



Red Team VS Blue Team in Microsoft Cloud

Mustafa Toroman

Saša Kranjac





Thank you, sponsors!

DATA ONE

Alegri



Nigel Frank
International

The Global Leader in Microsoft Recruitment

arvato
BERTELSMANN



Azure Saturday 2018



Speaker Introduction

- Mustafa Toroman
- Senior System Engineer @ Authority Partners
- @toromust
- <http://toroman.cloud/>
- Microsoft Azure MVP
- MCSE, MCP, MCSA, MCITP, MCSD, MCT, MS v-TSP



Speaker Introduction

- Saša Kranjac
- CEO and Security Expert @ Kranjac - IT Training and Consulting
- @SasaKranjac
- MCSE, MCP, MCSA, MCITP, MCT, MCT Regional Lead, Certified EC-Council Instructor, CEH



The Microsoft Cloud -A Cloud You Can Trust

Security



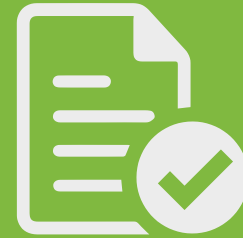
The confidentiality, integrity, and availability of your data is protected.

Privacy & Control



No one is able to use your data in a way that you do not approve.

Compliance



You have visibility into how your data is being handled and used.

Transparency











Your content is stored and managed in compliance with applicable laws, regulations and standards.







Azure Platform Services







Security & Management

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





Compute

-  Cloud Services
-  Service Fabric
-  Batch
-  Remote App

Web and Mobile

-  Web Apps
-  API Apps
-  API Management
-  Mobile Apps
-  Logic Apps
-  Notification Hubs





Developer Services

-  Visual Studio
-  Azure SDK
-  Team Project
-  Application Insights







Hybrid Operations

-  Azure AD Connect Health
-  AD Privileged Identity Management
-  Backup
-  Operational Insights
-  Import/Export
-  Site Recovery
-  StorSimple

Integration

-  Storage Queues
-  Biztalk Services
-  Hybrid Connections
-  Service Bus

Analytics & IoT

-  HDInsight
-  Machine Learning
-  Data Factory
-  Event Hubs
-  Stream Analytics
-  Mobile Engagement

Data

-  SQL Database
-  SQL Data Warehouse
-  Redis Cache
-  Search
-  DocumentDB
-  Tables

Media & CDN

-  Media Services
-  Content Delivery Network (CDN)

Azure Infrastructure Services

Compute

-  Virtual Machines
-  Containers

Storage

-  BLOB Storage
-  Azure Files
-  Premium Storage

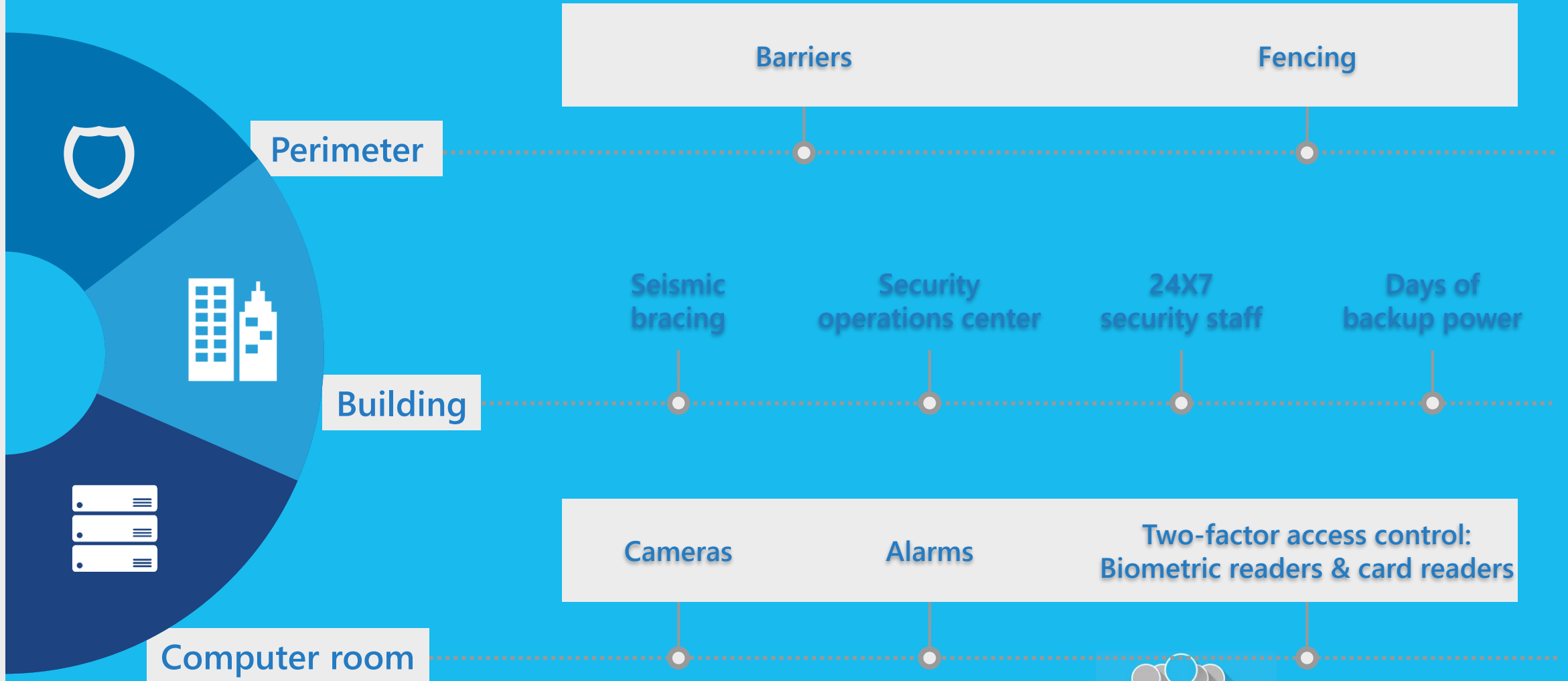
Networking

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

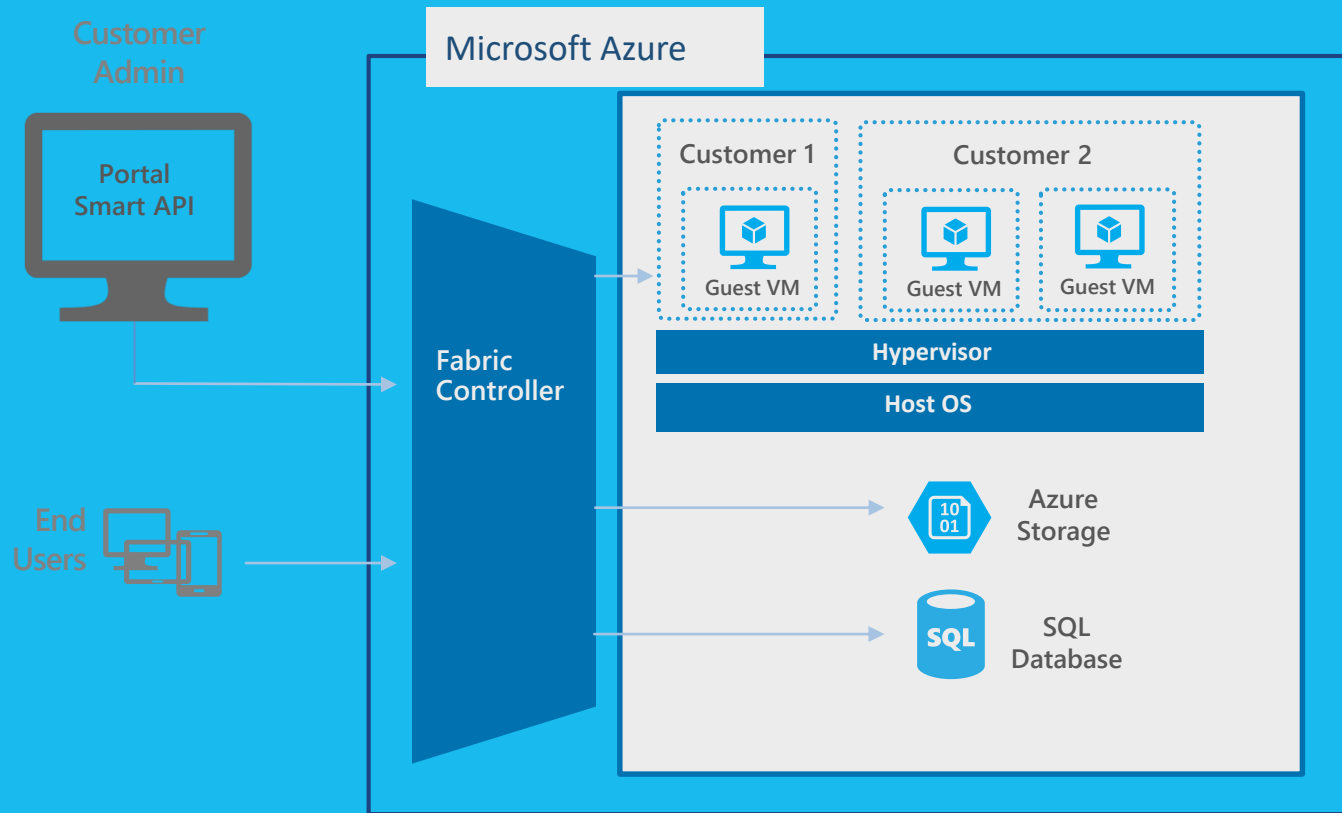
Azure Datacenter Infrastructure (30 Regions, 22 Online)



Datacenter Security



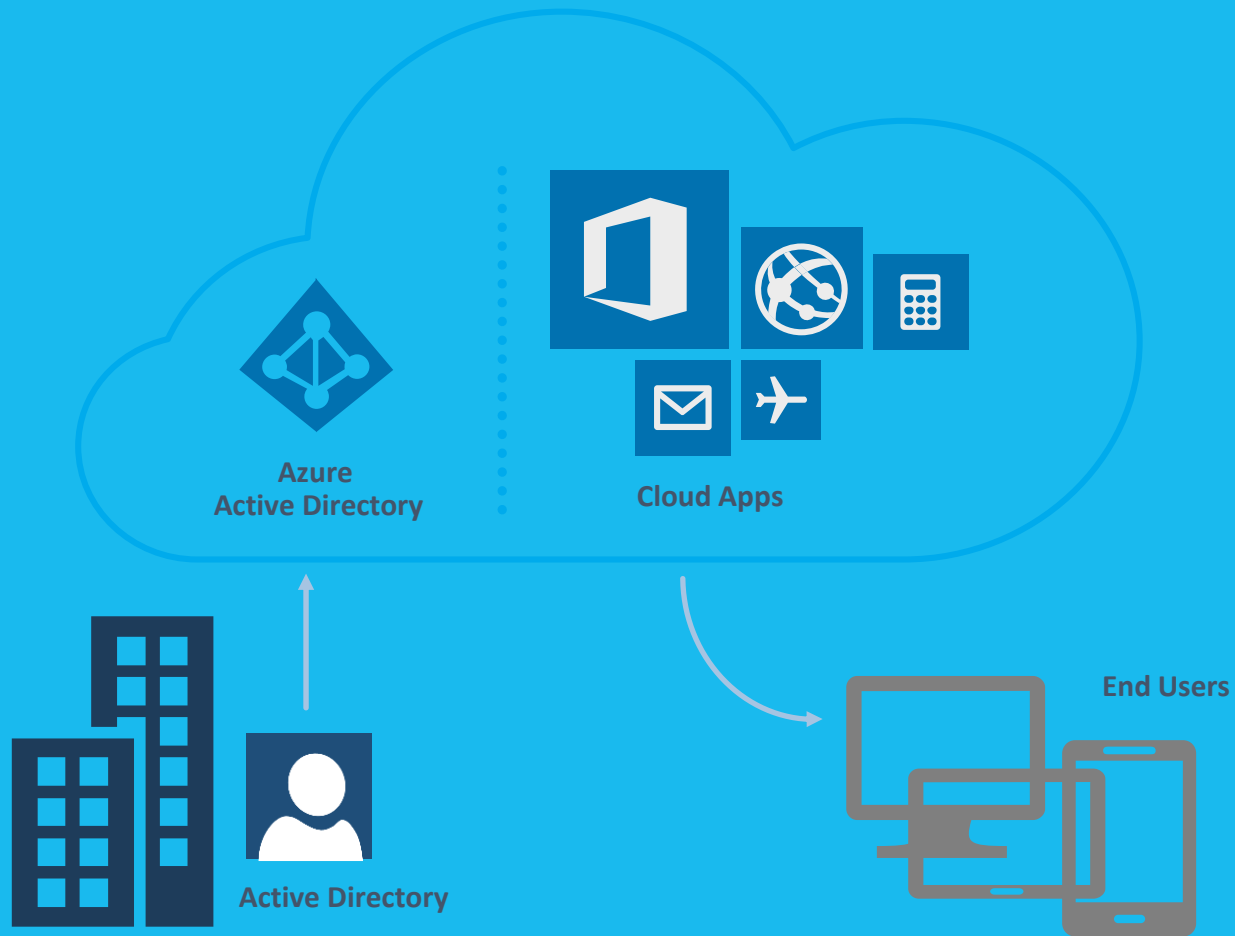
Secure Multi-tenancy



- ✓ 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



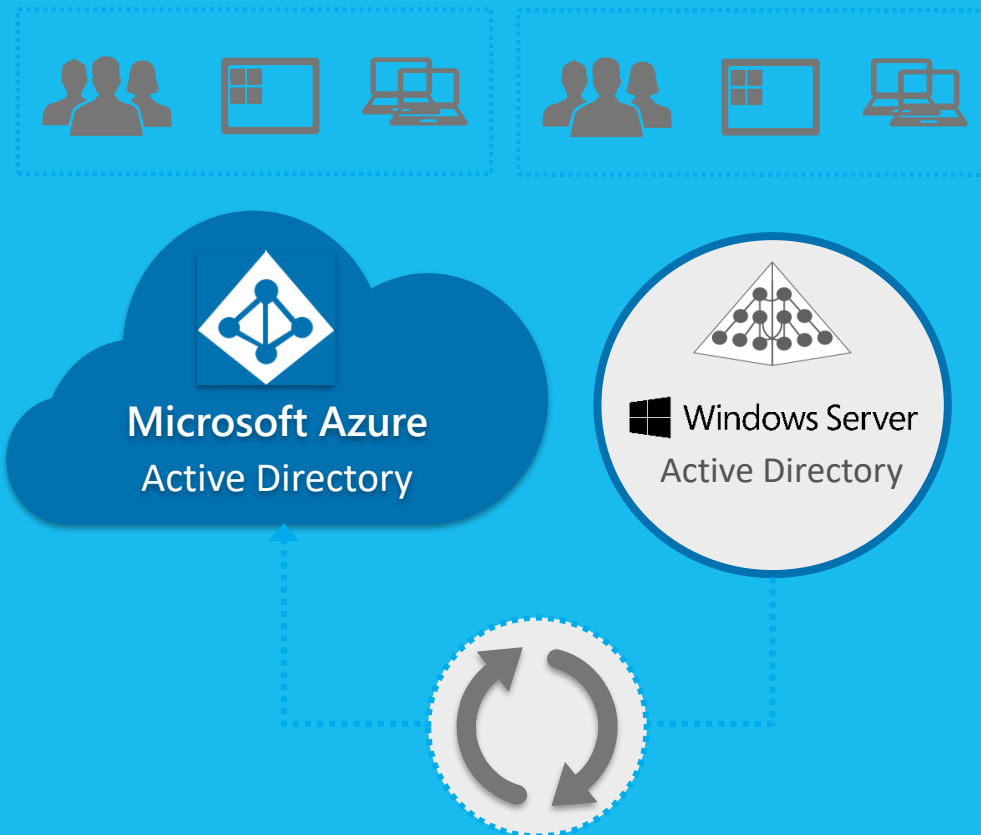
Identity & Access: Azure AD



- ✓ Centrally manage users and access to Azure, O365, and hundreds of pre-integrated cloud applications
- ✓ Build Azure AD into your web and mobile applications
- ✓ Can extend on-premises directories to Azure AD through synchronization



Identity & Access: Multi Factor Authentication



- ✓ Protect sensitive data and applications both on-premises and in the cloud with Multi Factor Authentication
- ✓ Can use Active Directory (on-premises) with Azure Active Directory (in cloud) to enable single sign-on, a single directory, and centralized identity management
- ✓ Multi Factor Authentication can be implemented with Phone Factor or with AD on-premises



Data Protection

Data segregation

Logical isolation segregates each customer's data from that of others.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

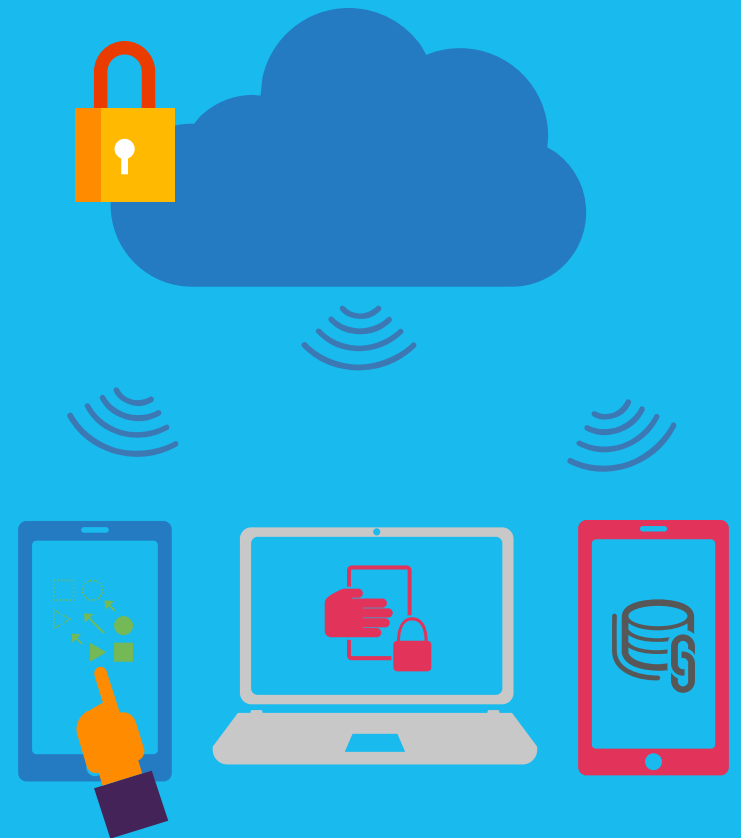
Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy

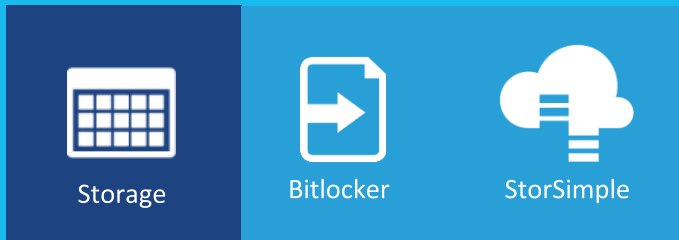
Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

Data destruction

When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer's data inaccessible.



Options for Encryption at Rest



Virtual Machines:

- ✓ Data drives – full disk encryption through BitLocker
- ✓ Boot drives – partner solutions
- ✓ SQL Server – Transparent Data Encryption
- ✓ Files & folders - EFS in Windows Server

Storage:

- ✓ Bitlocker encryption of drives for import/export of data
- ✓ Server-side encryption of Blob Storage using AES-256
- ✓ Client-side encryption w/.NET and Java support
- ✓ StorSimple with AES-256 encryption

Applications:

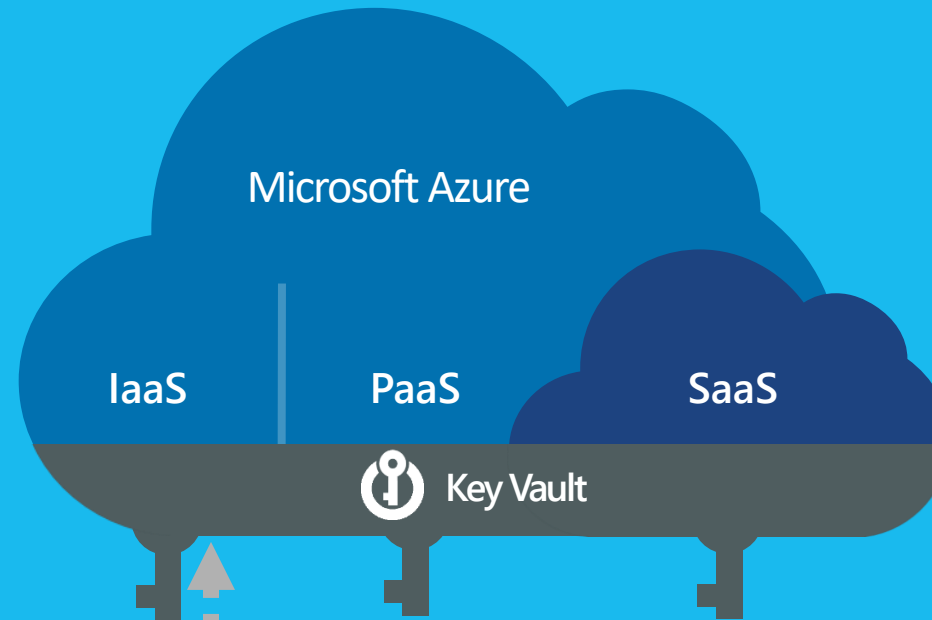
- ✓ Client Side encryption through .NET Crypto API
- ✓ RMS SDK for file encryption by your applications



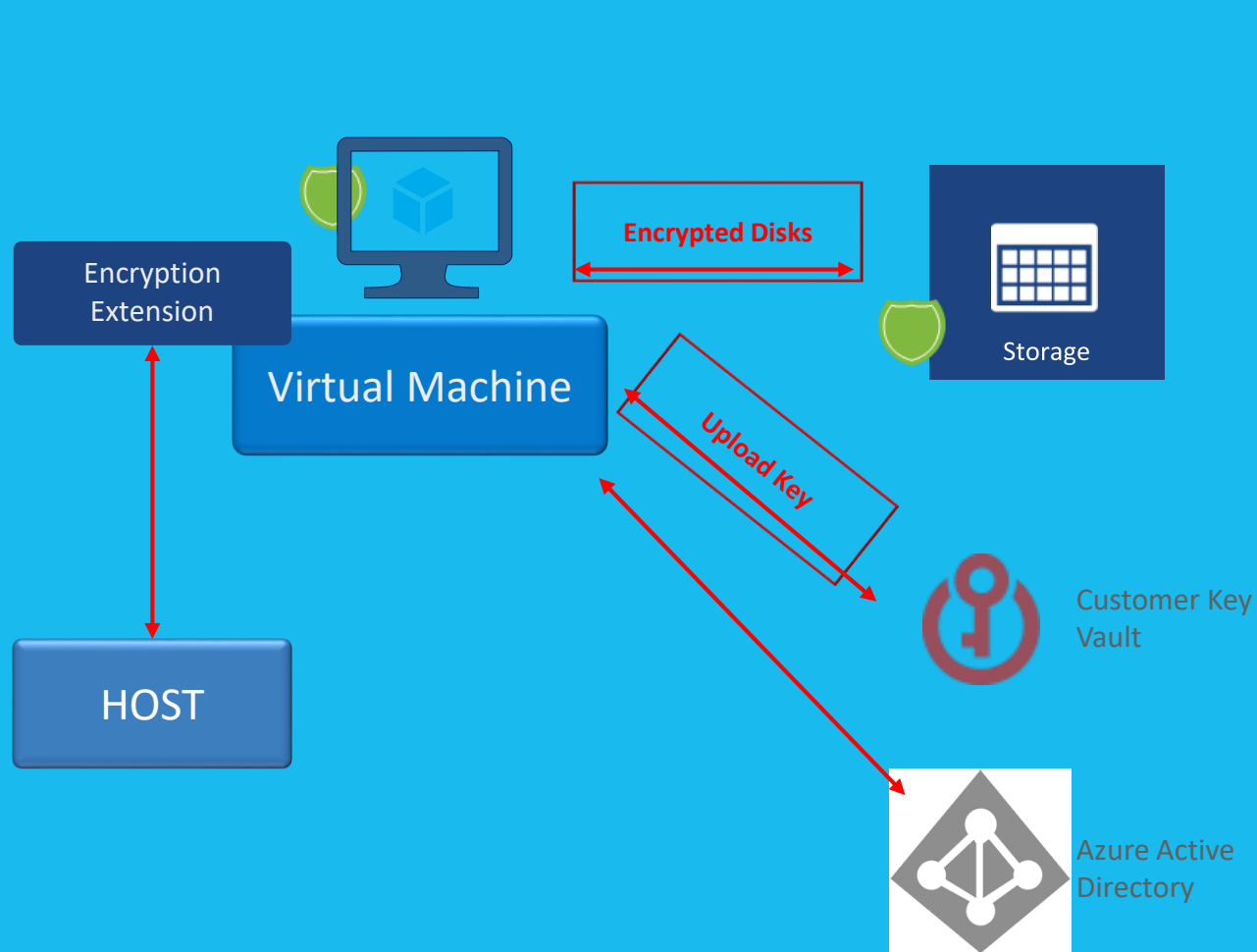
Microsoft Azure Key Vault

Key Vault offers an easy, cost-effective way to safeguard keys and other secrets used by cloud apps and services using HSMs.

- ✓ You manage your keys and secrets
- ✓ Applications get high performance access to your keys and secrets... on your terms



Disk Encryption



- ✓ VM's are secured at rest using industry standard encryption technology to address organizational security and compliance requirements.
- ✓ VM's boot under customer controlled keys and policies, and they can audit their usage in Key Vault.



SQL Encryption: Overview

Encryption Type	Type	Customer Value
Encryption-In-Transit	TLS from Client to Server TLS = Transport Layer Security	Protects data between client and server against snooping & man-in-the-middle attacks. SQL DB is phasing out SSL 3.0 and TLS 1.0 in favor of TLS 1.2.
Encryption-At-Rest	TDE for SQL DB TDE = Transparent Data Encryption	Protects data on disk. Key management done by Azure. Makes it easier to obtain compliance.
Encryption-End-To-End	Client-side column encryption for SQL DB (library available for download)	Data protected end-to-end but application is aware of encrypted columns. Used in the absence of data masking and TDE for compliance related scenarios.

End-To-End



In-Transit



Customer Data



At-Rest



Database Files,
Backups, Tx Log,
TempDB



Azure Saturday 2018

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

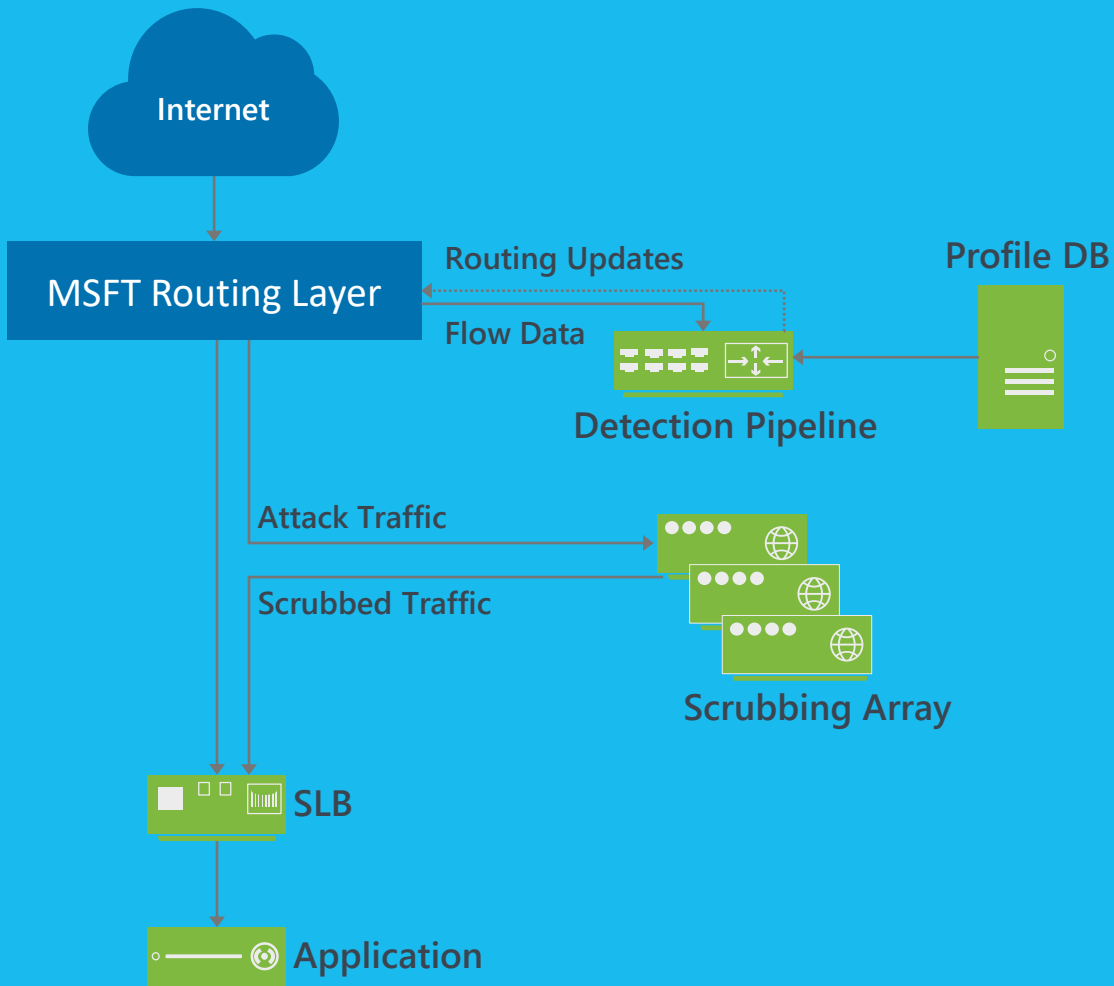
Customers can securely connect to a virtual network from anywhere.

ExpressRoute

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



DDoS Defense System

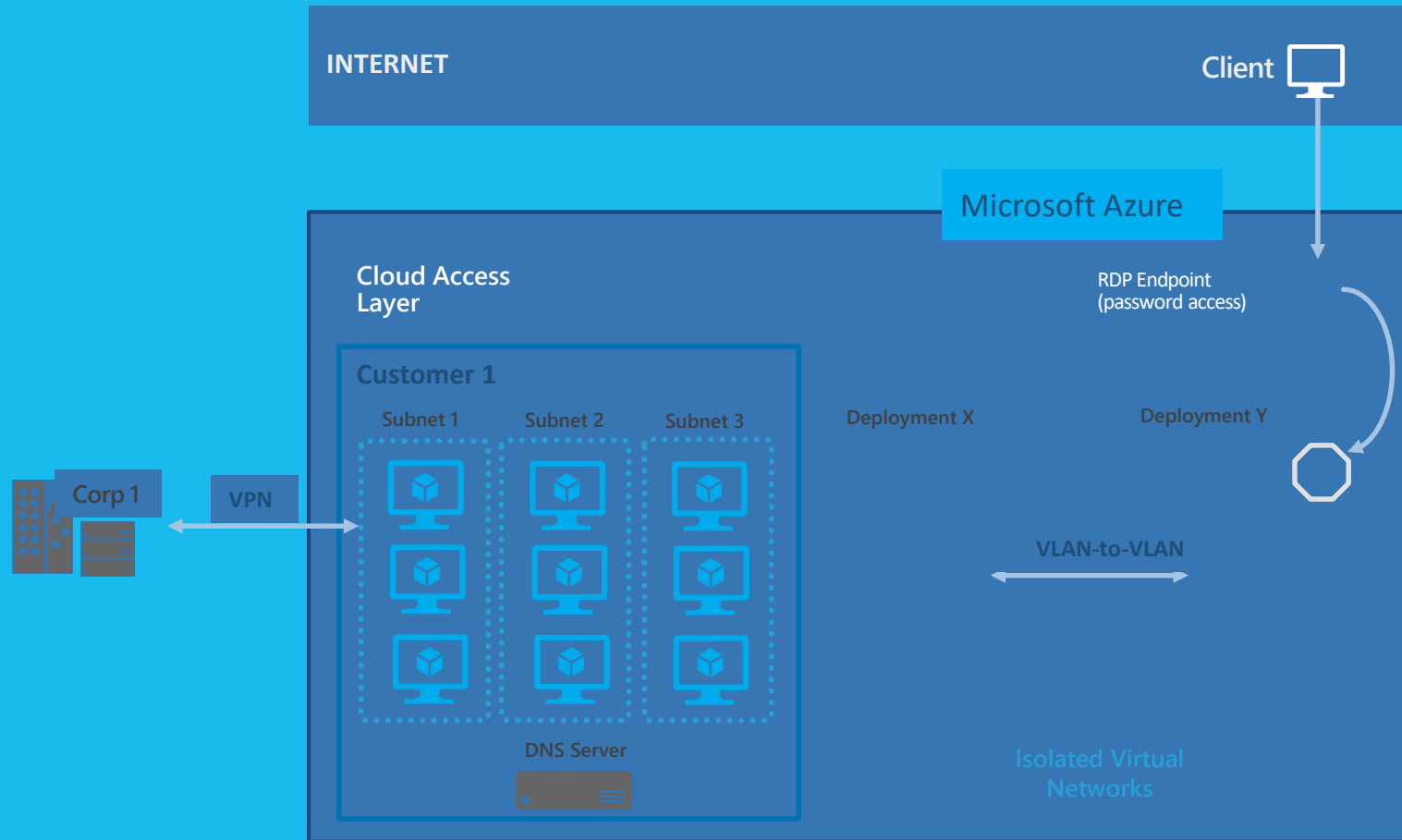


- ✓ Azure's DDoS defense system is designed not only to withstand attacks from the outside, but also from within.
- ✓ Azure monitors and detects internally initiated DDoS attacks and removes offending VMs from the network



Azure Saturday 2018

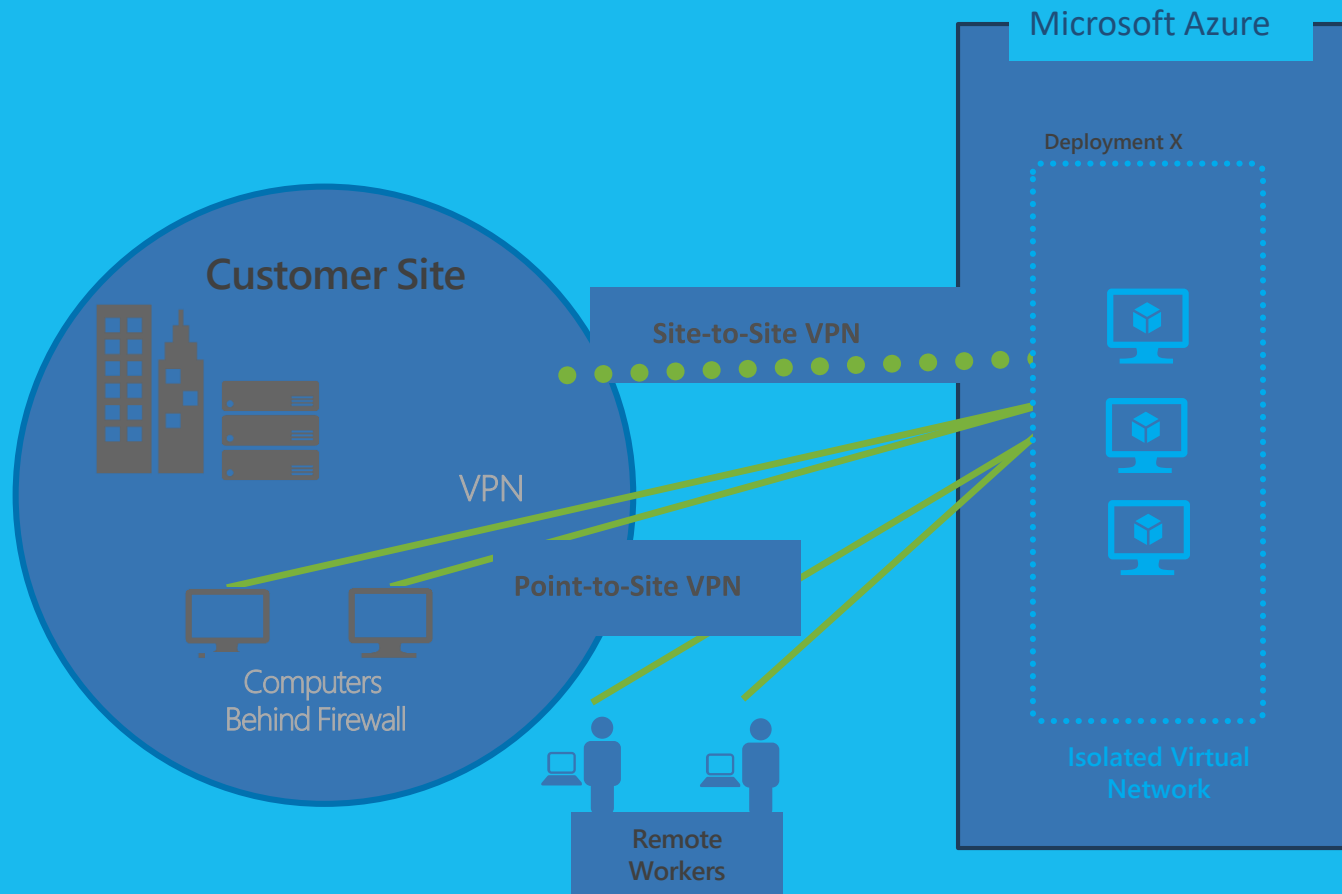
Virtual Networks & Security Groups



- ✓ 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



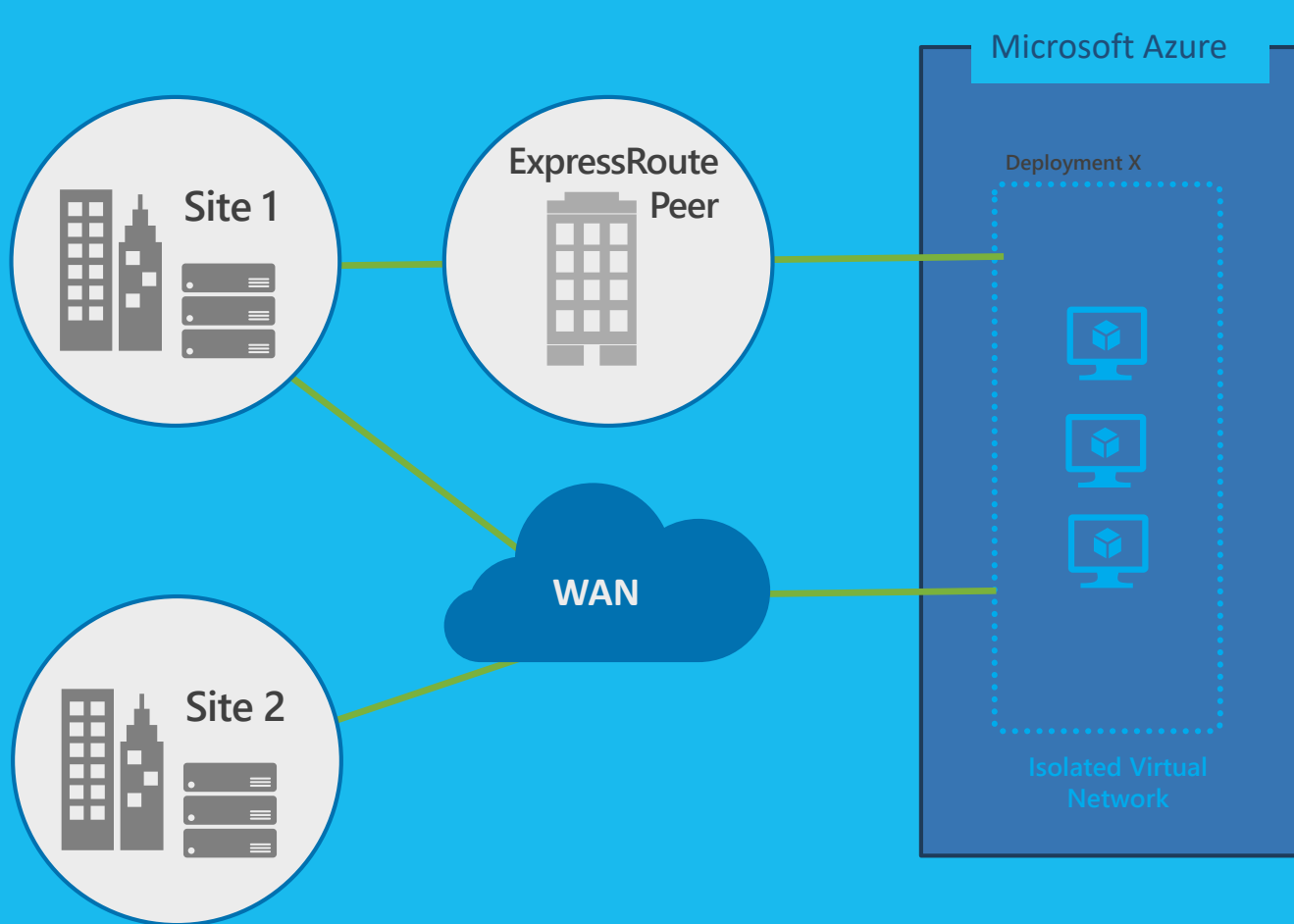
VPN Connections



- ✓ 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



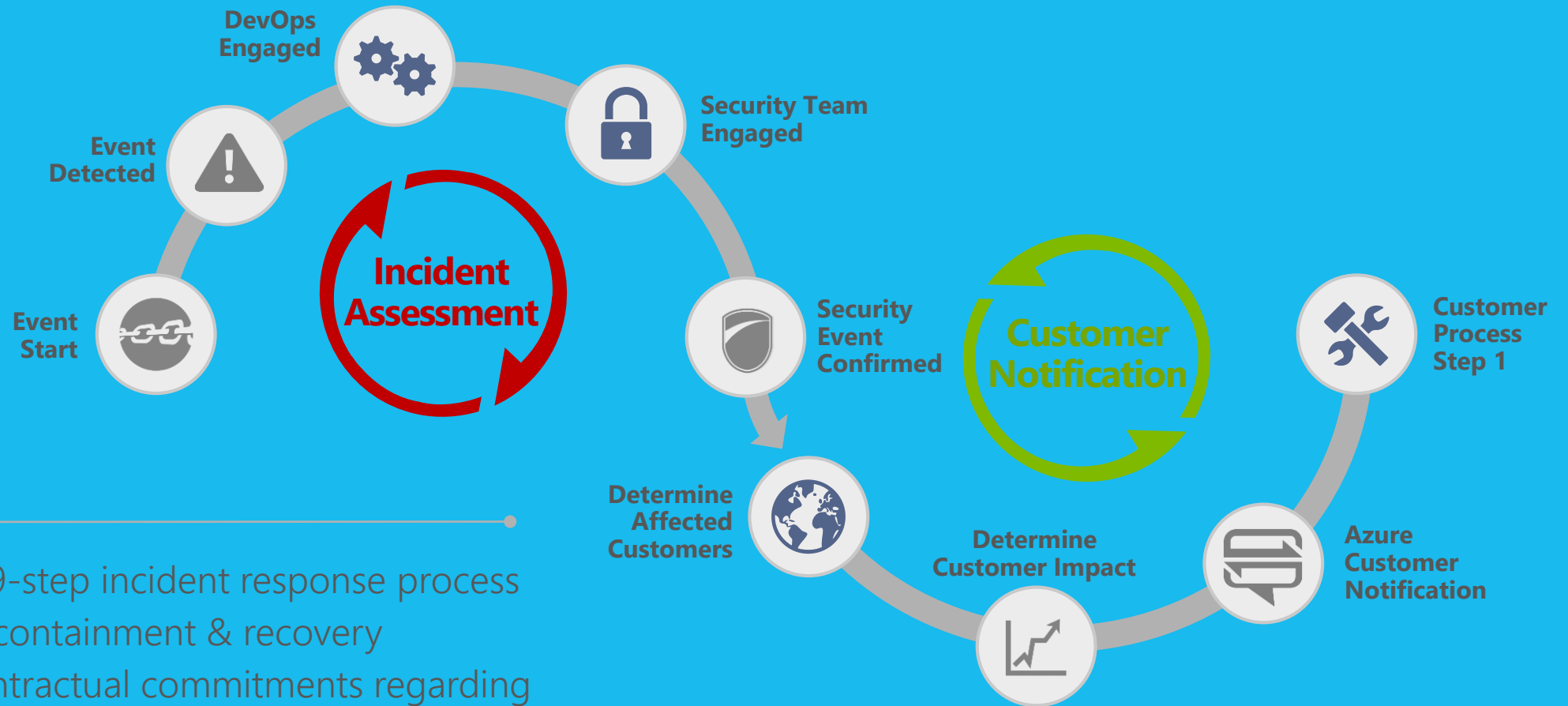
Forensics



- ✓ Provides coordination, analysis of logs and VHD images in the event of platform-level incident
- ✓ Provides forensic data to customers when needed



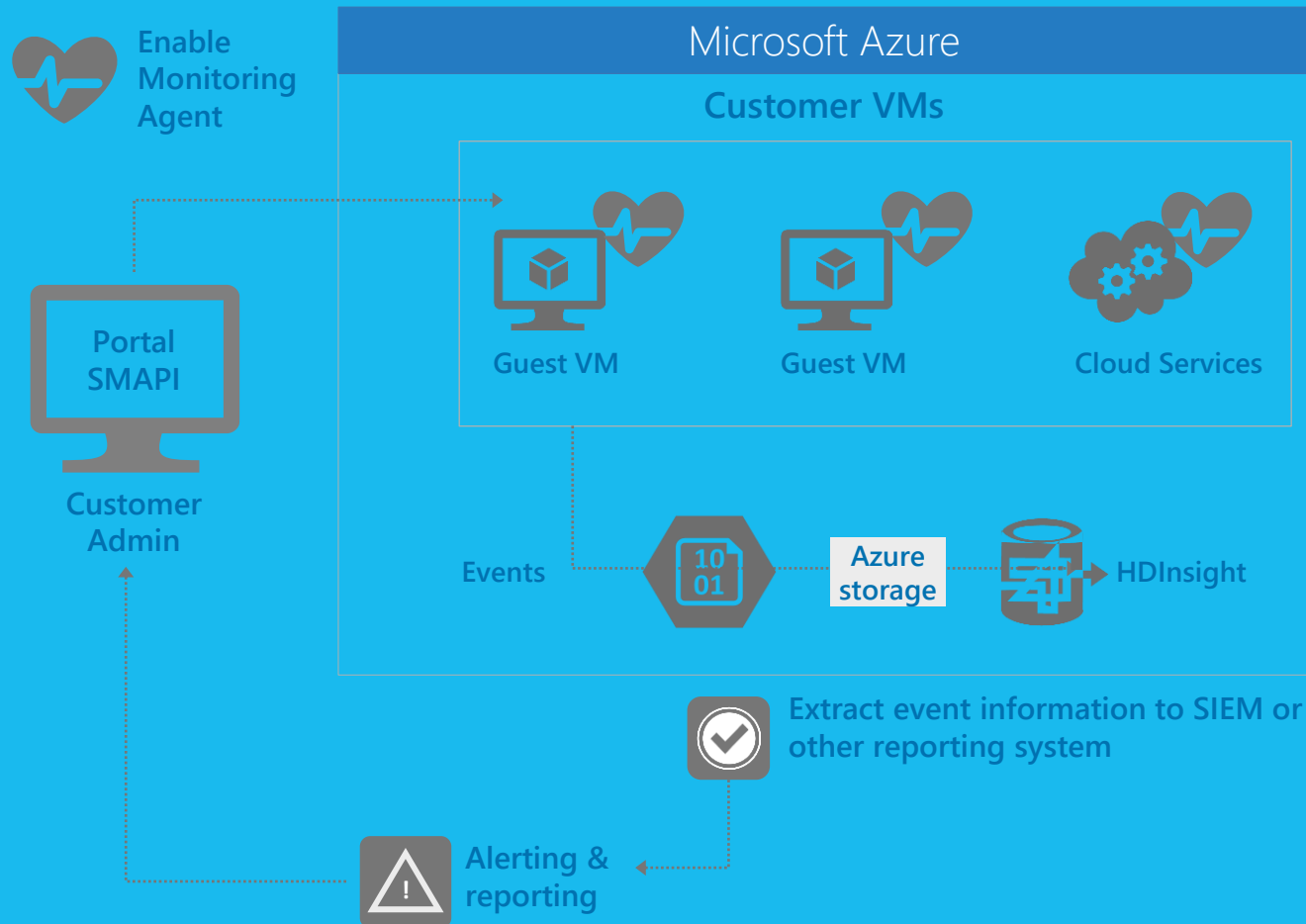
Incident Response






- ✓ In-depth 9-step incident response process
- ✓ Focus on containment & recovery
- ✓ Makes contractual commitments regarding customer notification + provides forensics



Host Protection: Monitoring, Firewalls, AV



- ✓ Configure monitoring, export events for analysis 
- ✓ Configure Microsoft Antimalware or an AV/AM solution from a partner
- ✓ Apply corporate firewall using site-to-site VPN, configures endpoints 
- ✓ Define access controls between tiers and provide additional protection via the OS firewall
- ✓ Monitor and respond to alerts 

Azure Saturday 2018

Update Management



AZURE:

- ✓ Apply patch management as a service
- ✓ Rigorously reviews & tests all changes

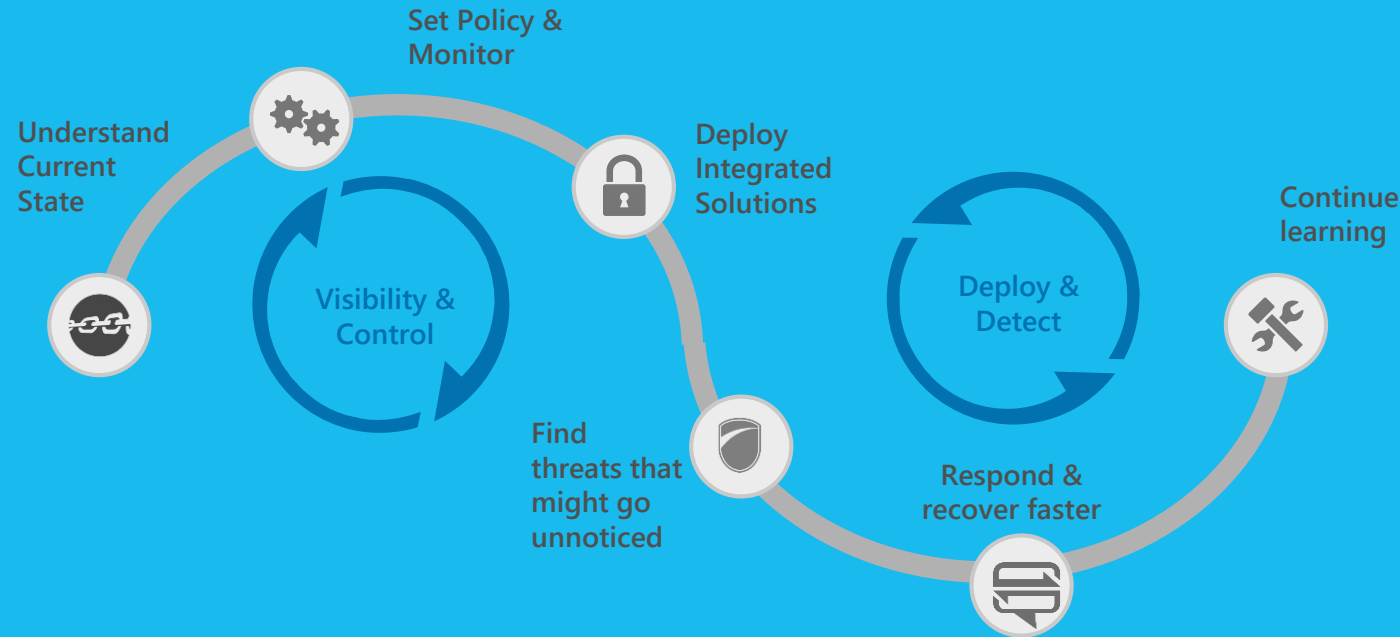
CUSTOMER:

- ✓ Applies similar patch management strategies for their Virtual Machines



Azure Saturday 2018

Protect, Detect and Respond to Threats with Native Azure Security Center



- ✓ Gain visibility and control
- ✓ Integrated security, monitoring, policy management
- ✓ Built in threat detections and alerts
- ✓ Works with broad ecosystem of security solutions

 **Check Point®**
SOFTWARE TECHNOLOGIES LTD.

 **TREND MICRO™**

 **IMPERVA SECURESPHERE**

 **CLOUDFLARE™**

 **Barracuda**

 **f5®**

 **CISCO™**

 **IMPERVA INCAPSULA**

 **FORTINET™**

Operations Management Suite

- Collect security-related events and perform forensic, audit, and breach analysis



Identification of missing system updates across data centers or in a public cloud

Comprehensive updates assessment across datacenters and public clouds



Comprehensive view into your organization's IT security posture

Detection of breaches and threats with malware assessment

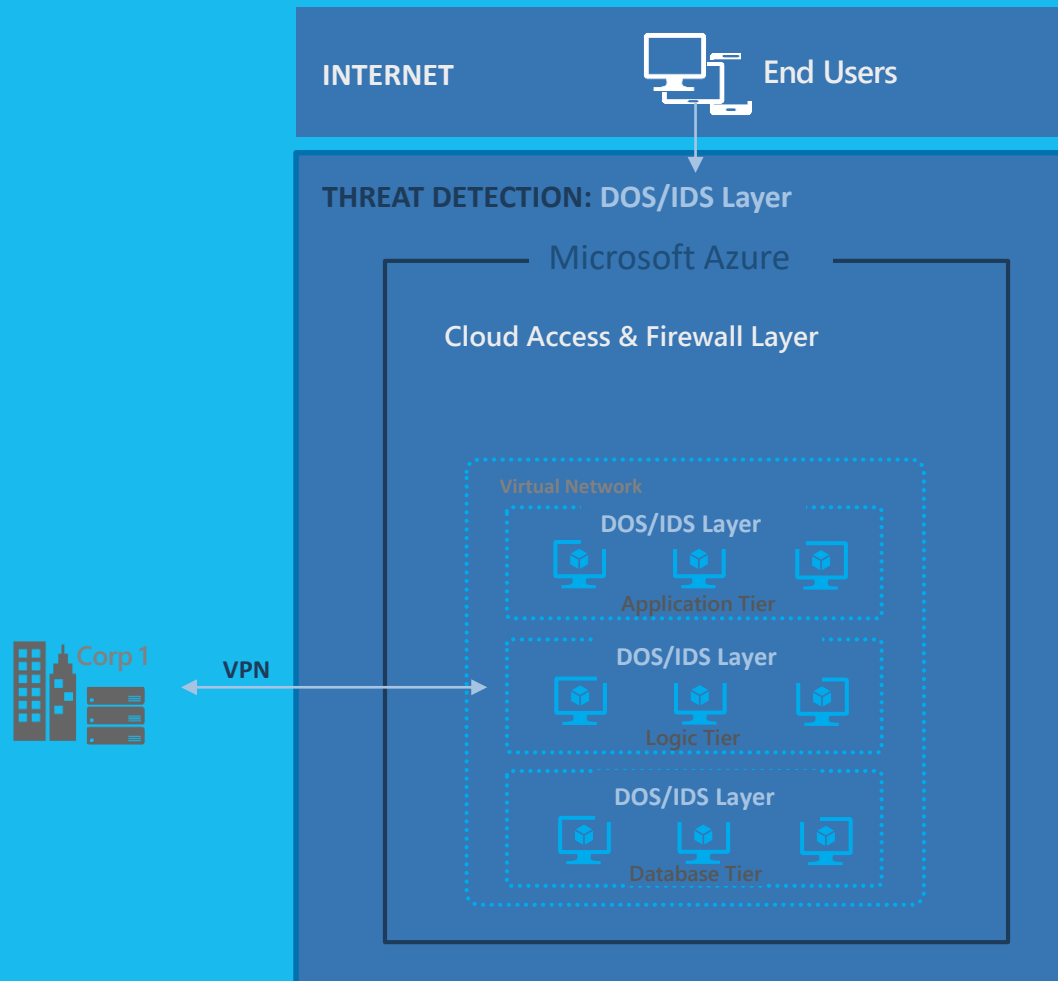


Collection and analysis of security related events

Perform forensic, audit and breach analysis



Threat Detection



- ✓ Provides 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



Q&A?



Please complete survey 😊

<https://form.responster.com/OKm4ds>

OR



Azure Saturday 2018

Thank you!

