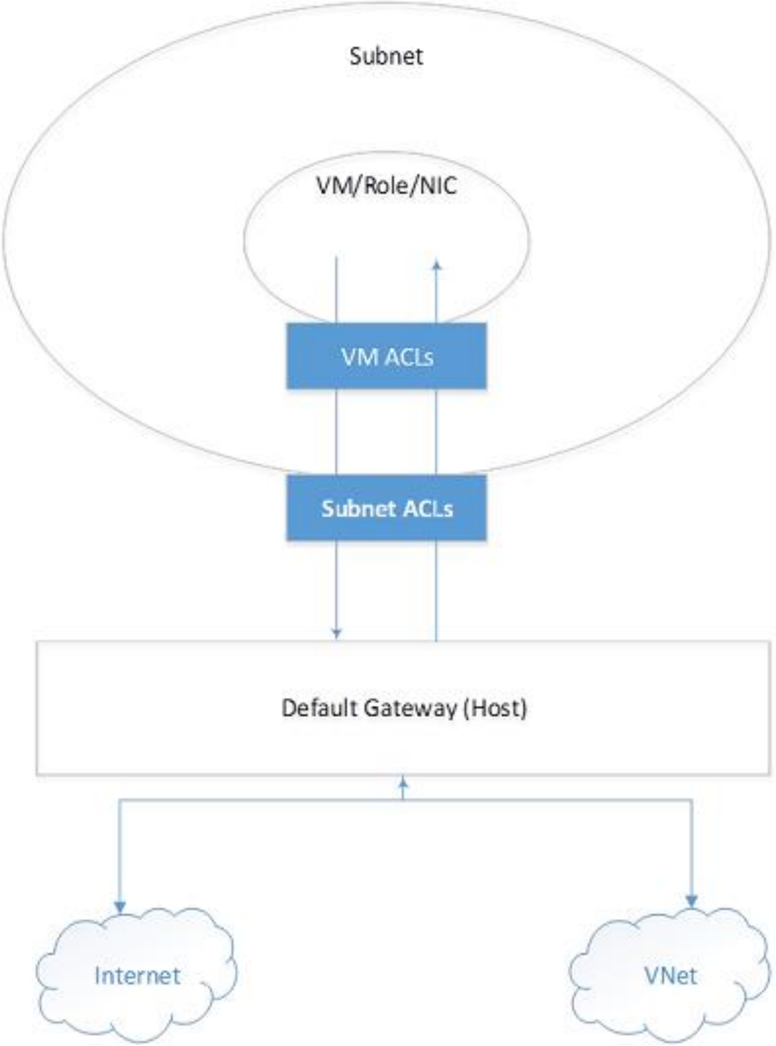
Network Security Groups (NSG)

- Define access control rules for inbound/outbound traffic to a VM or group of VMs in a subnet
- NSG rules can be changed at any time and apply to all instances
- NSG can be associated with:
  - A single VM in a VNet
  - A subnet in a VNet
  - A VM and a Subnet together for added security
- Rules are processed in order of priority
- Rules are based on 5-tuple (source/dest IP/port, protocol)



Network Security Groups (continued)

- Two different ACL groups, one for individual VM, one for Subnet
- Rules are applied to inbound traffic for subnet followed by rules for the VM
- Outbound rules are applied for VM first and then followed by subnet rules



Example PowerShell:

```
New-AzureNetworkSecurityGroup -Name "MyVNetSG" -Location uswest
-Label "Security group for my Vnet in West US"

Get-AzureNetworkSecurityGroup -Name "MyVNetSG" | Set-
AzureNetworkSecurityRule -Name WEB -Type Inbound -Priority 100
-Action Allow -SourceAddressPrefix 'INTERNET'  -SourcePortRange
'*' -DestinationAddressPrefix '*' -DestinationPortRange '*' -
Protocol TCP
```

Demos

@nelmedia
mike@geektweakers.com

Common issues / mistakes

- Do not put static IP configuration inside the OS
- Although we support Multiple VIPs per Virtual Network, you cannot create 2 endpoint with the same LocalPort using 2 different VIPs
- VMs lose IPs when are deallocated, use static IP for your VMs
- Machines in a virtual network lose the IP when all the instances are deallocated, use Reserved IP
- VMs secondary NIC cannot be used for public facing
- VMs requires Internet Access to contact license server (while using force tunneling). You can use custom routes in this scenario
  - http://blogs.msdn.com/b/mast/archive/2015/05/20/use-azure-custom-routes-to-enable-kms-activation-with-forced-tunneling.aspx
- ILPIP do not persist – similar to VIP
- Do not block (Allow) the IP address is 168.63.129.16. Microsoft Azure platform uses a static, publicly routable IPv4 address for a variety of administrative scenarios like ILB monitoring.

Common issues / mistakes

- NSG : First matching NSG is applied (not most restrictive)
- NSG: VM NSGs processed before subnet NSGs
- Express Route - Forced routing works with ExpressRoute enabled VNETS by BGP advertisement of default route:

  Windows Activation failures – be sure to setup Public Peering

  Effectively disables RDP access to VIP Endpoint
- Express Route - Billing begins with New-AzureDedicatedCircuit (not with connectivity)
- Azure PowerShell Version obsolete, check or use available scripts to be up to date.
- A region do not have the same services than other - Review Networking service availability in your region
  - http://azure.microsoft.com/en-us/regions/#services

Key Takeaways

Secure

Secure the VMs on creation & through lifecycle

Encrypt

Encrypt VM disks, storage, and data

Control

Control network traffic flows, rules, firewalls – limit exposure

Monitor

Monitor everything

Collect data

Collect security data and archive based on retention/compliance