Intelligent Cloud Conference

Copenhagen May 29-30

An advanced guide through the Azure Security jungle

Eric Berg

- Lead IT-Architekt – Team Azure / Team Modern Workplace
- Azure, Datacenter and Modern Workplace
- Azure, System Center, Windows Server and Client
- info@ericberg.de
- @ericberg_de | @GeekZeugs
- www.ericberg.de | www.geekzeugs.de

MVP Microsoft® Most Valuable Professional

GEEKZEUGS HOME OF

GEEKSPRECH Podcast

GEEKSCHAU Webcast

GEEKTREFF Community

Azure Meetup THÜRINGEN

Event Sponsors

INSPARI

Microsoft

it-Craft
SQL Specialisterne

Expo Sponsors

kapacity
Business Analytics

solvo it
Microsoft Partner

The Software Experts
Crayon

CTGlobal

ADVECTAS
Excellence in your decisions

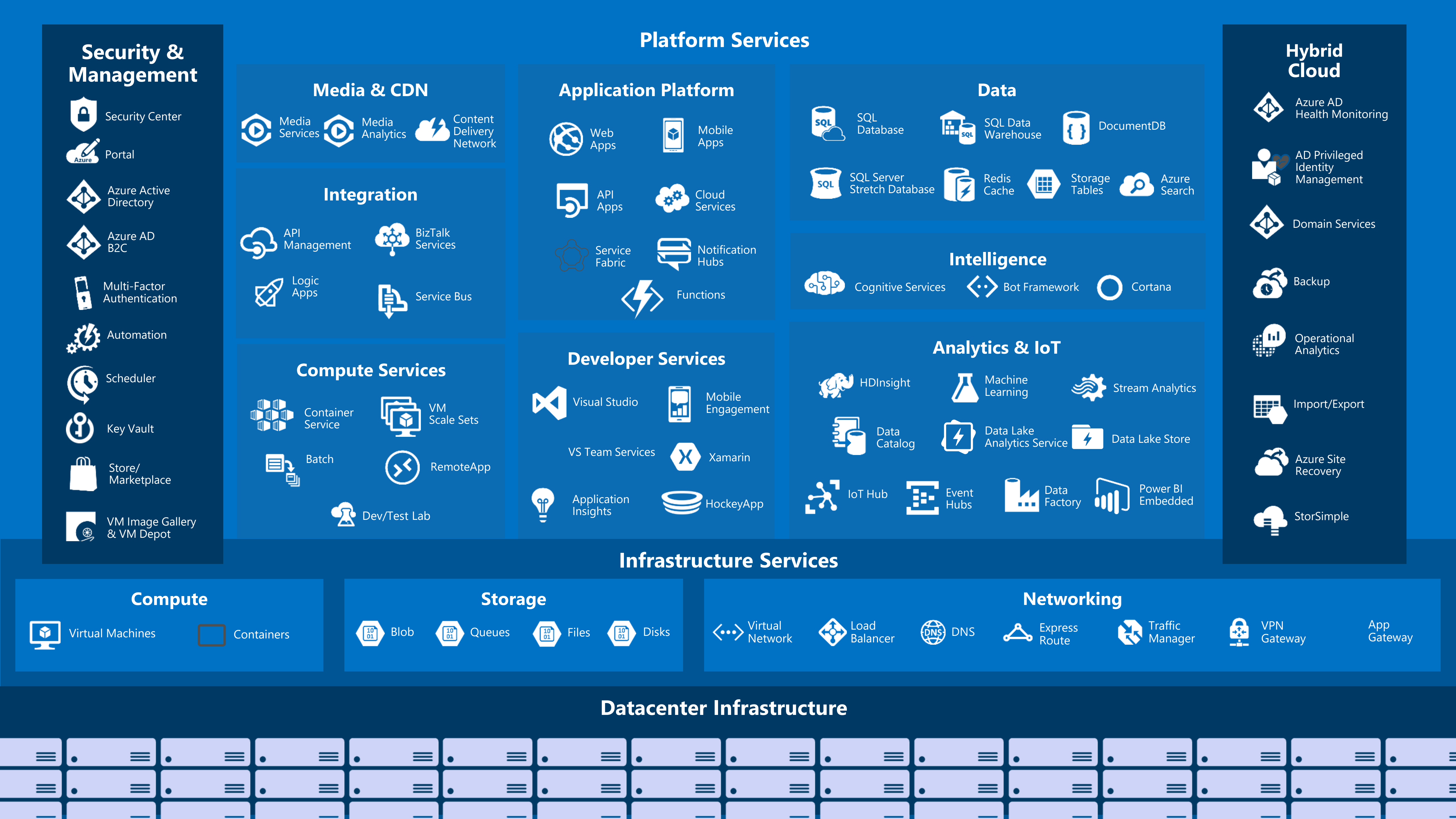
Expo Light Sponsors

CLOUDEON

SUPERUSERS

PROACTIVE

Security Jungle?!



Platform Services

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

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

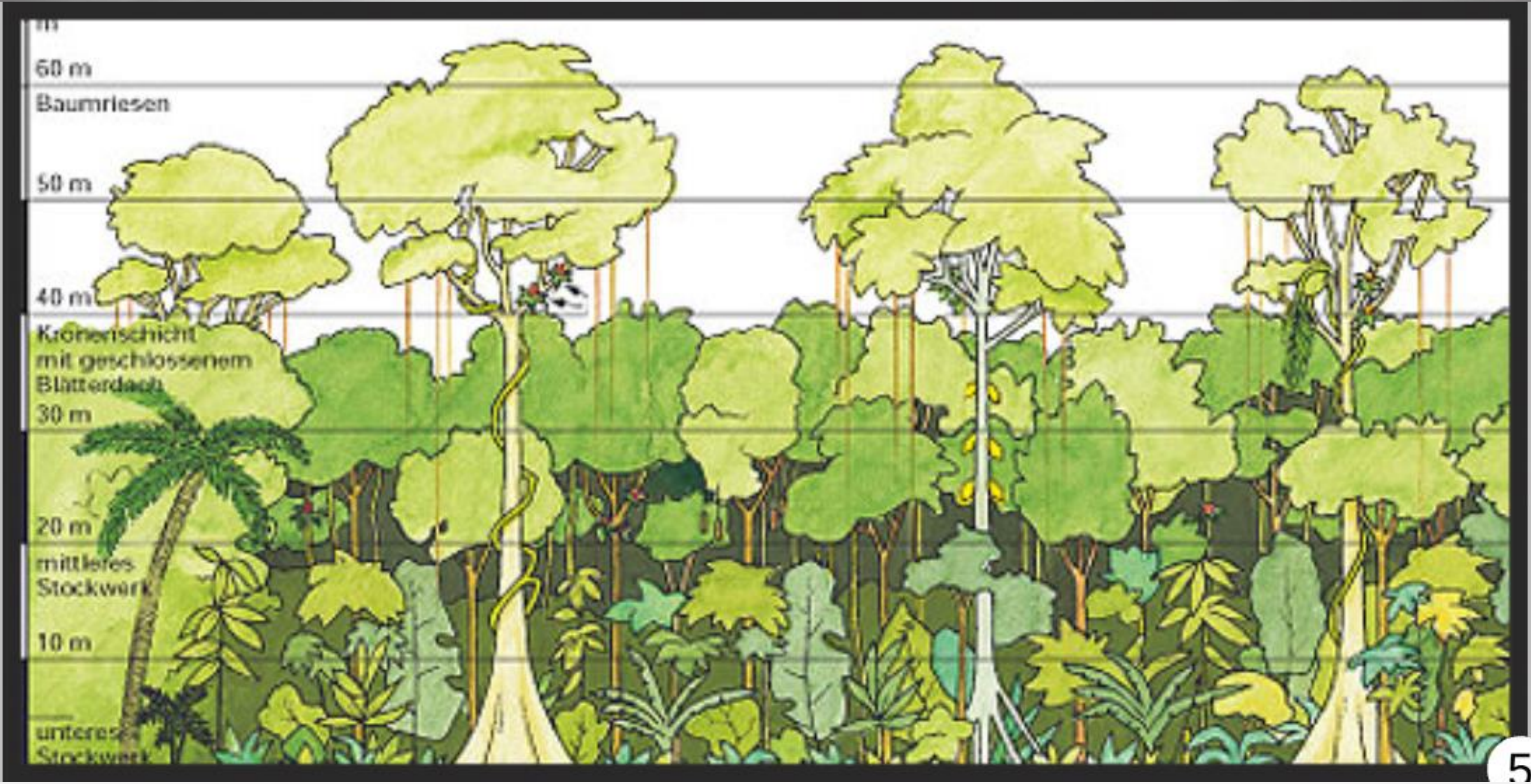
Storage

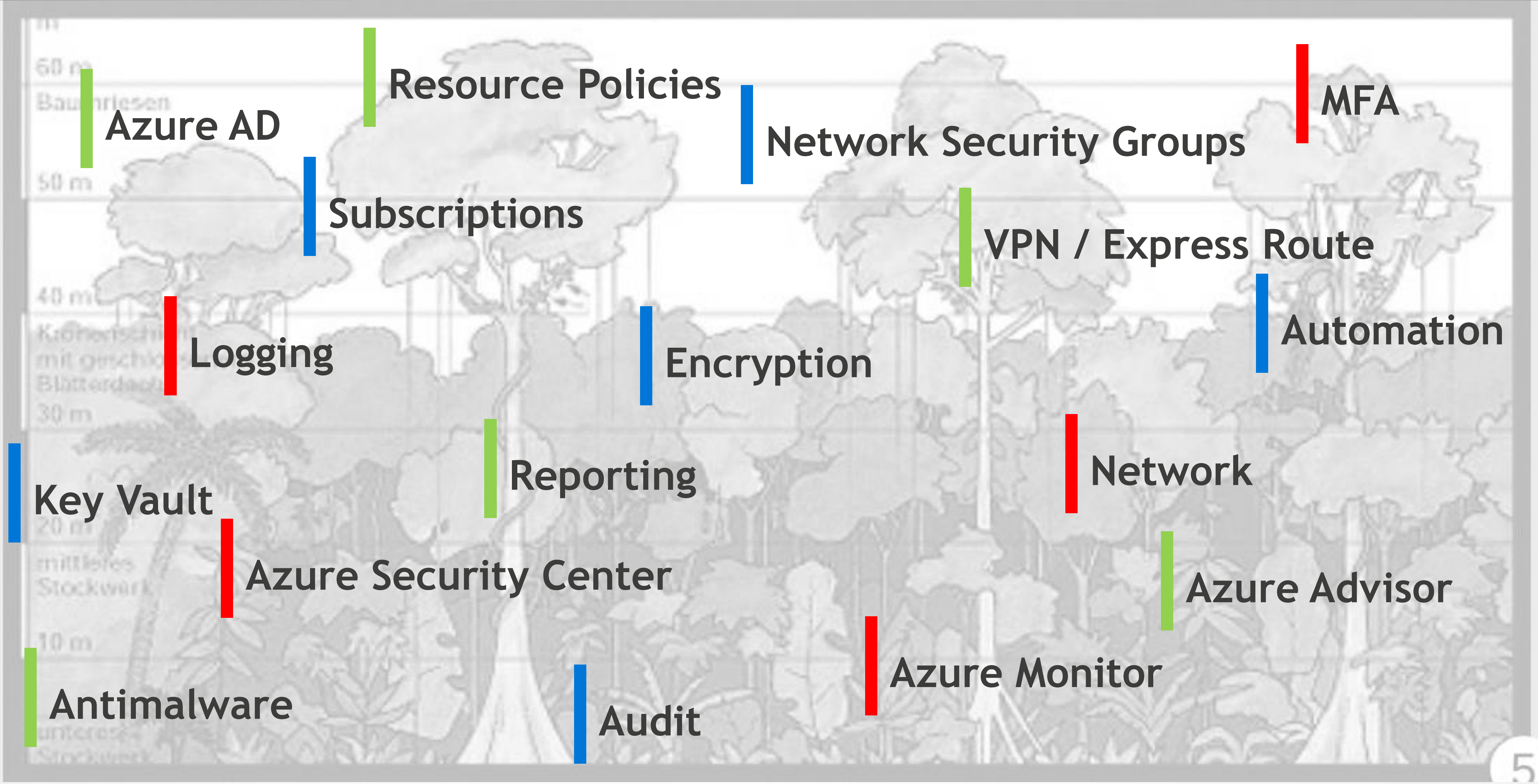
- Blob
- Queues
- Files
- Disks

Networking

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

Datacenter Infrastructure


m
60 m
Baumriesen
50 m
40 m
Kronenschicht
mit geschlossenem
Blätterdach
30 m
20 m
mittleres
Stockwerk
10 m
unteres
Stockwerk



Resource Policies

Azure AD

MFA

Network Security Groups

Subscriptions

VPN / Express Route

Automation

Logging

Encryption

Reporting

Network

Key Vault

Azure Security Center

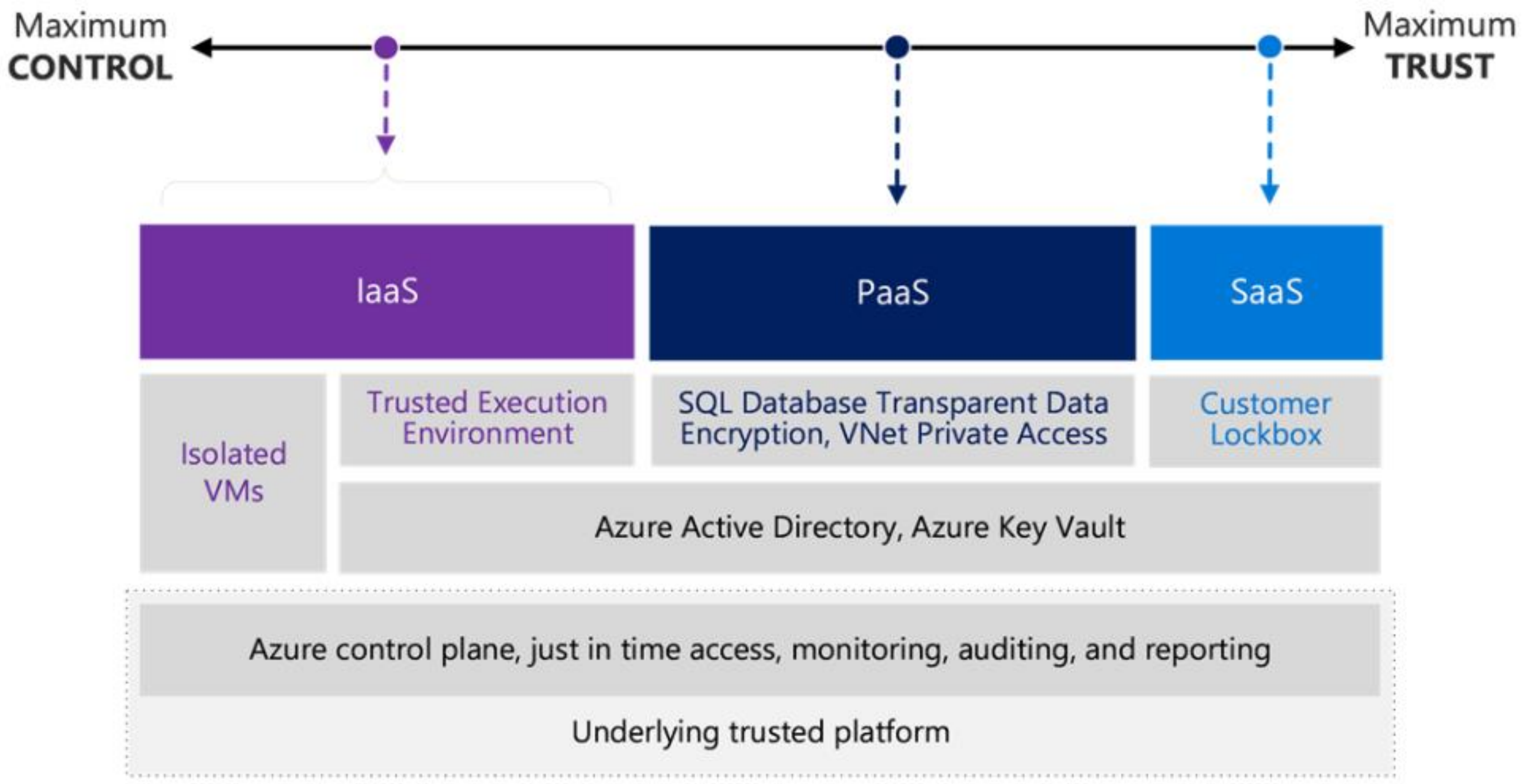
Azure Advisor

Azure Monitor

Antimalware

Audit

COMPAREX Software · Consulting · Services



Maximum CONTROL

Maximum TRUST

IaaS

PaaS

SaaS

Isolated VMs

Trusted Execution Environment

SQL Database Transparent Data Encryption, VNet Private Access

Customer Lockbox

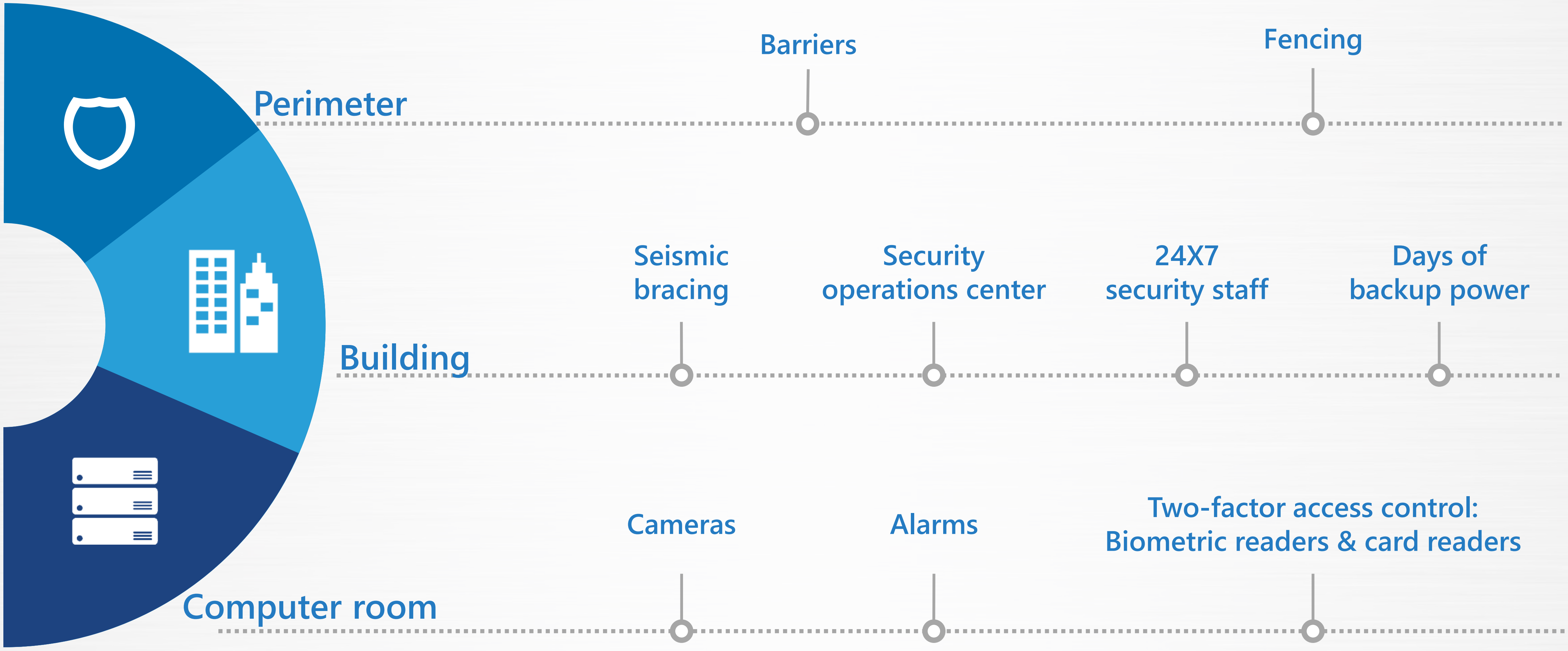
Azure Active Directory, Azure Key Vault

Azure control plane, just in time access, monitoring, auditing, and reporting

Underlying trusted platform

Security Components?!

Datacenter Security



Perimeter

Barriers

Fencing

Building

Seismic bracing

Security operations center

24X7 security staff

Days of backup power

Computer room

Cameras

Alarms

Two-factor access control:
Biometric readers & card readers

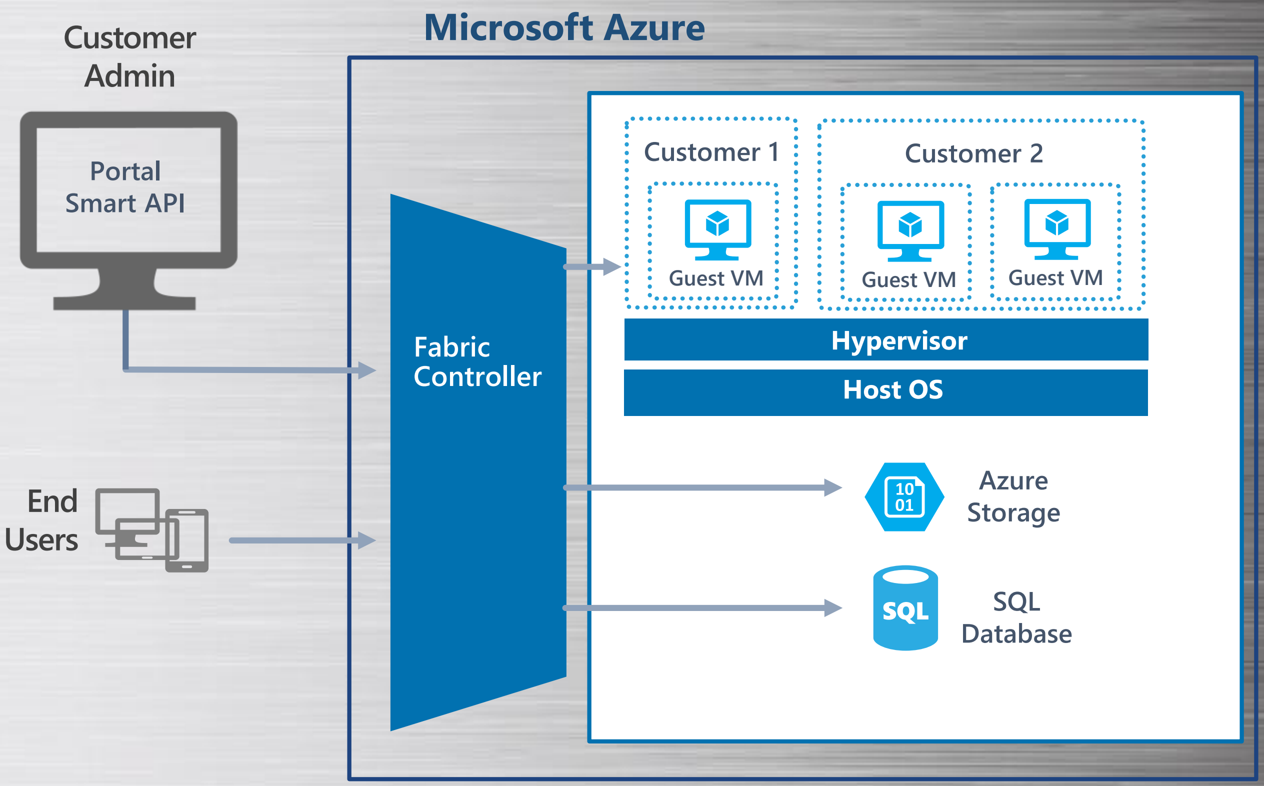
Physical Security

- Azure regions
- access control
- video surveillance
- weight locks
- In-house disc destruction

https://cloud-platform-assets.azurewebsites.net/datacenter

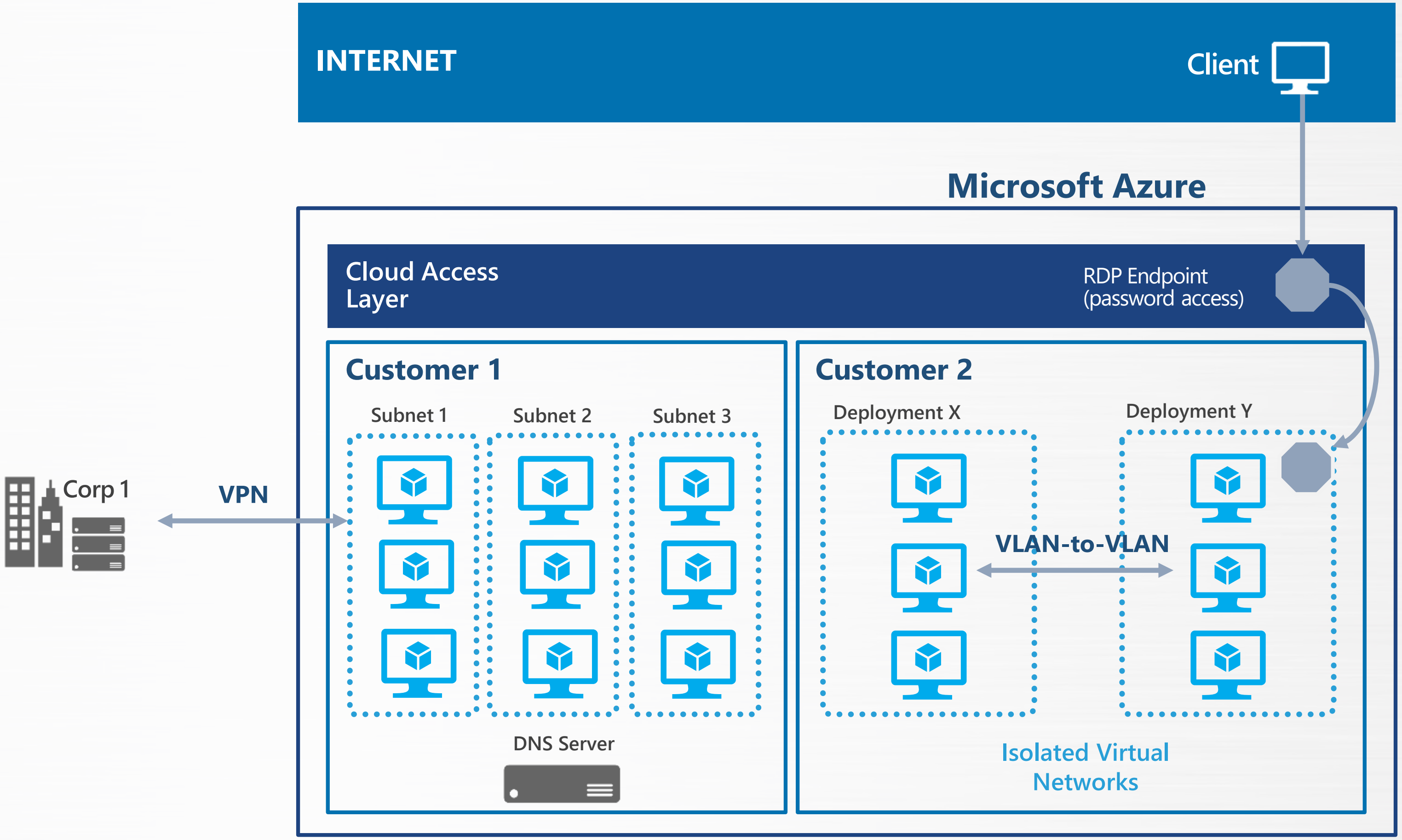
Secure Multi-tenancy

- 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



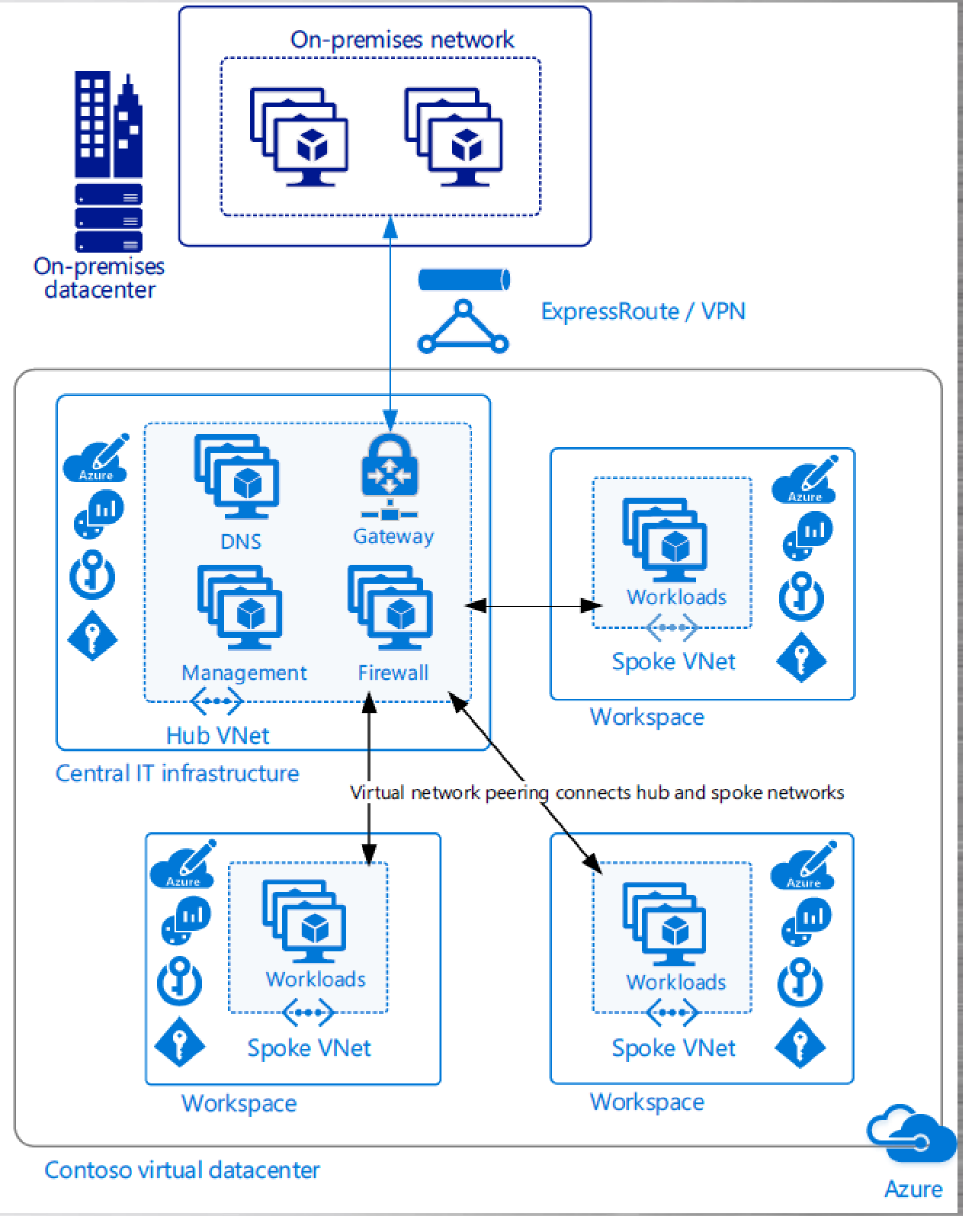
Network Protection

- 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



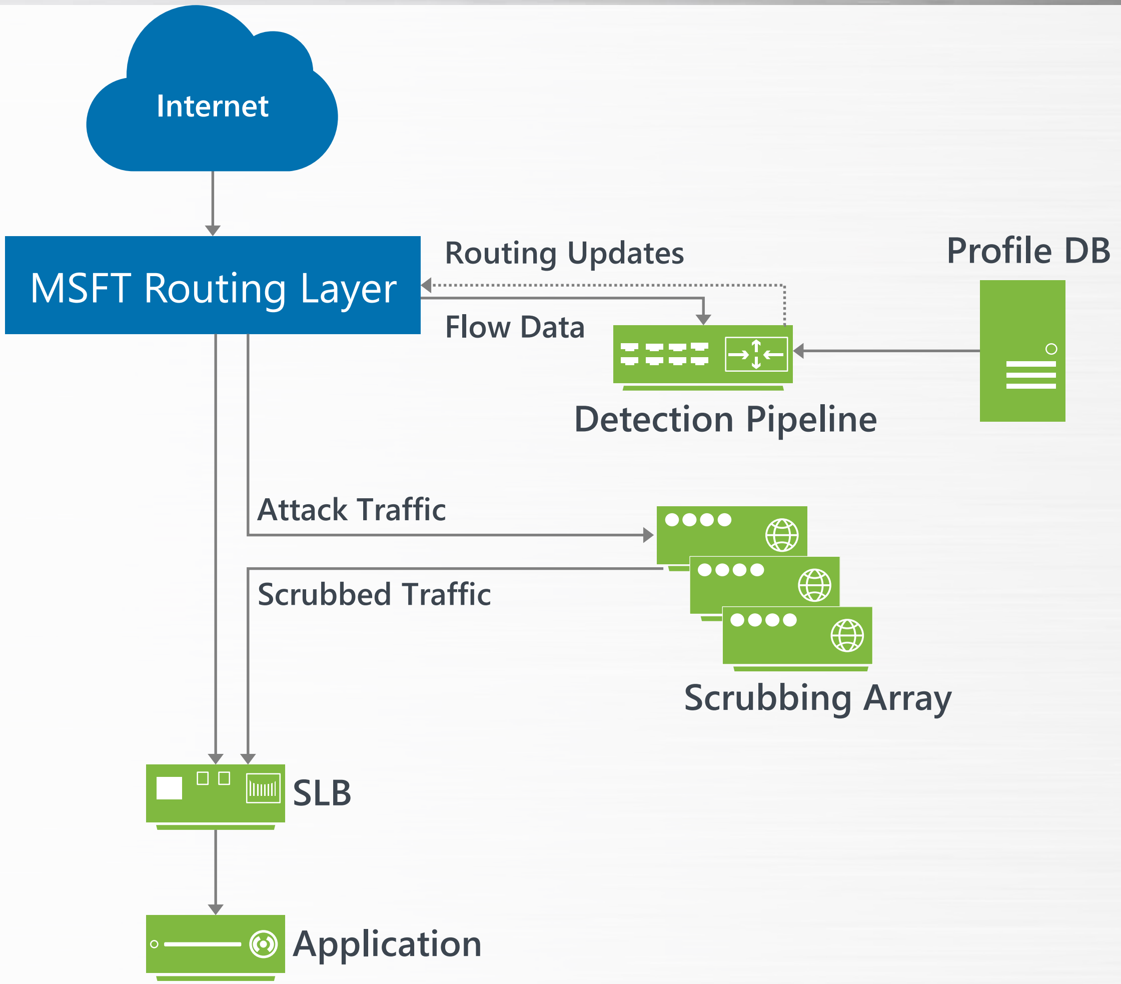
Virtual Networks / VPN

- Extension of own Datacenter to Azure
- Dedicated Express Route connection
- Management over VPN
- Network Security Group (NSG)
- Azure Software Defined Network



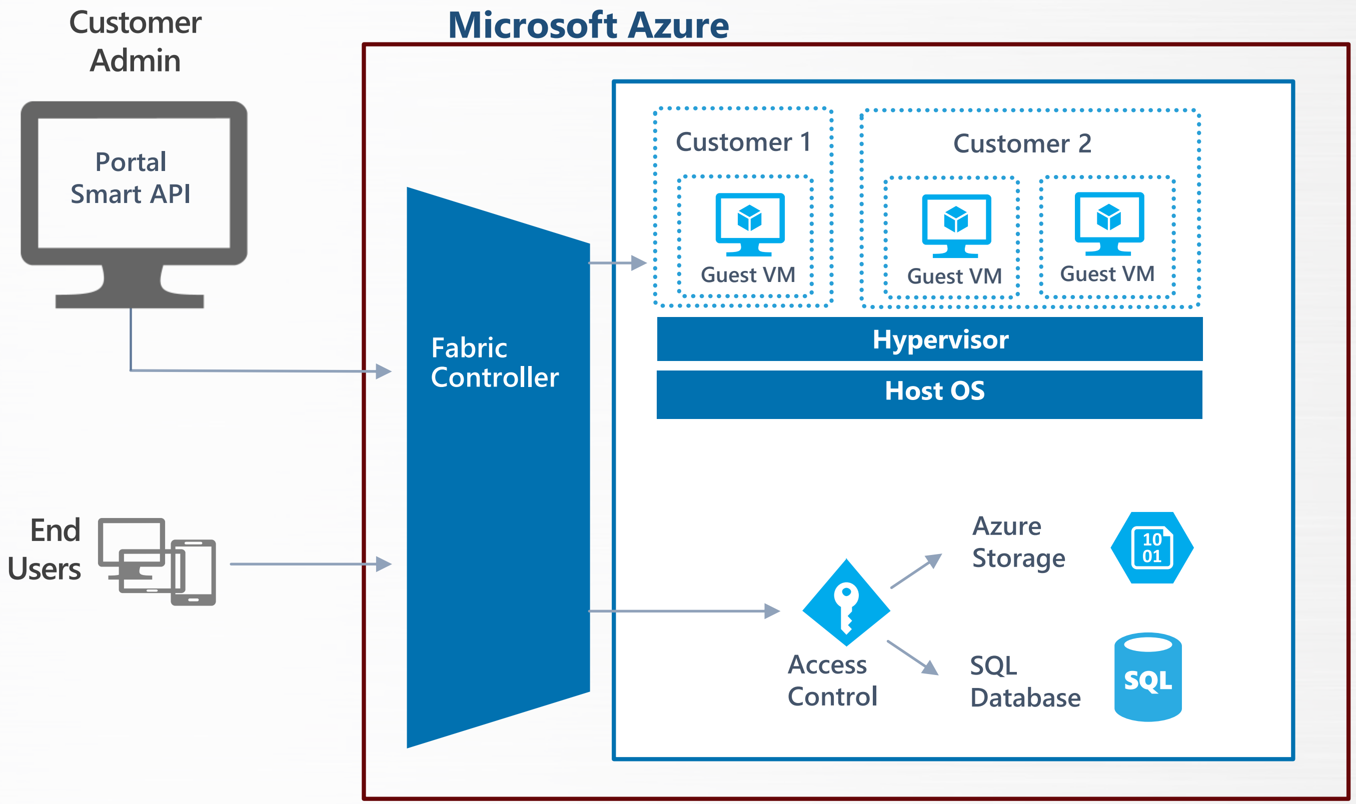
DDoS Defense System

- 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



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



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

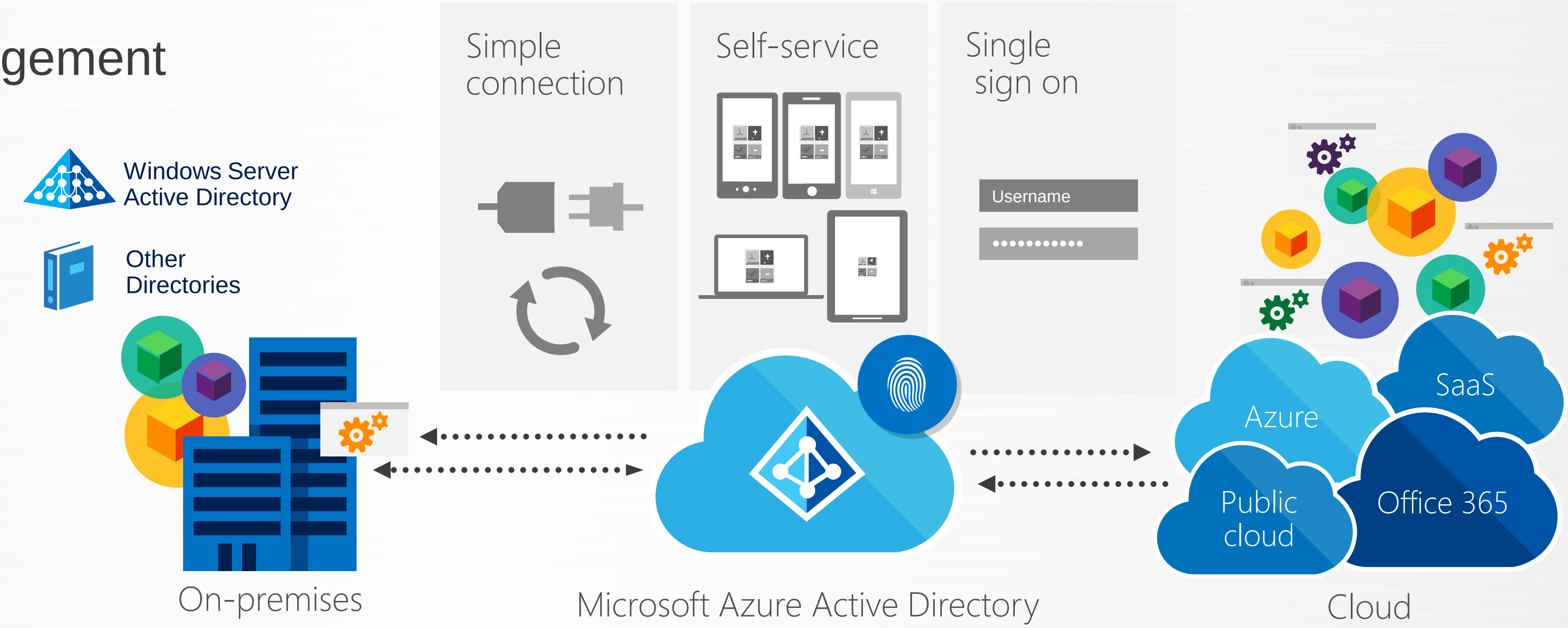
Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

Data destruction

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

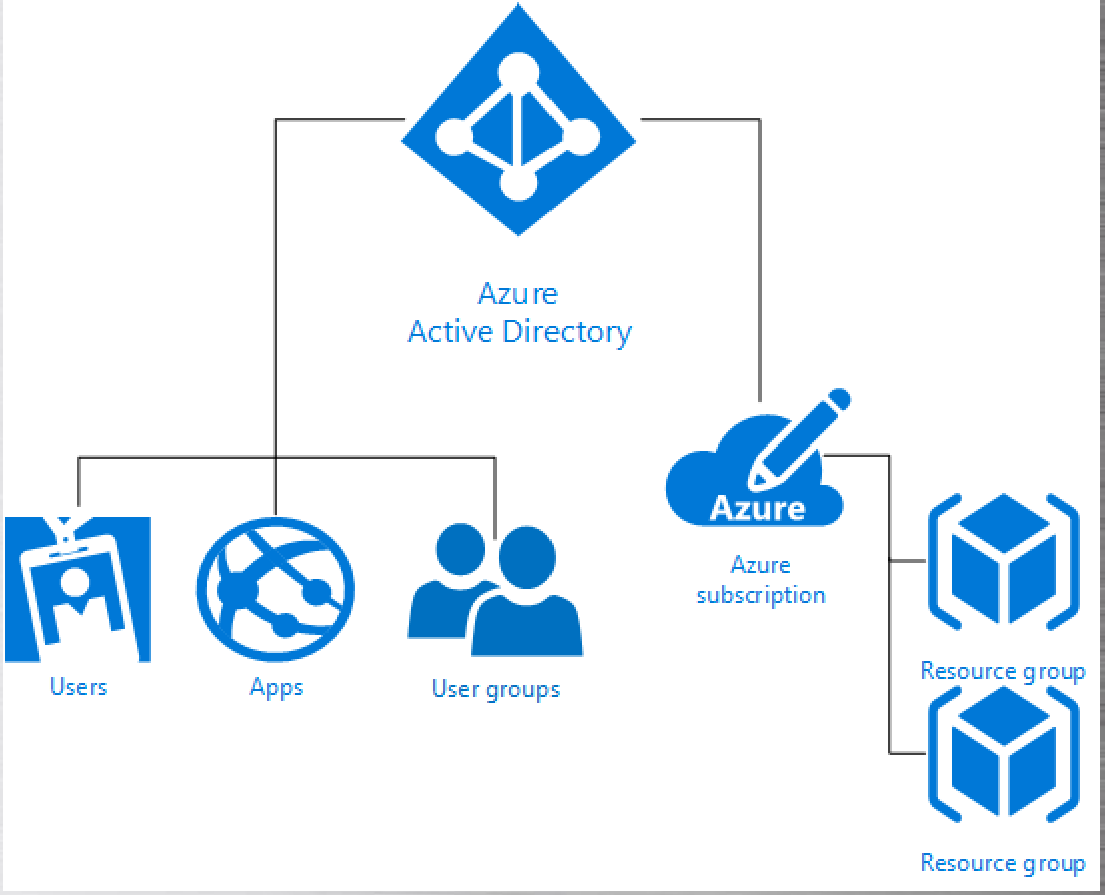
Azure Active Directory

- Only authorized Access allowed
- MFA
- Privileged Identity Management
- Standard Protocols
- Stand-Alone or Hybrid
- Application Integration

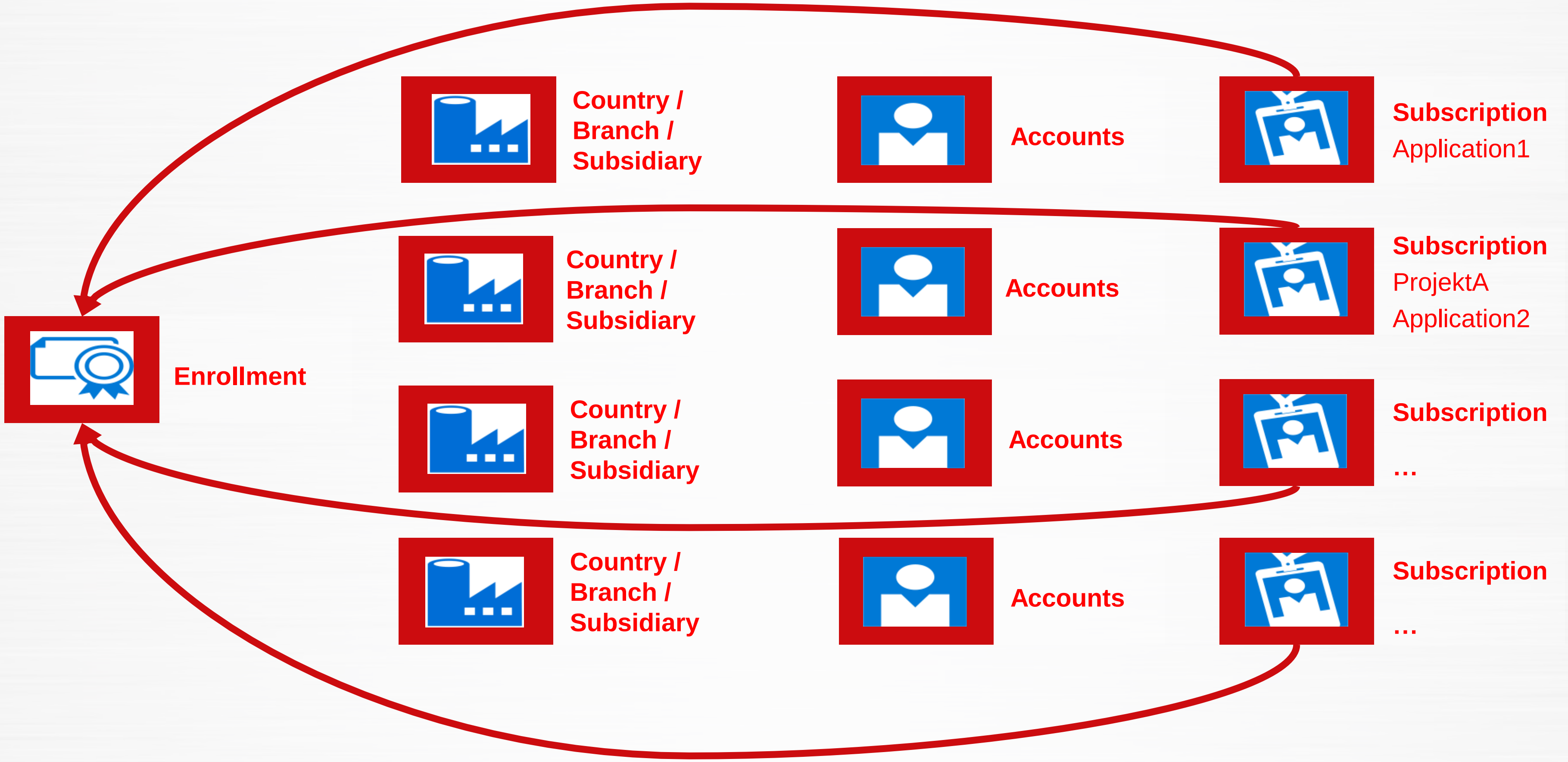


RBAC

- Connection between Azure AD and Subscription
- Default Roles
  - Owner
  - Contributor
  - Reader
- Other Roles
  - Automation Operator
  - DevTest Labs User
  - …
- Own Roles



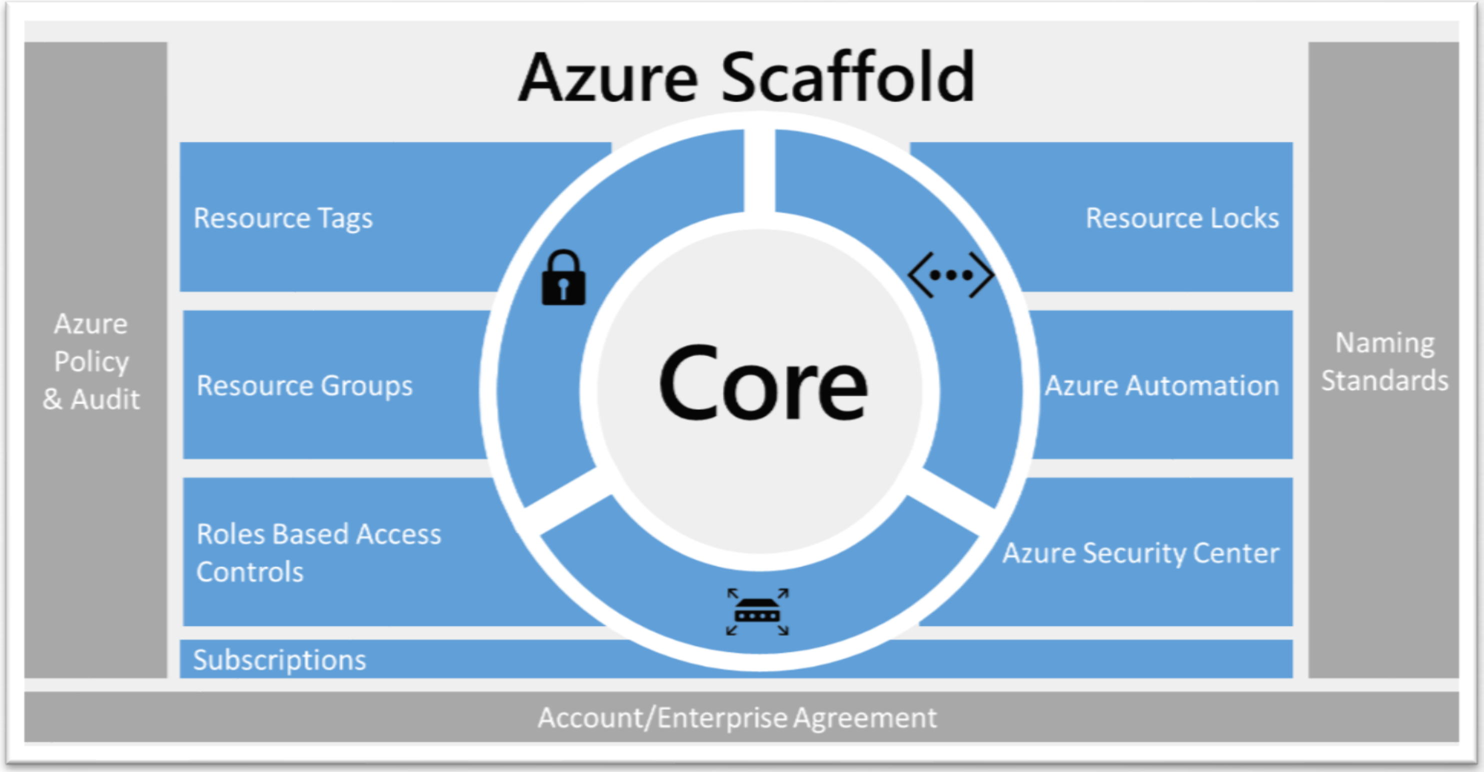
Azure Hierarchy



Azure Governance

„IT‘s not going to be easy…“

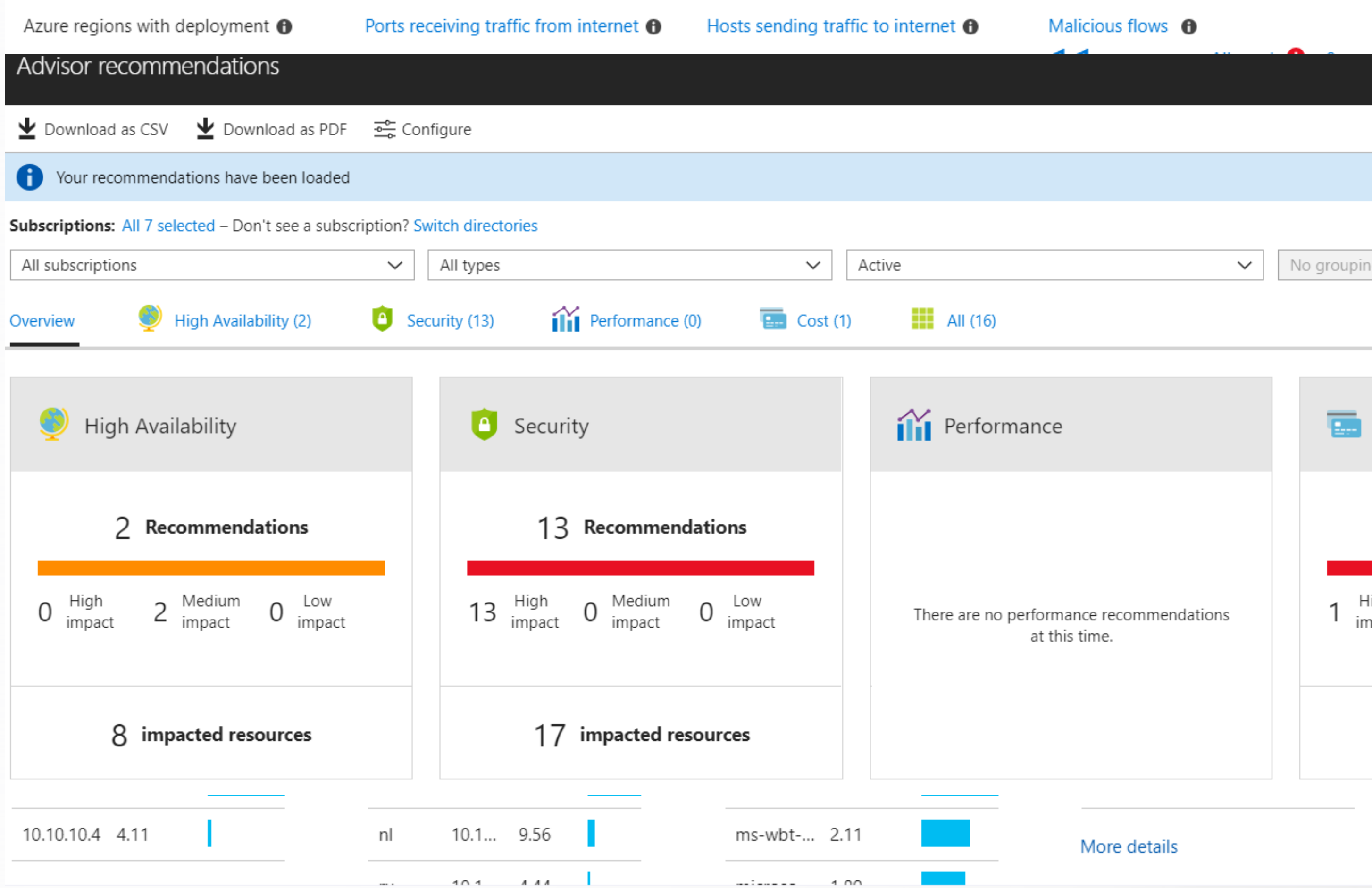
- Billing?!
- User Rights?!
- Protection?!
- Standards?!
- Audits?!



Guide?!

Azure Security Guide

- Operations Management Suite
- Azure Monitor
- Azure AD
- Azure Security Center
- Azure Investigation Dashboard
- Azure Network Watcher
- Traffic Analytics / NSG Flow
- Azure Advisor



Azure regions with deployment   Ports receiving traffic from internet   Hosts sending traffic to internet   Malicious flows

Advisor recommendations

Your recommendations have been loaded

Subscriptions: All 7 selected – Don't see a subscription? Switch directories

All subscriptions | All types | Active | No groupin

High Availability

2 **Recommendations**

0 High impact   2 Medium impact   0 Low impact

8 **impacted resources**

Security

13 **Recommendations**

13 High impact   0 Medium impact   0 Low impact

17 **impacted resources**

Performance

There are no performance recommendations at this time.

1 Hi im

10.10.10.4   4.11

nl   10.1...   9.56

ms-wbt-...   2.11

More details

Azure Security Center

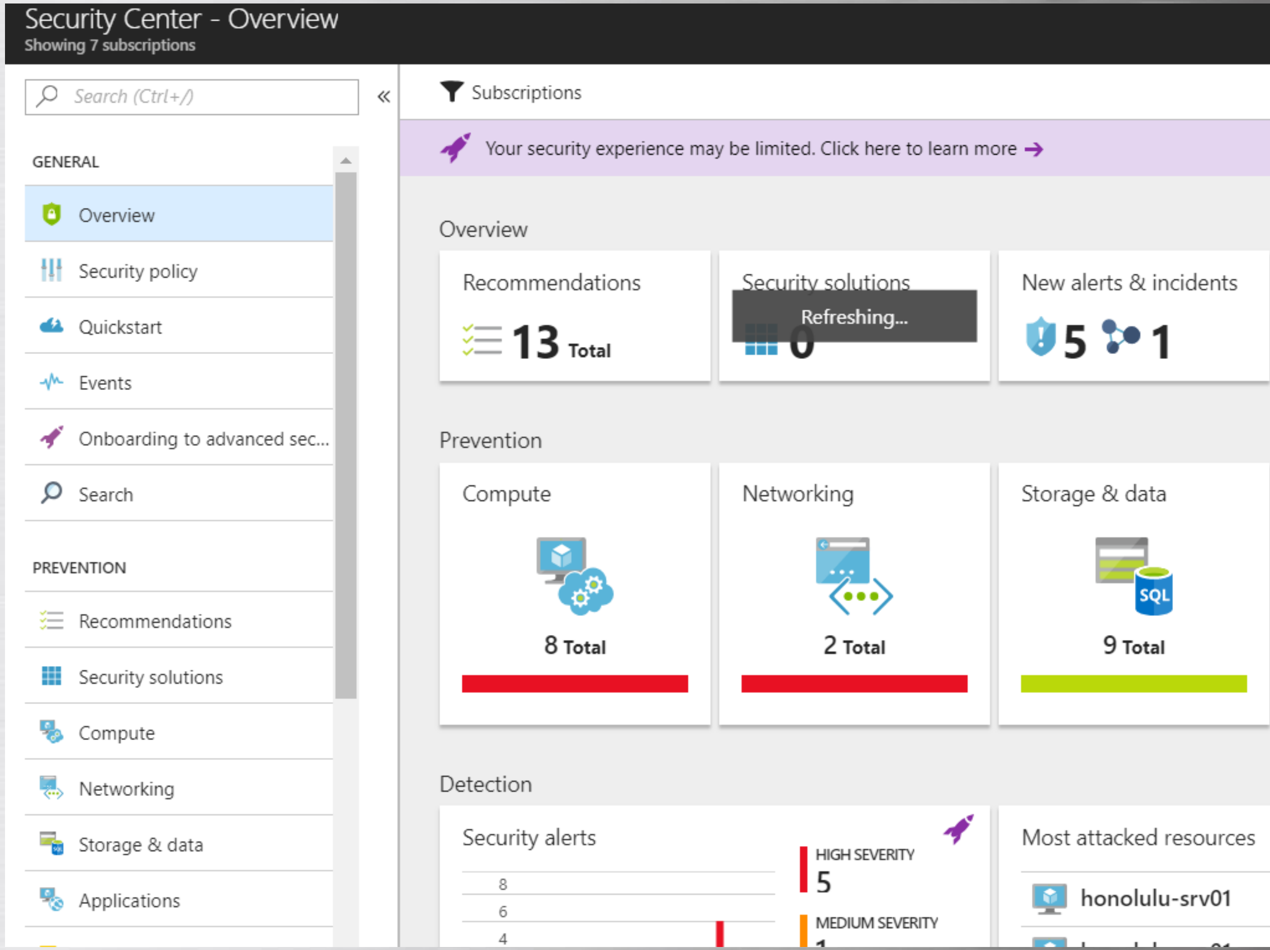
Azure Security Center

Free for Azure Ressources

- Security policy, assessment, and recommendations
- Connected partner solutions

15 $ / Month Azure and Hybrid (incl. free)

- Security event collection and search
- Just in time VM Access
- Adaptive application controls
- Advanced threat detection for networks, VMs/servers, and Azure services
- Built-in and custom alerts
- Threat intelligence



Security Center - Overview

Showing 7 subscriptions

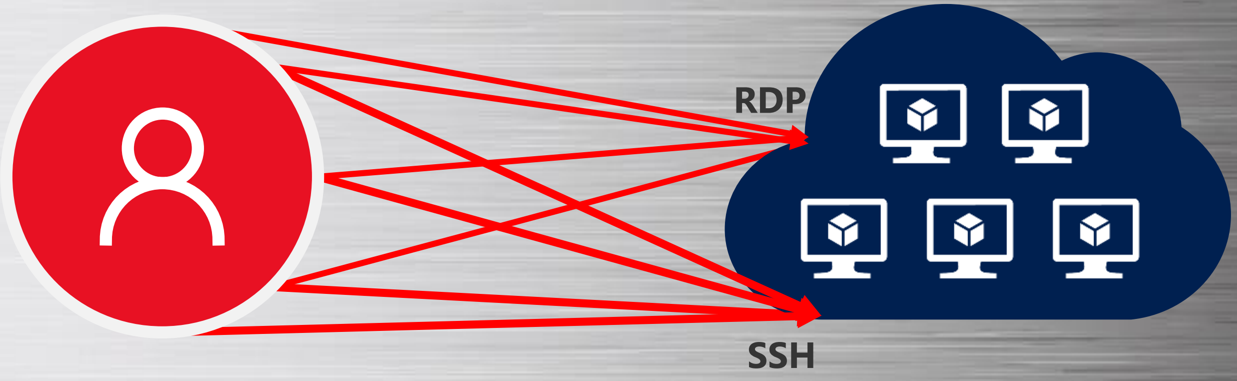
Your security experience may be limited. Click here to learn more →

Quiz:
What is the most common attack targeting IaaS VMs?

COMPAREX
Software · Consulting · Services

Azure Security Center
JIT VM Access

- Known IP ranges
- 100,00 attacks/month/VM (RDP and SSH)
- Easy access to local accounts
- Always open

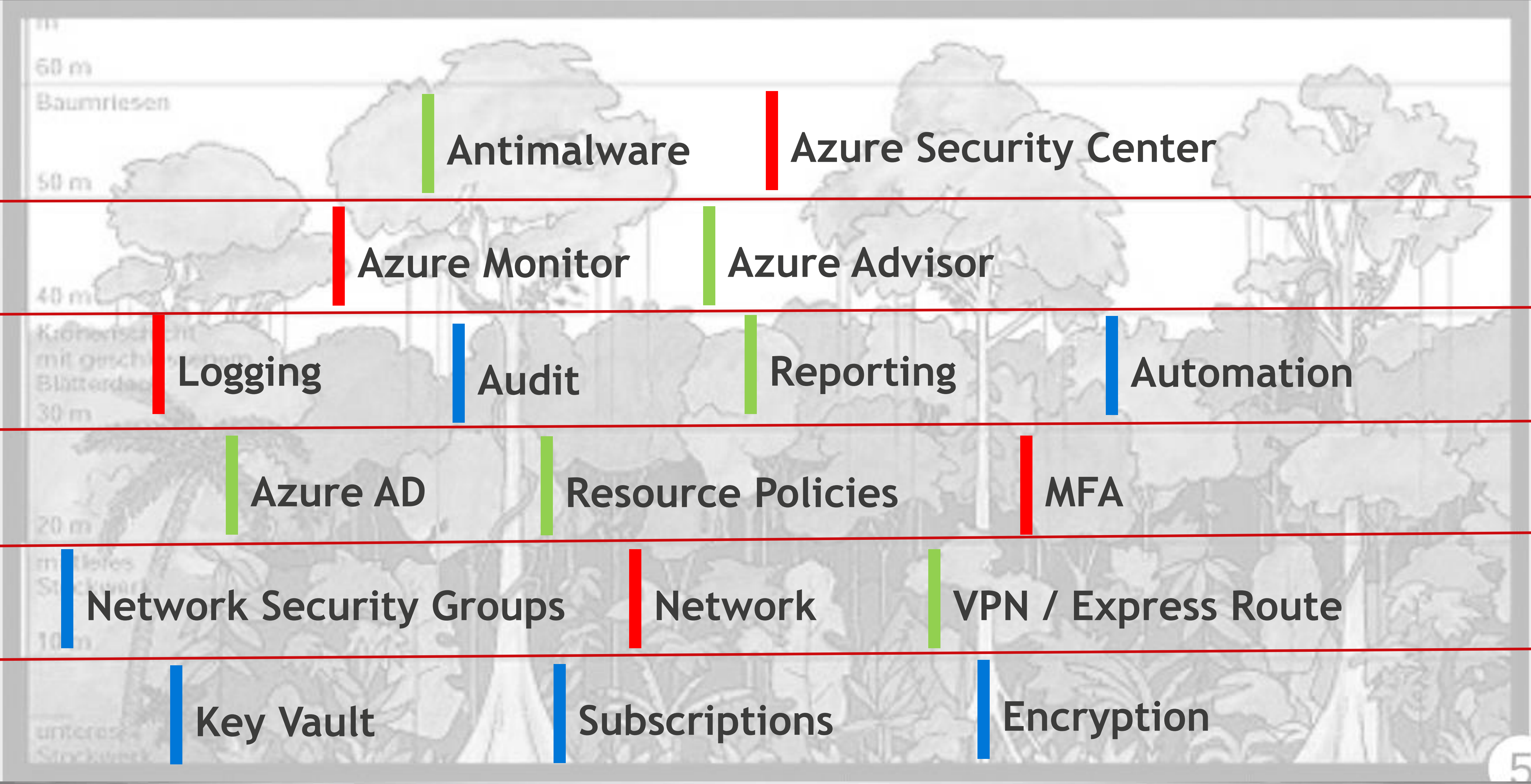


DEMO

Next Steps?!

Reading educates …

- Azure Virtual Datacenter Whitepaper
  - https://azure.microsoft.com/de-de/blog/azure-virtual-datacenter/
- Azure Security Overview
  - https://docs.microsoft.com/en-us/azure/security/azure-security
- Azure Trust Center
  - https://www.microsoft.com/en-us/trustcenter/security/azure-security



Antimalware | Azure Security Center

Azure Monitor | Azure Advisor

Logging | Audit | Reporting | Automation

Azure AD | Resource Policies | MFA

Network Security Groups | Network | VPN / Express Route

Key Vault | Subscriptions | Encryption

Questions?!

Follow: @ericberg_de | Slides: www.ericberg.de | Contact: info@ericberg.de