Microsoft

#AzureEvent
#BuildWithAzure

Azure Workshop

GDPR, Security and Privacy features for cloud applications

Ben Roscorla, Mike Ormond, Robin Lester

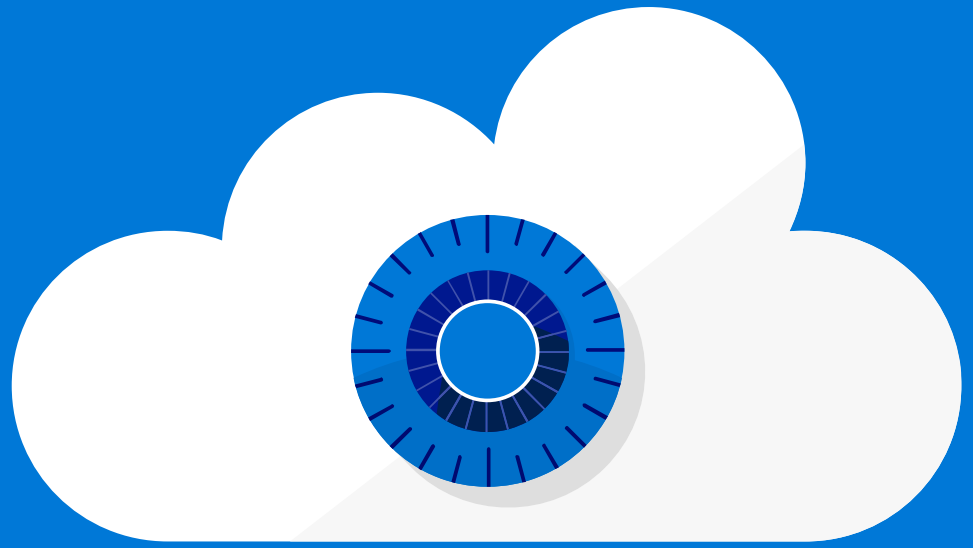
vipazure@microsoft.com

Securing your infrastructure

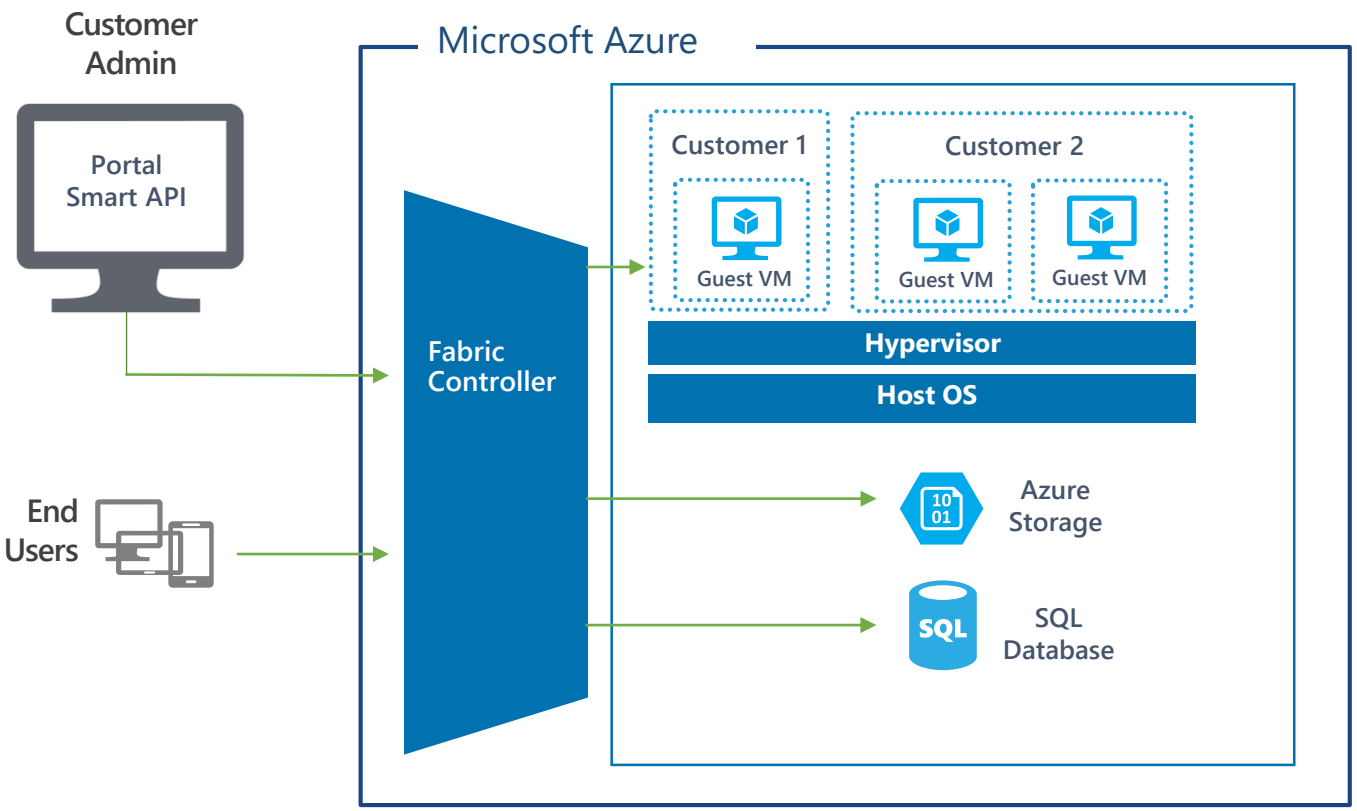
Two Perspectives

Best practices for securing compute and networking resources

What other steps should you take to secure your solution

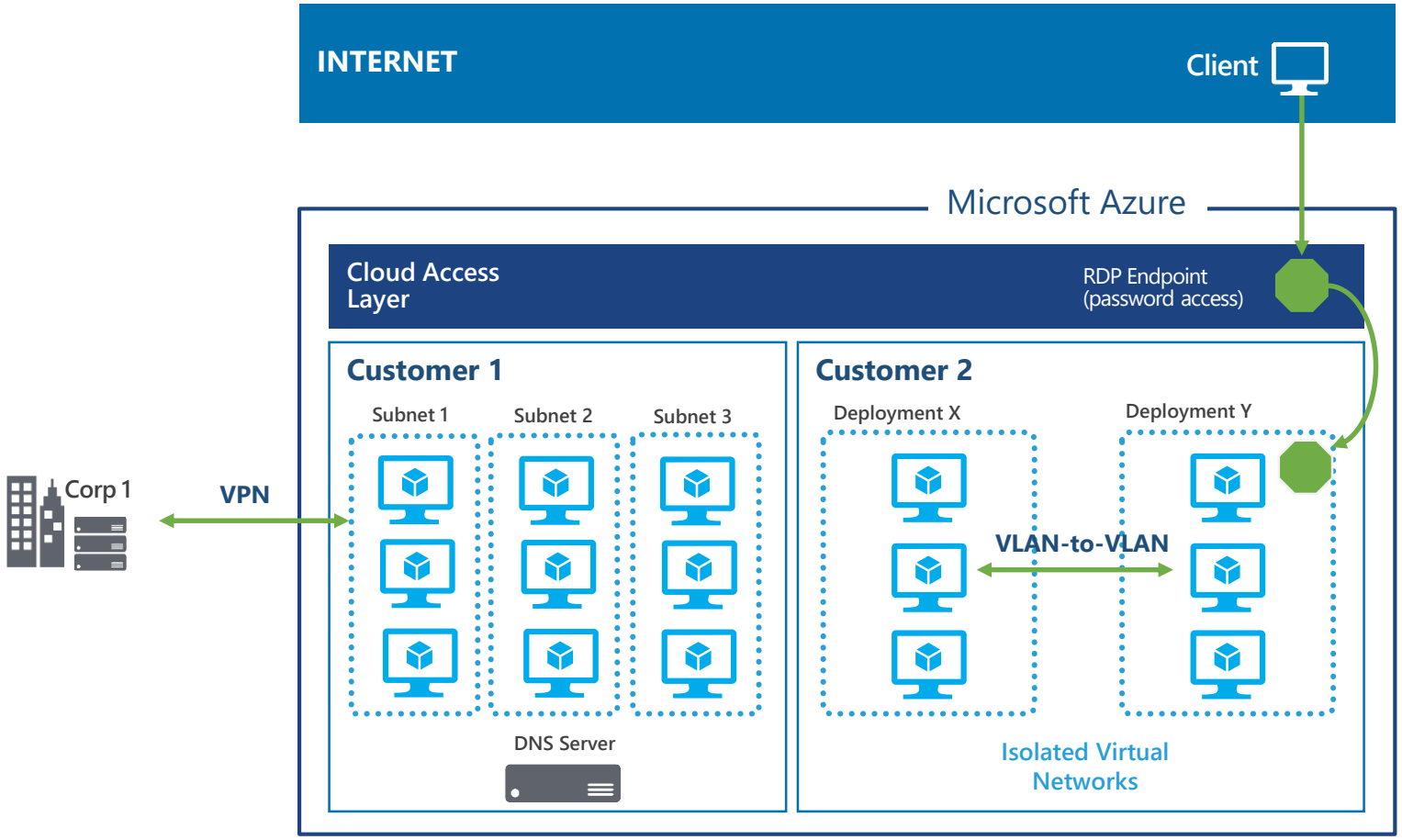


Secure Multi-tenancy



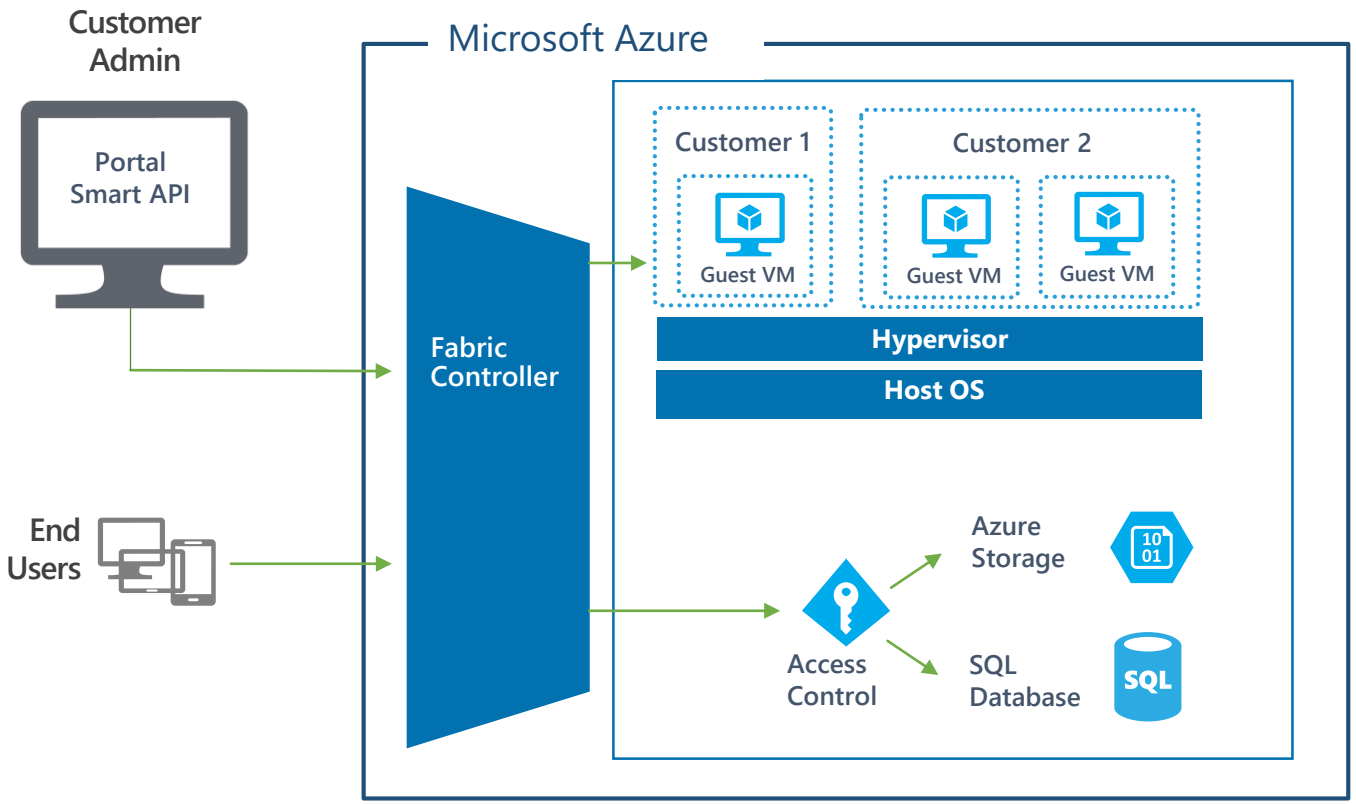
- ✓ Isolates customer environments using the Fabric Controller
- ✓ Runs a configuration-hardened version of Windows Server as the Host OS
- ✓ Uses Hyper-V – a battle tested and enterprise proven hypervisor

Network Protection



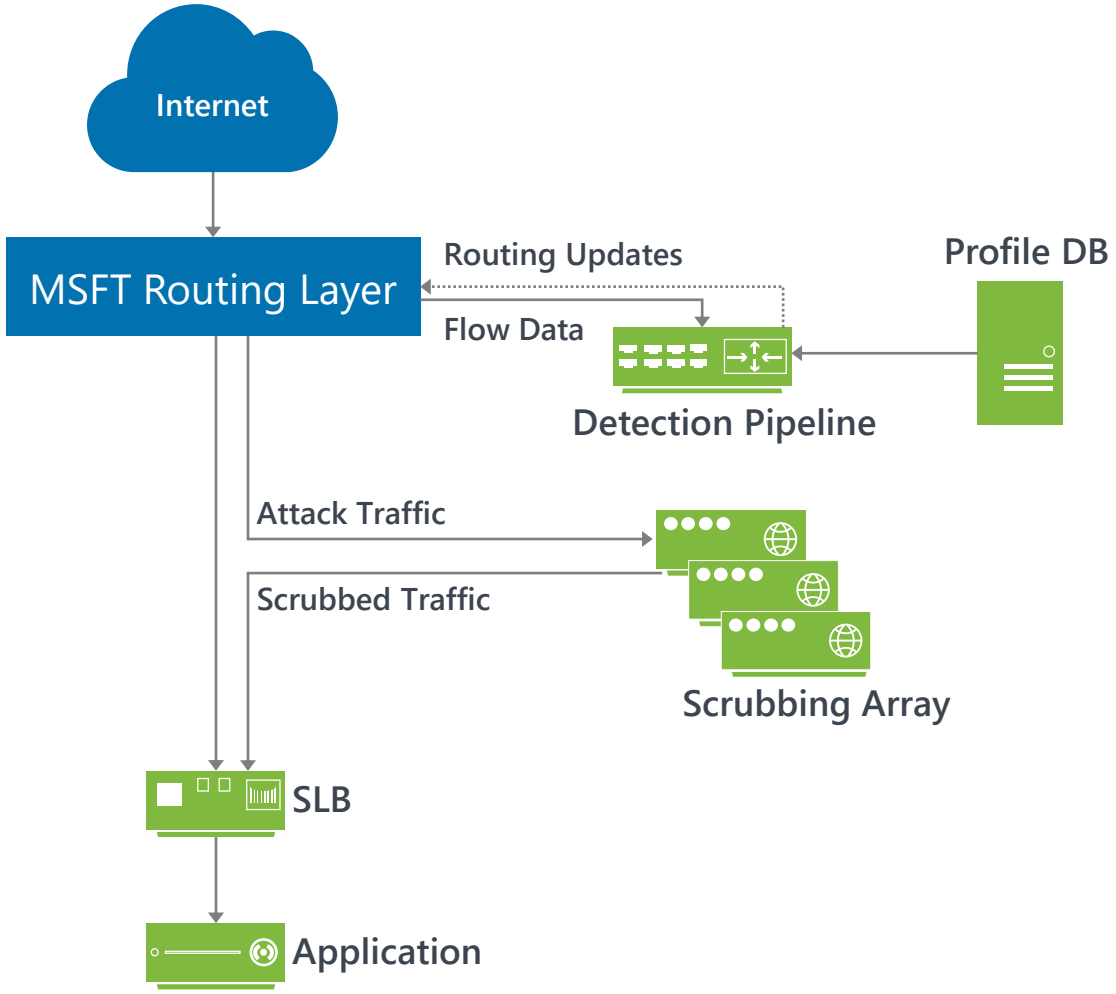
- ✓ Provides logical isolation while enabling customer control
- ✓ Restricts access from the Internet, permits traffic only to endpoints, and provides load balancing and NAT at the Cloud Access Layer
- ✓ Private IP addresses are isolated from other customers

Data Segregation



- ✓ Stored data accessible only through claims-based IDM & access control with private key
- ✓ Storage blocks are hashed by the hypervisor to separate accounts
- ✓ SQL Azure isolates separate account databases
- ✓ VM switch at the host level blocks inter-tenant communication

DDoS Defense System



- ✓ Azure's DDoS defense system is designed not only to withstand attacks from the outside, but also from within.
- ✓ Azure monitors and detects internally initiated DDoS attacks and removes offending VMs from the network

VM Best Practice (1/2)

- ❑ Access Control
  - ❑ RBAC
  - ❑ Policies (eg require blob encryption)
  - ❑ Password discipline
  - ❑ Use ARM templates to enforce security settings
- ❑ Availability
  - ❑ Load balanced availability / scale set

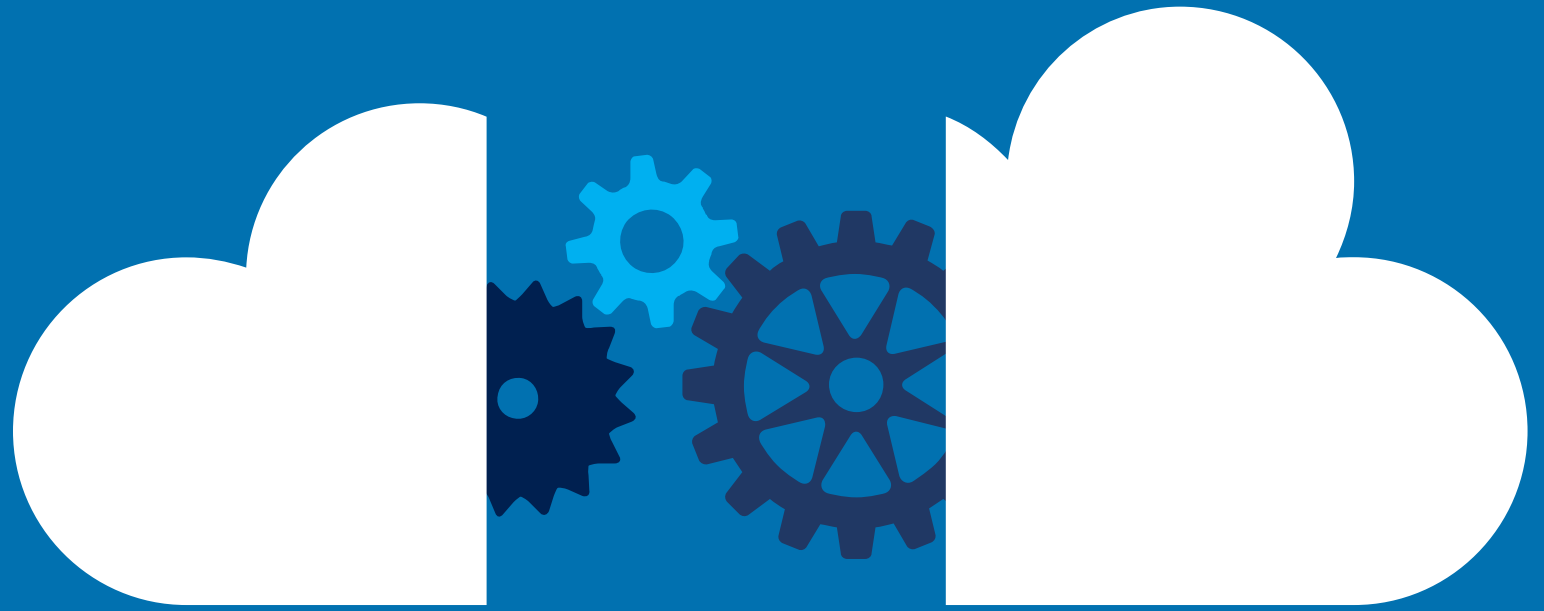
VM Best Practice (2/2)

- ❑ Networking
  - ❑ Control traffic
  - ❑ JIT Access Control
- ❑ Protect data at rest
  - ❑ Enabled disk encryption on VM
- ❑ VM updates
  - ❑ Enforce update policies
- ❑ Monitor & manage the state of VMs

Microsoft

Demo

JIT Access Control
Update Management



Secure Networking: Options

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

Virtual Networks

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

Network Security Groups

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

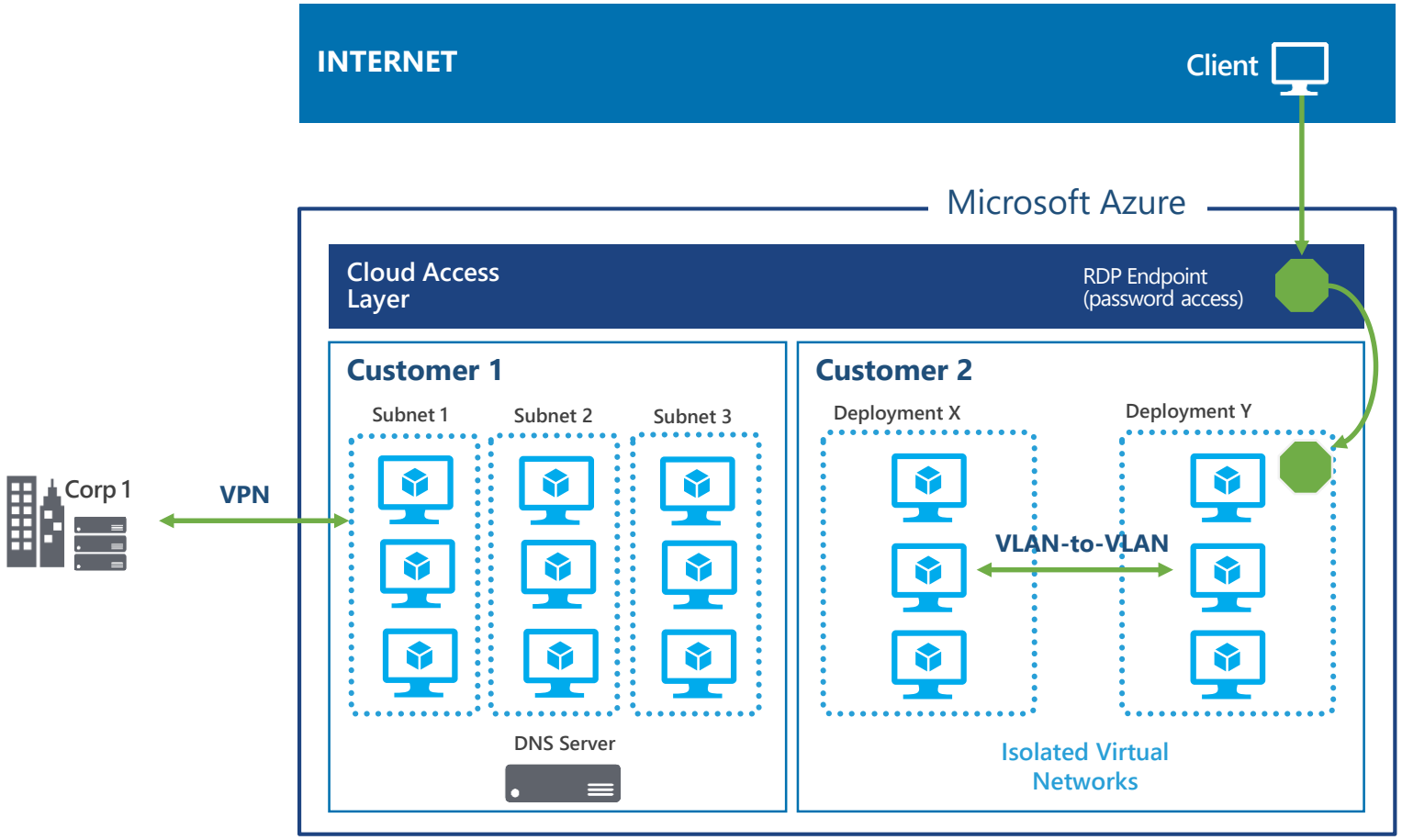
VPN

Customers can securely connect to a virtual network from anywhere.

ExpressRoute

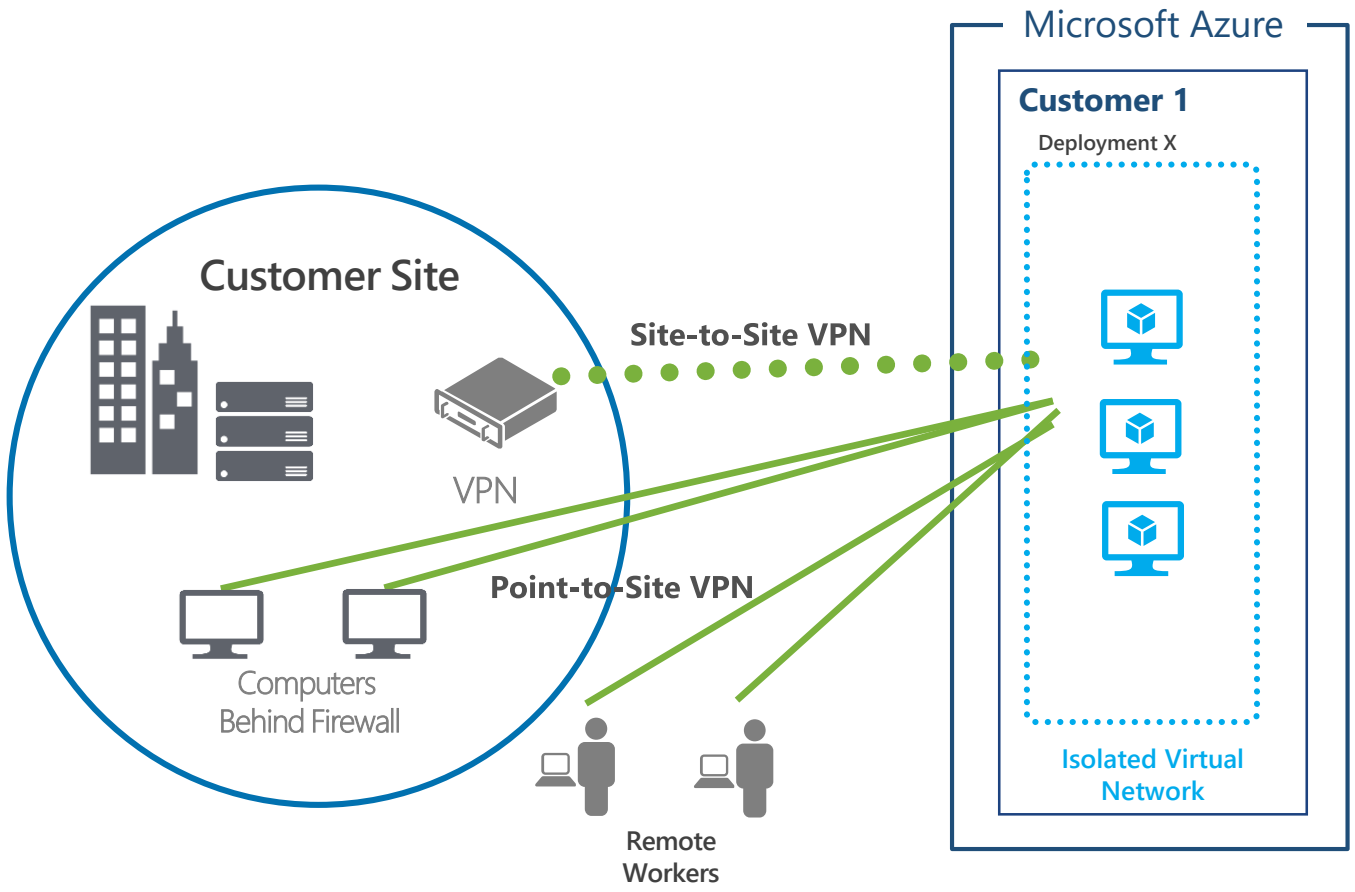
Customers can create private connections between Azure datacenters and infrastructure that's on your premises or in a colocation environment.

Virtual Networks & Security Groups



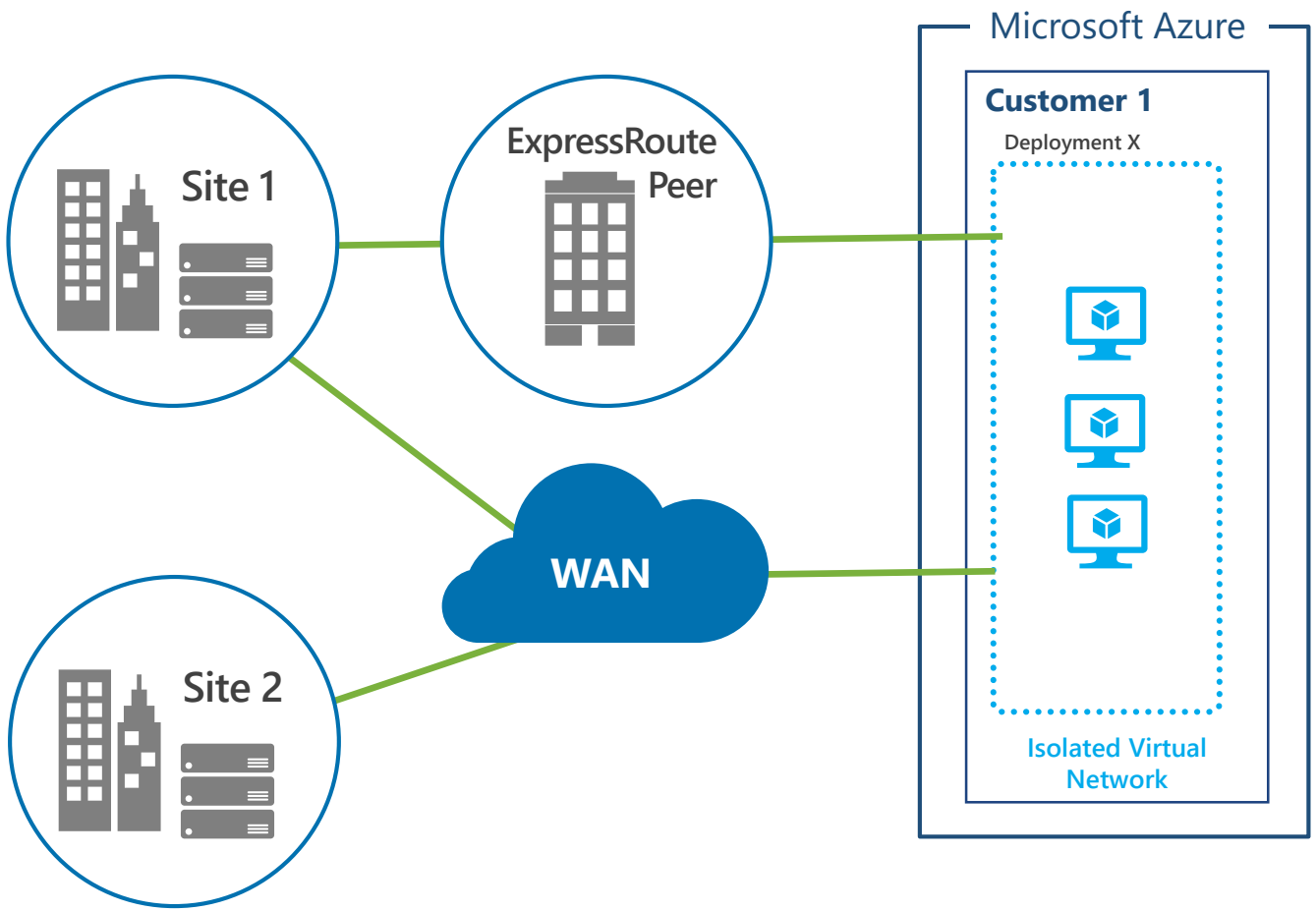
- ✓ Create Virtual Networks with Subnets and Private IP addresses
- ✓ Configure access control rules, which can be applied across Virtual Networks to thousands of machines in seconds
- ✓ Can bring your own DNS and can domain join your VMs

VPN Connections



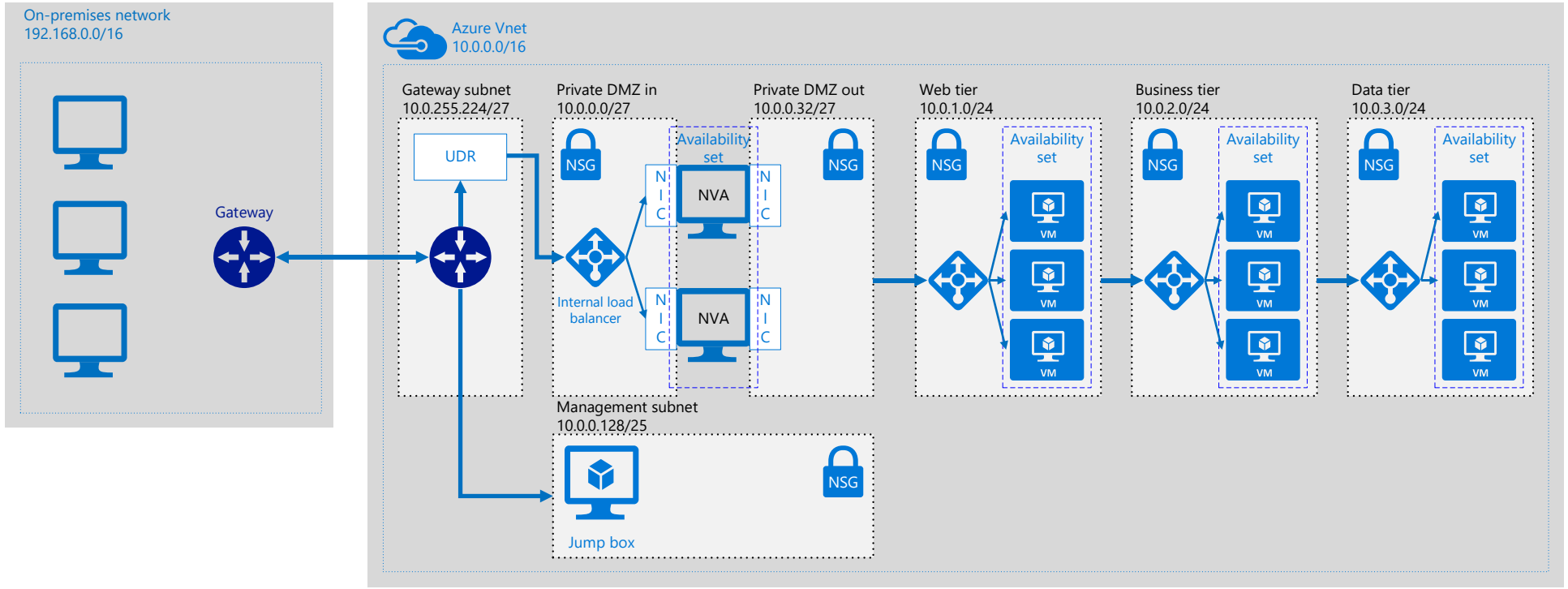
- ✓ Connect your sites and remote workers to Azure Virtual Networks using Site-to-Site or Point-to-Site VPNs
- ✓ You own and manage certificates, policies, and user access

Azure ExpressRoute



- ✓ Can establish connections to Azure at an ExpressRoute location (Exchange Provider facility)
- ✓ Can directly connect to Azure from your existing WAN network (such as a MPLS VPN) provided by a network service provider
- ✓ You own and manage certificates, policies, and user access

Virtual Networks & NVAs



Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

CITRIX

f5

FORTINET

IMPERVA

Infoblox

KEMP

Netgate

paloalto NETWORKS

riverbed Think fast.

TREND MICRO

Security Imperative | Securing Investment | Securing Infrastructure | Securing Data | Securing Applications | Monitoring & Ops

Network Security Best Practice (1/2)

- ❑ Logically segment subnets
  - ❑ Use NSGs to control flow between subnets
- ❑ User defined routes
- ❑ Enable forced tunnelling (control outbound traffic)
- ❑ Employ a Virtual Network Appliance (NVA)
- ❑ Use a DMZ – concentrate your defences
- ❑ Consider a dedicated WAN link

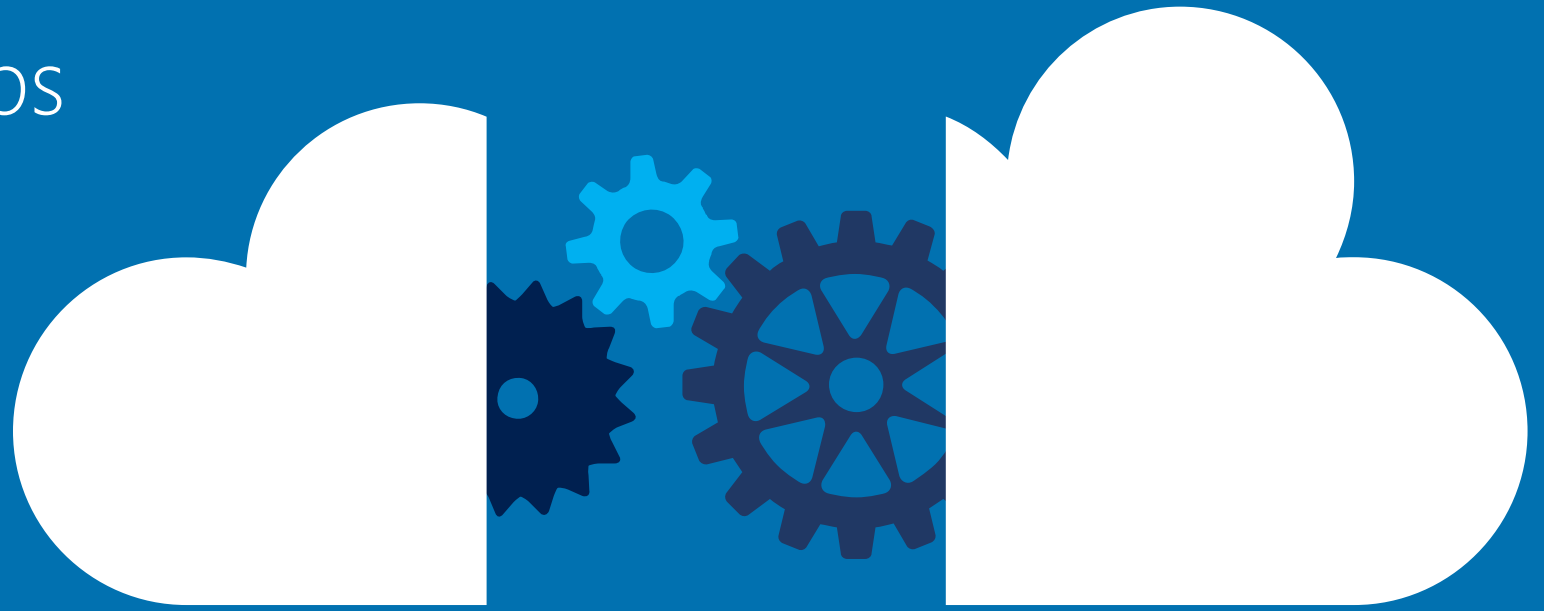
Network Security Best Practice (2/2)

- Make use of load balancers
  - Azure load balancer (Layer-4)
  - Application Gateway (HTTP load balancer)
  - Traffic Manager (DNS load balancer)
- Disable RDP / SSH access

Microsoft

Demo

Network Security Groups
VNet Peering
NVA (WAF)
VPN



Defence in depth

- ❑ Enable Azure Security Centre
- ❑ Enable Azure Backup on VMs
- ❑ Monitor Cloud Health

Security Partners

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

Antimalware

Virtual machines

- Kaspersky
- Trend Micro

Active Directory integrations

- Symantec
- McAfee

Networking security

- aiScaler
- Barracuda
- Check Point
- Riverbed
- Cohesive Networks
- F5
- Cisco
- CloudFlare
- Imperva
- Fortinet
- Stormshield

Encryption

- CloudLink
- Townsend Security

Monitoring and alerts

- Alert Logic
- Derdack
- Nagios
- Imperva
- Dome9
- Trend Micro

Messaging Security

- Kaspersky
- Barracuda
- Trend Micro
- GreatHorn

Application Security

- Waratek
- DataSunrise
- Tinfoil Security
- CipherPoint

Authentication

- Login People
- Auth0

Microsoft

Resources

Azure Security
Best Practices for Azure Security – VMs
Best Practices for Azure Security – Networking
Express Route