Microsoft

Azure Security Compass

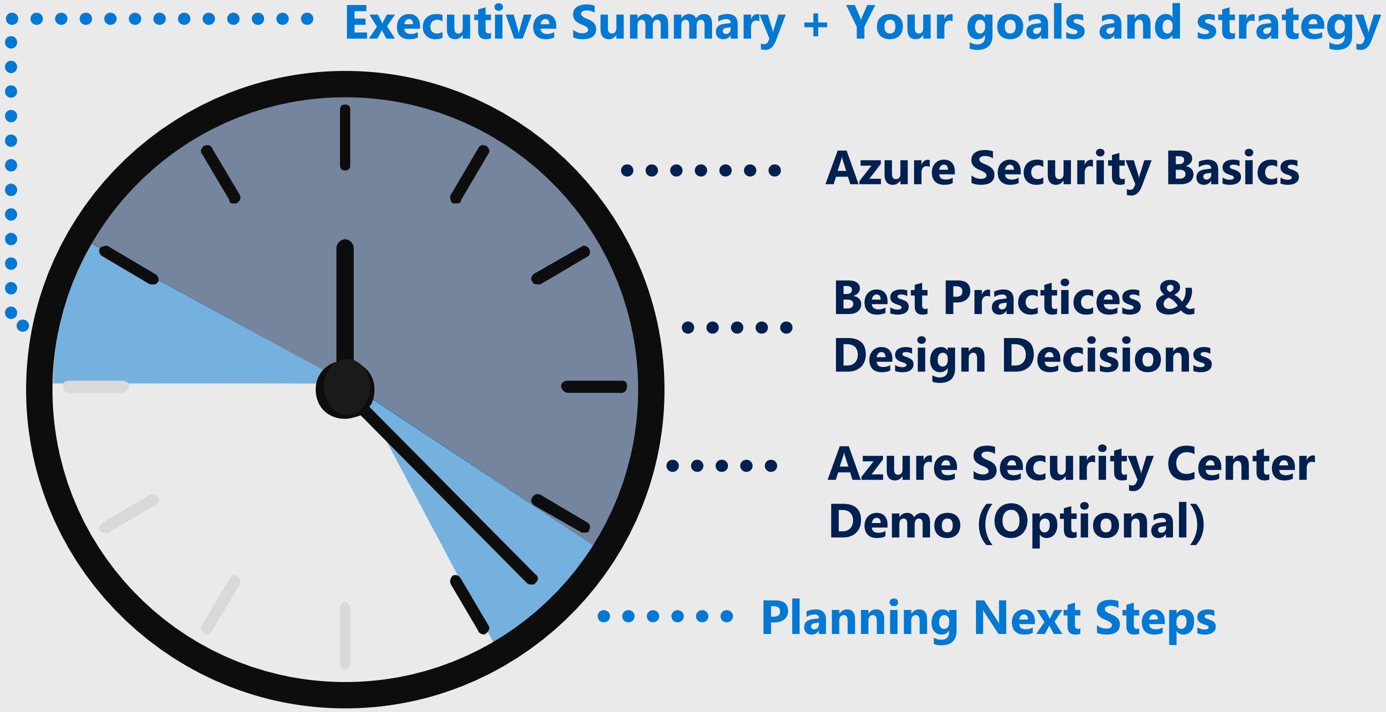
Cybersecurity Solutions Group

https://aka.ms/AzureSecurityCompass

Version 1.1 – September 2019

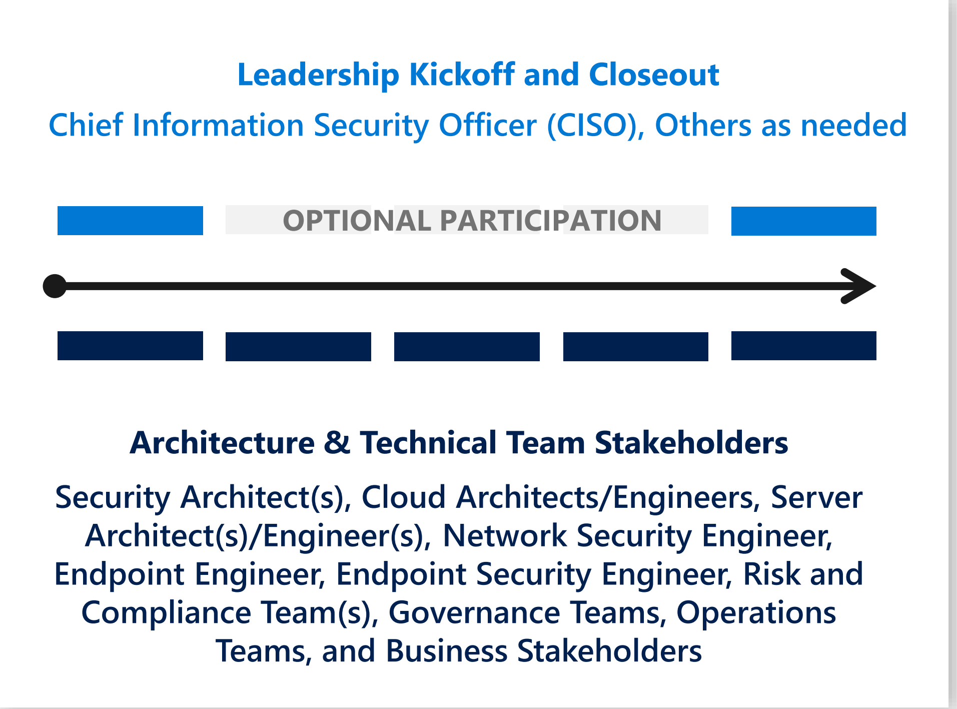
Microsoft Azure Security Compass Workshop

TYPICAL SCHEDULE



Executive Summary + Your goals and strategy
Azure Security Basics
Best Practices & Design Decisions
Azure Security Center Demo (Optional)
Planning Next Steps

TYPICAL STAKEHOLDERS



Leadership Kickoff and Closeout

Chief Information Security Officer (CISO), Others as needed

Architecture & Technical Team Stakeholders

Security Architect(s), Cloud Architects/Engineers, Server Architect(s)/Engineer(s), Network Security Engineer, Endpoint Engineer, Endpoint Security Engineer, Risk and Compliance Team(s), Governance Teams, Operations Teams, and Business Stakeholders

WORKSHOP OBJECTIVE:

Learn how to securely operate your workloads on Azure

Azure Security Compass - Purpose

Designed to rapidly increase your Azure security posture

Make the right security decisions with best practices, choices and context/recommendations

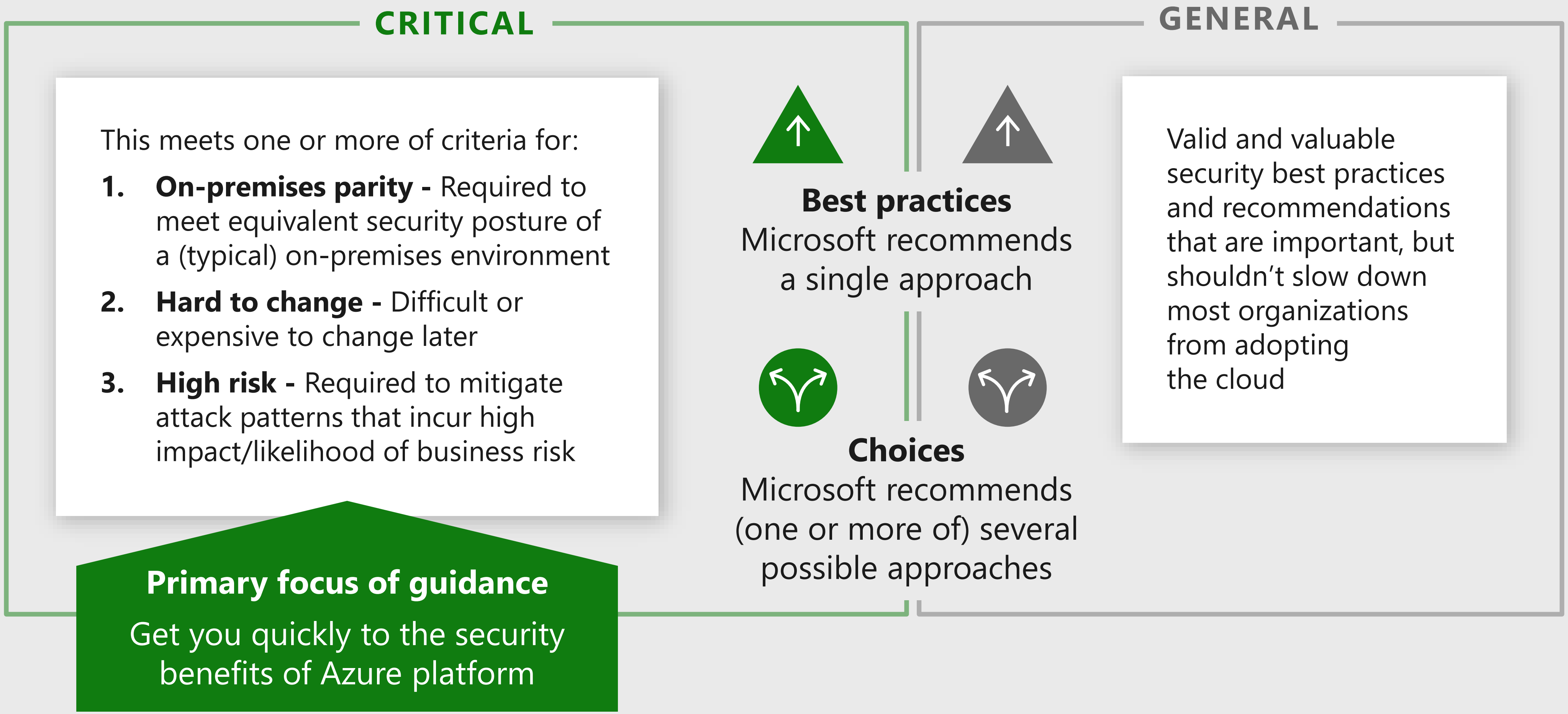
Increase familiarity with Azure Platform Security and Azure Security Center

Tips

- **Mix of old & new -** Bring your experience and knowledge, but expect changes
- **You can't learn everything -** Cloud capabilities evolve too fast to master them all, prioritization is critical

Guidance Structure

Actionable and Prioritized



CRITICAL

This meets one or more of criteria for:

1. **On-premises parity -** Required to meet equivalent security posture of a (typical) on-premises environment
2. **Hard to change -** Difficult or expensive to change later
3. **High risk -** Required to mitigate attack patterns that incur high impact/likelihood of business risk

Primary focus of guidance

Get you quickly to the security benefits of Azure platform

Best practices

Microsoft recommends a single approach

Choices

Microsoft recommends (one or more of) several possible approaches

GENERAL

Valid and valuable security best practices and recommendations that are important, but shouldn't slow down most organizations from adopting the cloud

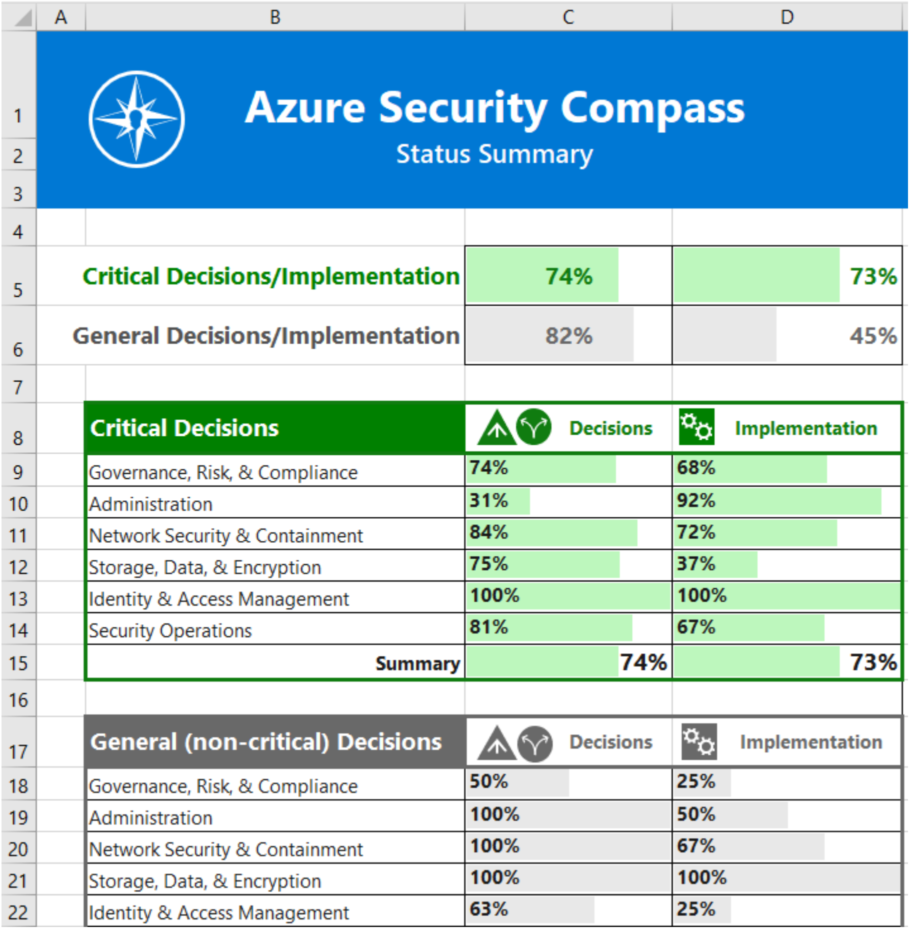
Note: *These represent Microsoft's default opinion based on our experience and knowledge. Your organization may prioritize risk and mitigations differently based on your unique business needs, business risks, or other factors.*

Executive Summary

OVERALL GUIDANCE

	Critical	General
Governance, Risk, and Compliance	16	10
Administration	12	2
Network Security & Containment	12	6
Information Protection & Storage	3	0
Identity & Access Management	5	4
Security Operations	4	4
Total	**42**	**26**

TRACKING SPREADSHEET



Azure Security Compass
Status Summary

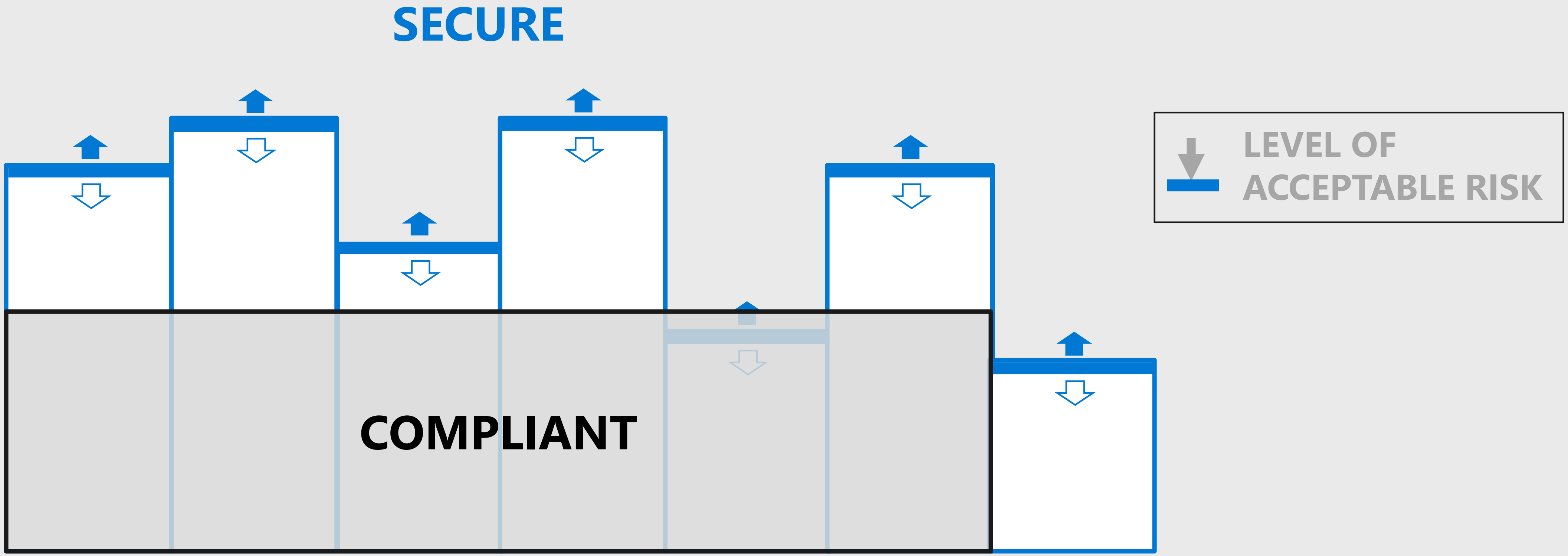
Critical Decisions/Implementation	74%	73%
General Decisions/Implementation	82%	45%

Critical Decisions	Decisions	Implementation
Governance, Risk, & Compliance	74%	68%
Administration	31%	92%
Network Security & Containment	84%	72%
Storage, Data, & Encryption	75%	37%
Identity & Access Management	100%	100%
Security Operations	81%	67%
Summary	74%	73%

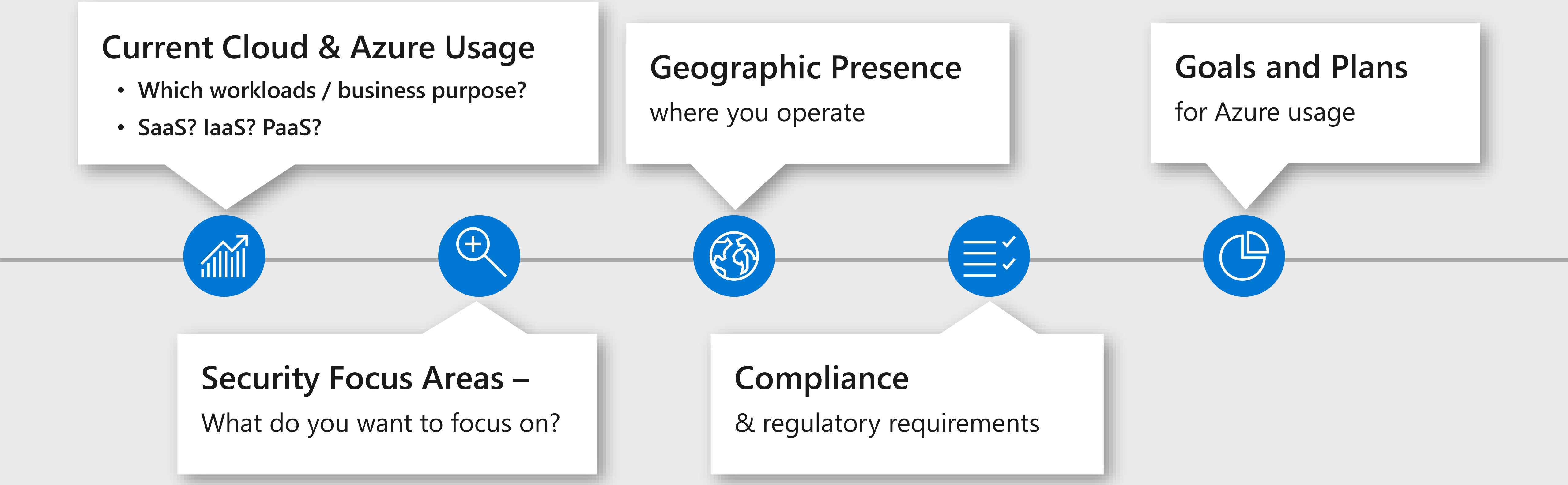
General (non-critical) Decisions	Decisions	Implementation
Governance, Risk, & Compliance	50%	25%
Administration	100%	50%
Network Security & Containment	100%	67%
Storage, Data, & Encryption	100%	100%
Identity & Access Management	63%	25%

COMPLIANT ≠ SECURE

COMPLIANT = Meets a specific standard at point in time (e.g. not negligent)
SECURE = Lowers business risk to acceptable level by disrupting attacker return on investment (ROI)



Whiteboard – Your Journey and Goals



Current Cloud & Azure Usage

- Which workloads / business purpose?
- SaaS? IaaS? PaaS?

Security Focus Areas –

What do you want to focus on?

Geographic Presence

where you operate

Compliance

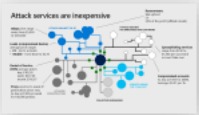
& regulatory requirements

Goals and Plans

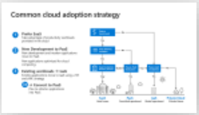
for Azure usage

Azure Security Compass

BASICS


Attack services are inexpensive

TRANSFORMING TOOLS, SKILLS, & PRACTICES


Common cloud adoption strategy

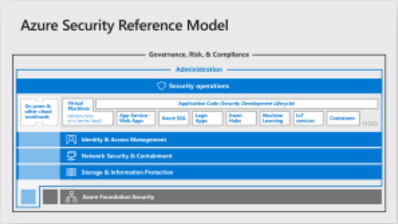
STRATEGIES & THREATS EVOLVE

AZURE REGIONS & SERVICES

Microsoft protecting Microsoft

MICROSOFT SECURITY PRACTICES

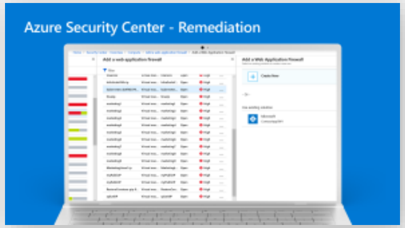
SECURITY GUIDANCE


Azure Security Reference Model

Governance, Risk, & Compliance
Administration
Security operations
On-prem & other cloud workloads
Virtual Machines
Infrastructure as a Service (IaaS)
Application Code (Security Development Lifecycle)
App Service - Web Apps
Azure SQL
Logic Apps
Event Hubs
Machine Learning
IoT services
Containers
Identity & Access Management
Network Security & Containment
Storage & Information Protection
Azure Foundation Security

COMPONENTS & MODELS

AZURE SECURITY CENTER (ASC)


Azure Security Center - Remediation

Governance, Risk, & Compliance

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/governance

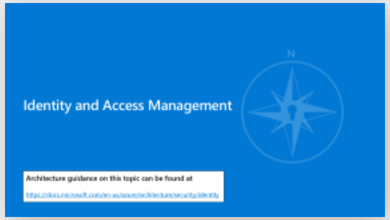
GOVERNANCE, RISK, & COMPLIANCE

Security Operations

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/security-operations

SECURITY OPERATIONS


Identity and Access Management

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/identity

IDENTITY

Network Security & Containment

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/network-security-containment

NETWORK CONTAINMENT

Administration

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/critical-impact-accounts

ADMINISTRATION

Information Protection & Storage

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/storage-data-encryption

INFO PROTECTION & STORAGE

Attack services are inexpensive

Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

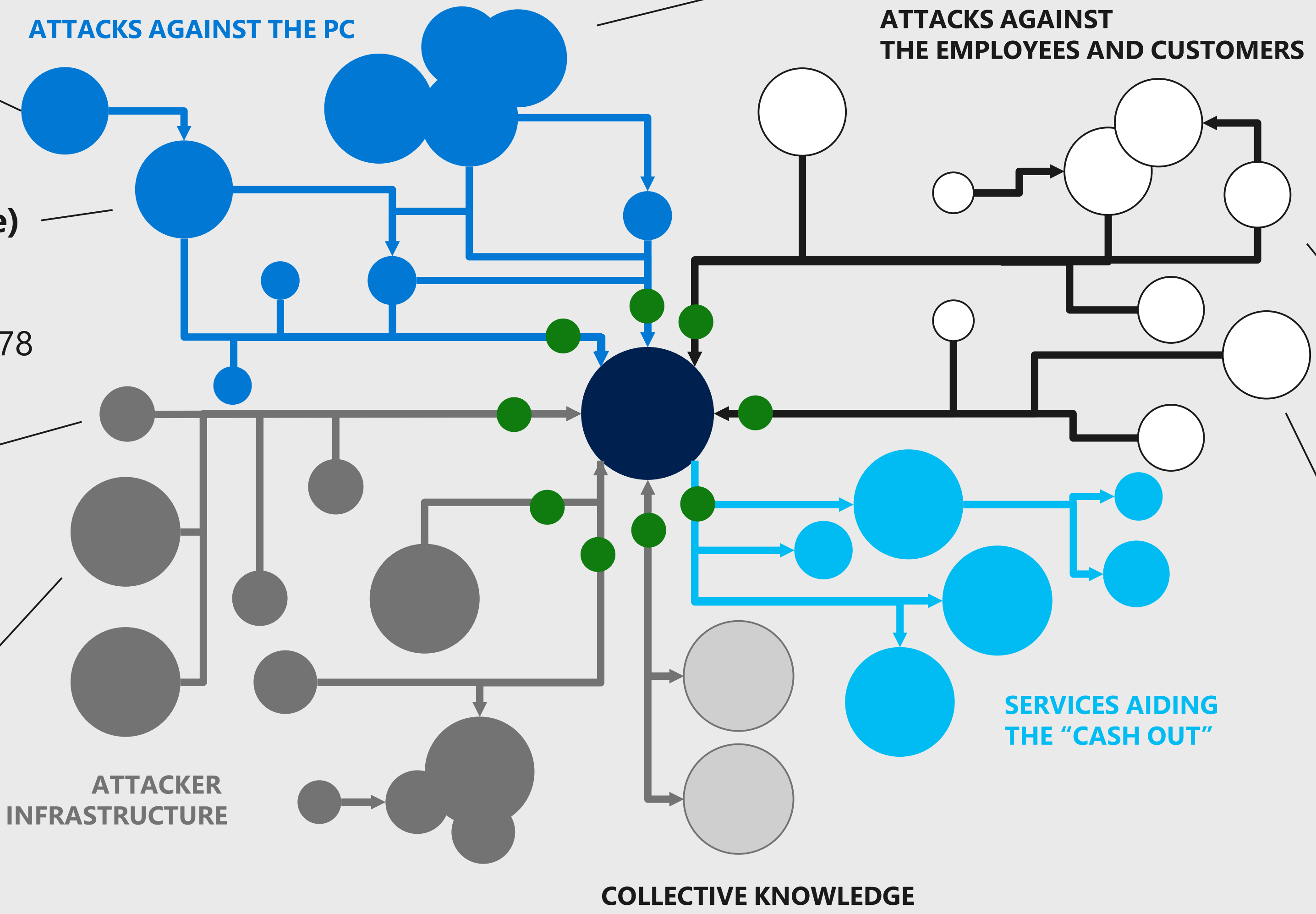
0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges

- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

Proxy services to evade IP geolocation prices vary As low as $100 per week for 100,000 proxies.


ATTACKS AGAINST THE PC
ATTACKS AGAINST THE EMPLOYEES AND CUSTOMERS
ATTACKER INFRASTRUCTURE
COLLECTIVE KNOWLEDGE
SERVICES AIDING THE "CASH OUT"

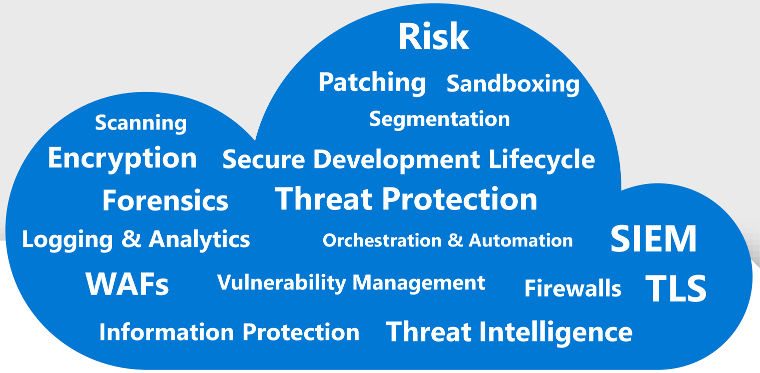
Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

Transforming from Legacy to Cloud

Evolving architecture, tools, skills, & practices

MAIN MENU



Risk

Patching Sandboxing

Segmentation

Scanning

Encryption Secure Development Lifecycle

Forensics Threat Protection

Logging & Analytics Orchestration & Automation SIEM

WAFs Vulnerability Management Firewalls TLS

Information Protection Threat Intelligence

Architectures change, but principles & outcomes remain the same

Roles, responsibilities, and skillsets will evolve

Same

Changed

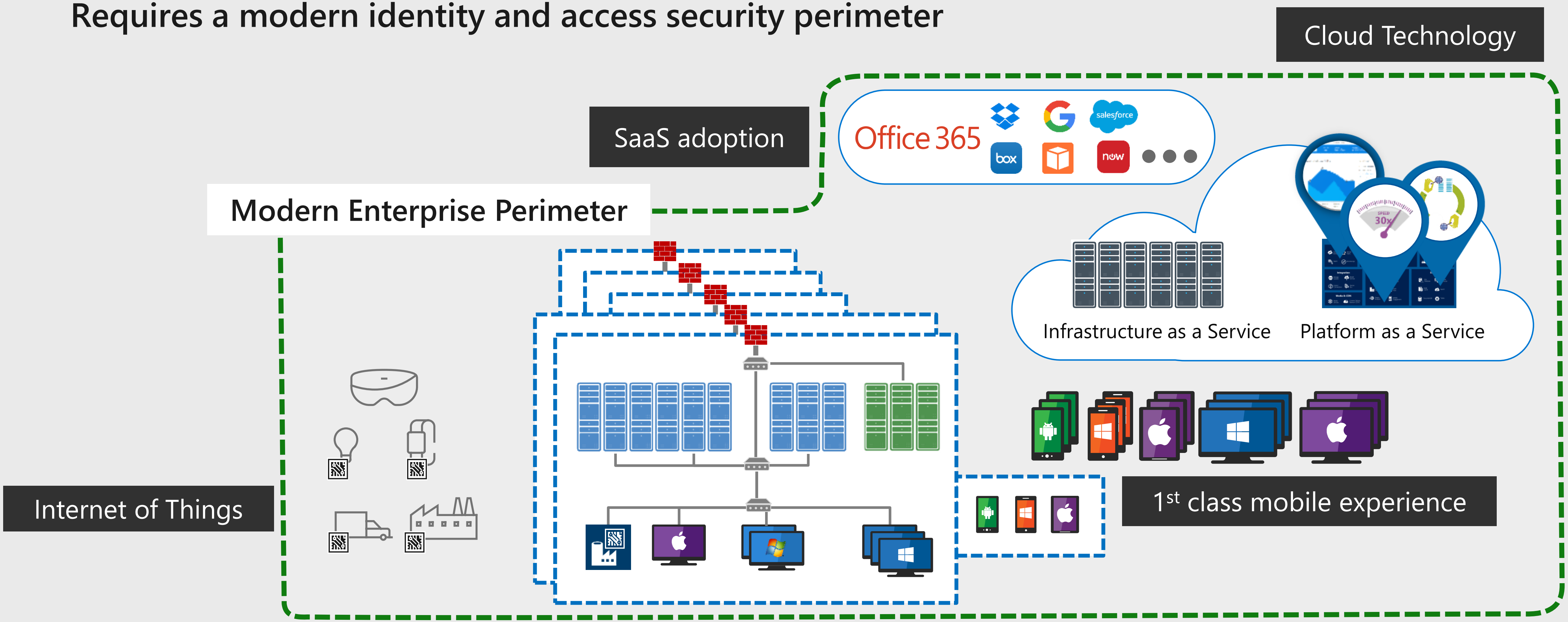
New

Controls, tools, and processes will evolve

Note: Legacy ‘technical debt’ persists with legacy workloads/applications in IaaS

Your enterprise in transformation

Requires a modern identity and access security perimeter



Cloud Technology

SaaS adoption

Modern Enterprise Perimeter

Internet of Things

1st class mobile experience

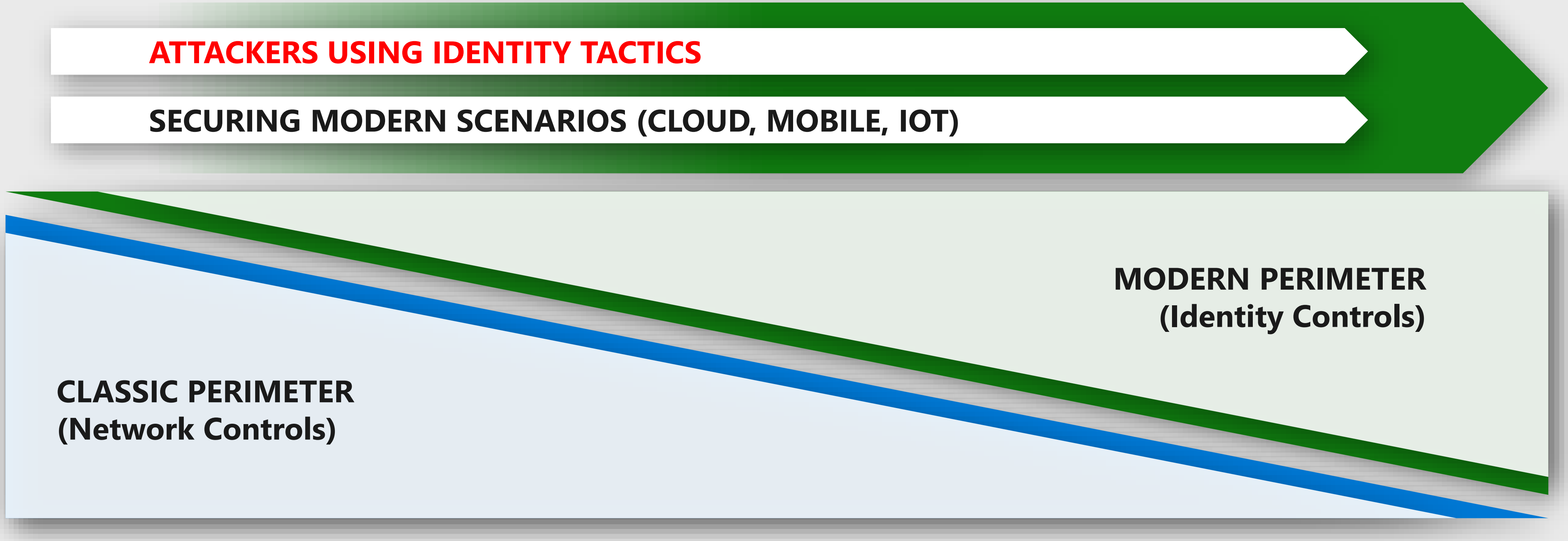
ENGAGE YOUR CUSTOMERS

EMPOWER YOUR EMPLOYEES

OPTIMIZE YOUR OPERATIONS

TRANSFORM YOUR PRODUCTS

Running Dual Perimeters



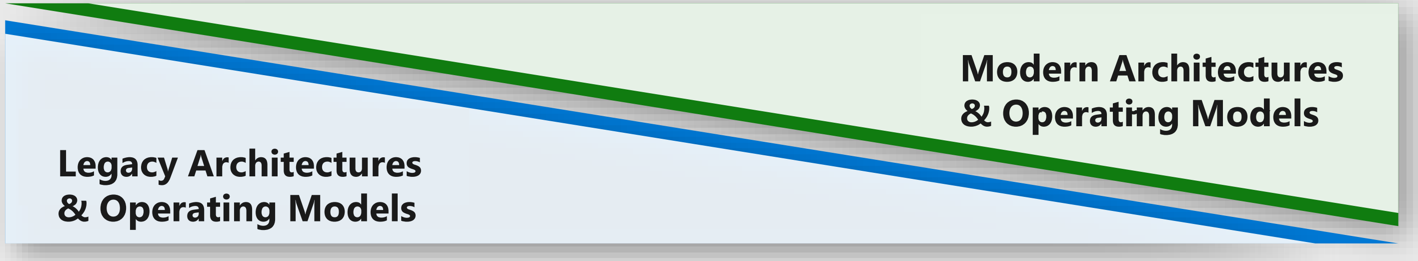
ATTACKERS USING IDENTITY TACTICS

SECURING MODERN SCENARIOS (CLOUD, MOBILE, IOT)

MODERN PERIMETER
(Identity Controls)

CLASSIC PERIMETER
(Network Controls)

Evolution of Roles and Responsibilities



Legacy Architectures & Operating Models

Modern Architectures & Operating Models

“STOP THE PRESSES!” → CONTINUOUS VALIDATION

Security roles will change with architectural/operational models

Manual Resource Administration	**Administration** →	Author & Govern Automation
Containment with Network	Network → **Containment** →	Containment at all layers (Net, App, Identity, Data, etc.)
Quality Check Before Release	**Development** →	Security SME in DevOps process
Project based Engagement	**Architecture** →	Continuous Engagement & Improvement

Common cloud adoption strategy

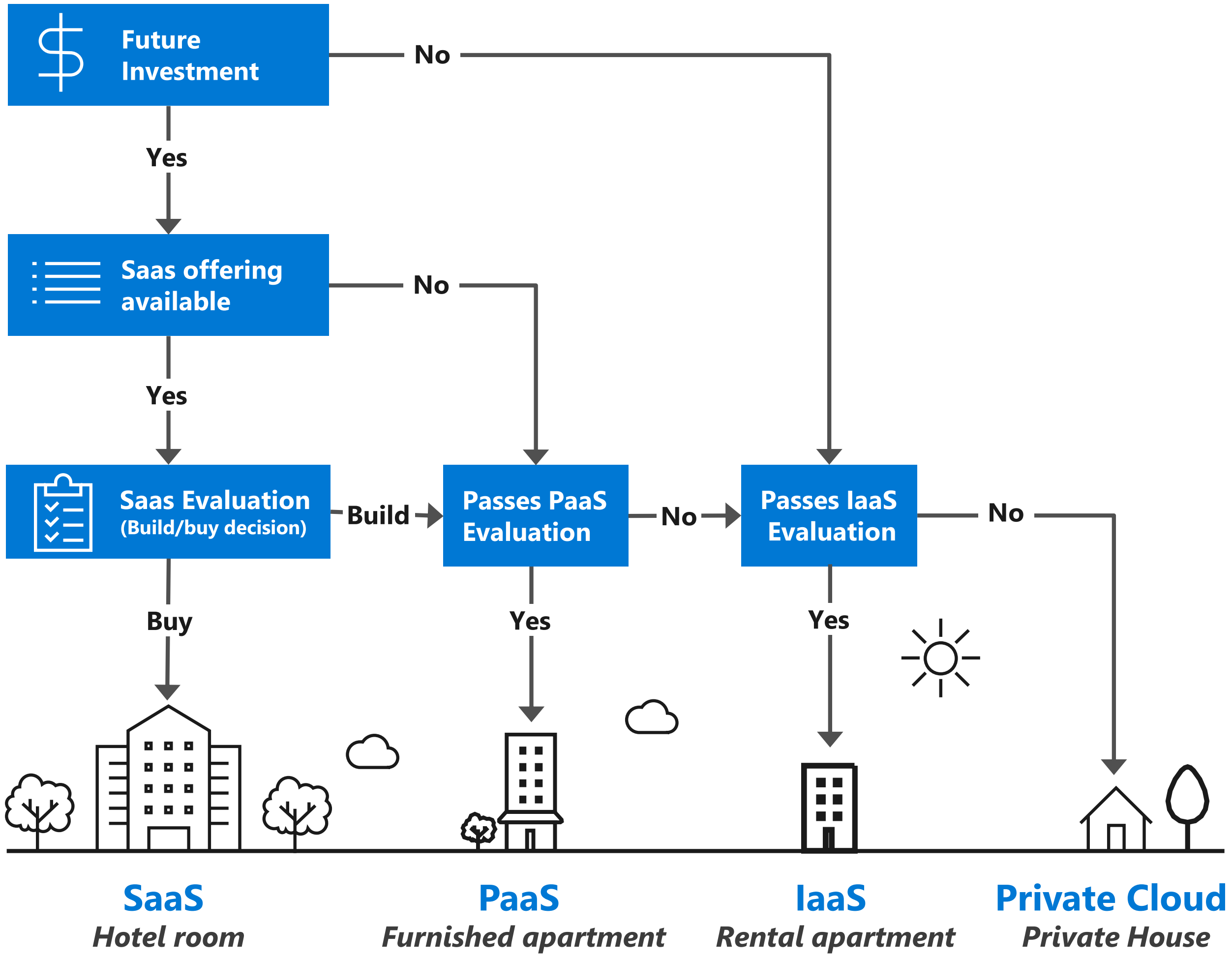
1 **Prefer SaaS**
Take advantage of productivity workloads provided in the cloud

2 **New Development to PaaS**
New development and modern applications move to PaaS.

New applications optimized for cloud computing.

3 **Existing workloads → IaaS**
Existing applications move to IaaS using a 'lift and shift' strategy

3a **→ Convert to PaaS**
Plan to refactor applications into PaaS



Shared Responsibility and Key Strategies

MAIN
MENU

Azure Security Compass

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and Data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and Identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◪	◪	🟦	🟦
Applications	⬜	◪	🟦	🟦
Network Controls	⬜	◪	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

⬜ Microsoft 🟦 Customer

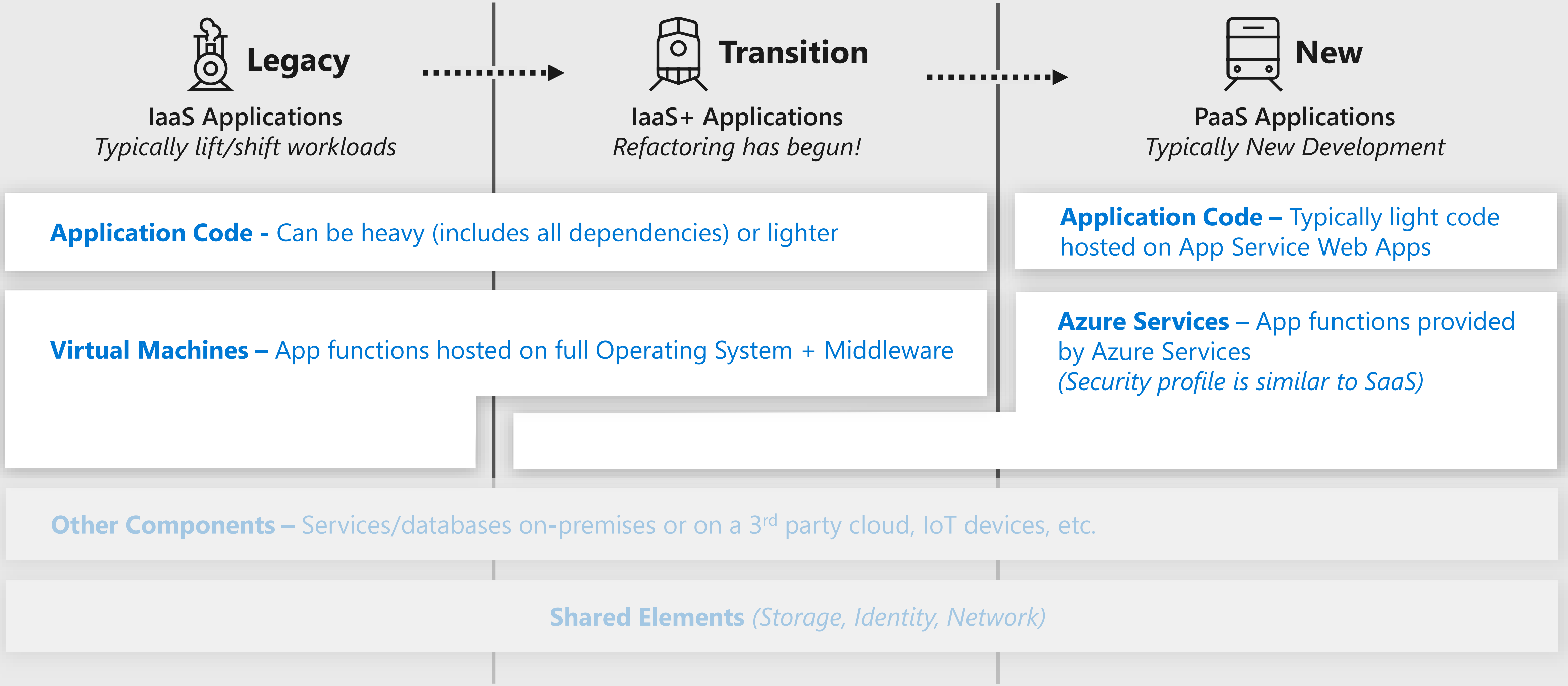
ESTABLISH A MODERN PERIMETER

MODERNIZE INFRASTRUCTURE SECURITY

“TRUST BUT VERIFY” EACH CLOUD PROVIDER

IaaS and PaaS Application Models

Standalone Applications or Components of Larger Solutions



Legacy

IaaS Applications
Typically lift/shift workloads

Transition

IaaS+ Applications
Refactoring has begun!

New

PaaS Applications
Typically New Development

Application Code - Can be heavy (includes all dependencies) or lighter

Application Code – Typically light code hosted on App Service Web Apps

Virtual Machines – App functions hosted on full Operating System + Middleware

Azure Services – App functions provided by Azure Services
(Security profile is similar to SaaS)

Other Components – Services/databases on-premises or on a 3rd party cloud, IoT devices, etc.

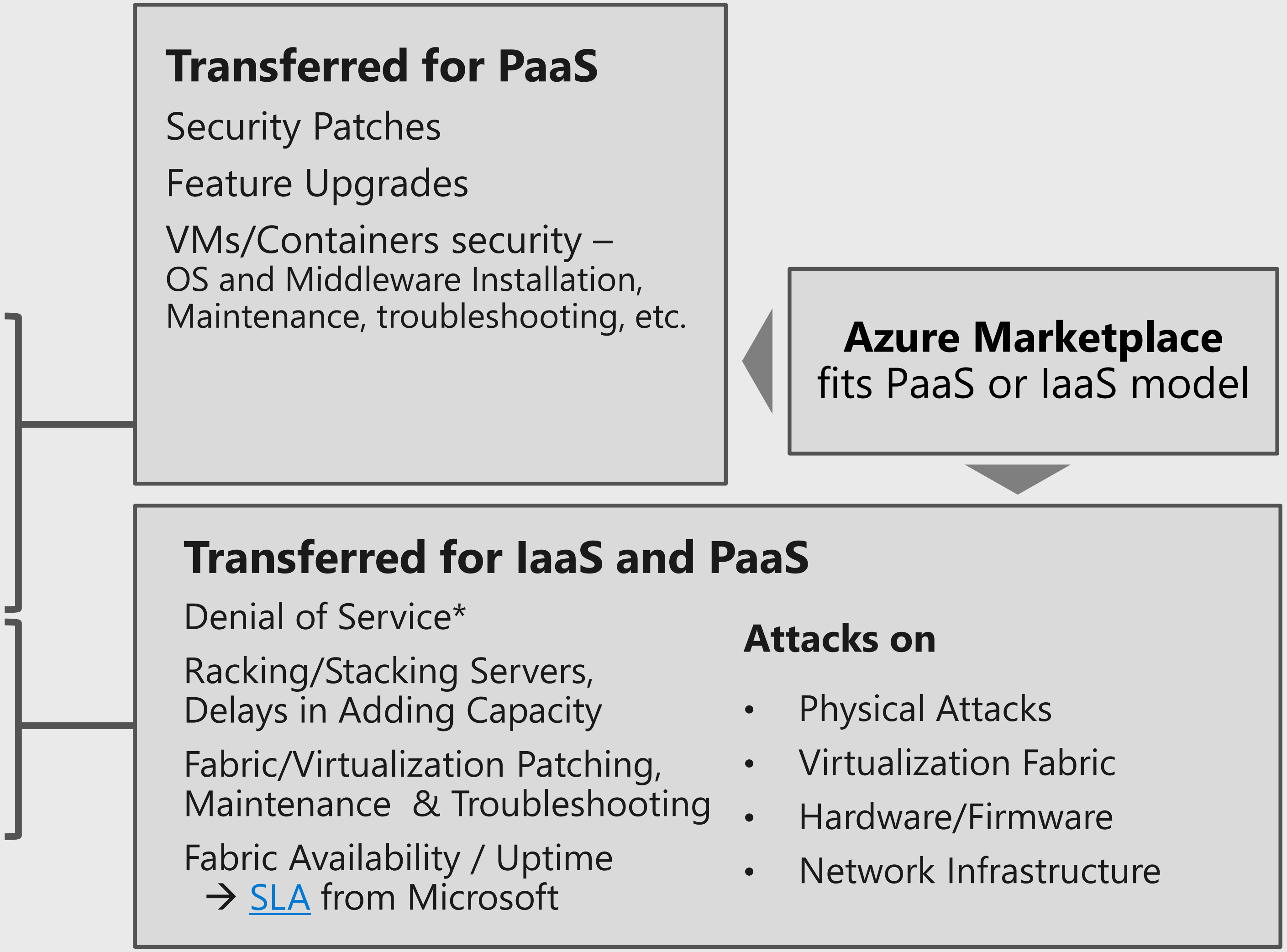
Shared Elements *(Storage, Identity, Network)*

Security Responsibilities Transfer to Cloud

MAIN MENU

Responsibility	PaaS	IaaS
Information and Data	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦
Accounts and Identities	🟦	🟦
Identity and directory infrastructure	◩	🟦
Application	◩	🟦
Network controls	◩	🟦
Operating system	⬜	🟦
Physical hosts	⬜	⬜
Physical network	⬜	⬜
Physical datacenter	⬜	⬜

⬜ Microsoft 🟦 Customer



Transferred for PaaS

Security Patches

Feature Upgrades

VMs/Containers security – OS and Middleware Installation, Maintenance, troubleshooting, etc.

Azure Marketplace fits PaaS or IaaS model

Transferred for IaaS and PaaS

Denial of Service*

Racking/Stacking Servers, Delays in Adding Capacity

Fabric/Virtualization Patching, Maintenance & Troubleshooting

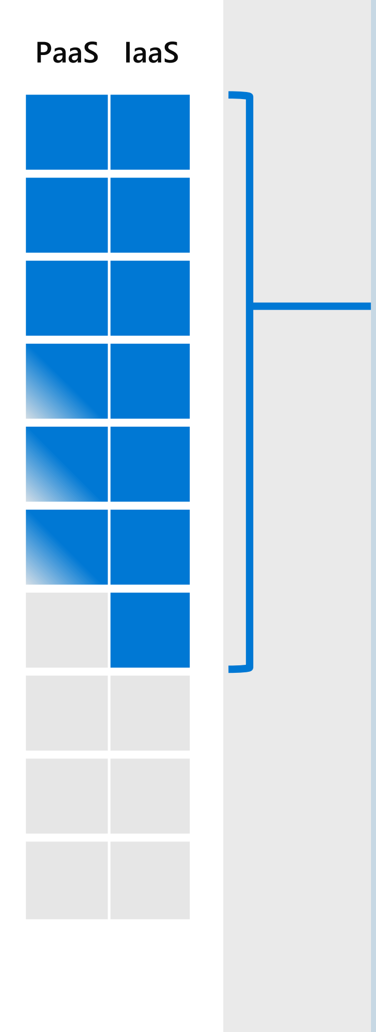
Fabric Availability / Uptime → SLA from Microsoft

Attacks on

- Physical Attacks
- Virtualization Fabric
- Hardware/Firmware
- Network Infrastructure

Azure Threats – Mix of Old & New...

MAIN
MENU

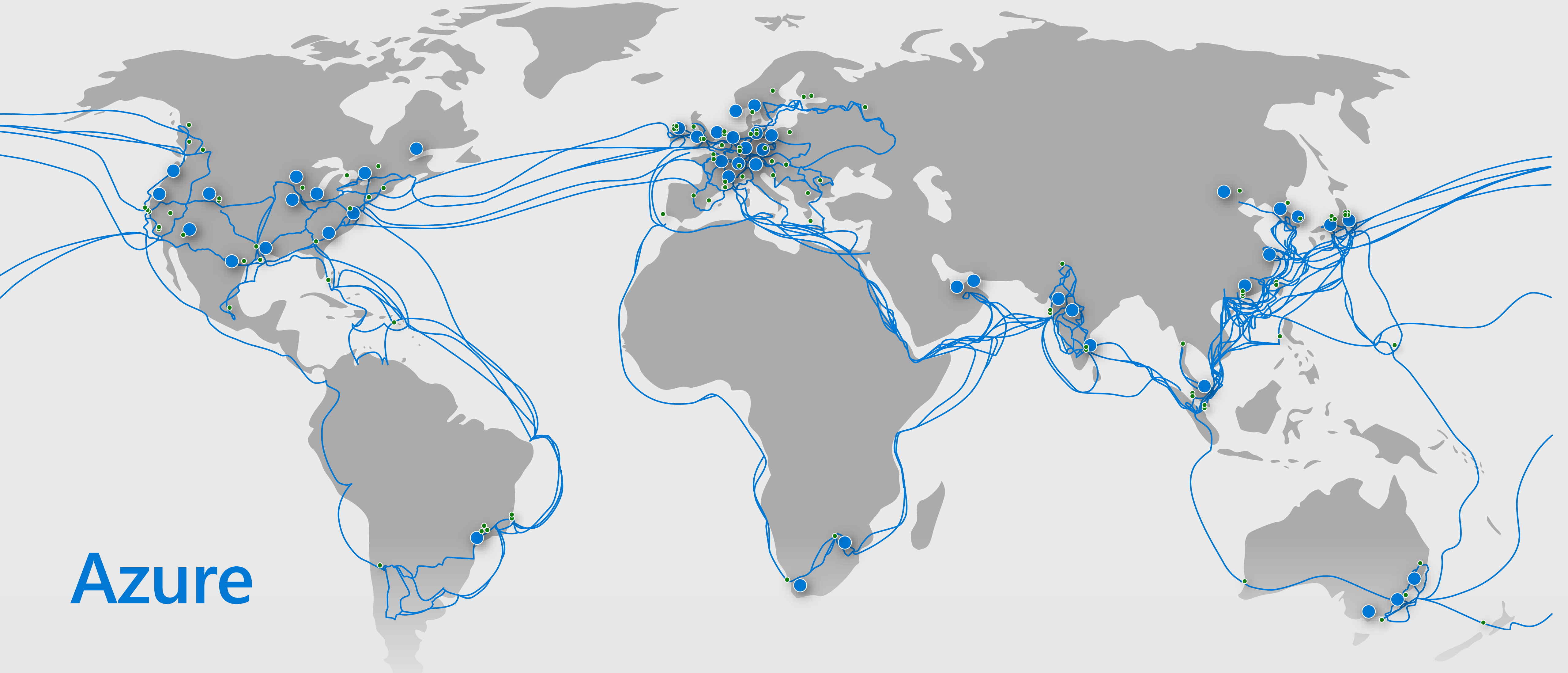


EXISTING TECHNIQUES (AT COMPARABLE LEVELS)

EXPLOIT/ENTER	TRAVERSAL	MONETIZATION
SOCIAL ENGINEERING	CREDENTIAL THEFT & ABUSE (HASHES, SSH...)	RANSOMWARE
PHISHING	SCAN & EXPLOIT	TARGETED DATA THEFT
GEO-FILTERING EVASION WITH PROXY		COMMODITY BOTNET/DDOS/ETC
●●●	●●●	●●●

New Techniques (☆) or Very High Usage (⇧)

☆ ACQUIRE TENANT KEYS FROM GITHUB/ETC	☆ PIVOT TO ON PREMISES FROM CLOUD	⇧ CRYPTOMINERS – (WEBSERVERS, VISITORS)
⇧ RDP/SSH PASSWORD SPRAY & BRUTE FORCE		



Azure

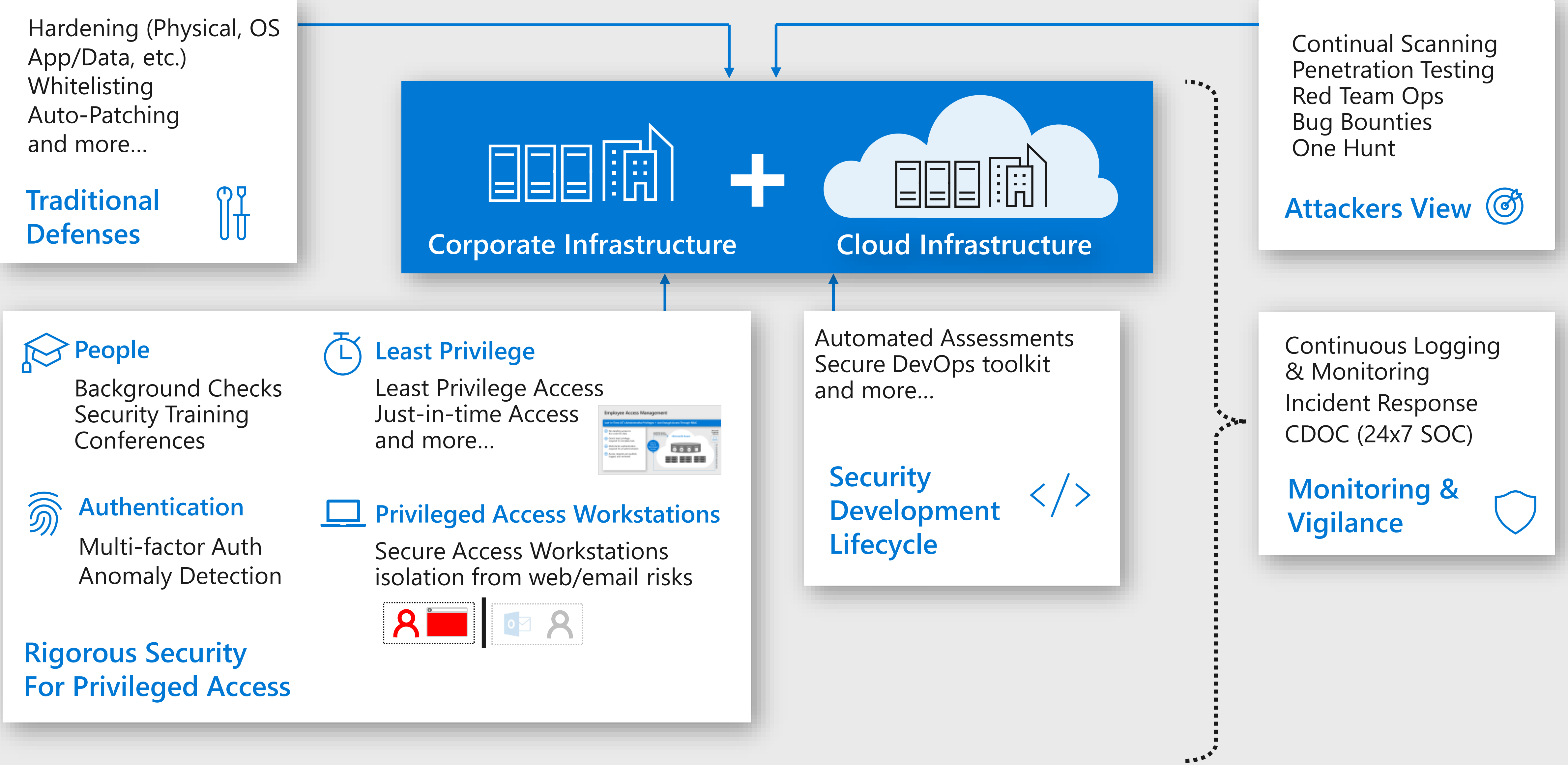
54 Azure regions

100K+ Miles of fiber & subsea cable

150+ Edge sites

200+ ExpressRoute partners

Microsoft protecting Microsoft



Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more…

Traditional Defenses

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt

Attackers View

People

Background Checks
Security Training
Conferences

Least Privilege

Least Privilege Access
Just-in-time Access
and more…

Authentication

Multi-factor Auth
Anomaly Detection

Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

Automated Assessments
Secure DevOps toolkit
and more…

Security Development Lifecycle

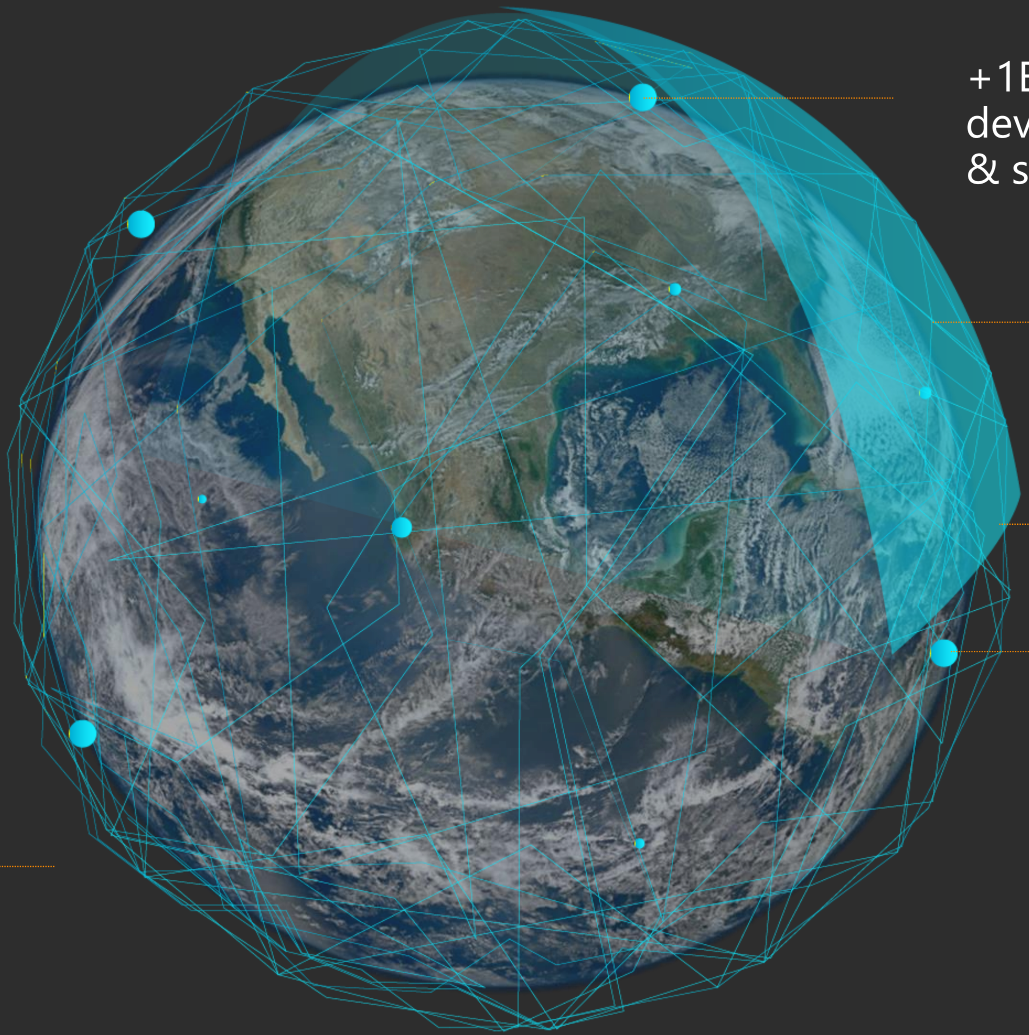
Continuous Logging & Monitoring
Incident Response
CDOC (24x7 SOC)

Monitoring & Vigilance

The Microsoft **Intelligent Security Graph**

Extensive machine learning to:

- Reduce manual effort
- Reduce wasted effort on false positives
- Speed up detection



+1B Windows devices updated & scanned

450B monthly authentications

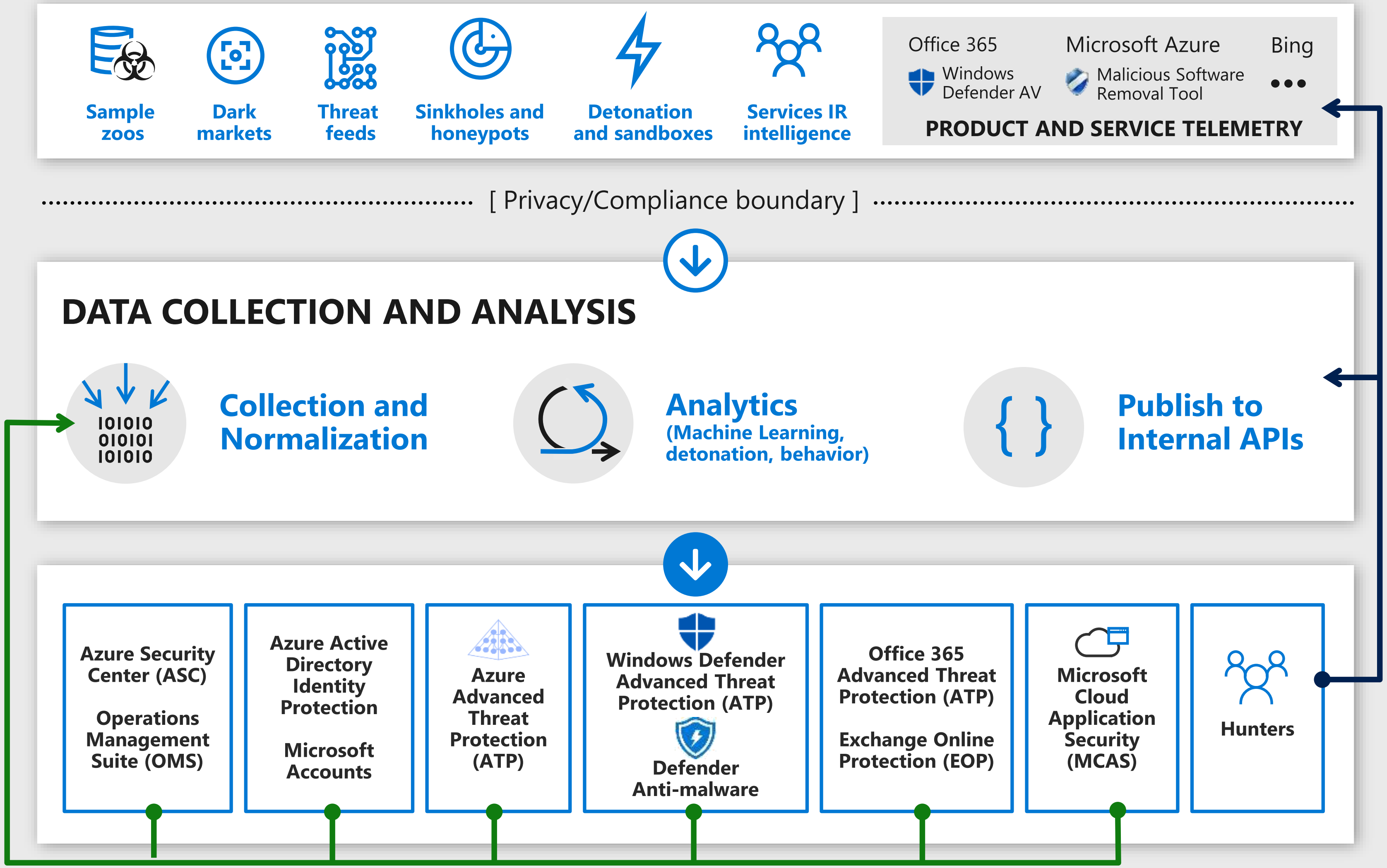
18+ billion web pages scanned

400B e-mails analyzed

930M threats detected on devices every month

Unparalleled cybersecurity visibility and insight

Inside The Intelligent Security Graph



Sample zoos

Dark markets

Threat feeds

Sinkholes and honeypots

Detonation and sandboxes

Services IR intelligence

Office 365

Windows Defender AV

Microsoft Azure

Malicious Software Removal Tool

Bing

•••

PRODUCT AND SERVICE TELEMETRY

[Privacy/Compliance boundary]

DATA COLLECTION AND ANALYSIS

Collection and Normalization

Analytics (Machine Learning, detonation, behavior)

Publish to Internal APIs

Azure Security Center (ASC)
Operations Management Suite (OMS)

Azure Active Directory Identity Protection
Microsoft Accounts

Azure Advanced Threat Protection (ATP)

Windows Defender Advanced Threat Protection (ATP)
Defender Anti-malware

Office 365 Advanced Threat Protection (ATP)
Exchange Online Protection (EOP)

Microsoft Cloud Application Security (MCAS)

Hunters

- Products instrumented to strict privacy/compliance standards

  See Microsoft Trust Center

- Analytics help fuel new discoveries
- Products send data to graph
- Products use Interflow APIs to access results
- Products generate data which feeds back into the graph
- Hunters identify attacks, improve analytics, feed back into product design

Technical Details on Azure internal architecture

Most current information in documentation

https://docs.microsoft.com/en-us/azure/security/azure-security-infrastructure

3rd party validated information in Service Trust Portal (STP) -

https://servicetrust.microsoft.com/ - *Requires NDA*

Most frequently requested information is:

- Azure & Azure Government SOC 2 Type 2 Report (in STP)
- Azure - FedRAMP Moderate System Security Plan (in STP)
- Cloud Security Alliance (CSA) STAR Self-Assessment https://www.microsoft.com/en-us/trustcenter/compliance/csa-self-assessment
- CIS Benchmark - https://azure.microsoft.com/en-us/resources/cis-microsoft-azure-foundations-security-benchmark/

Azure for AWS Professionals

- https://docs.microsoft.com/en-us/azure/architecture/aws-professional

Audit Reports

Resources to help information security and compliance professionals understand cloud features, and to verify technical compliance and control requirements

Azure compliance coverage extends across most industries and geographies

Global

- ☑ CSA STAR Attestation
- ☑ CSA STAR Certification
- ☑ CSA STAR Self-Assessment
- ☑ ISO 22301
- ☑ ISO 27001
- ☑ ISO 27017
- ☑ ISO 27018
- ☑ SOC 1 Type 2
- ☑ SOC 2 Type 2

U.S. Government

- ☑ CJIS
- ☑ DoD DISA SRG Level 2
- ☑ DoD DISA SRG Level 4
- ☑ DoD DISA SRG Level 5
- ☑ FedRAMP
- ☑ FIPS 140-2
- ☑ High JAB P-ATO
- ☑ IRS 1075
- ☑ ITAR
- ☑ Moderate JAB P-ATO
- ☑ Section 508 VPAT
- ☑ SP 800-171

Industry

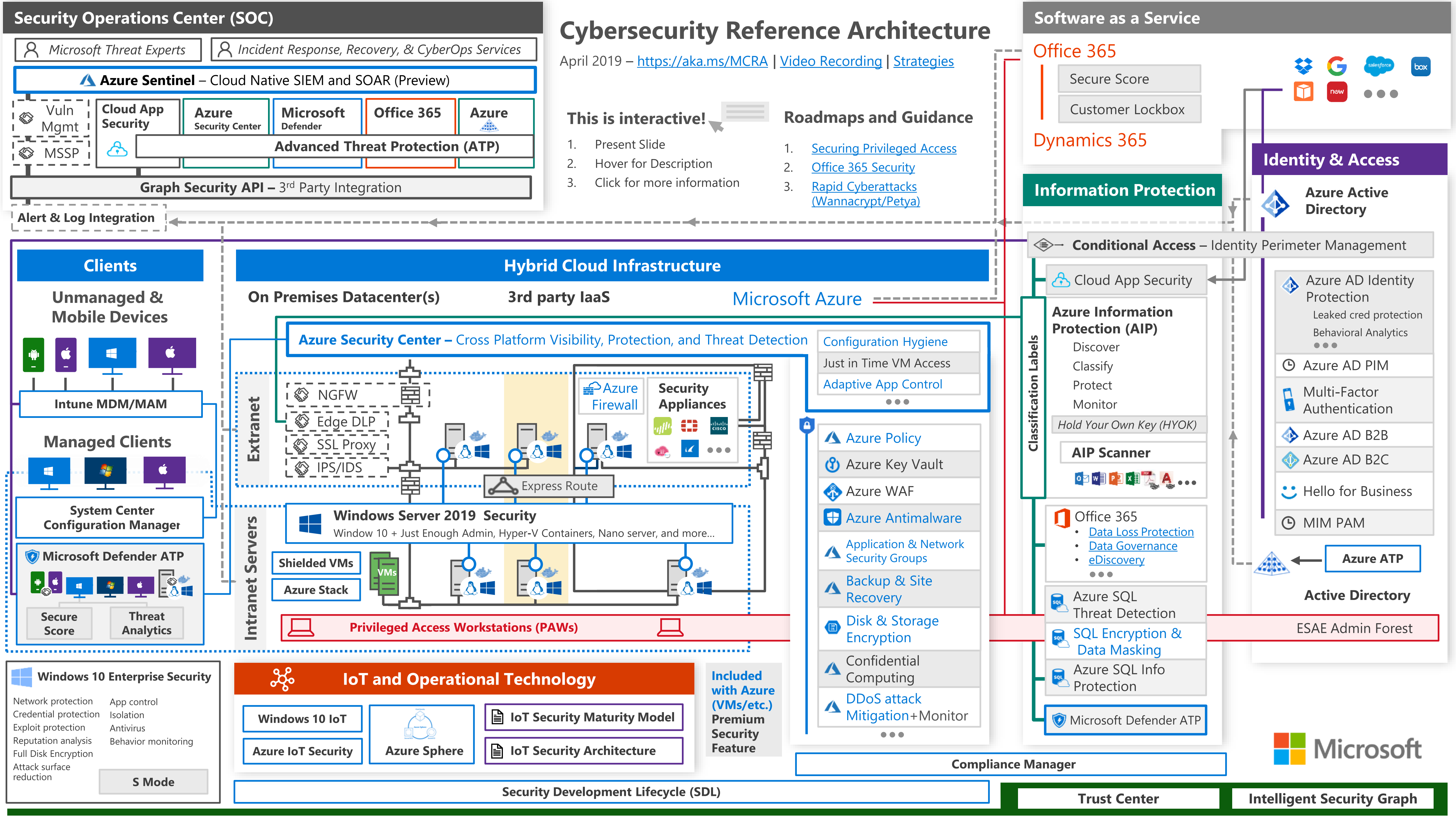
- ☑ CDSA
- ☑ FACT UK
- ☑ FERPA
- ☑ FFIEC
- ☑ FISC Japan
- ☑ GLBA
- ☑ GxP 21 CFR Part 11
- ☑ HIPAA / HITECH
- ☑ HITRUST
- ☑ IG Toolkit UK
- ☑ MARS-E
- ☑ MPAA
- ☑ PCI DSS Level 1
- ☑ Shared Assessments

Regional

- ☑ Argentina PDPA
- ☑ Australia IRAP/CCSL
- ☑ Canada Privacy Laws
- ☑ China DJCP
- ☑ China GB 18030
- ☑ China TRUCS
- ☑ ENISA IAF
- ☑ EU Model Clauses
- ☑ EU-US Privacy Shield
- ☑ Germany IT Grundschutz
- ☑ India MeitY
- ☑ Japan CS Mark Gold
- ☑ Japan My Number Act
- ☑ New Zealand GCIO
- ☑ Singapore MTCS
- ☑ Spain DPA
- ☑ Spain ENS
- ☑ UK G-Cloud

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies



This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

•••

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Cloud App Security

Classification Labels

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

•••

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

•••

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

•••

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

•••

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

•••

Included with Azure (VMs/etc.)

Premium Security Feature

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Compliance Manager

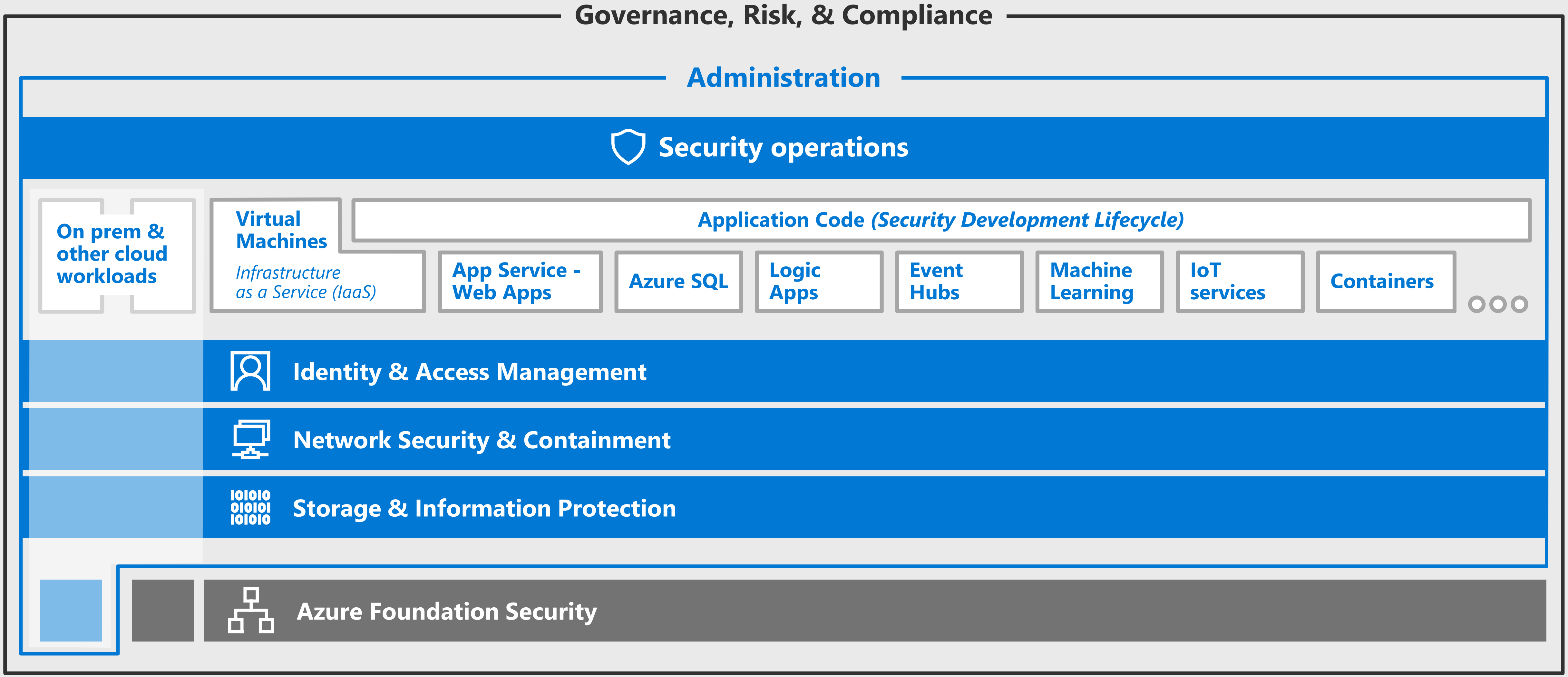
Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft

Azure Security Reference Model



Governance, Risk, & Compliance

Administration

Security operations

On prem & other cloud workloads

Virtual Machines

Infrastructure as a Service (IaaS)

Application Code *(Security Development Lifecycle)*

App Service - Web Apps

Azure SQL

Logic Apps

Event Hubs

Machine Learning

IoT services

Containers

○○○

Identity & Access Management

Network Security & Containment

Storage & Information Protection

Azure Foundation Security

Example - Securing Privileged Access is a team sport

Mitigating some risks requires action across multiple disciplines

Administration

Day to day use of privileged access accounts

Security Operations

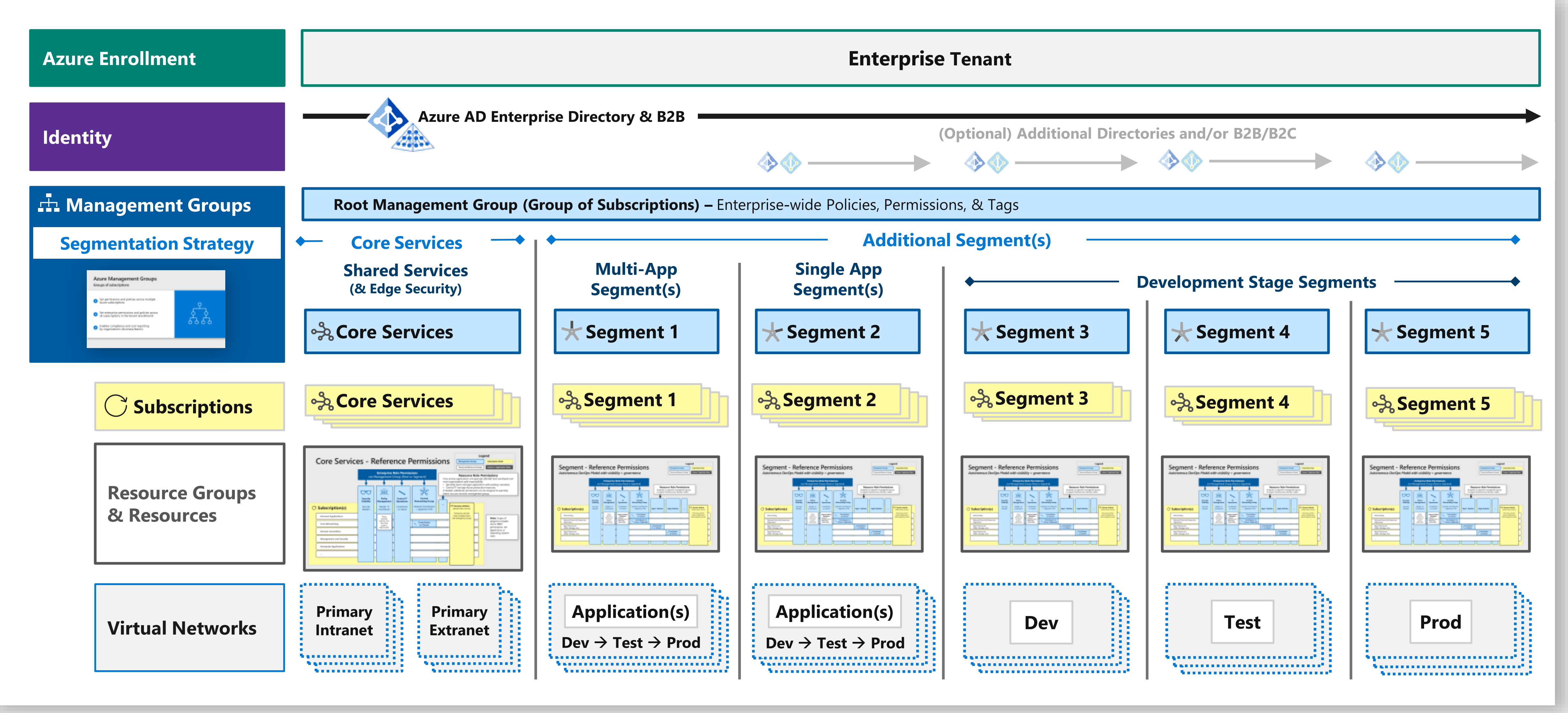
Monitor for anomalies to “normal” admin operations

Governance (& Architecture)

Standard Setting and Structure

Ongoing refinement and improvement to reduce potential risks

Reference Design - Azure Administration Model



Azure Enrollment

Enterprise Tenant

Identity

Azure AD Enterprise Directory & B2B

(Optional) Additional Directories and/or B2B/B2C

Management Groups

Segmentation Strategy

Azure Management Groups

Root Management Group (Group of Subscriptions) – Enterprise-wide Policies, Permissions, & Tags

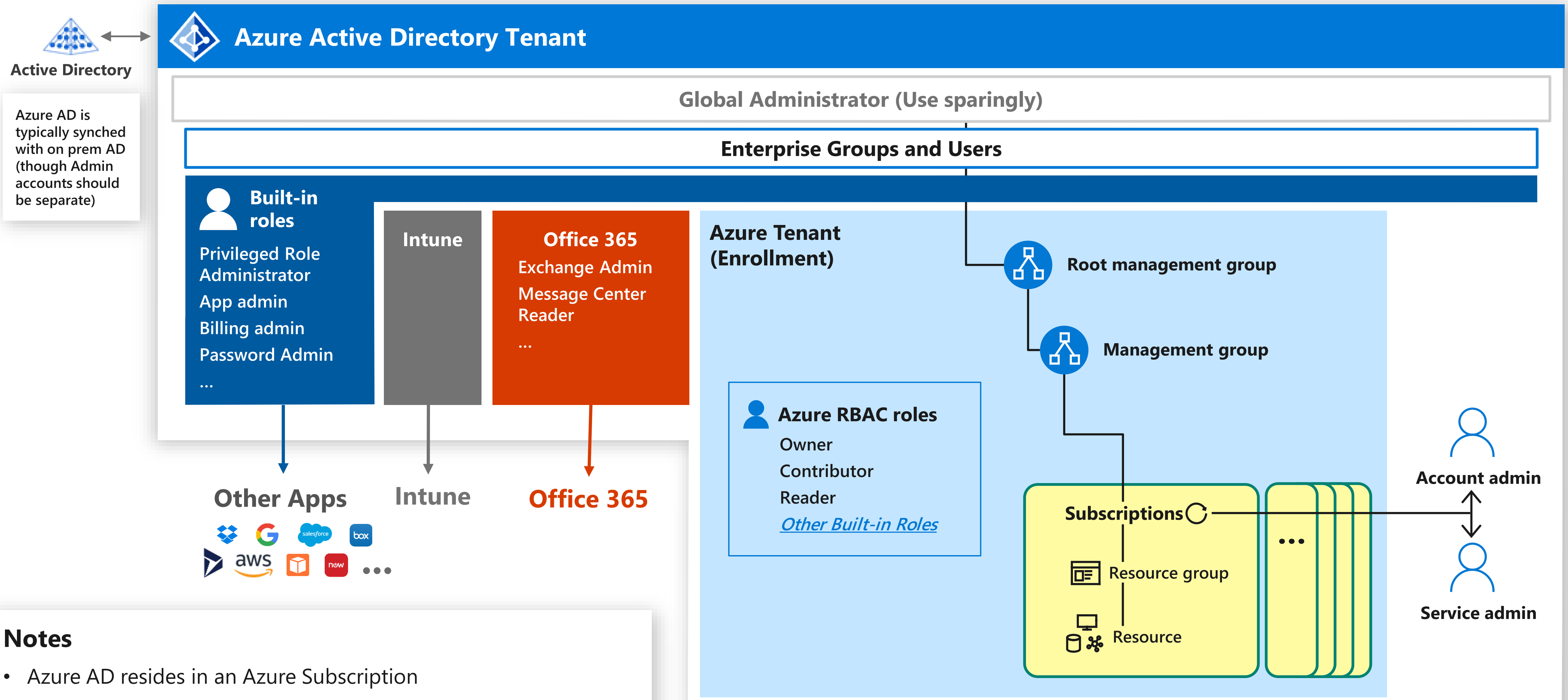
Core Services

Additional Segment(s)

Development Stage Segments

	Core Services	Additional Segment(s)				
	Shared Services (& Edge Security)	Multi-App Segment(s)	Single App Segment(s)	Development Stage Segments		
Management Groups	Core Services	Segment 1	Segment 2	Segment 3	Segment 4	Segment 5
Subscriptions	Core Services	Segment 1	Segment 2	Segment 3	Segment 4	Segment 5
Resource Groups & Resources	Core Services - Reference Permissions	Segment - Reference Permissions	Segment - Reference Permissions	Segment - Reference Permissions	Segment - Reference Permissions	Segment - Reference Permissions
Virtual Networks	Primary Intranet Primary Extranet	Application(s) Dev → Test → Prod	Application(s) Dev → Test → Prod	Dev	Test	Prod

Understanding Azure Roles and RBAC

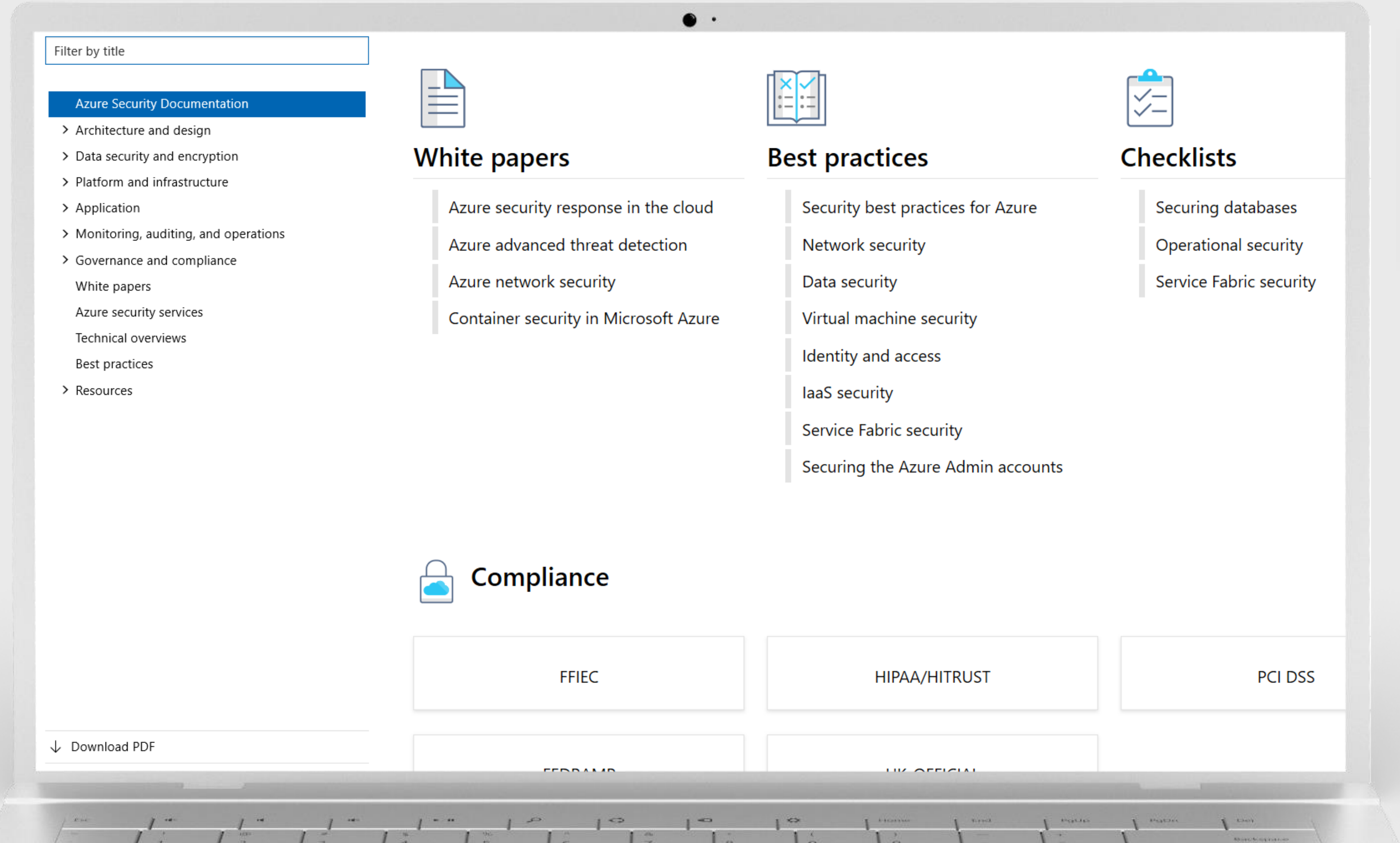


Notes

- Azure AD resides in an Azure Subscription
- Global Admin can self-assign permission to manage Azure
- Service & Account Admins are assigned on each subscription

Azure Security Documentation

https://aka.ms/MyASIS



Filter by title

- Azure Security Documentation
- › Architecture and design
- › Data security and encryption
- › Platform and infrastructure
- › Application
- › Monitoring, auditing, and operations
- › Governance and compliance
- White papers
- Azure security services
- Technical overviews
- Best practices
- › Resources

↓ Download PDF

White papers

- Azure security response in the cloud
- Azure advanced threat detection
- Azure network security
- Container security in Microsoft Azure

Best practices

- Security best practices for Azure
- Network security
- Data security
- Virtual machine security
- Identity and access
- IaaS security
- Service Fabric security
- Securing the Azure Admin accounts

Checklists

- Securing databases
- Operational security
- Service Fabric security

Compliance

FFIEC

HIPAA/HITRUST

PCI DSS

FEDRAMP

UK OFFICIAL

Azure Security Documentation Site has extensive information on security topics

Governance, Risk, & Compliance

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/governance

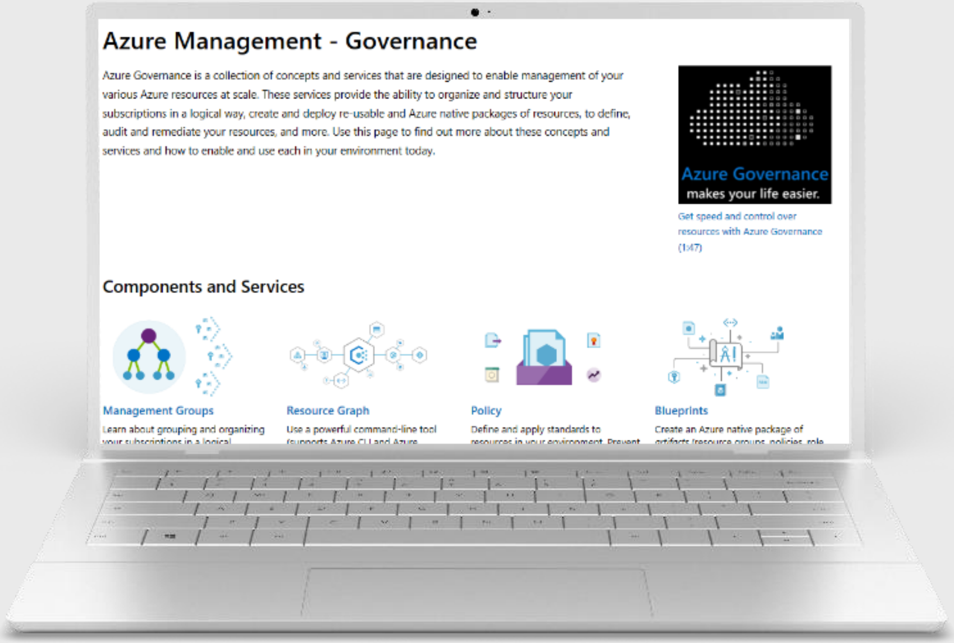
Governance, Risk, and Compliance (GRC)

Key Capabilities

- **Azure Security Center** – Identify & prioritize security hygiene issues (Secure Score), provide recommendations for meeting compliance with CIS, PCI, SOC and ISO
- **Management Groups** – Consistent management across subscriptions and resources.
- **Azure Policy** – Audits and enforce policy across all Azure Resources (or a subset).
- **Azure Blueprints** – Creates consistent, repeatable environments including resources, policies, role assignments, and more.

Azure Governance Site has extensive documentation to help with risk management

https://docs.microsoft.com/en-us/azure/governance/



Azure Management - Governance

Azure Governance is a collection of concepts and services that are designed to enable management of your various Azure resources at scale. These services provide the ability to organize and structure your subscriptions in a logical way, create and deploy re-usable and Azure native packages of resources, to define, audit and remediate your resources, and more. Use this page to find out more about these concepts and services and how to enable and use each in your environment today.

Get speed and control over resources with Azure Governance (1:47)

Components and Services

Management Groups

Learn about grouping and organizing your subscriptions in a logical

Resource Graph

Use a powerful command-line tool (supports Azure CLI and Azure

Policy

Define and apply standards to resources in your environment. Prevent

Blueprints

Create an Azure native package of artifacts (resource groups, policies, role

GRC – Managed Tenants & Subscriptions

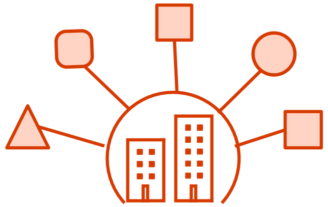
CRITICAL BEST PRACTICES

MANAGE CONNECTED TENANTS

- **What** – Ensure security organization(s) has visibility into all subscriptions connected to your enterprise environment (via ExpressRoute or Site-Site VPN)
- **Why –** Visibility is required to assess risk and to identify whether the policies of the organization and any regulatory requirements are being followed.
- **How** – Ensure all Azure environments that connect to your production environment/network apply governance controls.
  See http://aka.ms/magicbutton
  on how to discover existing connected subscriptions

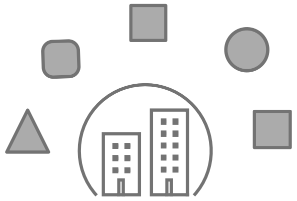
Managed & Connected

Ideal configuration is for subscriptions to be centrally controlled and managed



Unmanaged & Connected

This high-risk configuration has unmanaged Azure environments connected to corporate network/resources



Independent Un/Managed

This "lab" model can be useful for learning and testing, but ensure to appropriately protect any production data or code in it

GRC – Key Responsible Parties

CRITICAL BEST PRACTICES

CLEAR LINES OF RESPONSIBILITY

- **What** – Designate the parties responsible for specific functions in Azure
- **Why** – Consistency helps avoid confusion that can lead to human and automation errors that create security risk.
- **How** – Designate groups (or individual roles) that will be responsible for key centralized functions

Most organizations map these closely to current on premises models.

Tip *Document and Socialize this widely with all teams working on Azure*

Network Security	*Typically existing network security team* Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.
Network Management	*Typically existing network operations team* Enterprise-wide virtual network and subnet allocation
Server Endpoint Security	*Typically IT operations, security, or jointly* Monitor and remediate server security (patching, configuration, endpoint security, etc.)
Incident Monitoring and Response	*Typically security operations team* Investigate and remediate security incidents in SIEM or source console: • Azure Security Center • Azure AD Identity Protection
Policy Management	*Typically GRC team + Architecture* Set direction for use of Roles Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources
Identity Security and Standards	*Typically Security Team + Identity Team Jointly* Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards

GRC – Segmentation

CRITICAL CHOICE

BEST PRACTICE

CHOICE

SEGMENTATION STRATEGY

- **What** – Identify security segments that are needed for your organization to contain risk
- **Why** – A clear and simple segmentation strategy enables stakeholders (IT, Security, Business Units) can understand and support it. This clarity reduces the risk of human errors and automation failures that can lead to security vulnerabilities, operational downtime, or both
- **How** – Select the segmentation approaches from the reference design and assign permissions and network controls as appropriate.

Tip

Minimize Complexity *- Always consider whether a segment is needed or whether security monitoring provides enough risk mitigation*
(each segments adds friction and overhead)

A GOOD SEGMENTATION STRATEGY:

1. **Enables Operations** – Minimizes operation friction by aligning to business practices and applications
2. **Contains Risk** - Adds cost and friction to attackers by
   - Isolating sensitive workloads from compromise of other assets
   - Isolating high exposure systems from being used as a pivot to other systems
3. **Is Monitored** – Security Operations should monitor for potential violations of the integrity of the segments (account usage, unexpected traffic, etc.)

GRC – Management Groups

CRITICAL BEST PRACTICES

Management Groups
Segmentation Strategy
Root Management Group (Group of Subscriptions) – Enterprise-wide Policies, Permissions & Tags
Core Services
Additional Segment(s)
Shared Services (& Edge Security)
App/Region/Org Segment(s)
PaaS Segment(s)
Development Stage Segments
Core Services
Segment 1
Segment 2
Segment 3
Segment 4
Segment 5

Azure Administration Model
Management Groups

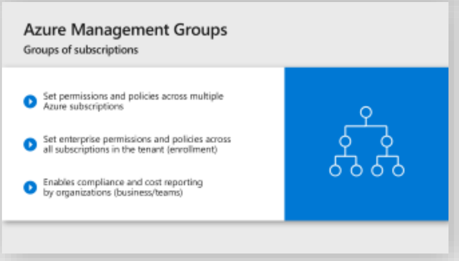
ROOT MANAGEMENT GROUP

- **What** – Use the Root Management Group (MG) for enterprise consistency
- **Why** – This enables you to apply governance elements like policies and tags consistently across multiple subscriptions.
- **How –** Assign enterprise-wide elements that apply to all Azure assets such as:
- Policy (Azure Policy)
- Resource Tags
- Sovereignty Policy for Data/Services

See next slide for "Root MG Usage" guidance and MG documentation

TOP LEVEL MANAGEMENT GROUPS

- **What** –Align top level of management groups (MGs) with segmentation strategy
- **Why** – This provides a point for control and policy consistency within each segment as this management group will affect all subscriptions in it
- **How** – Create a single MG for each segment under the root MG and do not create any other MGs under the root. See reference administration model for more details.



Azure Management Groups

Groups of subscriptions

- Set permissions and policies across multiple Azure subscriptions
- Set enterprise permissions and policies across all subscriptions in the tenant (enrollment)
- Enables compliance and cost reporting by organizations (business/teams)

MANAGEMENT GROUP DEPTH

- **What** – Limit management group depth
- **Why** – Too much complexity creates confusion that impedes both operations and security. This was illustrated by overly complex Organizational Unit (OU) and Group Policy Objects (GPO) designs for Active Directory
- **How** – Limit to 2 levels if possible and 3 only if needed. (e.g. finance department has a segment with both extremely sensitive applications and others that aren't)

Using all 4 levels of depth (including root) is not recommended unless absolutely required.

GRC – Root MG Usage

CRITICAL BEST PRACTICES

BEST PRACTICE   CHOICE

USE OF ROOT MANAGEMENT GROUP (MG)

- **What –** Carefully select what items to apply to the entire enterprise with the root management group.
- **How –** Ensure root MG elements have a clear requirement to be applied across every resource and/or low impact

Good candidates include

- **Regulatory requirements** with clear business risk/impact (e.g. restrictions related to data sovereignty)
- **Near-zero potential negative impact** on operations such as policy with audit effect, Tag assignment, RBAC permissions assignments that have been carefully reviewed.

PLAN & TEST ROOT MG CHANGES

- **What –** Carefully plan and test all enterprise-wide changes on the root management group before applying
- **How –** Test all changes to Root MG in a:
  - **Test Lab** - Representative lab tenant or lab segment in production tenant
  - **Production Pilot -** Segment MG or Designated subset in subscription(s) / MG

Testing should include manual changes, scripted changes, and implementation of Azure Blueprints

- **Why –** Changes in the root management group can affect *every resource on Azure*. While this is a powerful way to ensure consistency across the enterprise, errors or incorrect usage can negatively impact production operations.

GRC – Top Risk

CRITICAL GUIDANCE

BEST PRACTICE   CHOICE

UNPATCHED VM + DIRECT INTERNET = COMMON INCIDENT

VIRTUAL MACHINE (VM) SECURITY UPDATES

- **What** – Rapidly apply security updates to virtual machines
- **How** – Enable Azure Security Center to identify missing security updates

  https://docs.microsoft.com/en-us/azure/security-center/security-center-apply-system-updates

  Apply updates using enterprise patch management or Azure Update Management

VM DIRECT INTERNET CONNECTIVITY

- **What** – Monitor and restrict direct internet connectivity
- **How** – Use one or more of the following methods
  - **Enterprise-wide prevention** - Prevent inadvertent exposure via network routing/security + RBAC Permissions (in this guidance)
  - **Identify and Remediate** exposed VMs with Azure Security Center
  - **Restrict management ports** (RDP, SSH) using Just in Time access

Why – Attackers constantly scan public cloud IP ranges for open management ports and attempt “easy” attacks that exploit common passwords and unpatched vulnerabilities

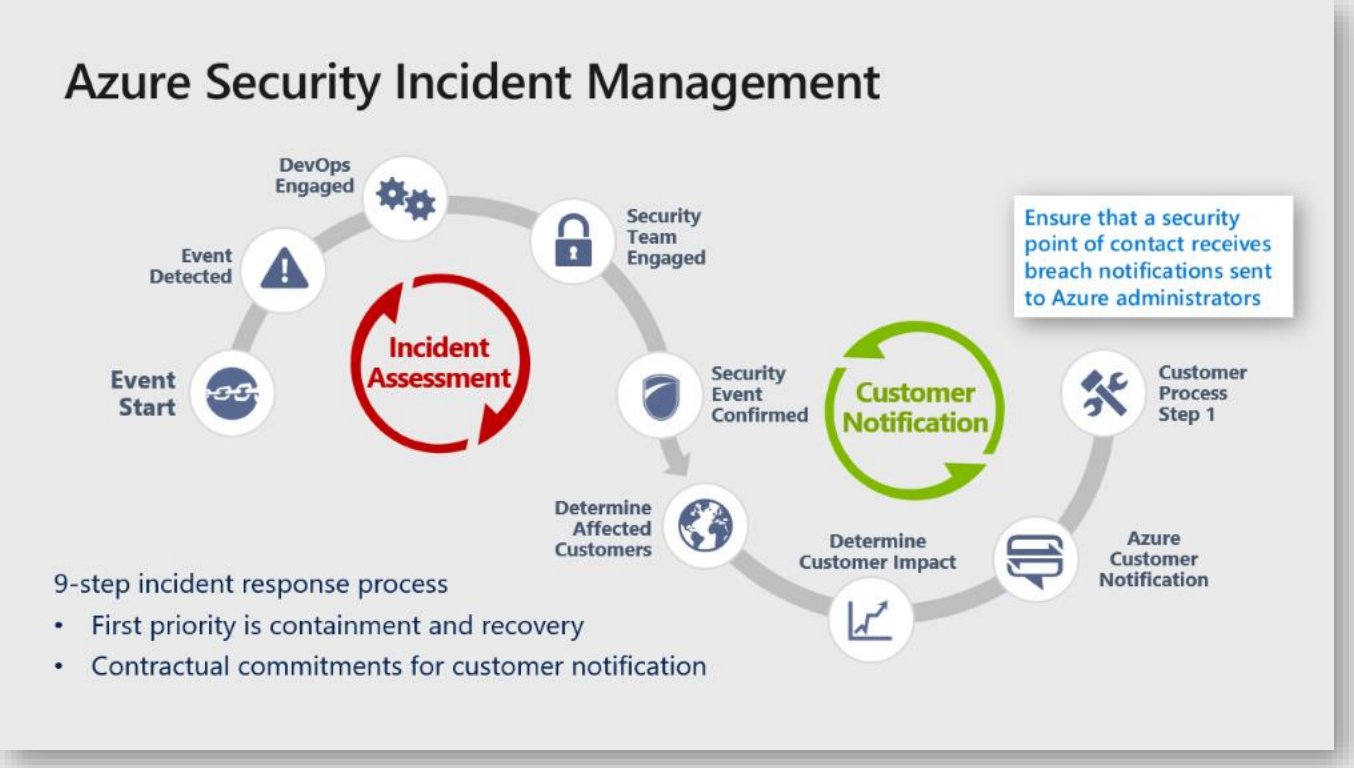
GRC – Security Incident Notification

CRITICAL GUIDANCE

BEST PRACTICE CHOICE

INCIDENT NOTIFICATION

- **What** – Ensure a security contact receives Azure incident notifications from Microsoft (typically a notification that your resource is compromised and/or attacking another customer)
- **Why** – Enables security operations to rapidly respond to potential security risks and remediate them.
- **How** – Ensure administrator contact information in the Azure enrollment portal includes contact information that will notify security operations (directly or rapidly via an internal process)



Azure Security Incident Management

Ensure that a security point of contact receives breach notifications sent to Azure administrators

9-step incident response process

- First priority is containment and recovery
- Contractual commitments for customer notification

See online service terms “Security Incident Notification” section for specific contractual commitments

GRC – Access Reviews

CRITICAL GUIDANCE

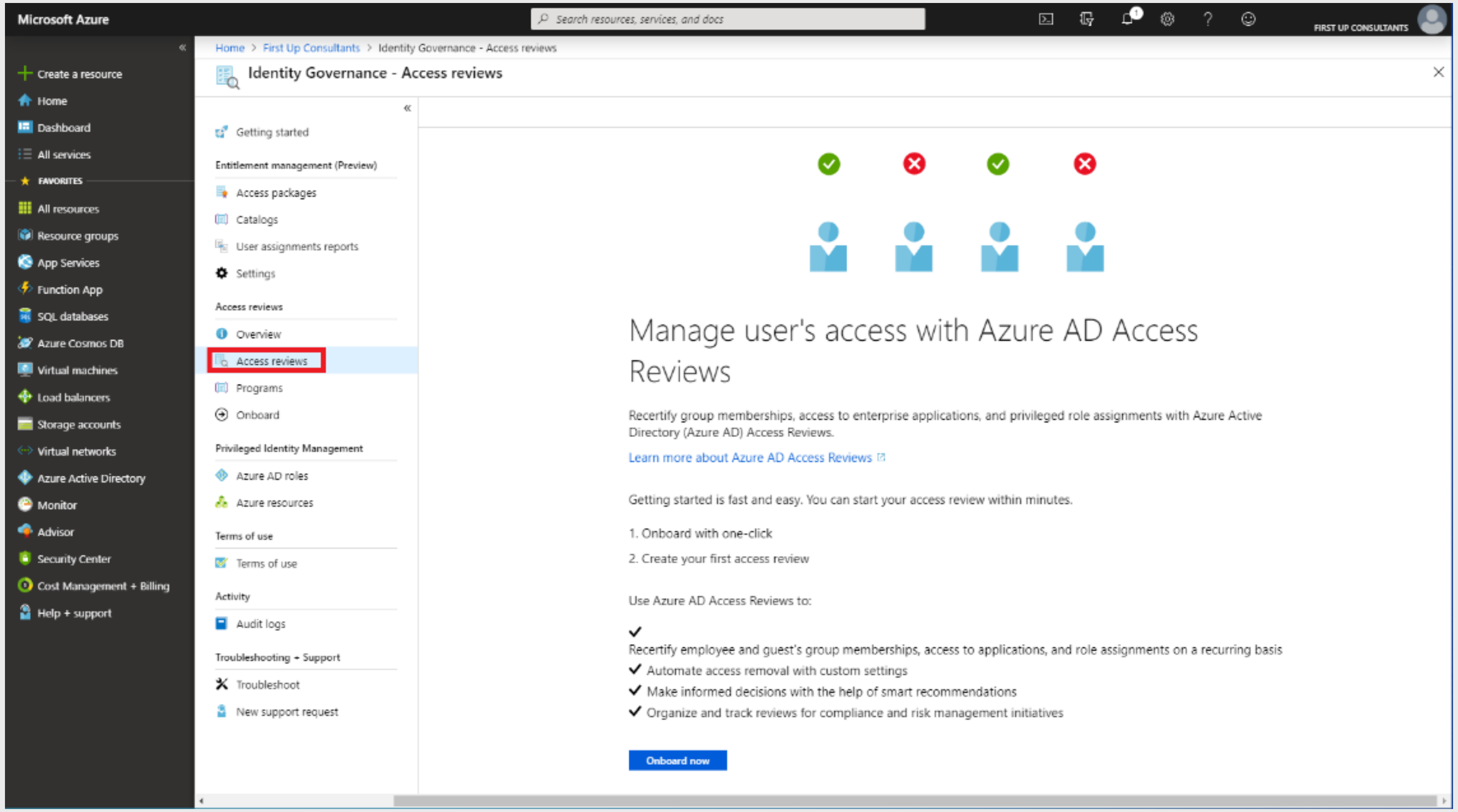
BEST PRACTICE CHOICE

REGULARLY REVIEW CRITICAL ACCESS

- **What** – Regularly review privileges with a business-critical impact
- **Why** – Access requirements change over time but technical privileges typically only grow (accruing significant risk).
- **How** – Set up a recurring review pattern
  - **Manual Process**
  - **Automated -** Using Azure AD access reviews for all groups with critical business impact

    https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

See administration section for guidance on identifying roles with a critical business impact



Manage user's access with Azure AD Access Reviews

Recertify group memberships, access to enterprise applications, and privileged role assignments with Azure Active Directory (Azure AD) Access Reviews.

Learn more about Azure AD Access Reviews

Getting started is fast and easy. You can start your access review within minutes.

1. Onboard with one-click
2. Create your first access review

Use Azure AD Access Reviews to:

✓
Recertify employee and guest's group memberships, access to applications, and role assignments on a recurring basis
✓ Automate access removal with custom settings
✓ Make informed decisions with the help of smart recommendations
✓ Organize and track reviews for compliance and risk management initiatives

GRC – Security Posture Improvement

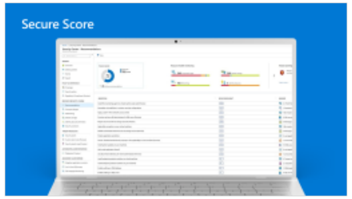
CRITICAL GUIDANCE

BEST PRACTICE CHOICE

MONITOR AZURE SECURE SCORE

- **What** – Use Secure Score in Azure Security Center to identify key recommendations and monitor progress
- **How** – Review your Azure secure score to see the recommendations resulting from the Azure policies and initiatives built into Azure Security center. These include top risks such as security updates, endpoint protection, encryption, security configurations, missing WAF, internet connected VMs, and many more.

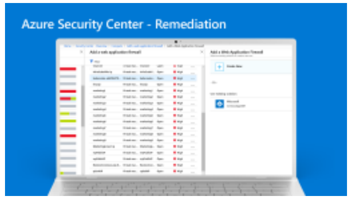
https://docs.microsoft.com/en-us/azure/security-center/security-center-secure-score



REMEDIATE IDENTIFIED RISKS

- **What** – Monitor the security posture of machines, networks, storage and data services, and applications to discover potential security issues.
- **How** – Follow the security recommendations in Azure Security Center starting with the highest priority items. The remediations can frequently be initiated from within the console.

https://docs.microsoft.com/en-us/azure/security-center/security-center-recommendations



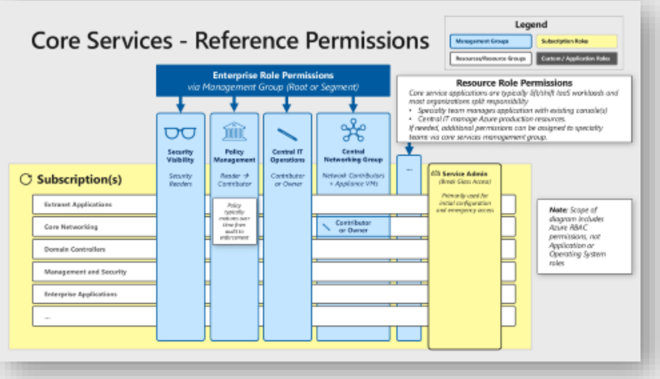
Why – Rapidly identifying and remediating common security hygiene risks can significantly reduce overall risk

Governance – Access for Security Personnel

CRITICAL BEST PRACTICES

SECURITY TEAM VISIBILITY

- **What** – Provide security teams security visibility to all Azure resources
- **Why** – Security requires visibility in order to assess and report on risk
- **How** – Assign security teams *with Azure responsibilities* to the **Security Readers** role using either:
  - **Root management group (MG) –** for teams responsible for all Azure resources
  - **Segment MG –** for teams with limited scope (commonly because of regulatory or other organizational boundaries)



Core Services - Reference Permissions

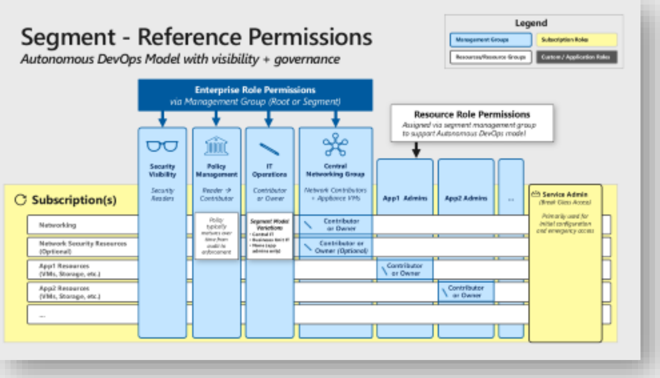
Resource Role Permissions

Core service applications are typically IaaS/PaaS workloads and most organizations split responsibility

- *Specialty team manages application with existing console(s)*
- *Central IT manage Azure production resources.*

If needed, additional permissions can be assigned to specialty teams via core services management group.

Note: *Scope of diagram includes Azure RBAC permissions, not Application or Operating System roles*



Segment - Reference Permissions

Autonomous DevOps Model with visibility + governance

Resource Role Permissions

Assigned via segment management group to support Autonomous DevOps model

Legend
Management Groups
Subscription Roles
Resources/Resource Groups
Custom / Application Roles
Enterprise Role Permissions
via Management Group (Root or Segment)
Security Visibility
Security Readers
Policy Management
Reader → Contributor
Policy typically matures over time from audit to enforcement
IT Operations
Contributor or Owner
Segment Model Variations
• Central IT
• Business Unit IT
• None (app admins only)
Central Networking Group
Network Contributors + Appliance VMs
Contributor or Owner
Contributor or Owner (Optional)
App1 Admins
Contributor or Owner
App2 Admins
Contributor or Owner
...
Service Admin
(Break Glass Access)
Primarily used for initial configuration and emergency access
Subscription(s)
Networking
Network Security Resources (Optional)
App1 Resources (VMs, Storage, etc.)
App2 Resources (VMs, Storage, etc.)
...

AZURE SECURITY CENTER ACCESS

- **What** – Provide access to Azure Security Center (ASC) for teams using this tool to remediate risk in Azure
- **Why** – Azure Security Center allows teams to quickly identify and remediate security risks
- **How** – Assign teams requiring access to ASC to the **security admins** role
  - **Set/enforce policies**
  - **Take actions** to remediate recommendations
- This can be assigned at the the root management group or segment management group(s) depending on the scope of responsibilities.

GRC – Insecure Legacy Protocols

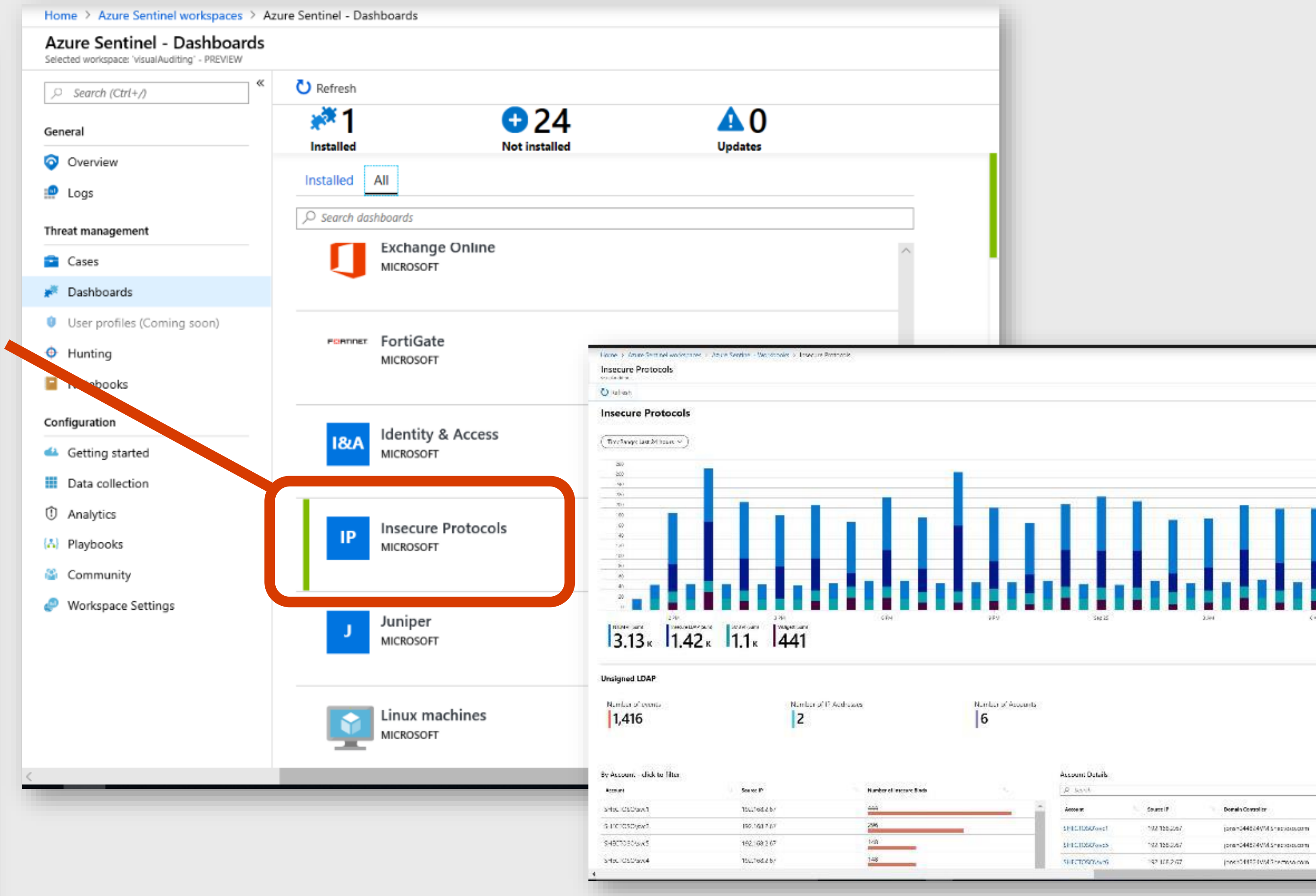
BEST PRACTICE

BEST PRACTICE CHOICE

DISABLE INSECURE PROTOCOLS

- **What** – Discover and disable the use of SMBv1, LM/NTLMv1, wDigest, Unsigned LDAP Binds, and Weak ciphers in Kerberos.
- **Why** – Authentication protocols are critical to nearly all security assurances. Attackers with access to your network can exploit weaknesses in older versions of these protocols.
- **How** –
  - **Discover** usage by reviewing logs with Azure Sentinel Insecure Protocol Dashboard or 3rd party tools
  - **Restrict or Disable** use of these protocols (recommend pilot/testing).

  Guidance for SMB, NTLM, WDigest

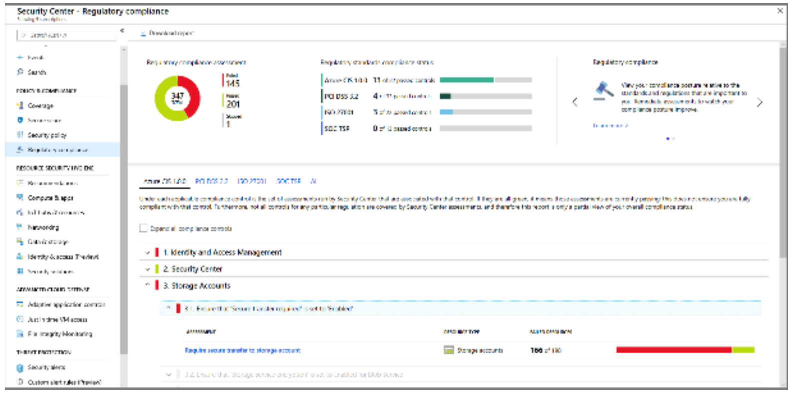


GRC – Compliance

GUIDANCE

REGULATORY COMPLIANCE

- **What** – Use Azure Security Center to report on compliance with regulatory standards


Security Center - Regulatory compliance
Download report
Search
Coverage
Security policy
Regulatory compliance
Compute & apps
Networking
Identity & access (Preview)
Adaptive application controls
Just in time VM access
File integrity Monitoring
Security alerts
Custom alert rules (Preview)
Regulatory compliance assessment
347
Failed
145
Passed
201
Skipped
1
Regulatory standards compliance status
Azure CIS 1.0.0
PCI DSS 3.2
ISO 27001
SOC TSP
Regulatory compliance
1. Identity and Access Management
2. Security Center
3. Storage Accounts
Require secure transfer to storage account
Storage accounts
186 of 190

- **How** – https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard

AZURE BLUEPRINTS

- **What** – Use Azure Blueprints to rapidly and consistently deploy compliant workloads
- **How** – [Azure Blueprint Service](#)automates deployment of environments including RBAC roles, policies, resources (VM/Net/Storage/etc.), and more. Several [Security and Compliance Blueprints](#) templates are available

Why – These capabilities help you stay compliant with regulatory standards

GRC – Benchmarks

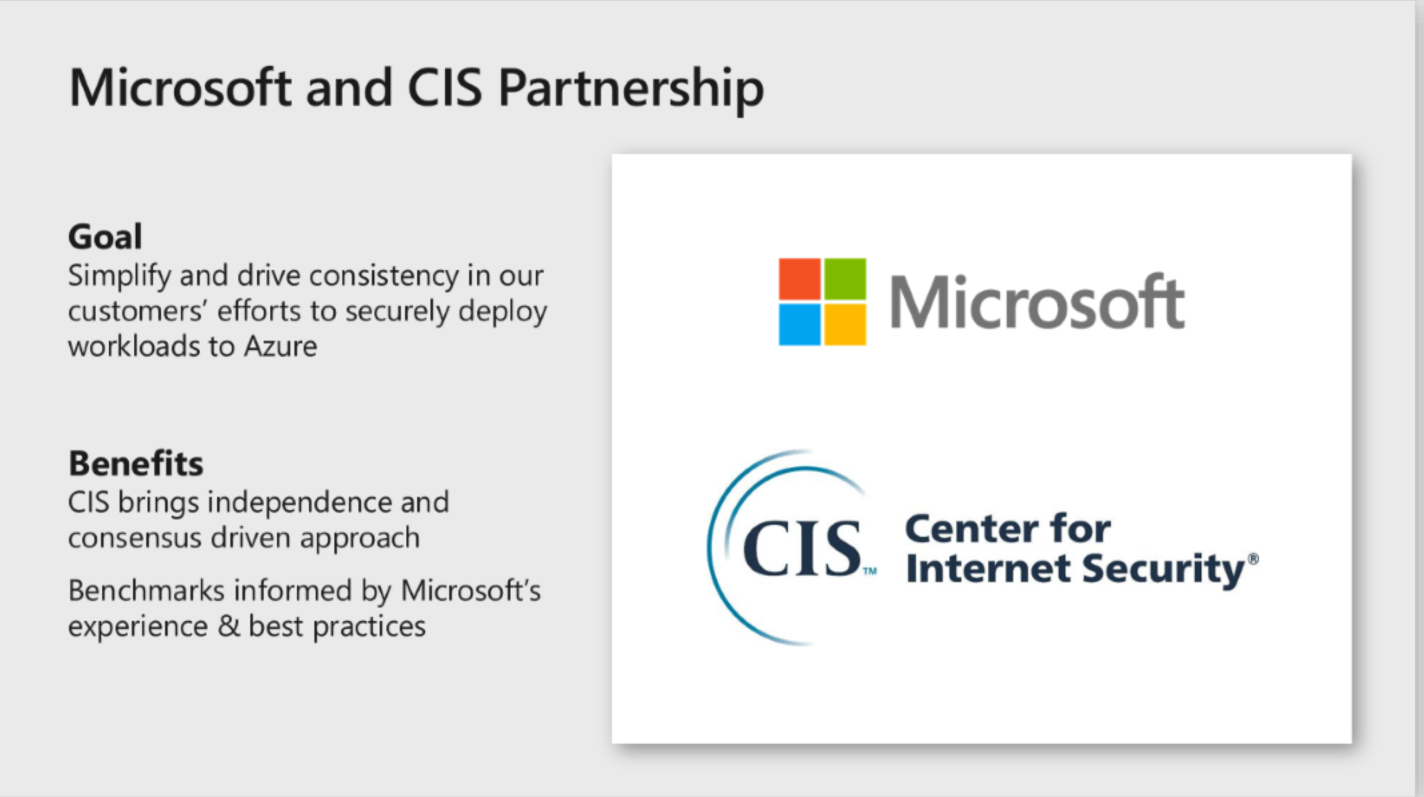
GUIDANCE

EVALUATE USING BENCHMARKS

- **What –** Benchmark your organization's Azure security against external sources
- **Why** – External comparisons help validate and enrich your team's security strategy.
- **How** – Compare your configuration to guidance like Center for Internet Security (CIS) Benchmarks

Benchmark - https://www.cisecurity.org/benchmark/azure/

ASC Compliance Check https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard



Microsoft and CIS Partnership

Goal
Simplify and drive consistency in our customers' efforts to securely deploy workloads to Azure

Benefits
CIS brings independence and consensus driven approach

Benchmarks informed by Microsoft's experience & best practices

Microsoft
CIS Center for Internet Security®

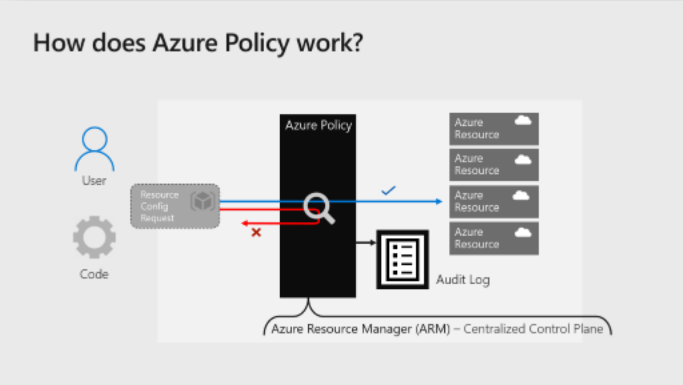
GRC – Azure Policy

GENERAL BEST PRACTICE

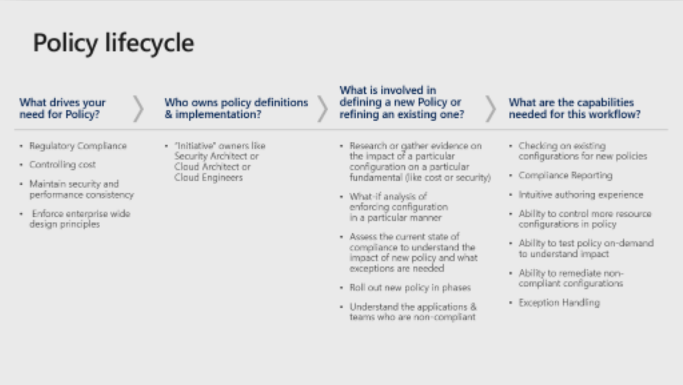
IMPLEMENT AZURE POLICY

- **What –** Use Azure policy to monitor and enforce your organization's security policy
- **Why** – Ensure compliance with your security strategy and/or regulatory security requirements across your Azure workloads.
- **How** – Follow the instructions in the Azure Policy documentation to plan and create policies

  https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage



How does Azure Policy work?



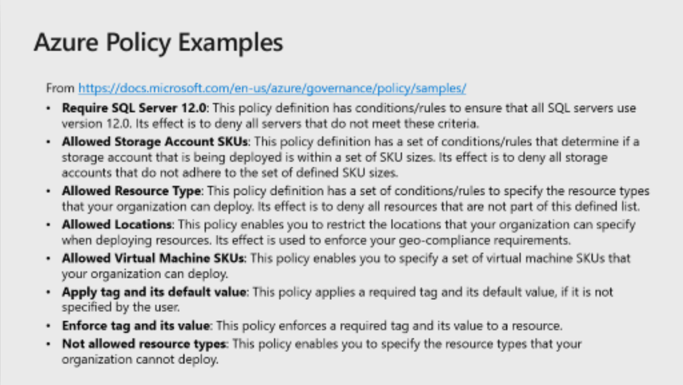
Policy lifecycle

What drives your need for Policy?
- Regulatory Compliance
- Controlling cost
- Maintain security and performance consistency
- Enforce enterprise wide design principles

Who owns policy definitions & implementation?
- "Initiative" owners like Security Architect or Cloud Architect or Cloud Engineers

What is involved in defining a new Policy or refining an existing one?
- Research or gather evidence on the impact of a particular configuration on a particular fundamental (like cost or security)
- What-if analysis of enforcing configuration in a particular manner
- Assess the current state of compliance to understand the impact of new policy and what exceptions are needed
- Roll out new policy in phases
- Understand the applications & teams who are non-compliant

What are the capabilities needed for this workflow?
- Checking on existing configurations for new policies
- Compliance Reporting
- Intuitive authoring experience
- Ability to control more resource configurations in policy
- Ability to test policy on-demand to understand impact
- Ability to remediate non-compliant configurations
- Exception Handling



Azure Policy Examples

From https://docs.microsoft.com/en-us/azure/governance/policy/samples/

- **Require SQL Server 12.0**: This policy definition has conditions/rules to ensure that all SQL servers use version 12.0. Its effect is to deny all servers that do not meet these criteria.
- **Allowed Storage Account SKUs**: This policy definition has a set of conditions/rules that determine if a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
- **Allowed Resource Type**: This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of this defined list.
- **Allowed Locations**: This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geo-compliance requirements.
- **Allowed Virtual Machine SKUs**: This policy enables you to specify a set of virtual machine SKUs that your organization can deploy.
- **Apply tag and its default value**: This policy applies a required tag and its default value, if it is not specified by the user.
- **Enforce tag and its value**: This policy enforces a required tag and its value to a resource.
- **Not allowed resource types**: This policy enables you to specify the resource types that your organization cannot deploy.

GRC – Elevated Security Capabilities

GENERAL GUIDANCE

▲ BEST PRACTICE ● CHOICE

Azure Customer Lockbox
Determine whether your personnel are required to review and approve or reject access requests from Microsoft support engineers where your data must be accessed to resolve a support issue.
https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

A small number of regulatory bodies explicitly require specialized security measures.
While broadly available, these capabilities often increase overhead and cost.

Dedicated Hardware Security Modules (HSMs)
Identify whether you need to utilize dedicated Hardware Security Modules (HSMs) to meet regulatory or security requirements
https://docs.microsoft.com/en-us/azure/dedicated-hsm/

Confidential Computing
Identify whether you need to utilize Confidential Computing to meet regulatory or security requirements
https://azure.microsoft.com/en-us/blog/azure-confidential-computing/

GRC

GENERAL GUIDANCE

▲ BEST PRACTICE ● CHOICE

▲ **Monitor Azure AD Risk Reports**

Monitor your Azure AD Risk Reports for

- Risky sign-in
- Risky users

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events

▲ **Penetration Testing**

Use Penetration Testing or Red Team activities to validate security defenses

https://technet.microsoft.com/en-us/mt784683

Security Operations

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/security-operations

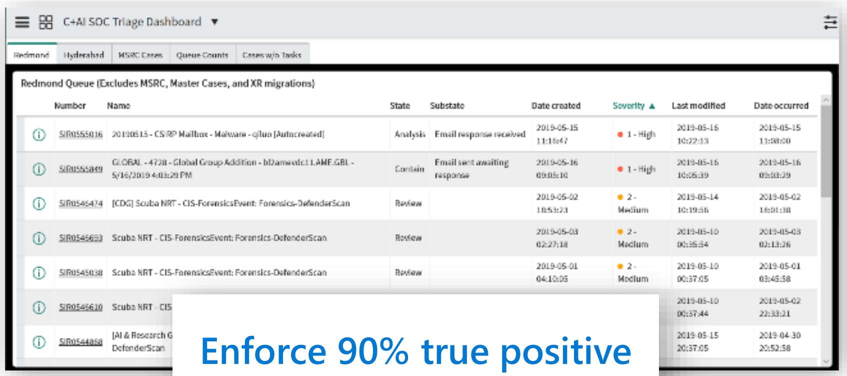
Microsoft’s approach (from our SOC)

Enforce Quality + Apply Technology

Detect

Respond

Billions of events per month



C+AI SOC Triage Dashboard ▼

Redmond Queue (Excludes MSRC, Master Cases, and XR migrations)

Number	Name	State	Substate	Date created	Severity ▲	Last modified	Date occurred
SIR0555016	20190515 - CSIRP Mailbox - Malware - qjluo [Autocreated]	Analysis	Email response received	2019-05-15 11:16:47	● 1 - High	2019-05-16 10:22:13	2019-05-15 11:08:00
SIR0555849	GLOBAL - 4728 - Global Group Addition - bl2amevdc11.AME.GBL - 5/16/2019 4:03:29 PM	Contain	Email sent awaiting response	2019-05-16 09:05:10	● 1 - High	2019-05-16 10:06:39	2019-05-16 09:03:29
SIR0546474	[CDG] Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan	Review		2019-05-02 18:53:23	● 2 - Medium	2019-05-14 10:19:56	2019-05-02 18:01:38
SIR0546693	Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan	Review		2019-05-03 02:27:18	● 2 - Medium	2019-05-10 00:35:54	2019-05-03 02:13:26
SIR0545038	Scuba NRT - CIS-ForensicsEvent: Forensics-DefenderScan	Review		2019-05-01 04:10:05	● 2 - Medium	2019-05-10 00:37:05	2019-05-01 03:45:58
SIR0546610	Scuba NRT - CIS					2019-05-10 00:37:44	2019-05-02 22:33:21
SIR0544868	[AI & Research G DefenderScan					2019-05-15 20:37:05	2019-04-30 20:52:58

Enforce 90% true positive on alert feeds

Machine Learning
(Artificial Intelligence)

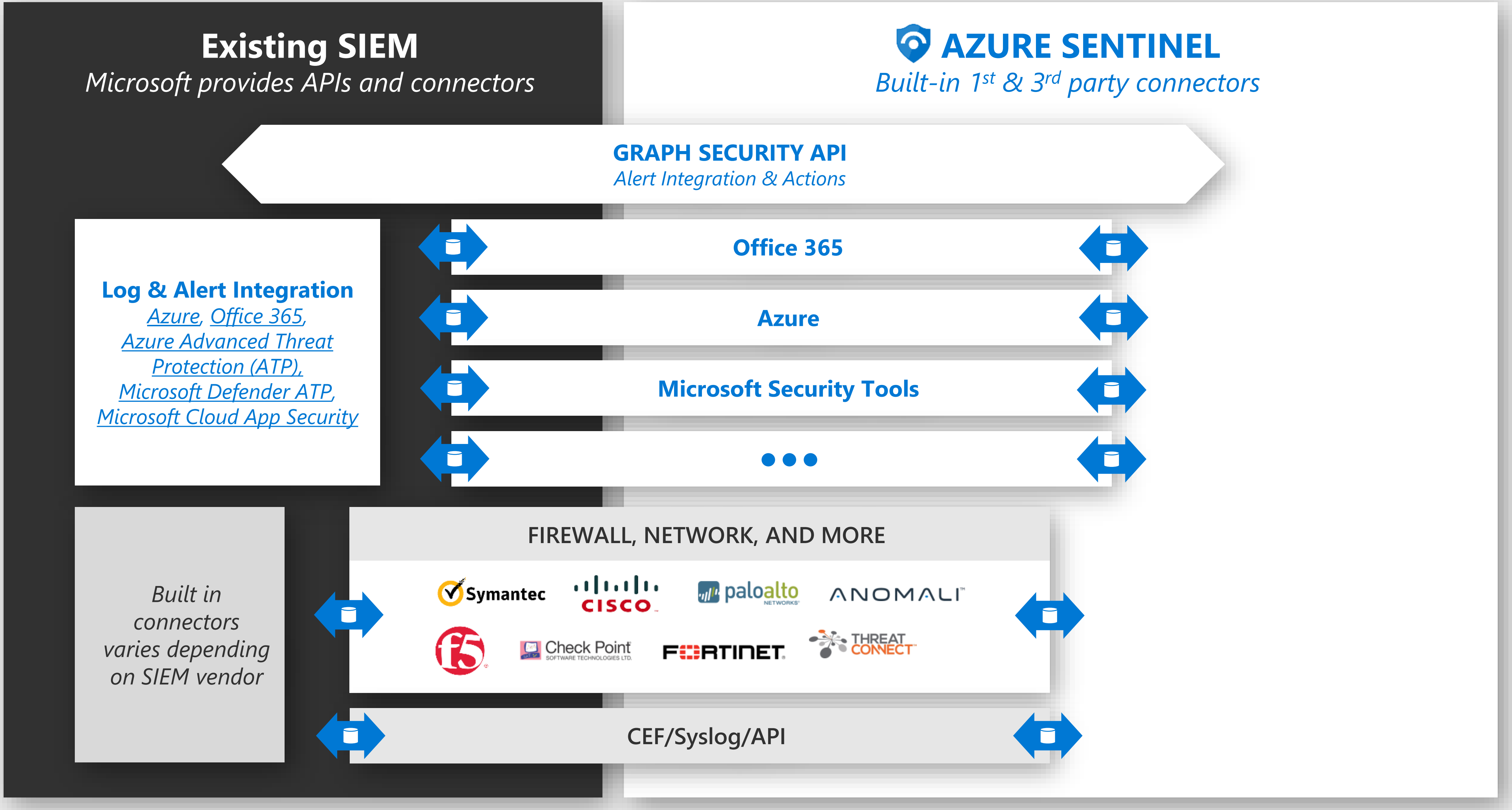
Behavioral Analytics (UEBA)
(User and Entity)

Focus on time to acknowledge and remediate

Security Orchestration, Automation, and Remediation (SOAR)

Hundreds of investigations

SIEM Integration



Existing SIEM

Microsoft provides APIs and connectors

AZURE SENTINEL

Built-in 1st & 3rd party connectors

GRAPH SECURITY API

Alert Integration & Actions

Log & Alert Integration

Azure, Office 365, Azure Advanced Threat Protection (ATP), Microsoft Defender ATP, Microsoft Cloud App Security

Office 365

Azure

Microsoft Security Tools

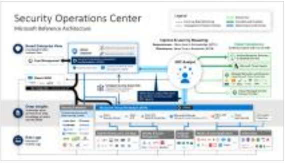
● ● ●

Built in connectors varies depending on SIEM vendor

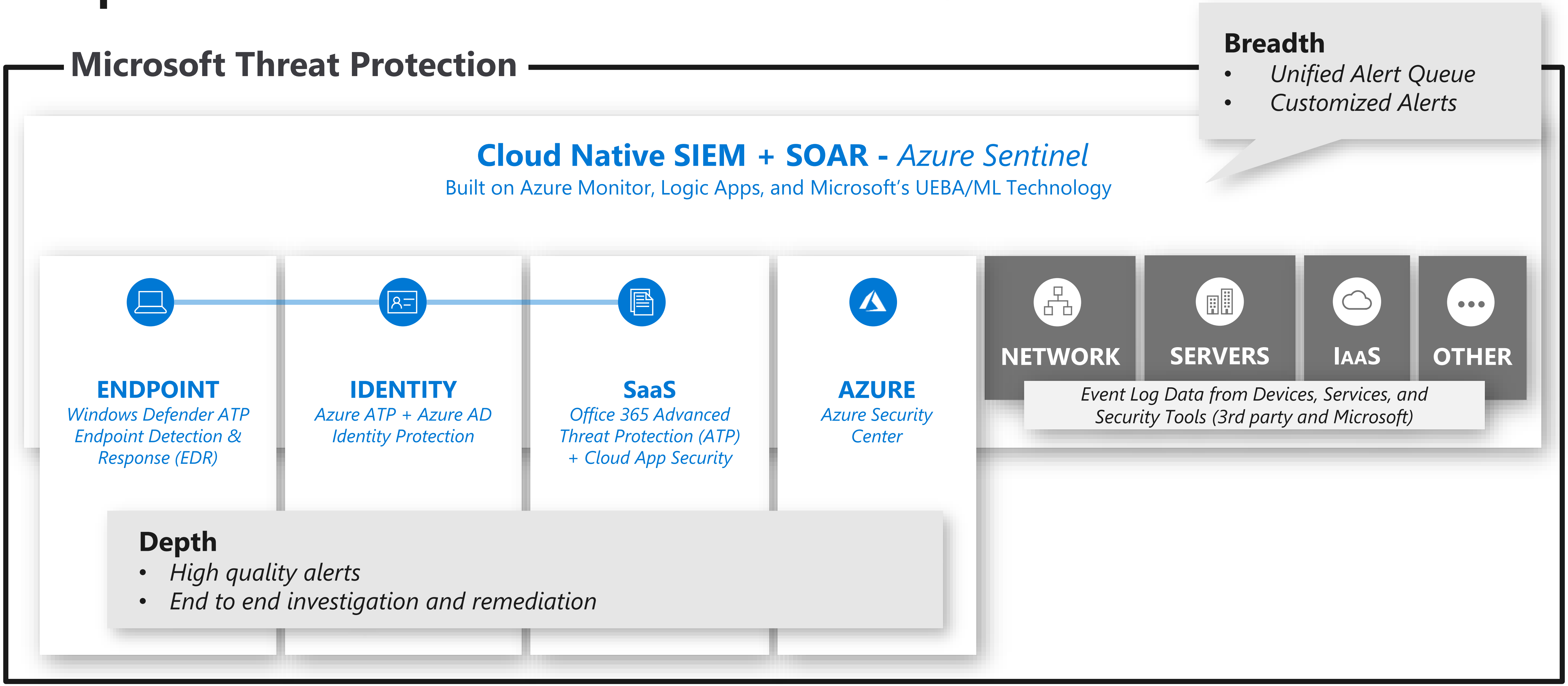
FIREWALL, NETWORK, AND MORE

CEF/Syslog/API

Integrated toolset for rapid threat remediation



SOC Reference Architecture



Microsoft Threat Protection

Breadth

- *Unified Alert Queue*
- *Customized Alerts*

Cloud Native SIEM + SOAR - *Azure Sentinel*

Built on Azure Monitor, Logic Apps, and Microsoft's UEBA/ML Technology

ENDPOINT
Windows Defender ATP Endpoint Detection & Response (EDR)

IDENTITY
Azure ATP + Azure AD Identity Protection

SaaS
Office 365 Advanced Threat Protection (ATP) + Cloud App Security

AZURE
Azure Security Center

NETWORK

SERVERS

IaaS

OTHER

Event Log Data from Devices, Services, and Security Tools (3rd party and Microsoft)

Depth

- *High quality alerts*
- *End to end investigation and remediation*

Centralized Visibility

Azure Security Center

Azure Sentinel

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

GRC Professional

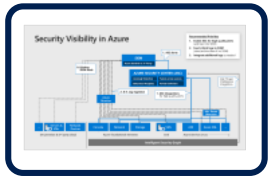
Assess Risk & Compliance

IT / Security Professional

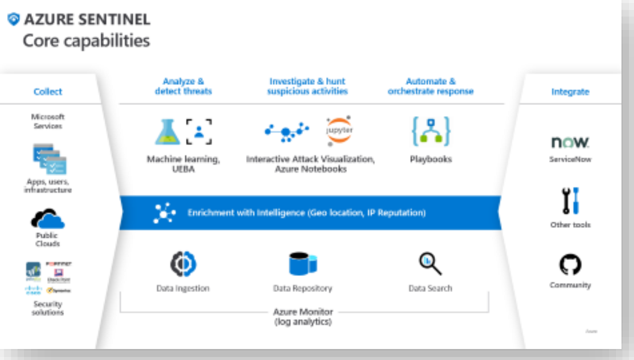
Implement Protections

SOC Analyst

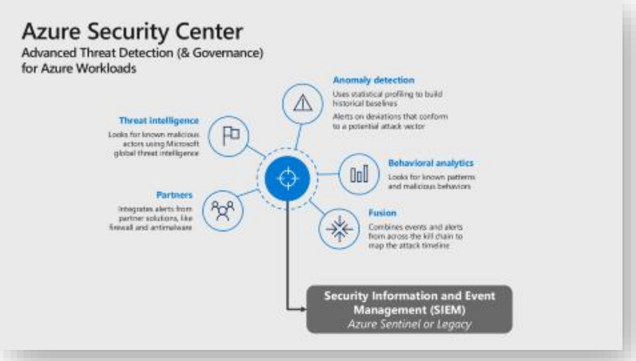
Primary Console
Alerts, Investigation


Security Visibility in Azure

Log Flow


AZURE SENTINEL
Core capabilities

Collect
Microsoft Services
Apps, users, infrastructure
Public Clouds
Security solutions
Analyze & detect threats
Machine learning, UEBA
Investigate & hunt suspicious activities
Interactive Attack Visualization, Azure Notebooks
Automate & orchestrate response
Playbooks
Enrichment with Intelligence (Geo location, IP Reputation)
Data Ingestion
Data Repository
Data Search
Azure Monitor (log analytics)
Integrate
ServiceNow
Other tools
Community


Azure Security Center
Advanced Threat Detection (& Governance) for Azure Workloads

Anomaly detection
Uses statistical profiling to build historical baselines
Alerts on deviations that conform to a potential attack vector
Threat intelligence
Looks for known malicious actors using Microsoft global threat intelligence
Behavioral analytics
Looks for known patterns and malicious behaviors
Partners
Integrates alerts from partner solutions, like firewall and antimalware
Fusion
Combines events and alerts from across the kill chain to map the attack timeline
Security Information and Event Management (SIEM)
Azure Sentinel or Legacy

Generate Alerts

Identity | Endpoint | Cloud | Network | and more

Security Operations – Azure Alerts

CRITICAL GUIDANCE

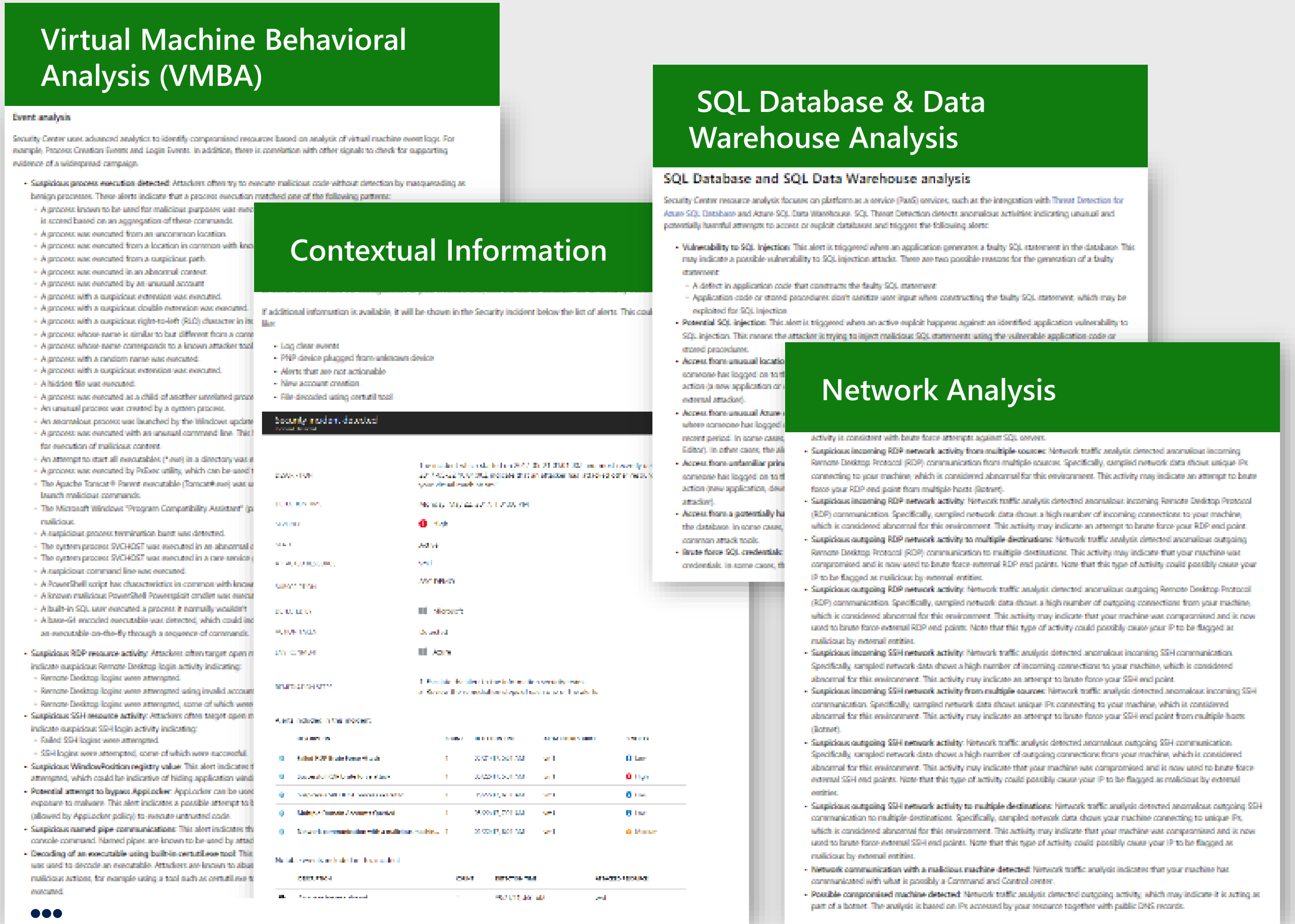
BEST PRACTICE CHOICE

ASC BUILT IN SECURITY ALERTS

- **What** – Enable Azure Security Center security Alerts
- **Why** – Azure Security Center provides actionable detections for common attack methods (Alert List depicted on this slide), which can save your team significant effort on query development.

  These alerts are focused on high true positive rate by leveraging Microsoft's extensive threat intelligence, advanced machine learning, industry leading Endpoint Detection & Response (EDR) (MITRE report), and other approaches.
- **How** – Enable Azure Security Center (Recommend Standard Tier) https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started

Azure Security Center Alerts



Virtual Machine Behavioral Analysis (VMBA)

Event analysis

Security Center uses advanced analytics to identify compromised resources based on analysis of virtual machine event logs. For example, Process Creation Events and Login Events. In addition, there is correlation with other signals to check for supporting evidence of a widespread campaign.

- **Suspicious process execution detected:** Attackers often try to execute malicious code without detection by masquerading as benign processes. These alerts indicate that a process execution matched one of the following patterns:
  - A process known to be used for malicious purposes was exec
    is scored based on an aggregation of these commands.
  - A process was executed from an uncommon location.
  - A process was executed from a location in common with kno
  - A process was executed from a suspicious path.
  - A process was executed in an abnormal context.
  - A process was executed by an unusual account
  - A process with a suspicious extension was executed.
  - A process with a suspicious double extension was executed.
  - A process with a suspicious right-to-left (RLO) character in its
  - A process whose name is similar to but different from a comm
  - A process whose name corresponds to a known attacker tool
  - A process with a random name was executed.
  - A process with a suspicious extension was executed.
  - A hidden file was executed.
  - A process was executed as a child of another unrelated proce
  - An unusual process was created by a system process.
  - An anomalous process was launched by the Windows update
  - A process was executed with an unusual command line. This
    for execution of malicious content.
  - An attempt to start all executables (*.exe) in a directory was m
  - A process was executed by PsExec utility, which can be used t
  - The Apache Tomcat® Parent executable (Tomcat#.exe) was u
    launch malicious commands.
  - The Microsoft Windows "Program Compatibility Assistant" (pc
    malicious.
  - A suspicious process termination burst was detected.
  - The system process SVCHOST was executed in an abnormal c
  - The system process SVCHOST was executed in a rare service g
  - A suspicious command line was executed.
  - A PowerShell script has characteristics in common with know
  - A known malicious PowerShell Powersploit cmdlet was execu
  - A built-in SQL user executed a process it normally wouldn't
  - A base-64 encoded executable was detected, which could ind
    an executable on-the-fly through a sequence of commands.
- **Suspicious RDP resource activity:** Attackers often target open m
  indicate suspicious Remote Desktop login activity indicating:
  - Remote Desktop logins were attempted.
  - Remote Desktop logins were attempted using invalid accoun
  - Remote Desktop logins were attempted, some of which were
- **Suspicious SSH resource activity:** Attackers often target open m
  indicate suspicious SSH login activity indicating:
  - Failed SSH logins were attempted.
  - SSH logins were attempted, some of which were successful.
- **Suspicious WindowPosition registry value:** This alert indicates t
  attempted, which could be indicative of hiding application windo
- **Potential attempt to bypass AppLocker:** AppLocker can be used
  exposure to malware. This alert indicates a possible attempt to b
  (allowed by AppLocker policy) to execute untrusted code.
- **Suspicious named pipe communications:** This alert indicates tha
  console command. Named pipes are known to be used by attac
- **Decoding of an executable using built-in certutil.exe tool:** This
  was used to decode an executable. Attackers are known to abus
  malicious actions, for example using a tool such as certutil.exe t
  executed.

●●●

Contextual Information

If additional information is available, it will be shown in the Security incident below the list of alerts. This coul
like:

- Log clear events
- PNP device plugged from unknown device
- Alerts that are not actionable
- New account creation
- File decoded using certutil tool

Security incident detected

SQL Database & Data Warehouse Analysis

SQL Database and SQL Data Warehouse analysis

Security Center resource analysis focuses on platform as a service (PaaS) services, such as the integration with Threat Detection for Azure SQL Database and Azure SQL Data Warehouse. SQL Threat Detection detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases and triggers the following alerts:

- **Vulnerability to SQL Injection:** This alert is triggered when an application generates a faulty SQL statement in the database. This may indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for the generation of a faulty statement:
  - A defect in application code that constructs the faulty SQL statement
  - Application code or stored procedures don't sanitize user input when constructing the faulty SQL statement, which may be exploited for SQL injection
- **Potential SQL injection:** This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.
- **Access from unusual locatio**
  someone has logged on to th
  action (a new application or
  external attacker).
- **Access from unusual Azure**
  where someone has logged
  recent period. In some cases
  Editor). In other cases, the al
- **Access from unfamiliar prin**
  someone has logged on to th
  action (new application, deve
  attacker).
- **Access from a potentially ha**
  the database. In some cases,
  common attack tools.
- **Brute force SQL credentials:**
  credentials. In some cases, th

Network Analysis

activity is consistent with brute force attempts against SQL servers.

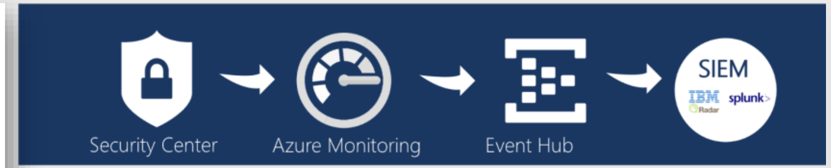
- **Suspicious incoming RDP network activity from multiple sources:** Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication from multiple sources. Specifically, sampled network data shows unique IPs connecting to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point from multiple hosts (Botnet).
- **Suspicious incoming RDP network activity:** Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication. Specifically, sampled network data shows a high number of incoming connections to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point.
- **Suspicious outgoing RDP network activity to multiple destinations:** Network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication to multiple destinations. This activity may indicate that your machine was compromised and is now used to brute force external RDP end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- **Suspicious outgoing RDP network activity:** Network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication. Specifically, sampled network data shows a high number of outgoing connections from your machine, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external RDP end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- **Suspicious incoming SSH network activity:** Network traffic analysis detected anomalous incoming SSH communication. Specifically, sampled network data shows a high number of incoming connections to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your SSH end point.
- **Suspicious incoming SSH network activity from multiple sources:** Network traffic analysis detected anomalous incoming SSH communication. Specifically, sampled network data shows unique IPs connecting to your machine, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your SSH end point from multiple hosts (Botnet).
- **Suspicious outgoing SSH network activity:** Network traffic analysis detected anomalous outgoing SSH communication. Specifically, sampled network data shows a high number of outgoing connections from your machine, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external SSH end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- **Suspicious outgoing SSH network activity to multiple destinations:** Network traffic analysis detected anomalous outgoing SSH communication to multiple destinations. Specifically, sampled network data shows your machine connecting to unique IPs, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external SSH end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.
- **Network communication with a malicious machine detected:** Network traffic analysis indicates that your machine has communicated with what is possibly a Command and Control center.
- **Possible compromised machine detected:** Network traffic analysis detected outgoing activity, which may indicate it is acting as part of a botnet. The analysis is based on IPs accessed by your resource together with public DNS records.

Security Operations – Alert & Log Integration

GENERAL GUIDANCE

NOW - ALERT INTEGRATION

- **What** – Integrate Alerts from Azure Security Center into your existing SIEM (if you are currently using one).
- **Why** – Organizations use SIEMs as a central clearinghouse for security alerts that require an analyst to respond
- **How** – Follow these instructions https://docs.microsoft.com/en-us/azure/security-center/security-center-export-data-to-siem
- Alternately, you can use Azure Security Center for central security dashboard function if
  - You don't have a SIEM
  - Your teams desire/require a console focused on Azure resources



NOW - CRITICAL LOGS

- **What** – Integrate Azure logs with your SIEM (or archive logs if no SIEM)
- **Why** – These logs enable security incident investigation and enable you to query data prior to the online log retention period of the service.
- **How** – Use Azure Monitor to gather logs

Azure Security Log Integration Guidance

Critical Logs

- Azure Activity (Logging Info)
- Azure AD Activities
  - Instructions for [illegible]
- Azure AD Identity Protection alerts
  - via Graph Security API
- NSG Logs (deny rule violations)
  - Documentation
- Azure Key Vault (Logging Info)
  - Log Analytics
- On Premises Identity Connectors
  - Active Directory Federation Services (if used)
- Business Critical Applications

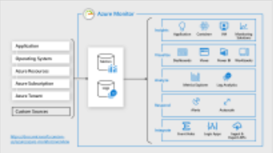
Additional Logs

Azure Monitor enables access to logs for various services

https://docs.microsoft.com/en-us/azure/azure-monitor/overview

AZURE MONITOR

CRITICAL LOGS



AZURE MONITOR

LATER - ADDITIONAL LOGS

- **What** – When required, integrate additional Azure service logs for Azure platform and services into your SIEM
- **Why** – Additional Logs may be required for investigation and for generating customized alerts for applications and Azure service usage.
- **How** – Follow these instructions and guidance to onboard appropriate logs

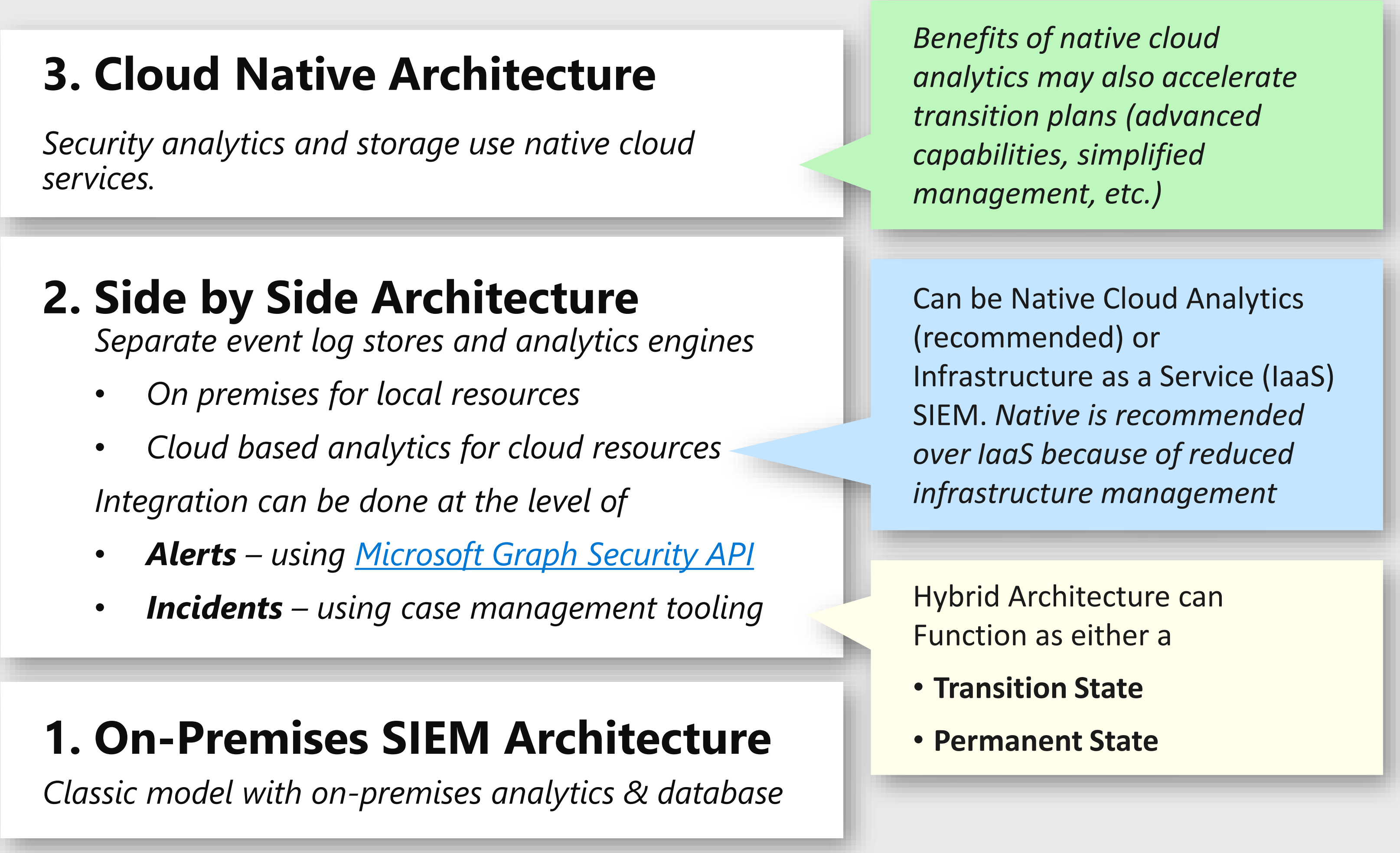
  https://docs.microsoft.com/en-us/azure/security/azure-log-audit

Security Operations – Journey to Cloud Analytics

CRITICAL CHOICE

CLOUD ANALYTICS STRATEGY

- **What** – Choose when and how to integrate cloud-based security analytics/SIEM (such as Azure Sentinel, ELK stack, etc.)
- **Why** – As more enterprise services generate security data in the cloud, hauling this data back to on premises becomes expensive and inefficient. This ‘Data Gravity’ will increasingly require security analytics to be hosted in the cloud as you migrate workloads.
- **How** – Ensure your strategy for security analytics & SIEM plans for this transition and includes thresholds & timing for progression into each phase.



3. Cloud Native Architecture

Security analytics and storage use native cloud services.

Benefits of native cloud analytics may also accelerate transition plans (advanced capabilities, simplified management, etc.)

2. Side by Side Architecture

Separate event log stores and analytics engines

- *On premises for local resources*
- *Cloud based analytics for cloud resources*

Integration can be done at the level of

- ***Alerts** – using Microsoft Graph Security API*
- ***Incidents** – using case management tooling*

Can be Native Cloud Analytics (recommended) or Infrastructure as a Service (IaaS) SIEM. *Native is recommended over IaaS because of reduced infrastructure management*

Hybrid Architecture can Function as either a

- **Transition State**
- **Permanent State**

1. On-Premises SIEM Architecture

Classic model with on-premises analytics & database

Security Operations

GENERAL GUIDANCE

▲ BEST PRACTICE   CHOICE

▲ ***Have analysts learn new authentication flows***

Many analysts may be unfamiliar with how newer authentication protocols like OAuth, SAML, and WS-Federation work. Ensure analysts get familiar with these protocols as they are different than on premises protocols like NTLM and Kerberos

▲ ***Prioritize critical impact admin accounts***

Ensure your SOC processes prioritize attacks on critical impact admins that could have a significant business impact if compromised. Prioritization should include admin only elements like Azure AD PIM as well as prioritizing general detections that include admin users like leaked credentials, behavior analytics, etc.

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-sumologic

▲ ***On-Premises Identity Attack Detection***

Attackers frequently use pass the hash/ticket/password and other credential theft/impersonation attacks which can affect Infrastructure as a Service (IaaS) Virtual Machines (VMs). Azure Security Center includes some detections on Azure, but you should also consider specialized identity security tools such as Azure ATP or a 3rd party solution (which can also protect on-premises components).

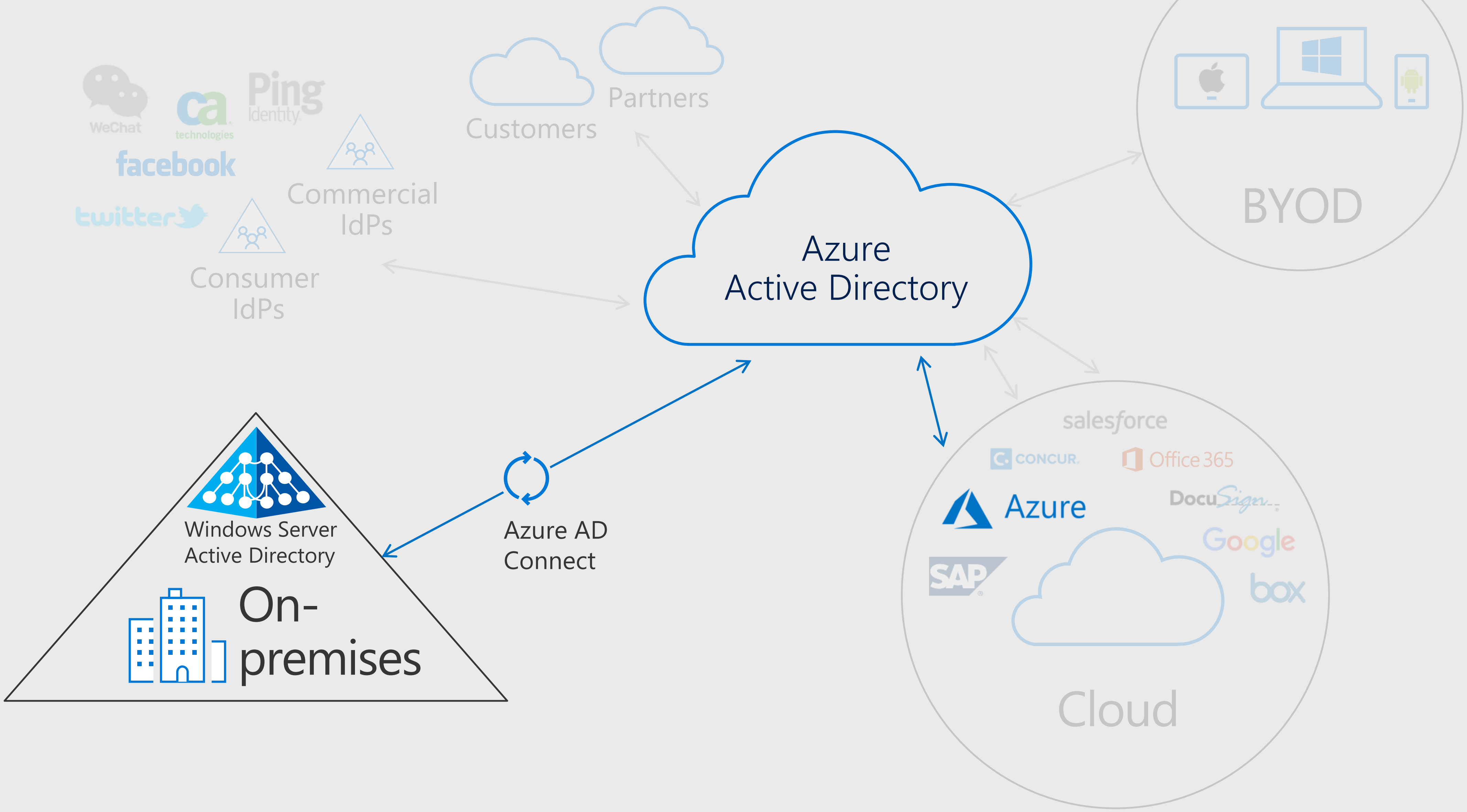
Identity and Access Management

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/identity

Identity as the Control Plane

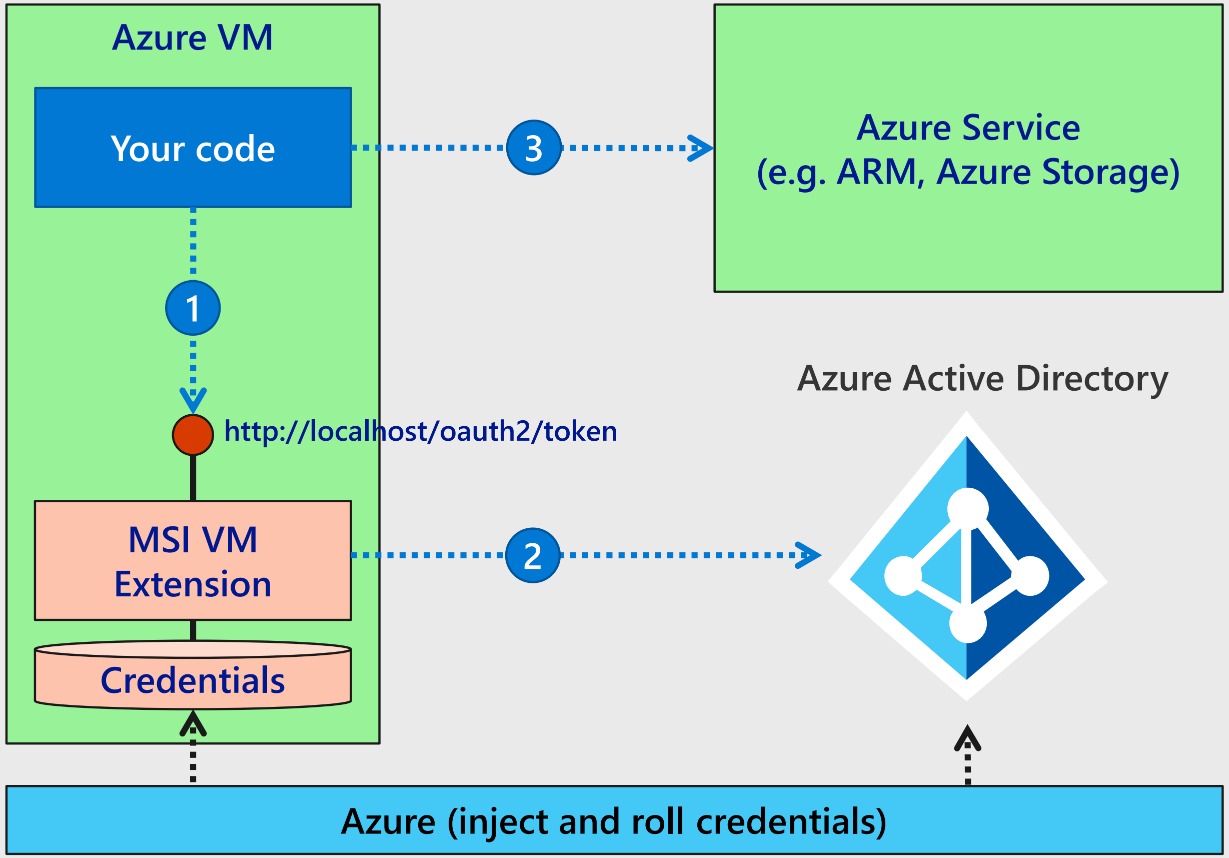
Single Sign-On and Zero Trust Access Control Across Your Enterprise



Managed identities for Azure resources

- Simplifies authentication/security for developers (vs. service principals)
  - Authenticate to services without inserting credentials into code
    - *Target Service must support Azure AD authentication*
  - E.g. Allow (code running on) a specific VM to access Azure Key Vault, Storage Account, Azure SQL, etc.

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview


Azure VM
Your code
1
http://localhost/oauth2/token
MSI VM Extension
Credentials
3
Azure Service (e.g. ARM, Azure Storage)
Azure Active Directory
2
Azure (inject and roll credentials)

Top 3 Attacks

Password Spray

200,000 accounts compromised in Aug 2018
(Primarily via legacy AuthN protocols)

Phishing

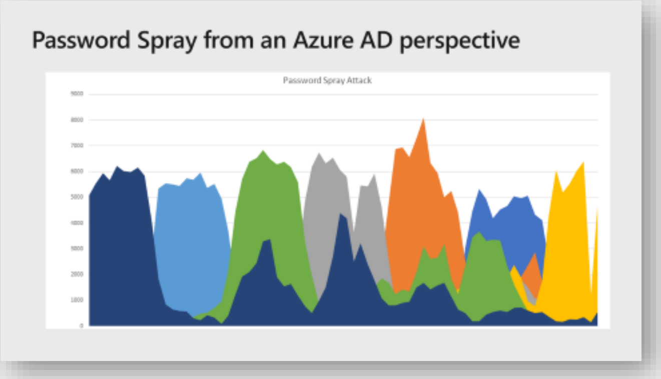
5B emails blocked in 2018

44M risk events in Aug 2018

Breach Replay

650,000 accounts with leaked credentials in 2018

Password Spray



Password Spray from an Azure AD perspective

Typical Attack

1. Attempt a common password used against many, many accounts.
   (stay below account lockout threshold)
2. After successful login, dump the GAL.
3. Start pivoting in environment.

Josi@contoso.com	Password123
Chance@wingtiptoys.com	Password123
Rami@fabrikam.com	Password123
TomH@cohowinery.com	Password123
AnitaM@cohovineyard.com	Password123
EitokuK@cpandl.com	Password123
Ramanujan@Adatum.com	Password123
Maria@Treyresearch.net	Password123
LC@adverture-works.com	Password123
EW@alpineskihouse.com	Password123
info@blueyonderairlines.com	Password123
AiliS@fourthcoffee.com	Password123
MM39@litwareinc.com	Password123
Margie@margiestravel.com	Password123
Ling-Pi997@proseware.com	Password123
PabloP@fineartschool.net	Password123
GiseleD@tailspintoys.com	Password123
Luly@worldwideimporters.com	Password123
Bjorn@woodgrovebank.com	Password123
NK@lucernepublishing.com	Password123

Identity – Consistency

CRITICAL BEST PRACTICES

SINGLE ENTERPRISE DIRECTORY

- **What** – Establish a single enterprise Azure Active Directory (Azure AD) instance
- **How** – Designate a single Azure AD directory as the authoritative source for corporate/organizational accounts.

SYNCHRONIZE WITH ACTIVE DIRECTORY & IDENTITY SYSTEMS

- **What** – Synchronize Azure AD with your existing on-premises AD
- **How** – Leverage Azure AD connect to synchronize with on premises AD and any identity management systems

https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect

AZURE AD FOR APPLICATIONS

- **What** – For new development, use Azure AD for consistent authentication
- **How** – Use appropriate capabilities to support authentication needs :
  - **Azure AD** – Employees
  - **Azure AD B2B** – Partners
  - **Azure AD B2C** - Customers/citizens

- **Why** – Consistency and single authoritative sources will increase clarity and reduce security risk from human errors and configuration/automation complexity.

Identity

CRITICAL BEST PRACTICES

BLOCK LEGACY AUTHENTICATION

- **What** – Block legacy authentication protocols for Azure AD
- **Why** – Weaknesses in older protocols are actively exploited by attackers daily, particularly for bypassing MFA and for password spray attacks (majority use legacy auth)
- **How** – Configure Conditional Access to block legacy protocols

  https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Conditional-Access-support-for-blocking-legacy-auth-is/ba-p/245417

For more information https://www.youtube.com/watch?v=wGk0J4z90GI

DON'T SYNCH AD ADMINS

- **What –** Don't synchronize accounts to Azure AD that have high privileges in your existing Active Directory
- **Why** – This mitigates the risk of adversaries pivoting from cloud to on premises assets (creating a potential major incident).
- **How –** This is blocked by default. Do not change the default Azure AD Connect configuration that filters out these accounts

See also the converse guidance in Administration section:

- ***Critical Impact Admin - Account***
- ***Critical Impact Admin - Workstation***

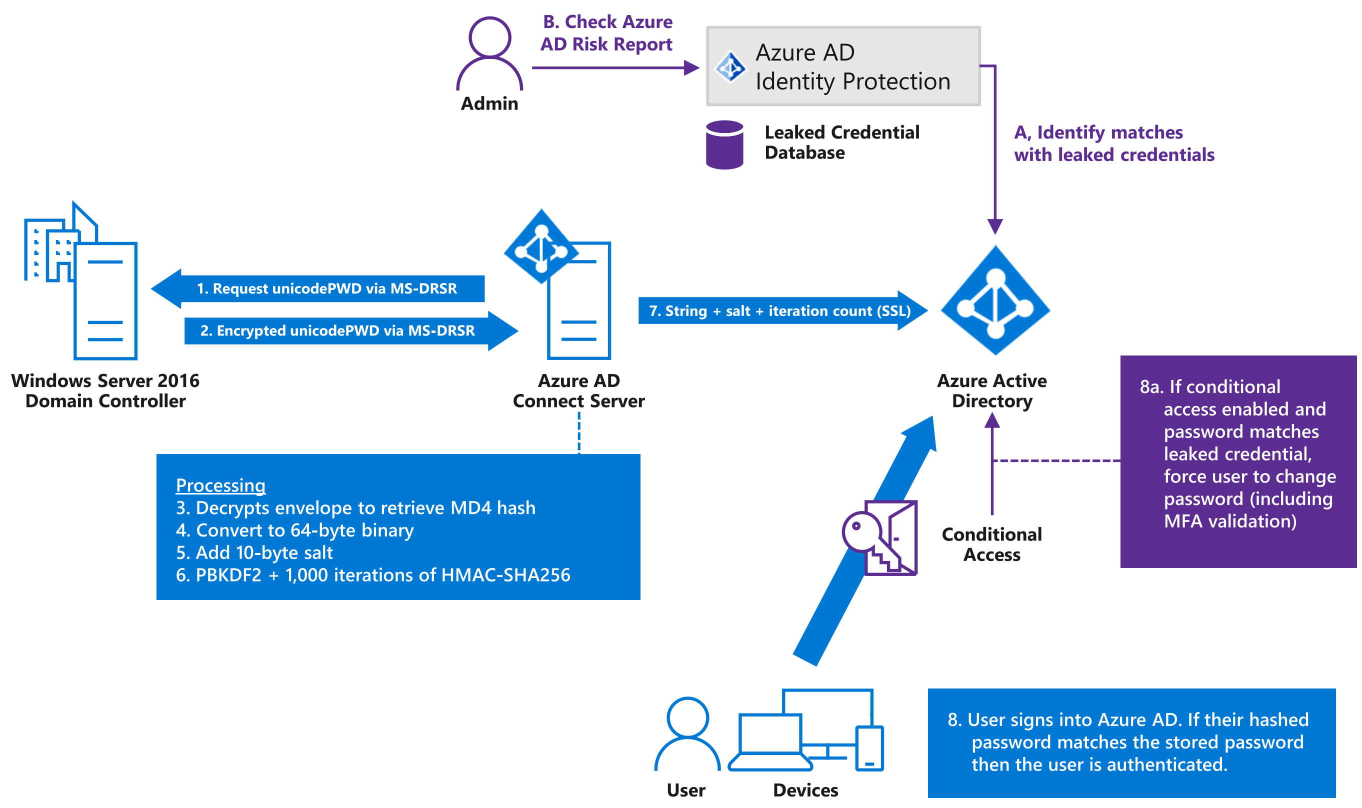
Identity – Password Synchronization

CRITICAL BEST PRACTICE

SYNCHRONIZE PASSWORD HASHES

- **What** – Synchronize your user password hashes from on-premises Active Directory instance to Azure Active Directory (Azure AD).
- **Why** – This increases both
  - **Security** - Protects against leaked credentials being replayed from previous attacks
  - **Reliability** - Customers affected by (Not)Petya attacks were able to continue business operations when password hashes were synced to Azure AD (vs. near zero IT functionality for customers who did not)
- **How** – Configure Azure AD Connect to synchronize password hashes

https://docs.microsoft.com/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization



Admin
B. Check Azure AD Risk Report
Azure AD Identity Protection
Leaked Credential Database
A, Identify matches with leaked credentials
Windows Server 2016 Domain Controller
1. Request unicodePWD via MS-DRSR
2. Encrypted unicodePWD via MS-DRSR
Azure AD Connect Server
7. String + salt + iteration count (SSL)
Azure Active Directory
Conditional Access
User
Devices

Processing
3. Decrypts envelope to retrieve MD4 hash
4. Convert to 64-byte binary
5. Add 10-byte salt
6. PBKDF2 + 1,000 iterations of HMAC-SHA256

8a. If conditional access enabled and password matches leaked credential, force user to change password (including MFA validation)

8. User signs into Azure AD. If their hashed password matches the stored password then the user is authenticated.

Identity – Password Protection from Cloud

CRITICAL BEST PRACTICES

AZURE AD PASSWORD PROTECTION

- **What** – Choose the level of password protection in Azure Active Directory
- **Why** – Static on-premises defenses capabilities can no longer protect password-based accounts.
  - **Microsoft** - https://www.microsoft.com/en-us/research/publication/password-guidance/
  - **NIST** - https://pages.nist.gov/800-63-3/sp800-63b.html

Passwordless solutions are ideal and MFA can help, but password-based accounts must be protected

How – Choose protection for Azure AD Passwords

2. Automatic Enforcement

Automatically remediate high risk passwords with Conditional Access (leveraging Azure AD Identity Protection risk assessments)

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview

1. Report & Remediate

View reports and manually remediate accounts

- **Azure AD reporting** - Risk events are part of Azure AD's security reports. For more information, see the users at risk security report and the risky sign-ins security report.
- **Azure AD Identity Protection** - Risk events are also part of the reporting capabilities of Azure Active Directory Identity Protection.
- Use the Identity Protection risk events API to gain programmatic access to security detections using Microsoft Graph.

~~0. Do Nothing (Not Recommended)~~

Identity

GENERAL GUIDANCE

▲ BEST PRACTICE   ● CHOICE

▲ ***AZURE AD FOR LINUX LOGIN***

Use Azure Active Directory for authenticating to Linux VMs to simplify management and security

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/login-using-aad

▲ ***CLOUD PROTECTION FOR ON PREMISES ACTIVE DIRECTORY***

Protect passwords in your on-premises AD using Azure AD

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Administration

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/critical-impact-accounts

Highest Protection for Highest Privileges

Critical Impact Accounts in Azure

1. Administrative Privileges

- **Global Azure AD Admins + Azure Tenant Admins**

2. Data Access

- **Groups & Accounts** with read/write/delete access to business-critical data

3. Operational Access

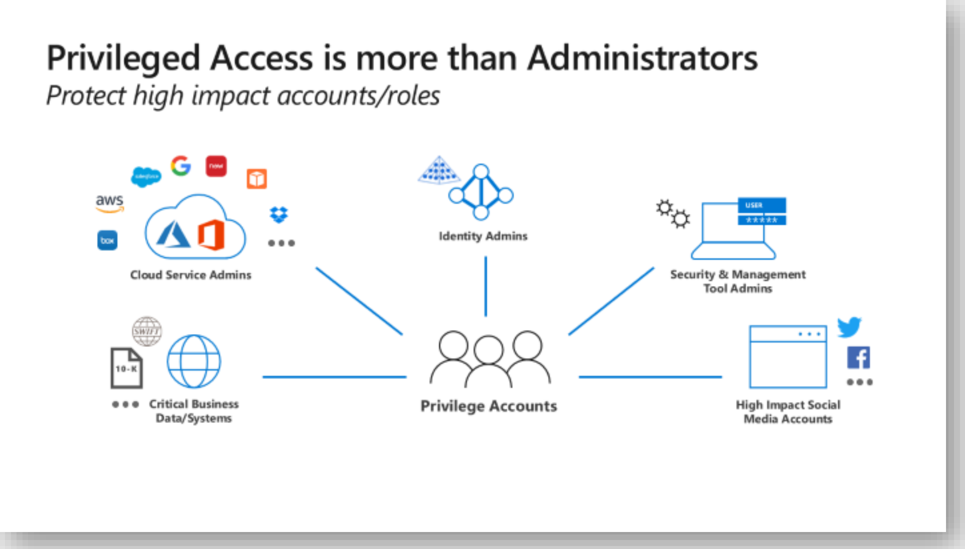
- **Groups & Accounts** with control of business-critical systems

  *Owners & Admins of Management Groups MGs/Subscriptions containing

  - Shared Services
  - Business Critical Apps

Most guidance in this section refers to protecting IT Admin accounts

You should consider applying similar procedures to other admins as well



Privileged Access is more than Administrators

Protect high impact accounts/roles

Cloud Service Admins
Identity Admins
Security & Management Tool Admins
Critical Business Data/Systems
Privilege Accounts
High Impact Social Media Accounts

Admin – Quantity

CRITICAL BEST PRACTICES

▲ BEST PRACTICE ● CHOICE

LEAST NUMBER OF CRITICAL IMPACT ADMINS

- **What** – Grant the fewest number of accounts to groups with critical business impact
- **Why** – Each admin account represents potential attack surface and business risk

How –

- Assign at least 2 accounts for business continuity
- When 2+ accounts, provide justification for each
- Regularly review members & justification

Tips

- Grant only required privileges (using built in RBAC roles) vs. global admin and segment owner roles
- For people outside your organization, use AAD B2B Collaboration instead of personal or corporate accounts

Admin – Accounts

CRITICAL BEST PRACTICE

▲ BEST PRACTICE ● CHOICE

MANAGED ACCOUNTS FOR ADMINS

- **What** – Ensure all critical impact admins are managed Azure AD accounts
- **Why –** This provides enterprise visibility into whether the policies of the organization and any regulatory requirements are followed.
- **How** – Ensure all critical impact admins are in your enterprise Azure AD. Remove any consumer accounts from these roles (e.g. Microsoft accounts like @Hotmail.com, @live.com, @outlook.com, etc.)

SEPARATE ACCOUNTS FOR ADMINS

- **What –** Ensure all critical impact admins have a separate account for administrative tasks
- **Why –** Adversaries regularly use phishing and web browser attacks to compromise administrative accounts.
- **How** – Create a separate administrative account for critical privileges. For these accounts, block productivity tools like Office 365 email (remove license) and arbitrary web browsing (with proxy and/or application controls if available)

Admin – Emergency Access

CRITICAL BEST PRACTICE

BREAK GLASS ACCESS

- **What** – Ensure you have a mechanism for obtaining emergency administrative access
- **Why** – Provide access in the event of where normal administrative accounts can't be used (federation unavailable, etc.)
- **How** – Follow the instructions at [Managing emergency access administrative accounts in Azure AD]() and ensure that security operations monitors these accounts carefully

Admin – Attack Pivot Risk

CRITICAL BEST PRACTICE

See identity section for converse guidance “Don’t Synch AD Admins”

CRITICAL IMPACT ADMIN - ACCOUNT

- **What –** For critical impact accounts, carefully choose the account type and directory

CRITICAL IMPACT ADMIN - WORKSTATION

- **What** – For critical impact accounts, choose whether the admin workstation they use will be managed by cloud services or existing on-premises processes

- **Why –** Leveraging existing management and identity de/provisioning processes can decrease some risk, but can also create risk of an attacker compromising an on-premises account and pivoting to the cloud. You may choose a different strategy for different roles (e.g. IT admins vs. business unit admins)

DEFAULT RECOMMENDATION

Native Azure AD Accounts

Create Native Azure AD Accounts that are not synchronized with on-premises Active Directory

Native Cloud Management & Protection

- Join to Azure AD & Manage/Patch with Intune/other
- Protect and Monitor with Windows Defender ATP/other

Synchronize from On Premises Active Directory

Leverage existing administrative roles

Manage with Existing Systems

Join AD domain & leverage existing management/security

Administration – Account protection

CRITICAL BEST PRACTICES

▲ BEST PRACTICE   ● CHOICE

▲ PASSWORDLESS OR MULTI-FACTOR AUTHENTICATION FOR ADMINS

- **What** – Require all critical impact admins to be passwordless (preferred) or require MFA.
- **Why –** Passwords cannot protect accounts against common attacks. https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK3016
- **How** –
  - **Passwordless (Windows Hello)** http://aka.ms/HelloForBusiness
  - **Passwordless (Authenticator App)** https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-phone-sign-in
  - **Multifactor Authentication** https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates
  - **3rd Party MFA Solution**

▲ NO STANDING ACCESS

- **What** – No standing access for critical impact admins
- **Why –** Permanent privileges increase business risk by increasing attack surface of accounts (time)
- **How** –
  - **Just in Time -** Enable Azure AD PIM or 3rd party solution) for all of these accounts
  - **Break glass –** Process for accounts (preferred for low use accounts like global admin)

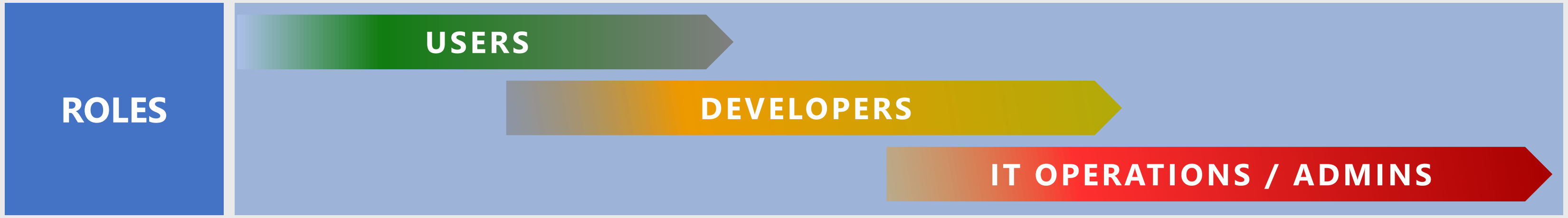
Note: Text Message based MFA is now relatively inexpensive for attackers to bypass, so focus on passwordless & stronger MFA

Admin – Workstation Security

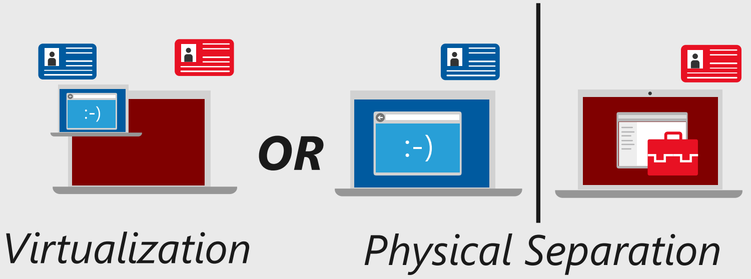
CRITICAL BEST PRACTICES

ADMIN WORKSTATION SECURITY

- **What** – For critical impact admins, choose what admin workstation security level to start with (and when you will progress to full admin workstations)
- **Why** – Attack vectors that use browsing and email (like phishing) are cheap and common. Isolating critical impact admins from these will significantly lower your risk of a major incident
- **How** – Choose level of admin workstation security (using either Microsoft security capabilities or equivalent from 3rd party security providers)



PROFILES	Low Security Workstation	Enhanced Security Workstation	High Security Workstation	Specialized Workstation	Secured Workstation –aka PAW
SECURITY CONTROLS	• **Productivity Apps** • **Application and browser activity monitored** • **User Managed policies** • **Antivirus**	• *Low Security Plus…* • **Centrally Managed Policies** • **Defender ATP**	• *Enhanced Security Plus…* • **No Local Admin**	• *High Security Plus…* • **Restricted applications** • **Restricted browsing**	• *High Security Plus…* • **No productivity applications** • **Restricted browsing** • **Separate identity**



Virtualization

Physical Separation

Secure Workstation Documentation

Overview- *http://aka.ms/SWoverview*

Implementation - *http://aka.ms/secureworkstation*

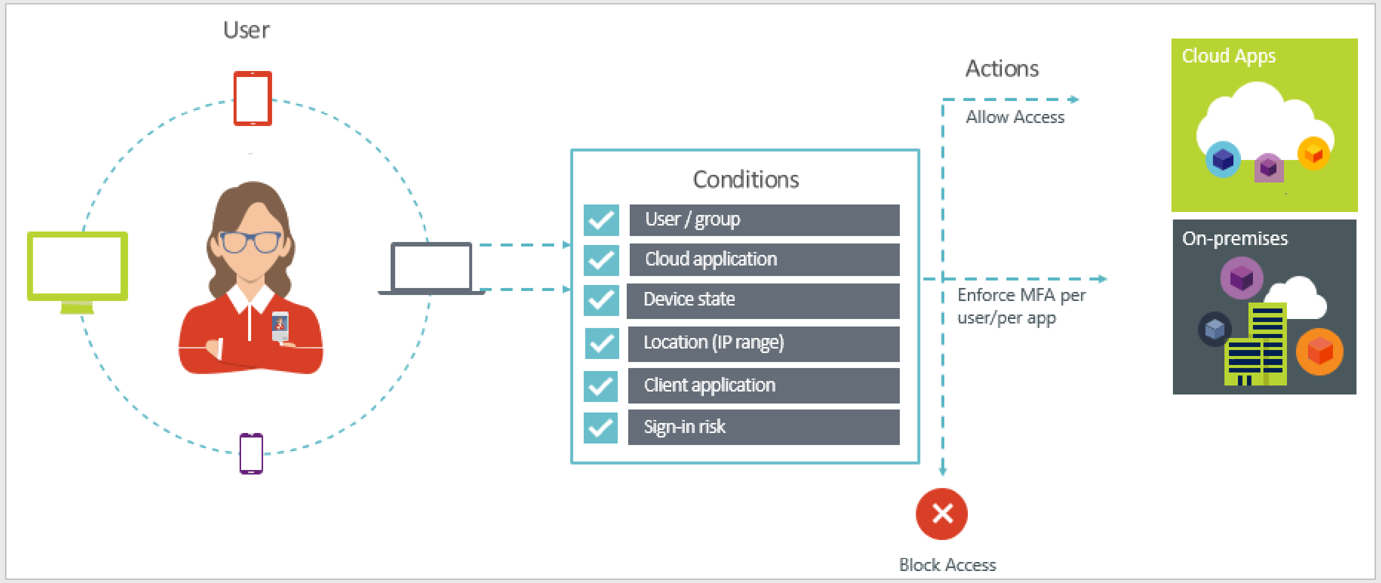
Admin – Conditional access

CRITICAL BEST PRACTICE

BEST PRACTICE CHOICE

ENFORCE ACCESS SECURITY

- **What** – Choose security requirements to enforce for admins managing Azure
- **Why** – Attackers compromising Azure Admin accounts can cause significant harm. Conditional Access can significantly reduce that risk by enforcing security hygiene before allowing access to Azure management
- **How** – Configure [Conditional Access policy for Azure management]() that meets your organizations risk appetite and operational needs
  - **Require Multifactor Authentication** and/or connection from designated work network
  - **Require Device [integrity with Windows Defender ATP]()** (Strong Assurance)



More information on Conditional Access:
[https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview]()

Admin – Simplify Permissions

CRITICAL BEST PRACTICES

USE BUILT IN ROLES

- **What –** Use built-in roles for assigning permissions
- **Why** – Customization leads to complexity that inhibits human understanding, security, automation, and governance.
- **How** – Evaluate the built-in roles designed to cover most common scenarios.

Custom roles are a powerful and sometimes useful capability, but they should be reserved for cases when built in roles won't work

AVOID GRANULAR AND CUSTOM PERMISSIONS

- **What** – Avoid permissions specifically referencing resources or users
- **Why** – Specific permissions create unneeded complexity and confusion, accumulating into a "legacy" configuration that is difficult to fix (without fear of "breaking something")
- **How** –

🚫 **Avoid Resource specific permissions –** Instead, you should use

➡ **Management Groups** for enterprise wide permissions

➡ **Resource groups** for permissions within subscriptions

🚫 **Avoid user specific permissions –** Instead, you should

➡ **Assign access to groups in Azure AD.**

If there isn't an appropriate group, work with the identity team to create one

This allows you to add and remove group members externally to Azure and ensure permissions are current, while also allowing the group to be used for other purposes such as mailing lists.

Admin – Account Lifecycle

GENERAL GUIDANCE

Automatic deprovisioning

Ensure you have a process for disabling or deleting administrative accounts when admin personnel leave the organization (or leave administrative positions)

See also “Regularly Review Critical Access” in *Governance, Risk, and Compliance* section

Attack Simulation

Regularly test administrative users using current attack techniques to educate and empower them. You can use Office 365 Attack Simulation capabilities or a 3rd party offering

https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

Network Security & Containment

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/network-security-containment

Azure Networking Services

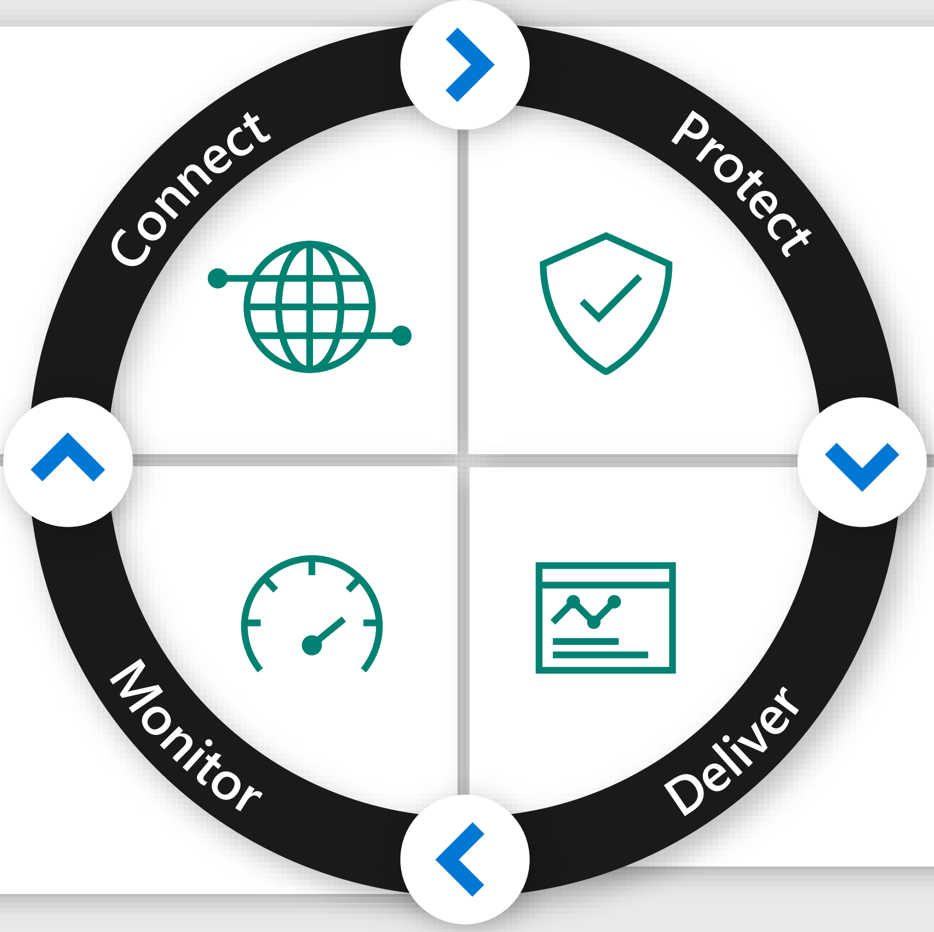
Virtual Network

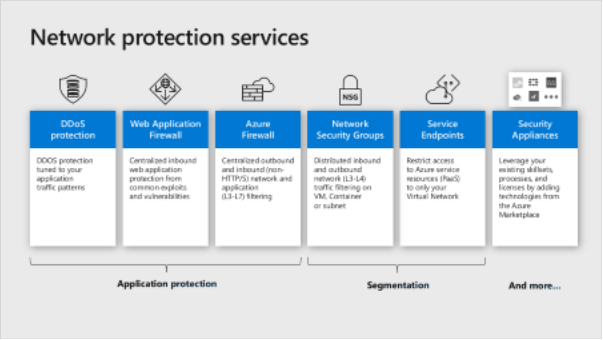
Virtual WAN

ExpressRoute

VPN

DNS





Network protection services

DDoS protection	Web Application Firewall	Azure Firewall	Network Security Groups	Service Endpoints	Security Appliances
DDOS protection tuned to your application traffic patterns	Centralized inbound web application protection from common exploits and vulnerabilities	Centralized outbound and inbound (non-HTTP/S) network and application (L3-L7) filtering	Distributed inbound and outbound network (L3-L4) traffic filtering on VM, Container or subnet	Restrict access to Azure service resources (PaaS) to only your Virtual Network	Leverage your existing skillsets, processes, and licenses by adding technologies from the Azure Marketplace
Application protection			Segmentation		And more...

Network Watcher

ExpressRoute Monitor

Azure Monitor

Virtual Network TAP

CDN

Front Door

Traffic Manager

Application Gateway

Load Balancer

Network protection services

Application protection

DDoS protection

DDOS protection tuned to your application traffic patterns

Web Application Firewall

Centralized inbound web application protection from common exploits and vulnerabilities

Azure Firewall

Centralized outbound and inbound (non-HTTP/S) network and application (L3-L7) filtering

Segmentation

Network Security Groups

Distributed inbound and outbound network (L3-L4) traffic filtering on VM, Container or subnet

Service Endpoints

Restrict access to Azure service resources (PaaS) to only your Virtual Network

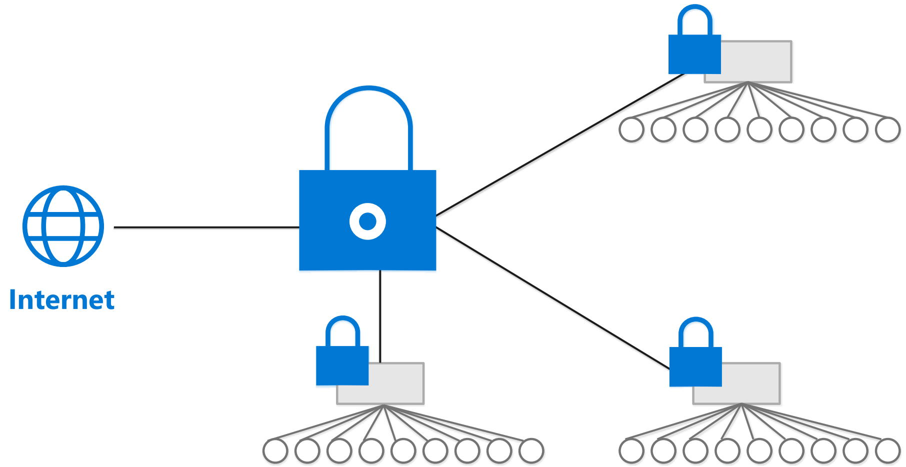
And more...

Security Appliances

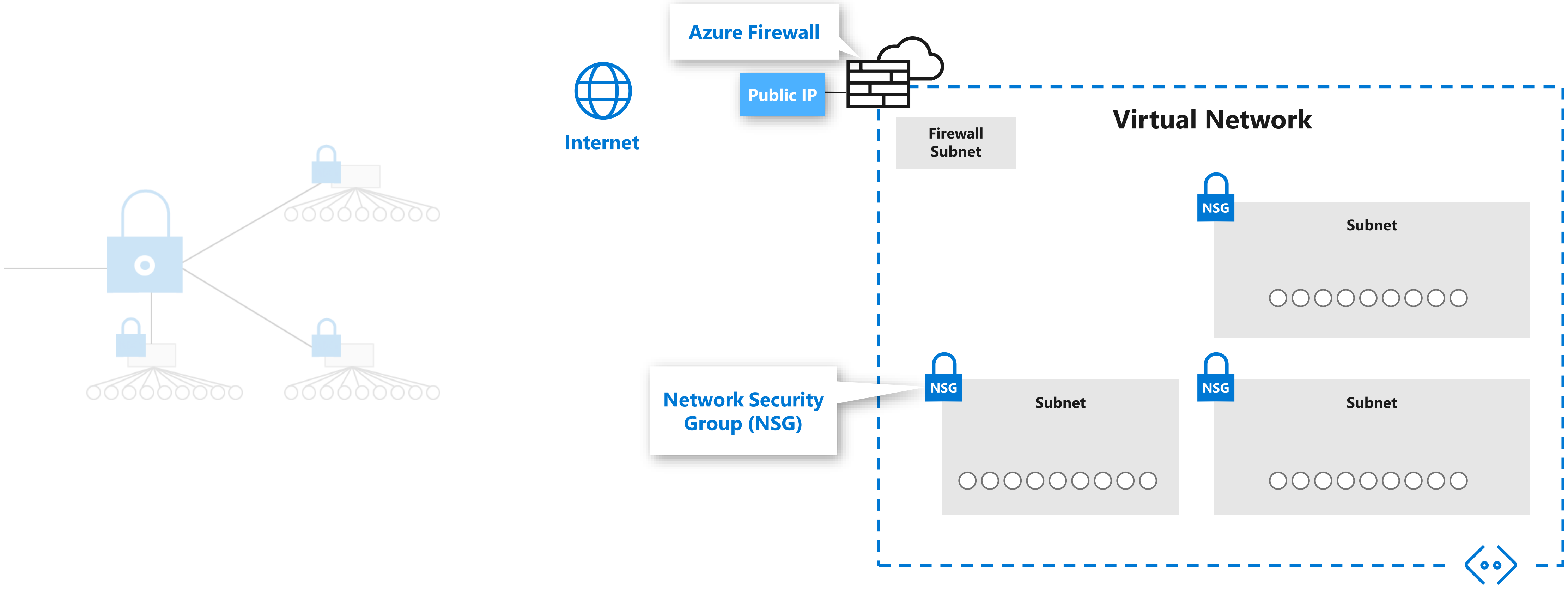
Leverage your existing skillsets, processes, and licenses by adding technologies from the Azure Marketplace

Physical vs. Software Defined Networking

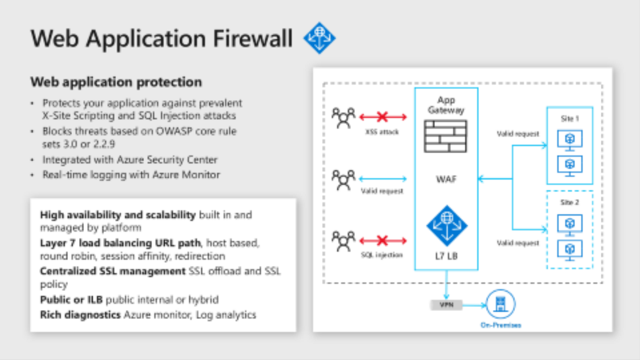
Intercept points → Controls on groups of assets



Physical vs. Software Defined Networking



Web App Firewalls



Web Application Firewall

Web application protection

- Protects your application against prevalent X-Site Scripting and SQL Injection attacks
- Blocks threats based on OWASP core rule sets 3.0 or 2.2.9
- Integrated with Azure Security Center
- Real-time logging with Azure Monitor

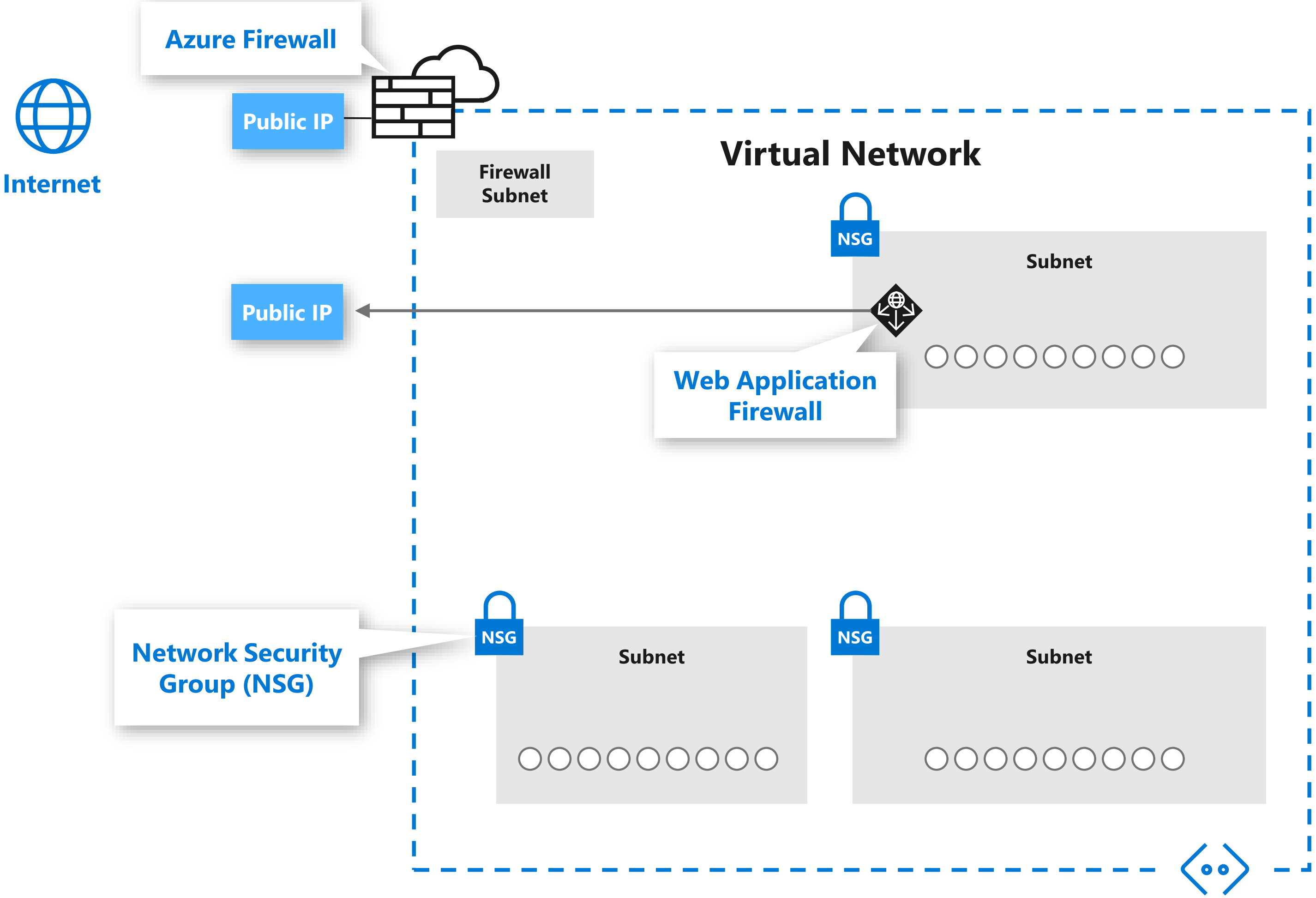
High availability and scalability built in and managed by platform

Layer 7 load balancing URL path, host based, round robin, session affinity, redirection

Centralized SSL management SSL offload and SSL policy

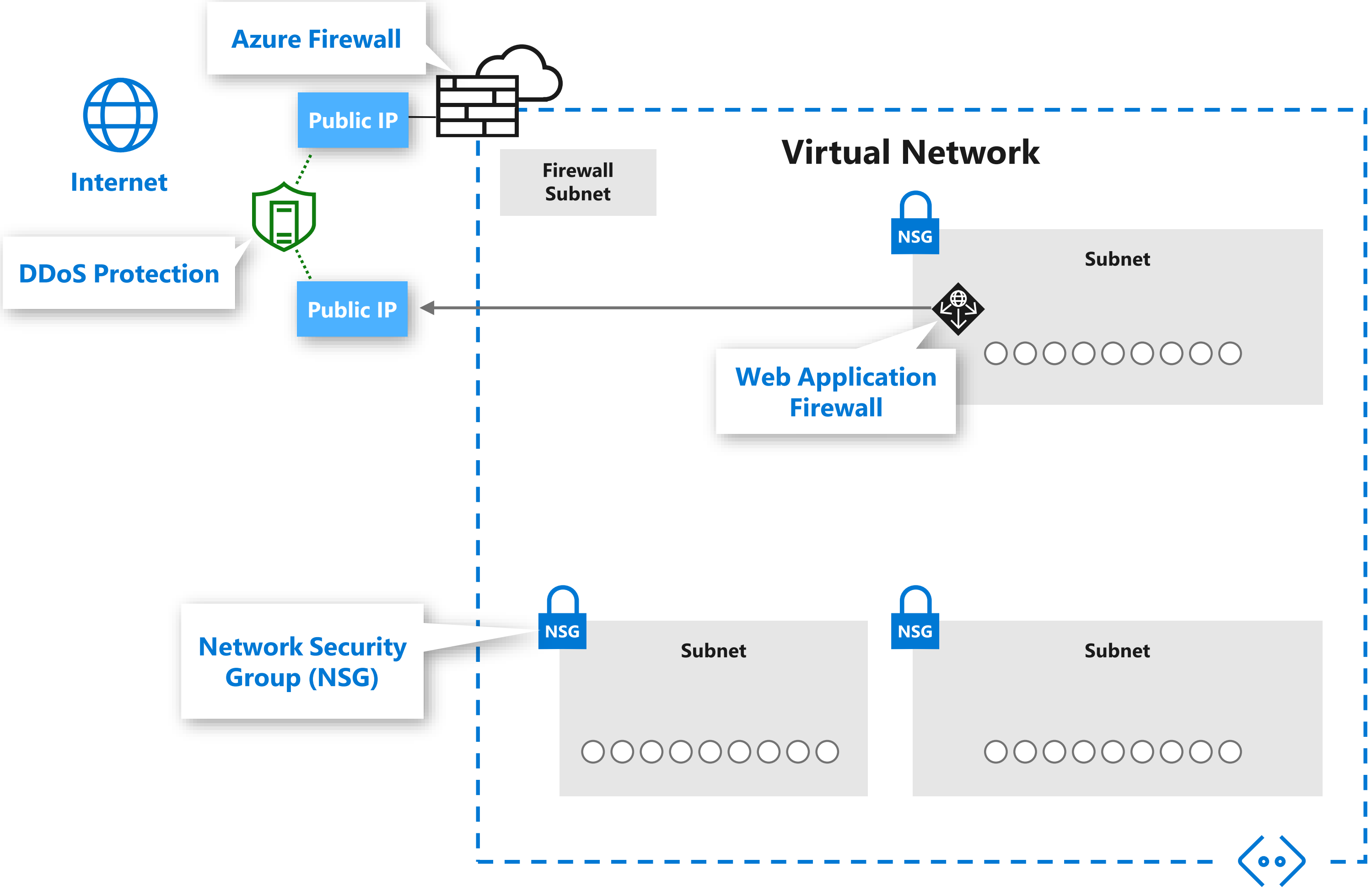
Public or ILB public internal or hybrid

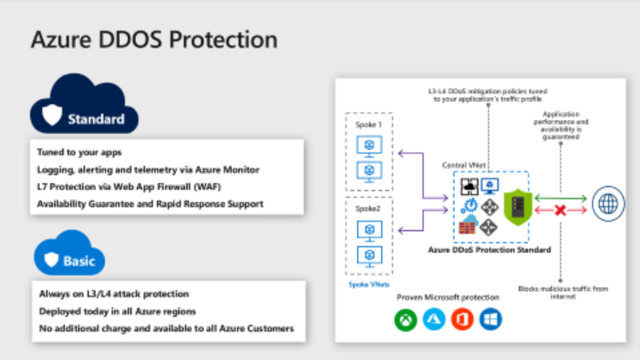
Rich diagnostics Azure monitor, Log analytics



Distributed Denial of Service (DDoS) protection

Basic Protection Built in + Available Advanced Protection





Azure DDOS Protection

Standard

- Tuned to your apps
- Logging, alerting and telemetry via Azure Monitor
- L7 Protection via Web App Firewall (WAF)
- Availability Guarantee and Rapid Response Support

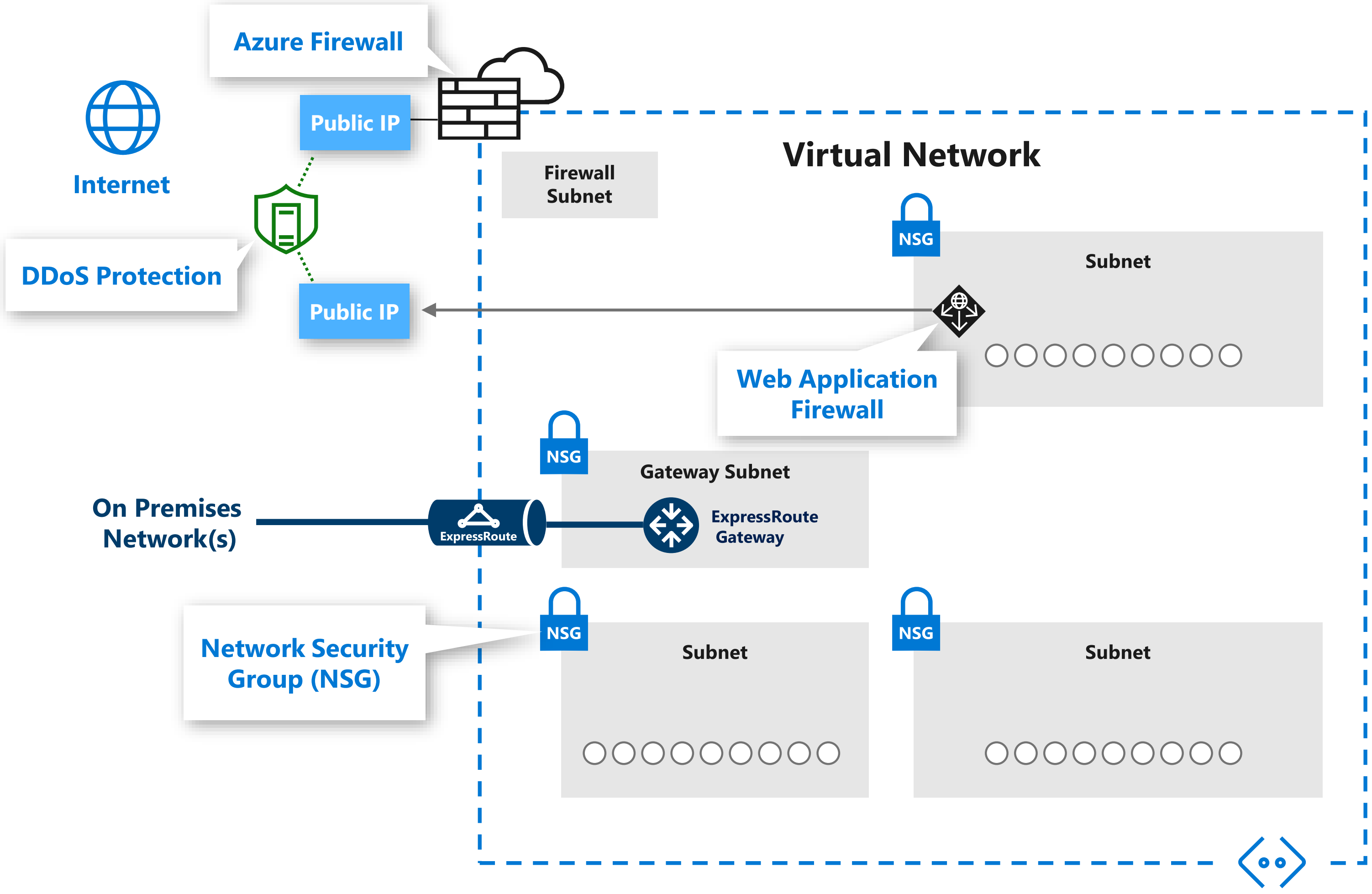
Basic

- Always on L3/L4 attack protection
- Deployed today in all Azure regions
- No additional charge and available to all Azure Customers

L3-L4 DDoS mitigation policies tuned to your application's traffic profile
Application performance and availability is guaranteed
Spoke 1
Spoke2
Spoke VNets
Central VNet
Azure DDoS Protection Standard
Blocks malicious traffic from internet
Proven Microsoft protection

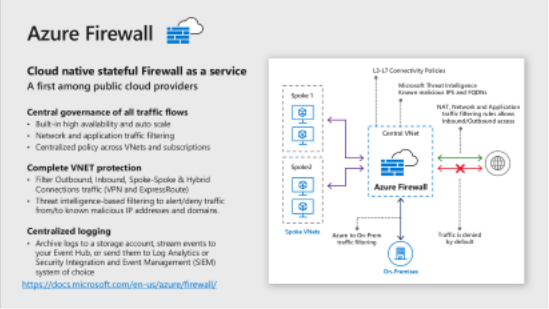
Connecting to On Premises Resources

ExpressRoute or VPN provides connectivity



Reference Configuration with Native Controls

Azure Firewall + Application Gateway with Web App Firewall (WAF)



Azure Firewall

Cloud native stateful Firewall as a service
A first among public cloud providers

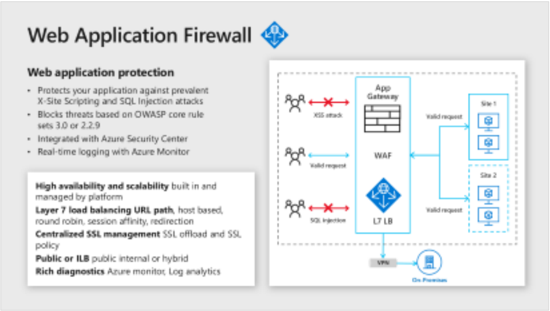
Central governance of all traffic flows
- Built-in high availability and auto scale
- Network and application traffic filtering
- Centralized policy across VNets and subscriptions

Complete VNET protection
- Filter Outbound, Inbound, Spoke-Spoke & Hybrid Connections traffic (VPN and ExpressRoute)
- Threat intelligence-based filtering to alert/deny traffic from/to known malicious IP addresses and domains.

Centralized logging
- Archive logs to a storage account, stream events to your Event Hub, or send them to Log Analytics or Security Integration and Event Management (SIEM) system of choice

https://docs.microsoft.com/en-us/azure/firewall/

L3-L7 Connectivity Policies
Microsoft Threat intelligence Known malicious IPS and FQDNs
NAT, Network and Application traffic filtering rules allows Inbound/Outbound access
Spoke 1
Spoke2
Spoke VNets
Central VNet
Azure Firewall
Azure to On Prem traffic filtering
Traffic is denied by default
On-Premises

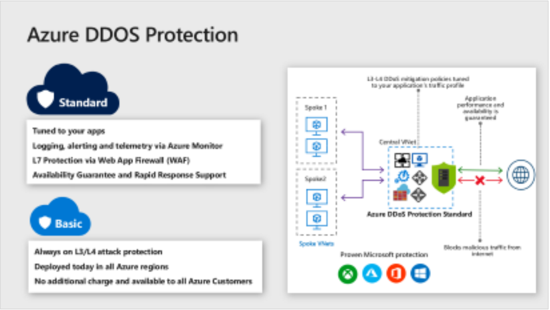


Web Application Firewall

Web application protection
- Protects your application against prevalent X-Site Scripting and SQL Injection attacks
- Blocks threats based on OWASP core rule sets 3.0 or 2.2.9
- Integrated with Azure Security Center
- Real-time logging with Azure Monitor

High availability and scalability built in and managed by platform
Layer 7 load balancing URL path, host based, round robin, session affinity, redirection
Centralized SSL management SSL offload and SSL policy
Public or ILB public internal or hybrid
Rich diagnostics Azure monitor, Log analytics

App Gateway
XSS attack
Valid request
SQL Injection
WAF
L7 LB
Valid request
Site 1
Site 2
Valid request
VPN
On Premises



Azure DDOS Protection

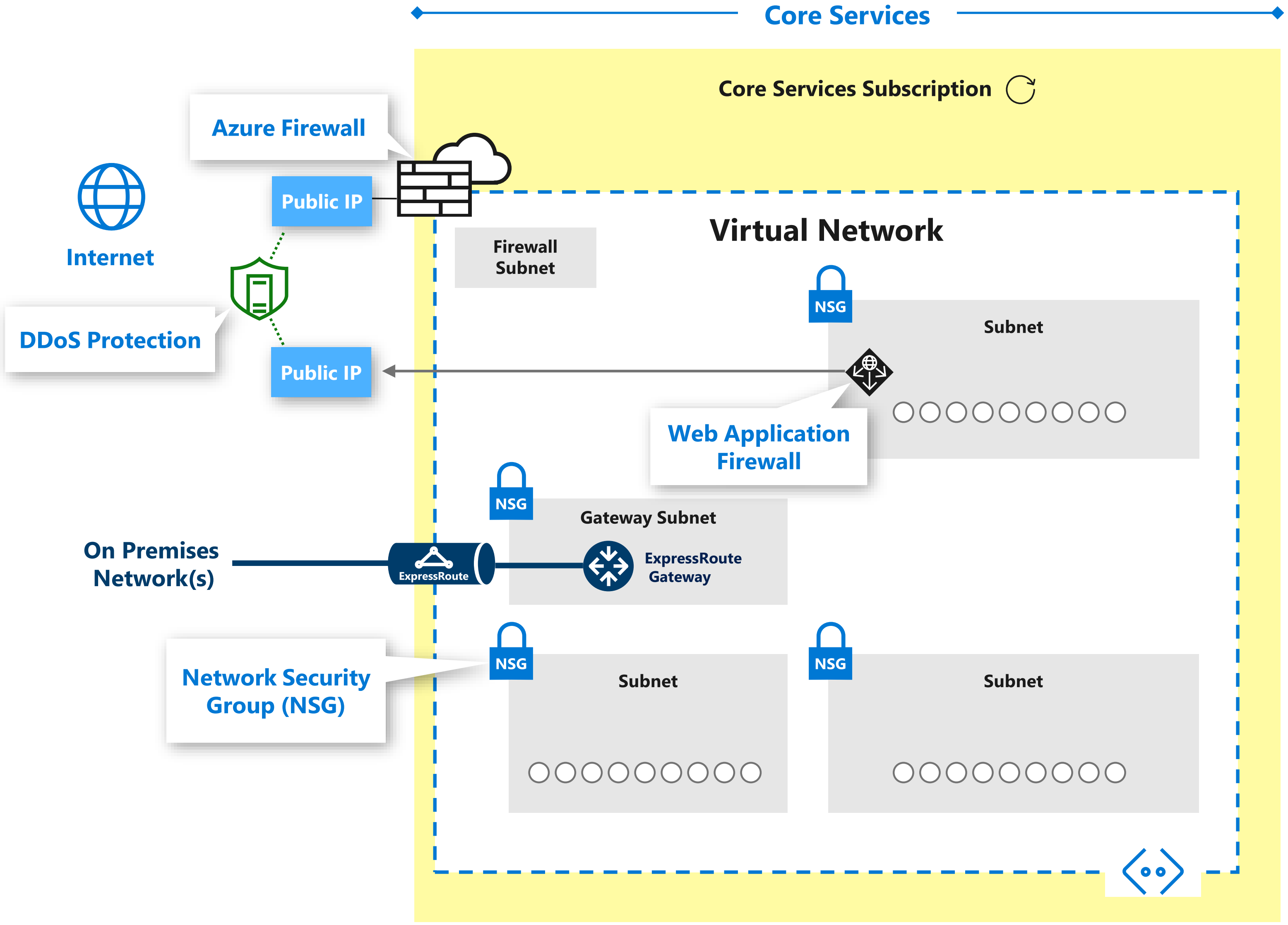
Standard

Tuned to your apps
Logging, alerting and telemetry via Azure Monitor
L7 Protection via Web App Firewall (WAF)
Availability Guarantee and Rapid Response Support

Basic

Always on L3/L4 attack protection
Deployed today in all Azure regions
No additional charge and available to all Azure Customers

L3-L4 DDoS mitigation policies tuned to your application's traffic profile
Application performance and availability is guaranteed
Spoke 1
Spoke2
Spoke VNets
Central VNet
Azure DDoS Protection Standard
Blocks malicious traffic from internet
Proven Microsoft protection



Reference Configuration with Virtual Appliance(s)

Next Generation Firewall with Integrated WAF/Proxy

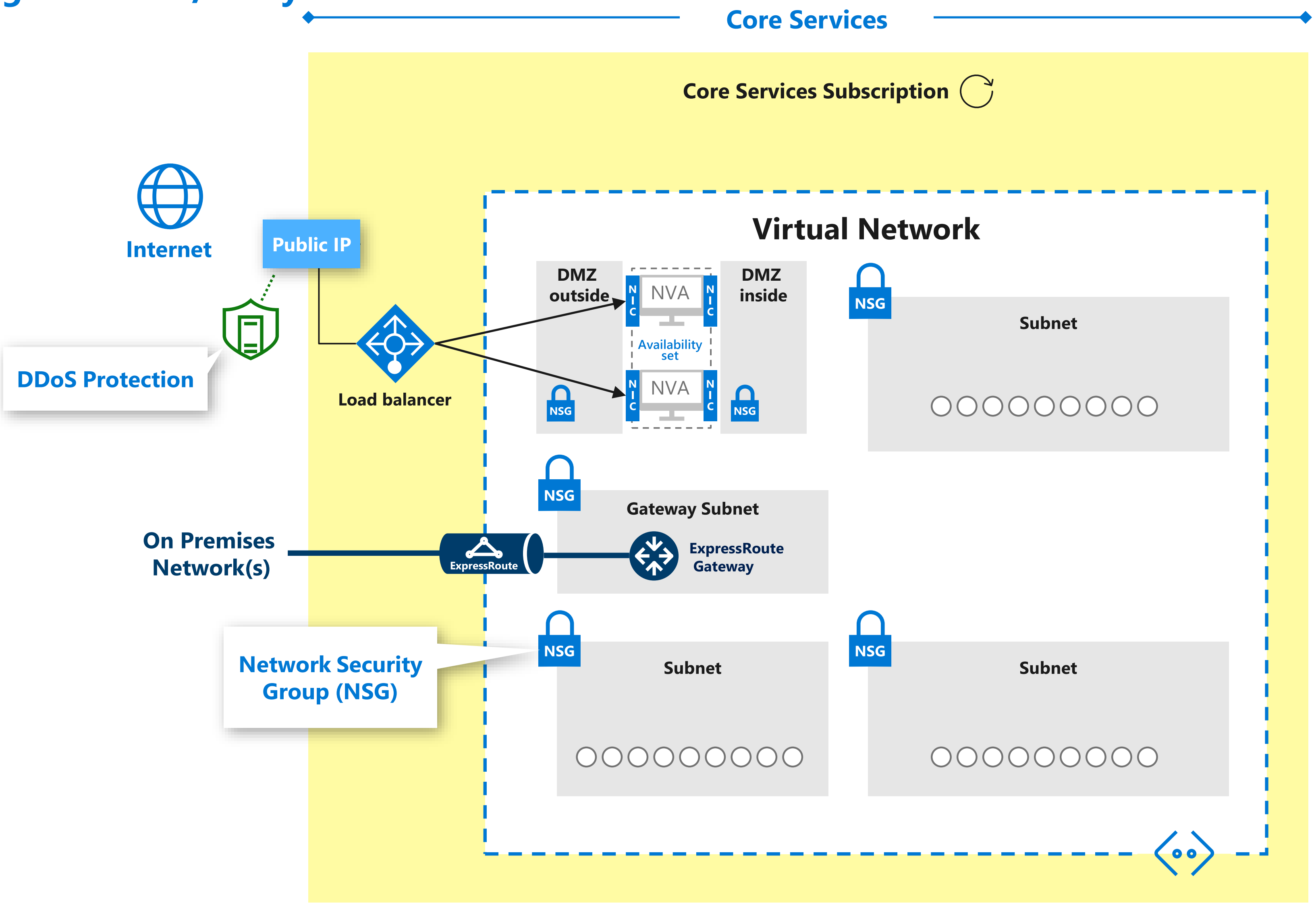
Popular Next Generation Firewalls available in Azure Marketplace

Load balancer enables scalability and availability

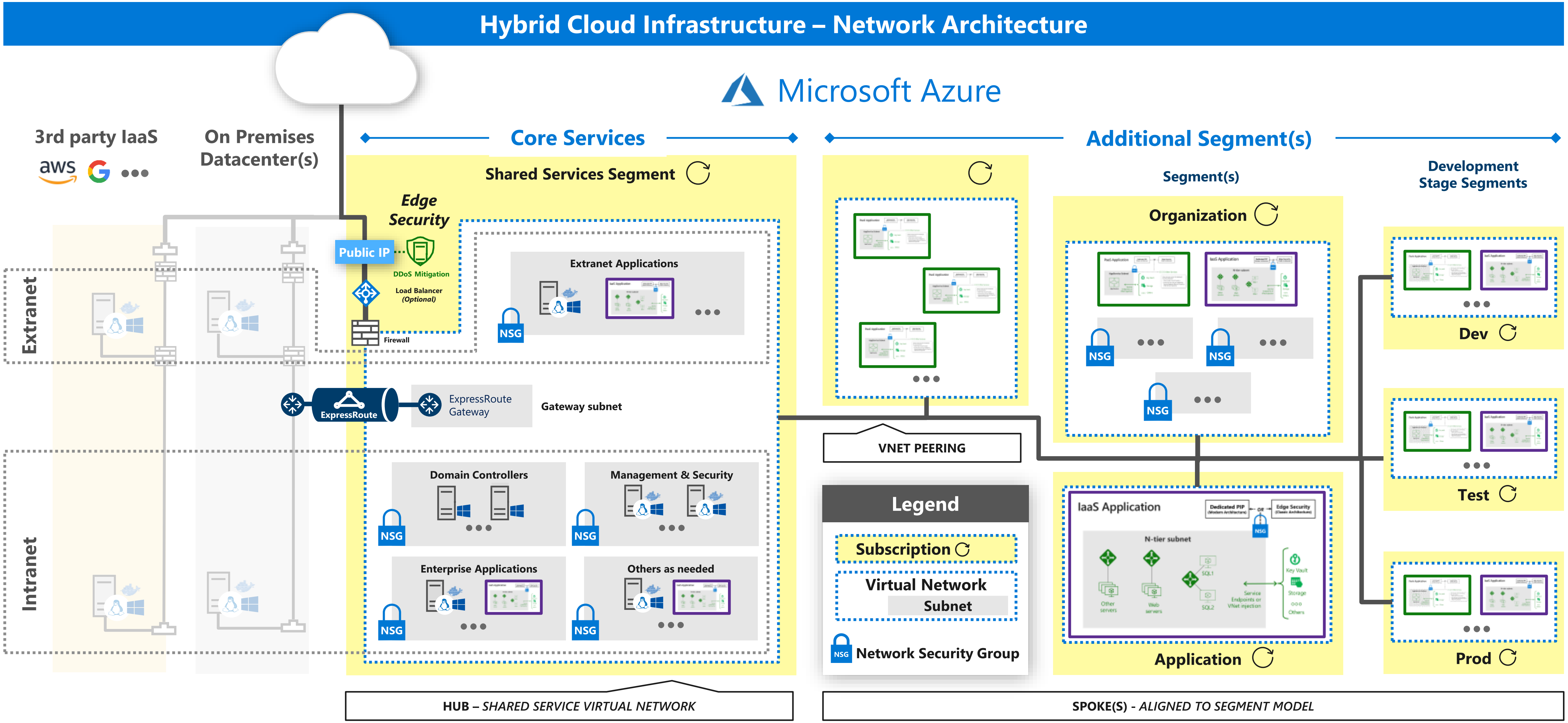
DDoS Protection Standard can be applied to public IP addresses.

More Information online

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/shared-services



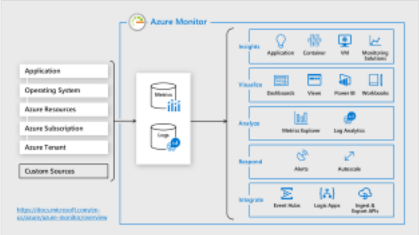
Reference Enterprise Design - Azure Network Security



Network Visibility

Security Information and Event Management (SIEM)

Azure Monitor
Log Aggregation



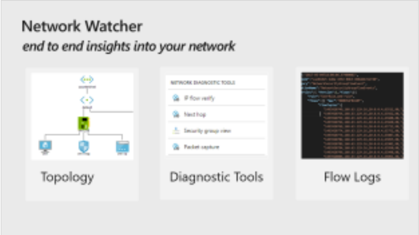
NSG Diagnostic Logs

WAF

Azure Firewall

Investigation Workflow

Network Watcher
Advanced Functions


Network Watcher

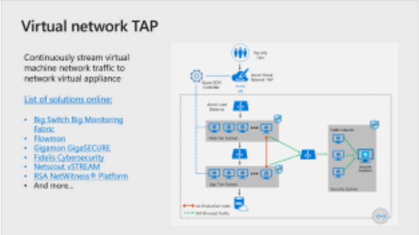
end to end insights into your network

NSG Flow Logs

Packet Capture
(Point in Time)

Analytics

Virtual Tap (Preview)
Raw Traffic Access


Virtual network TAP

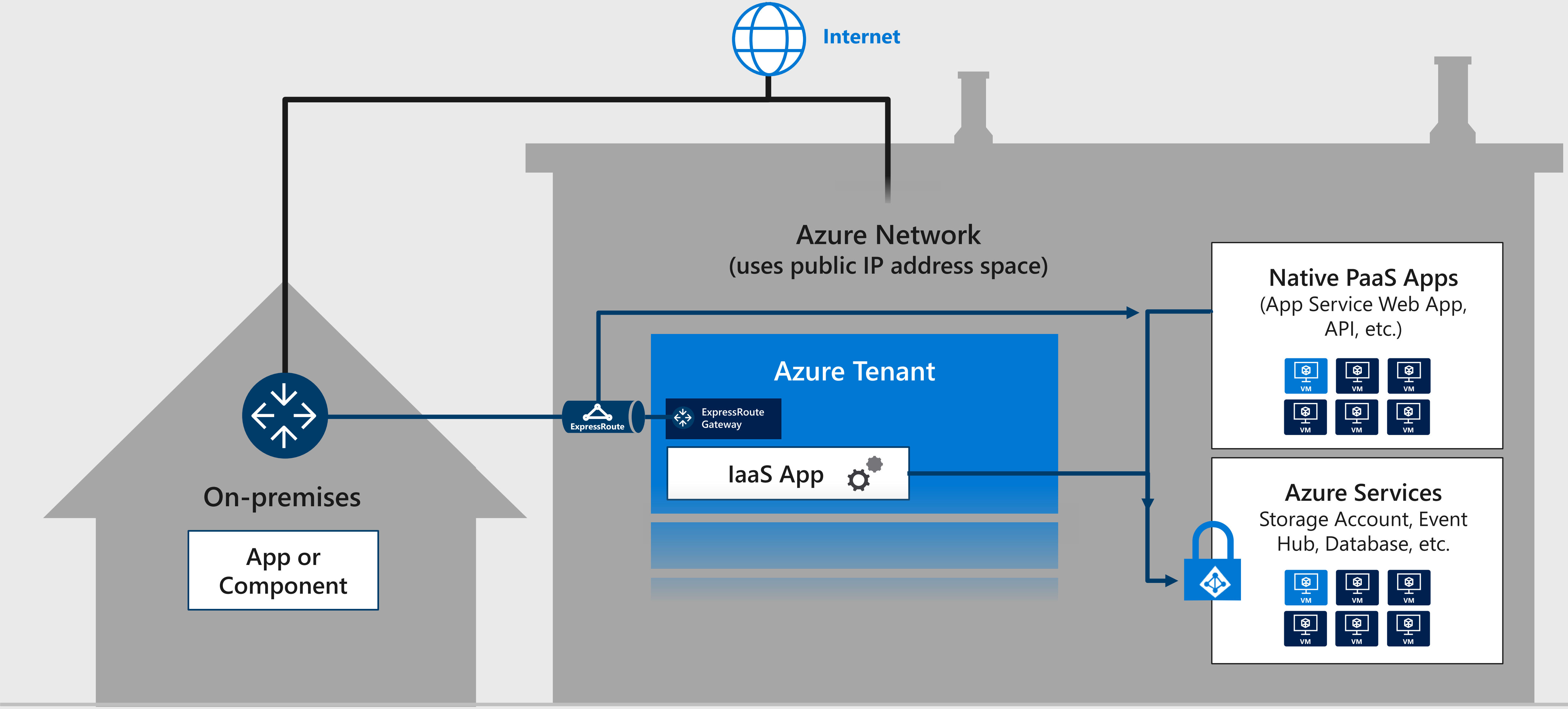
Continuously stream virtual machine network traffic to network virtual appliance

List of solutions online:

- Big Switch Big Monitoring Fabric
- Flowmon
- Gigamon GigaSECURE
- Fidelis Cybersecurity
- Netscout vSTREAM
- RSA NetWitness® Platform
- And more…

Virtual Network

Accessing Azure Services

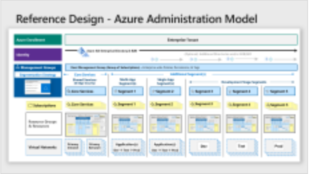


Networks & Containment – Enterprise Consistency

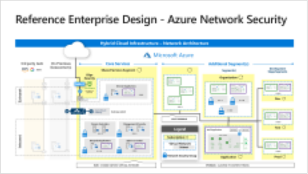
CRITICAL BEST PRACTICES

SEGMENTATION ALIGNMENT

- **What -** Align network model with overall segmentation and administrative model
- **Why** – A straightforward unified security strategy leads to less errors as it increases human understanding and automation reliability.
- **How** – Build your designs based on the reference models in this guidance



ADMINISTRATIVE



NETWORK SECURITY

CENTRAL NETWORK MANAGEMENT

- **What** – Centralize management of core network functions like ExpressRoute, virtual network and subnet provisioning, IP addressing, and related items.
- **How –** Recommend using an existing on premises process if applicable. This is typically a central networking group or a council of key stakeholder groups from business units.

CENTRALIZED NETWORK SECURITY

- **What** – Centralize governance and of network security elements such as Network virtual appliances functions like ExpressRoute, virtual network and subnet provisioning, IP addressing, etc.
- **How** – Recommend using an existing on premises process if applicable. This is typically a central networking group or a council of key stakeholder groups from business units.

- **Why –** Inconsistent strategy and management of these core functions can create significant security risks that an attacker can exploit

Networks and Containment

PRAGMATIC CONTAINMENT STRATEGY

- **What –** Build a risk containment strategy that blends the best available approaches
  - **Existing controls** and practices
  - **Native controls** available in Azure
  - **Zero trust** approaches to continuous validate
- **Why** – Containment of attack vectors within an environment is critical, but traditional approaches aren't enough and must evolve. Consistency of controls across on-premises and cloud infrastructure is important, but defenses are more effective and manageable when leveraging native azure security controls, dynamic (just in time) approaches, and integrated identity/password controls (e.g. zero trust / continuous validation)

Network Security Groups (NSGs) for subnets

Use Network Security Groups to protect against unsolicited traffic into Azure Subnets (replaces/supplements East-West traffic controls)

Choose host-based firewall strategy

Choose whether to continue existing practices for host-based firewalls in Azure or discontinue their use.

Zero Trust approach for new micro/segmentation initiatives

Adopt Zero-trust based approaches for new initiatives that validate trust at access time (instead of static network IP/Port controls)

1. **Conditional Access** to resources based on device, identity, assurance, network location, and more. More Info
2. **Just in Time Management Port Access –** using Azure Security Center to enable access only after workflow approval
3. **Just in Time Administrative Privileges –** using Azure AD PIM or a 3rd party PIM/PAM solution
4. **Just in Time Local Admin Account Access –** using Local Admin Password Solution (LAPS) or a 3rd party PIM/PAM solution

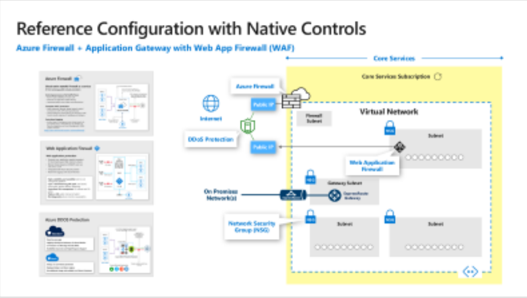
Networks and Containment

CRITICAL BEST PRACTICES

INTERNET EDGE STRATEGY

- **What** – Choose whether to use Native Azure Controls or 3rd party Network Virtual Appliances (NVAs) for internet edge security (North-South)
- **Why** – Legacy workloads require network protection from internet sources and there are advantages to using either 1st or 3rd party controls to provide this.
- **How** – Select a strategy using the comparison information →

Note – Some organizations choose a hybrid configuration where some VNets use advanced 3rd party controls and others use native controls



Reference Configuration with Native Controls

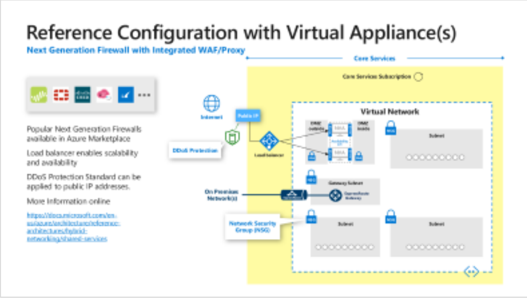
Azure Firewall + Application Gateway with Web App Firewall (WAF)

AZURE NATIVE CONTROLS

Basic capabilities with simple integration & management

Azure Firewall + Web App Firewall (in Application Gateway)

These offer basic security that is good enough for some scenarios with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration



Reference Configuration with Virtual Appliance(s)

Next Generation Firewall with Integrated WAF/Proxy

Popular Next Generation Firewalls available in Azure Marketplace

Load balancer enables scalability and availability

DDoS Protection Standard can be applied to public IP addresses.

More Information online

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/shared-services

3RD PARTY CAPABILITIES

Advanced security capabilities from existing vendors

Next Generation Firewall (NGFW) and other 3rd party offerings

Network virtual appliances in the Azure Marketplace include familiar security tools that provide enhanced network security capabilities

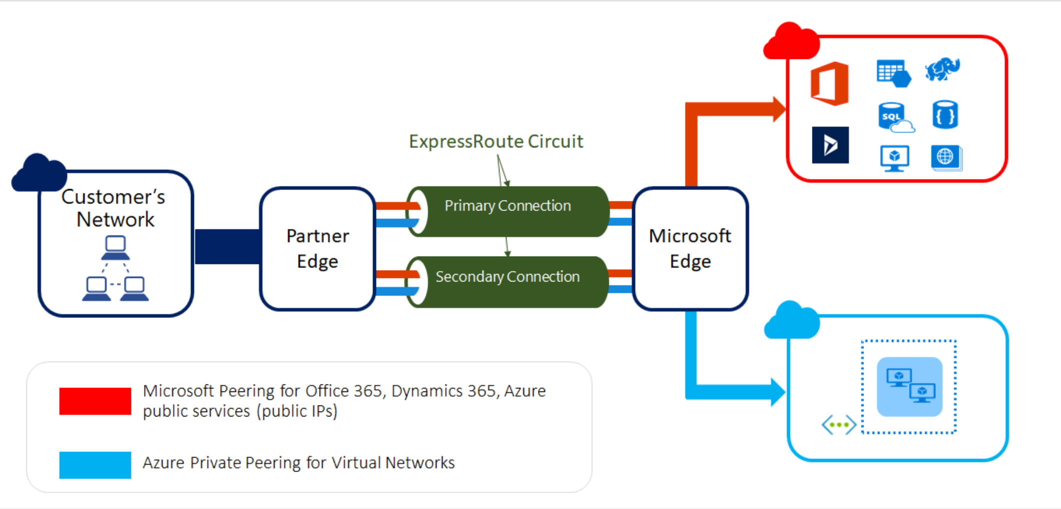
Configuration is more complex, but allows you to leverage existing capabilities, and skillets

Networks

CRITICAL CHOICE

EXPRESSROUTE TERMINATION

- **What** – Identify where to terminate ExpressRoute private peering (or Site to Site VPN) in existing (on-premises) network
- **Why** – The termination point can affect firewall capacity, scalability, reliability, and network traffic visibility
- **How** –
  - **Terminate outside the firewall** *(DMZ Paradigm)* If you require visibility into the traffic, continue an existing practice of isolating datacenters, or if you are solely putting extranet resources on Azure.
  - **Terminate inside the firewall** *(Network Extension Paradigm - Default Recommendation)* In all other cases, recommend treating Azure as a Nth datacenter


Customer's Network
Partner Edge
ExpressRoute Circuit
Primary Connection
Secondary Connection
Microsoft Edge
🟥 Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
🟦 Azure Private Peering for Virtual Networks

https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Network – Deprecating Legacy Technology

CRITICAL CHOICES

CLASSIC NETWORK INTRUSION DETECTION/PREVENTION SYSTEMS (NIDS/NIPS)

- **What** – Choose whether to add existing NIDS/NIPS capabilities on Azure
- **Why** – The Azure platform already filters malformed packets and most classic NIDS/NIPS solutions are typically based on outdated signature-based approaches which are easily evaded by attackers and typically produce high rate of false positives.
- **How** –
  - **Do Not Add (Default Recommendation)**
  - **Add to Azure tenant**

NETWORK DATA LOSS PREVENTION (DLP)

- **What** – Choose whether to add Network DLP capabilities on Azure
- **Why** – Network DLP is increasingly ineffective at identifying both inadvertent and deliberate data loss. This is because most modern protocols and most attackers use encryption (most available attacker toolkits have encryption built in)
- **How** –
  - **Do Not Add (Default Recommendation)**
  - **Add to Azure tenant**

Networks and Containment – Subnet & NSG Design

DESIGN VIRTUAL NETWORKS & SUBNETS FOR GROWTH

- **What** – Avoid provisioning small virtual networks and subnets
- **Why** – Most organizations add more resources than initially planned on top of VNets and subnets, triggering a labor-intensive re-allocation of addresses. There is limited security value in small subnet size + increased overhead to map an NSG to each.
- **How** – Define subnets broadly to ensure that you have flexibility for growth. A rule of thumb is to assume you will migrate all enterprise resources to Azure as an end state.

APPLICATION SECURITY GROUPS (ASGs)

- **What** – Simplify NSG rule management by defining application security groups (ASGs)
- **Why** – While their use is not required, defining ASGs allow you to simplify setup and maintenance of NSG rules.
- **How** – Define an ASG for lists of IP addresses that you expect may
  - Change in the future
  - Be used across many NSGs

Ensure to name them clearly for others to understand their content/purpose.

AVOID FULLY OPEN ALLOW RULES

- **What** – Don't assign allow rules with extremely broad ranges (e.g. allow 0.0.0.0 -255.255.255.255)
- **Why** – These lead to a false sense of security and are frequently found and exploited by red teams.
- **How** – Ensure your troubleshooting procedures discourage or ban these "fully open" allow rules

Discover these issues with Network Security Watcher and correct them

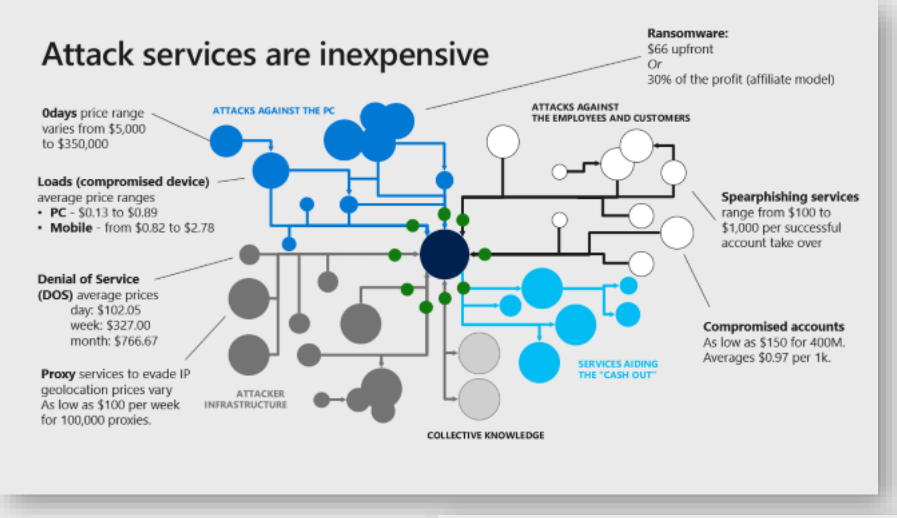
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-auditing-powershell

Networks and Containment – DDoS Mitigations

GENERAL GUIDANCE

DDoS MITIGATIONS

- **What –** Enable DDoS Mitigations for all business-critical web applications, and services
- **Why** – DDoS attacks are prevalent and are very inexpensive to access on the dark markets
- **How** – Evaluate and select the best option for protecting your critical applications and services
  - Azure DDoS basic
  - Azure DDoS standard
  - **3rd party service**



Attack services are inexpensive

0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges
- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

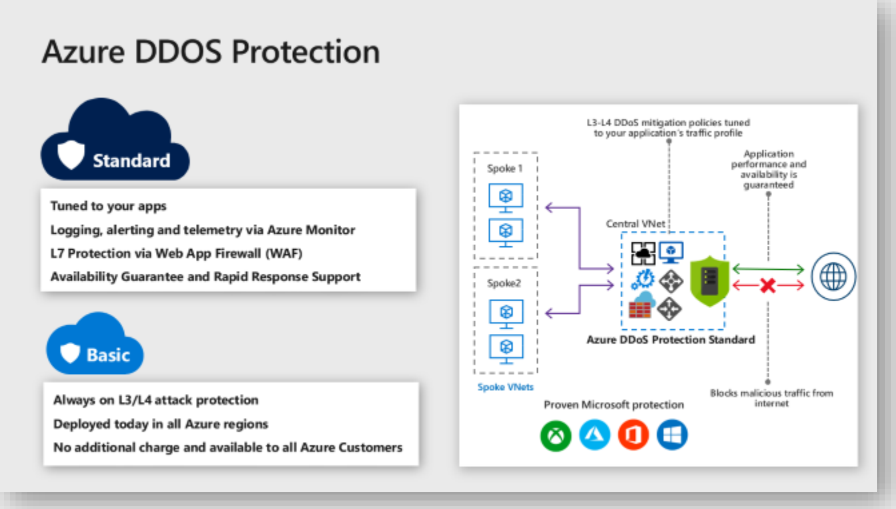
Proxy services to evade IP geolocation prices vary As low as $100 per week for 100,000 proxies.

Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts As low as $150 for 400M. Averages $0.97 per 1k.

ATTACKS AGAINST THE PC
ATTACKS AGAINST THE EMPLOYEES AND CUSTOMERS
ATTACKER INFRASTRUCTURE
COLLECTIVE KNOWLEDGE
SERVICES AIDING THE "CASH OUT"



Azure DDOS Protection

Standard

- Tuned to your apps
- Logging, alerting and telemetry via Azure Monitor
- L7 Protection via Web App Firewall (WAF)
- Availability Guarantee and Rapid Response Support

Basic

- Always on L3/L4 attack protection
- Deployed today in all Azure regions
- No additional charge and available to all Azure Customers

L3-L4 DDoS mitigation policies tuned to your application's traffic profile
Application performance and availability is guaranteed
Spoke 1
Spoke2
Spoke VNets
Central VNet
Azure DDoS Protection Standard
Blocks malicious traffic from internet
Proven Microsoft protection

Networks and Containment – Egress/Ingress

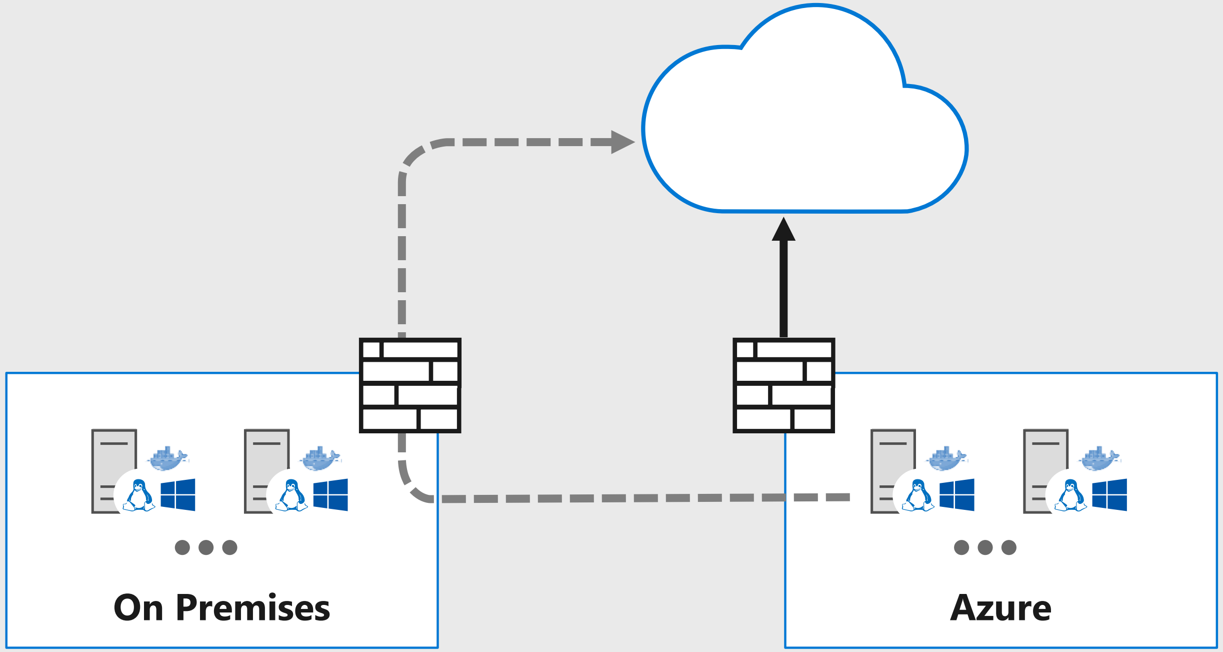
GENERAL GUIDANCE

NETWORK INGRESS/EGRESS SECURITY

- **What** – Choose whether to route Azure ingress/egress traffic through on-premises network edge security or via security hosted on Azure
- **Why** – Routing all internet traffic for Azure through on-premises ingress/egress points can add significant cost and latency at scale.
- **How** – Choose

↑ **Direct Internet (Default recommendation)** - Route traffic directly to internet using Azure hosted network edge security.

↱ **"Hairpin" (Not recommended) -** Route all traffic through existing network edge security on premises. with forced tunneling on Azure ExpressRoute or Site-to-Site VPN



Traffic hairpin approach fits a *Datacenter Expansion* paradigm and works well for a quick proof of concept, but scales poorly because of the increased traffic load/latency and cost.

Direct Internet approach fits a *N^{th} Datacenter* paradigm and scales much better for an enterprise deployment as it removes unnecessary hops.

Network – Advanced Visibility

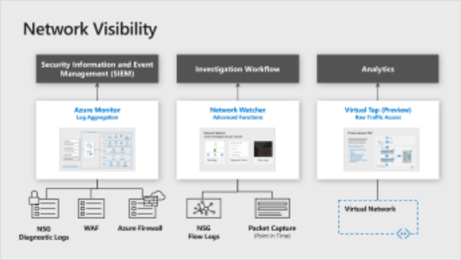
GENERAL GUIDANCE

BEST PRACTICE CHOICE

Network Logs

As required, integrate network logs into SIEM / analytics platform using Azure Monitor

- NSG Logs
- WAF Logs
- Azure Firewall Logs



NSG Flow Logs

If you do this today, Integrate NSG flow logs and packet capture (via Network Watcher) into your investigation workflow

Virtual TAP

If required, integrate virtual TAP into existing network monitoring program/analytics capability

Information Protection & Storage

Architecture guidance on this topic can be found at

https://docs.microsoft.com/en-us/azure/architecture/security/storage-data-encryption

Azure Storage

Azure Cloud Storage:

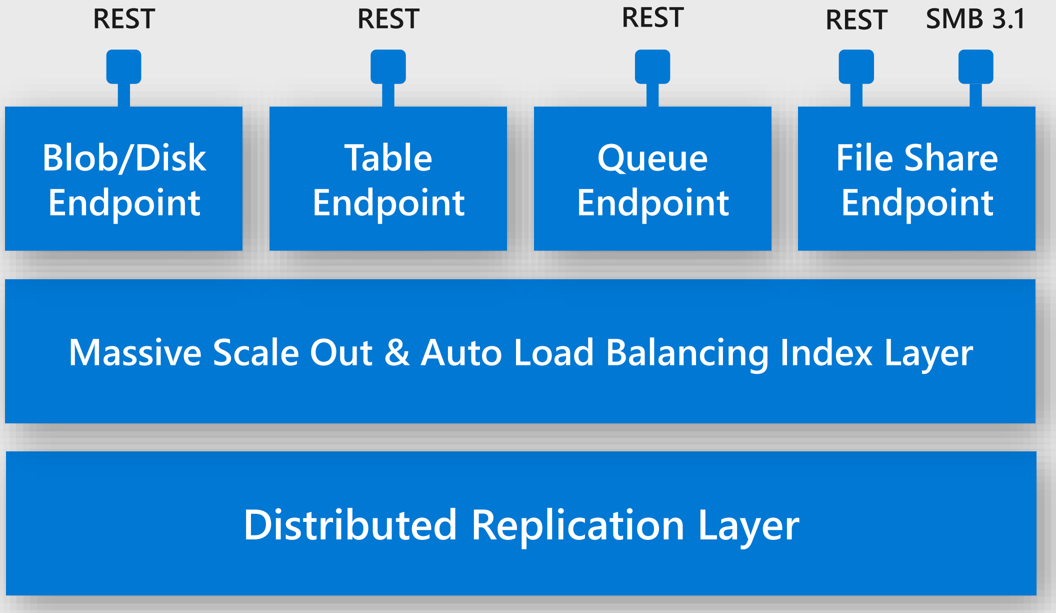
- Object based, durable, massively scalable storage
- Designed from ground up by Microsoft
- Presents as Blobs, Disks, Tables, Queues and Files
- Accessed via REST APIs, Client Libraries and Tools

Access Control

- Azure Active Directory (Azure AD)
- Symmetric Shared Key Authentication
- Shared Access Signature (SAS)

Notable Security Attributes

- All data is encrypted by the service
- No read without write (mitigate cross-tenant data leaks)
- Maintains 3 Synchronous copies of data
- Virtual storage, not dedicated disks
- Detailed activity logging availability (Opt in)
- Data will remain only in the region you choose



REST

REST

REST

REST

SMB 3.1

Blob/Disk Endpoint

Table Endpoint

Queue Endpoint

File Share Endpoint

Massive Scale Out & Auto Load Balancing Index Layer

Distributed Replication Layer

More Information

Storage System Design and Architecture:

Azure Storage Managed Disks

Azure Storage Firewalls

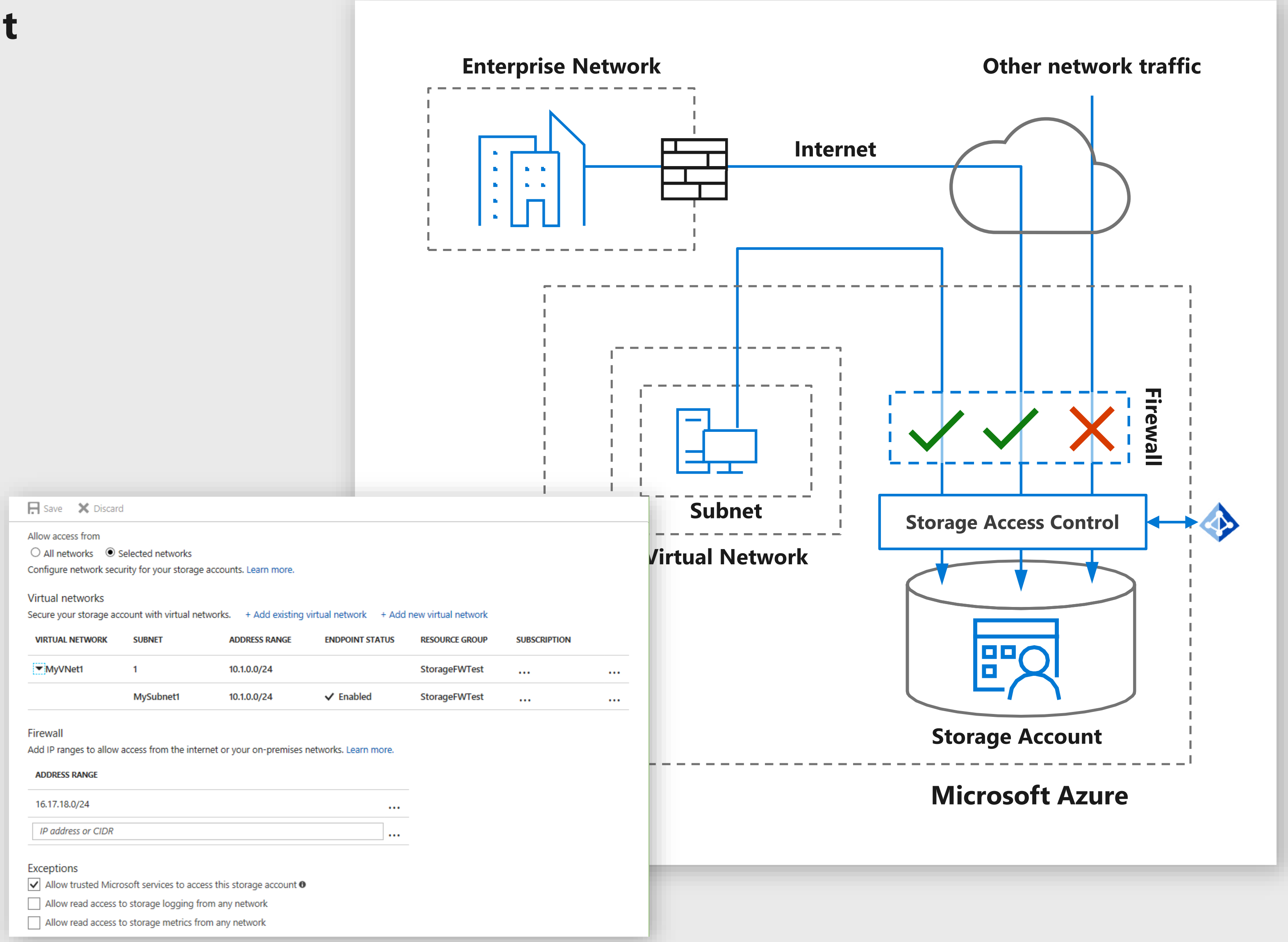
Configured on each Storage Account
(prompt during creation)

- Controls network access using ACLs
- Enforced on all network protocols
- If not configured, all networks can access

Authentication is still required
to access storage (Azure AD, SAS tokens, etc.)

Access by Azure Services
must be configured to allow connection (checkbox)

- VM Access to VM Disks not affected by storage firewall
- https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security



Save Discard

Allow access from

○ All networks ● Selected networks

Configure network security for your storage accounts. Learn more.

Virtual networks

Secure your storage account with virtual networks. + Add existing virtual network + Add new virtual network

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION	
MyVNet1	1	10.1.0.0/24		StorageFWTest	...	...
	MySubnet1	10.1.0.0/24	✓ Enabled	StorageFWTest	...	...

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

ADDRESS RANGE	
16.17.18.0/24	...
IP address or CIDR	...

Exceptions

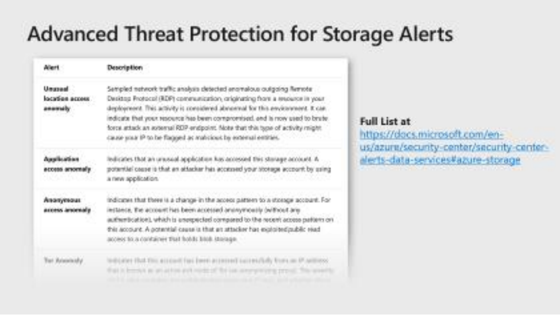
☑ Allow trusted Microsoft services to access this storage account

□ Allow read access to storage logging from any network

□ Allow read access to storage metrics from any network

Advanced Threat Protection for Azure Storage

- Alerts on **anomalous access** & potential **data exfiltration**
- Investigation & remediation guidance
- Alerts in Azure Security Center

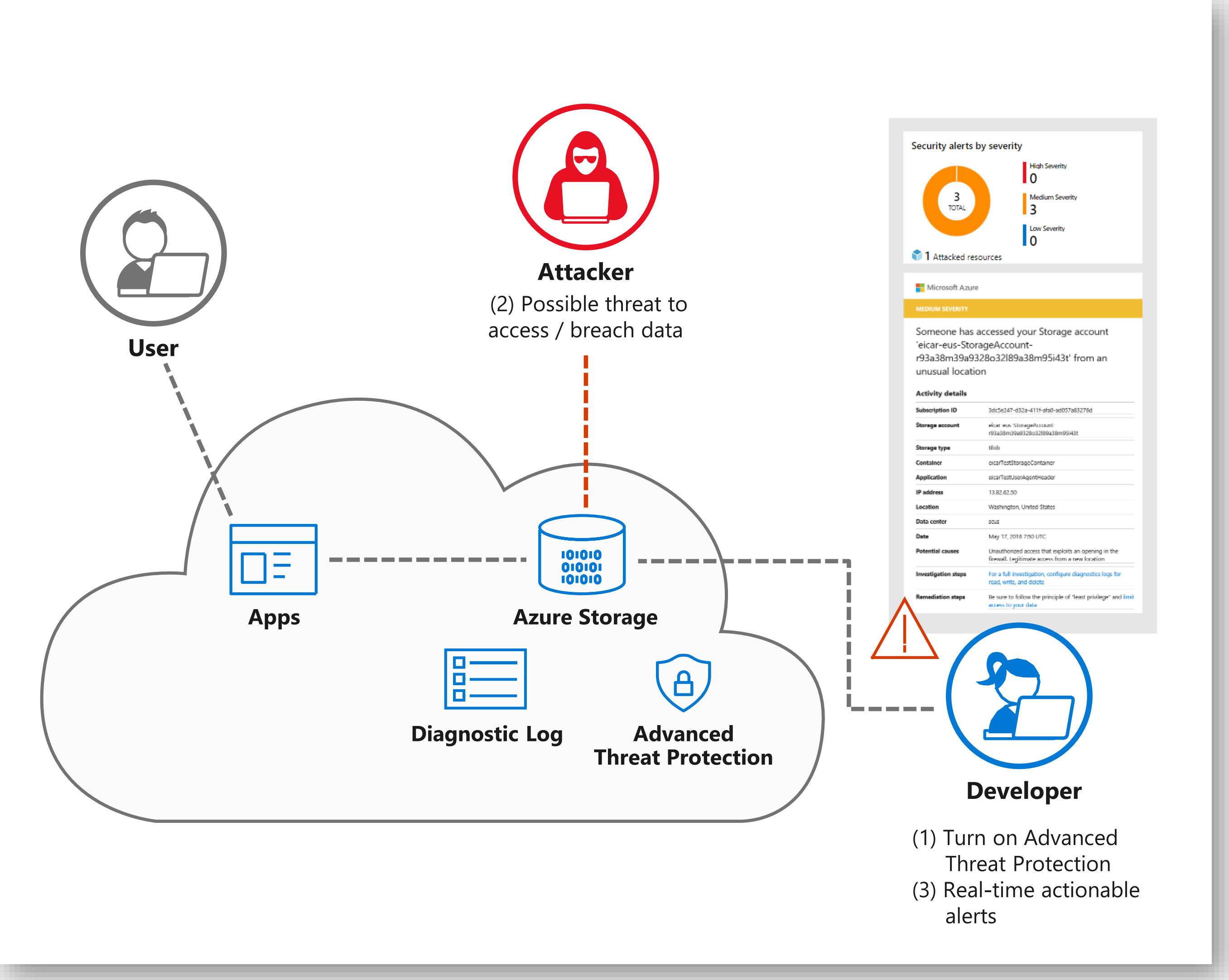


Advanced Threat Protection for Storage Alerts

Alert	Description
Unusual location access anomaly	Sampled network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication, originating from a resource in your deployment. This activity is considered abnormal for this environment. It can indicate that your resource has been compromised, and is now used to brute force attack an external RDP endpoint. Note that this type of activity might cause your IP to be flagged as malicious by external entities.
Application access anomaly	Indicates that an unusual application has accessed this storage account. A potential cause is that an attacker has accessed your storage account by using a new application.
Anonymous access anomaly	Indicates that there is a change in the access pattern to a storage account. For instance, the account has been accessed anonymously (without any authentication), which is unexpected compared to the recent access pattern on this account. A potential cause is that an attacker has exploited public read access to a container that holds blob storage.
Tor Anomaly	Indicates that this account has been accessed successfully from an IP address that is known as an active exit node of Tor [illegible]

Full List at https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-data-services#azure-storage

https://docs.microsoft.com/en-us/azure/storage/common/storage-advanced-threat-protection


User
Attacker
(2) Possible threat to access / breach data
Apps
Azure Storage
Diagnostic Log
Advanced Threat Protection
Developer
(1) Turn on Advanced Threat Protection
(3) Real-time actionable alerts

Security alerts by severity

3 TOTAL

High Severity 0

Medium Severity 3

Low Severity 0

1 Attacked resources

Microsoft Azure

MEDIUM SEVERITY

Someone has accessed your Storage account 'eicar-eus-StorageAccount-r93a38m39a9328o32l89a38m95i43t' from an unusual location

Activity details

Subscription ID	3dc5e247-d32a-411f-afa0-ad057a83276d
Storage account	eicar-eus-StorageAccount-r93a38m39a9328o32l89a38m95i43t
Storage type	Blob
Container	eicarTestStorageContainer
Application	eicarTestUserAgentHeader
IP address	13.82.62.50
Location	Washington, United States
Data center	eus
Date	May 17, 2018 7:50 UTC
Potential causes	Unauthorized access that exploits an opening in the firewall. Legitimate access from a new location
Investigation steps	For a full investigation, configure diagnostics logs for read, write, and delete
Remediation steps	Be sure to follow the principle of "least privilege" and limit access to your data

Azure Data Encryption

Encryption is not a panacea

Encryption is not a panacea

Encryption helps (consolidate) the data protection problem, but **you must protect and manage keys** to be successful

Restrict Access to Data
Large high-variability problem

Encryption

Restrict Access to Key(s)
Smaller "fixed-length" problem

Encrypted data can flow more freely but access to keys must both
- **Enable productivity** (to ensure users encrypt data)
- **Mitigate risk** (of both keys and data being stolen)

Layers (and why each is important)

Encrypt Documents and unstructured data

- Regulatory requirements
- Data Leakage (malicious or inadvertent)

Application Layer Encryption

- Meet regulatory requirements
- Mitigate against attacks on cloud provider/infrastructure

Azure Service Encryption

- Same as application layer
- Near zero management effort (for Microsoft managed key)

Virtual Machine / Operating Systems

- Mitigate against loss/leakage of VM Disks from storage account

Storage System

- Mitigate against attacks on cloud provider/infrastructure
- On by default and unable to disable

Encryption Technologies

- Azure Information Protection (AIP) or 3rd party solutions

- **BYO Encryption** - .NET Libraries, client-side encryption, etc.

- **SQL** Transparent Data Encryption, Always Encrypted>
- **HDInsight** Encryption
- **Azure Backup** Encrypted at Rest**,** Encrypted VM support

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

- **Azure Storage Service Encryption (server side encryption)** *<AES-256, Block, Append, and page Blobs>*

Storage and Encryption

CRITICAL GUIDANCE

▲ BEST PRACTICE ● CHOICE

USE AZURE AD FOR STORAGE AUTH

- **What** – Use Azure AD for authenticating access to storage unless another method is required and there is no other option
- **Why** – Azure AD provides flexible role-based access control while providing accountability
- **How** – Configure Storage objects to use Azure AD Authentication

https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad

ENABLE VM DISK ENCRYPTION

- **What** – Enable disk encryption on all IaaS VMs
- **Why** – This provides mitigation against data leakage from a VM disk being downloaded directly from storage (because of configuration error, etc.)
- **How** – Configure disk encryption on all Windows and Linux VMs

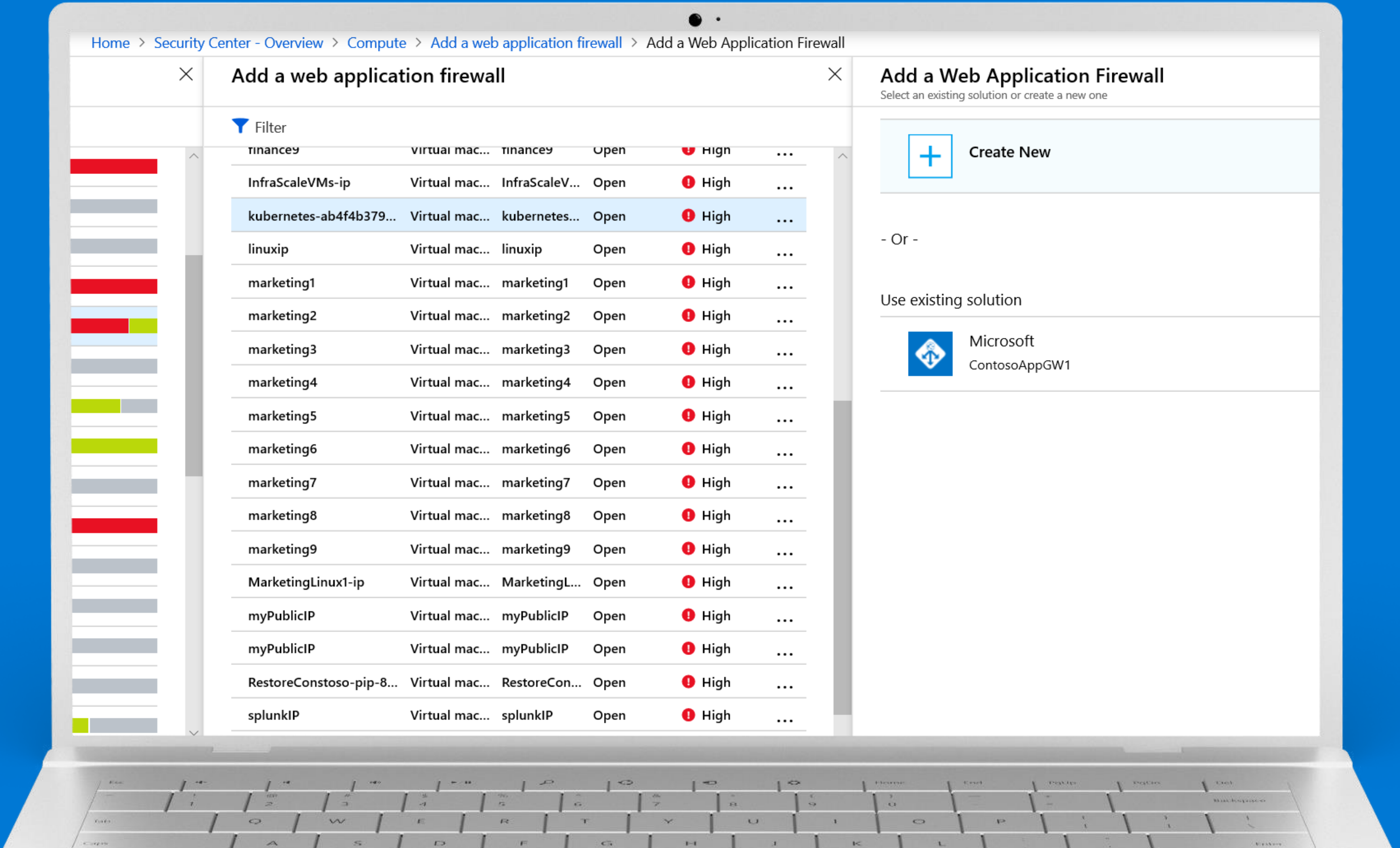
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

ENABLE ENCRYPTION IN AZURE AND CLOUD SERVICES

- **What** – Enable built in encryption features for any Azure services as well as 3rd party services you call from Azure applications.
- **Why** – Typically near zero overhead for using integrated encryption features
- **How** – See the table in the link below for which services offer encryption:

https://docs.microsoft.com/en-us/azure/security/azure-security-encryption-atrest

Azure Security Center - Remediation



Home > Security Center - Overview > Compute > Add a web application firewall > Add a Web Application Firewall

Add a web application firewall

Filter

finance9	Virtual mac...	finance9	Open	High	...
InfraScaleVMs-ip	Virtual mac...	InfraScaleV...	Open	High	...
kubernetes-ab4f4b379...	Virtual mac...	kubernetes...	Open	High	...
linuxip	Virtual mac...	linuxip	Open	High	...
marketing1	Virtual mac...	marketing1	Open	High	...
marketing2	Virtual mac...	marketing2	Open	High	...
marketing3	Virtual mac...	marketing3	Open	High	...
marketing4	Virtual mac...	marketing4	Open	High	...
marketing5	Virtual mac...	marketing5	Open	High	...
marketing6	Virtual mac...	marketing6	Open	High	...
marketing7	Virtual mac...	marketing7	Open	High	...
marketing8	Virtual mac...	marketing8	Open	High	...
marketing9	Virtual mac...	marketing9	Open	High	...
MarketingLinux1-ip	Virtual mac...	MarketingL...	Open	High	...
myPublicIP	Virtual mac...	myPublicIP	Open	High	...
myPublicIP	Virtual mac...	myPublicIP	Open	High	...
RestoreConstoso-pip-8...	Virtual mac...	RestoreCon...	Open	High	...
splunkIP	Virtual mac...	splunkIP	Open	High	...

Add a Web Application Firewall

Select an existing solution or create a new one

- Or -

Use existing solution

Microsoft
ContosoAppGW1

Microsoft and CIS Partnership

Goal

Simplify and drive consistency in our customers' efforts to securely deploy workloads to Azure

Benefits

CIS brings independence and consensus driven approach

Benchmarks informed by Microsoft's experience & best practices

Microsoft

CIS™ Center for Internet Security®

What are CIS Benchmarks?

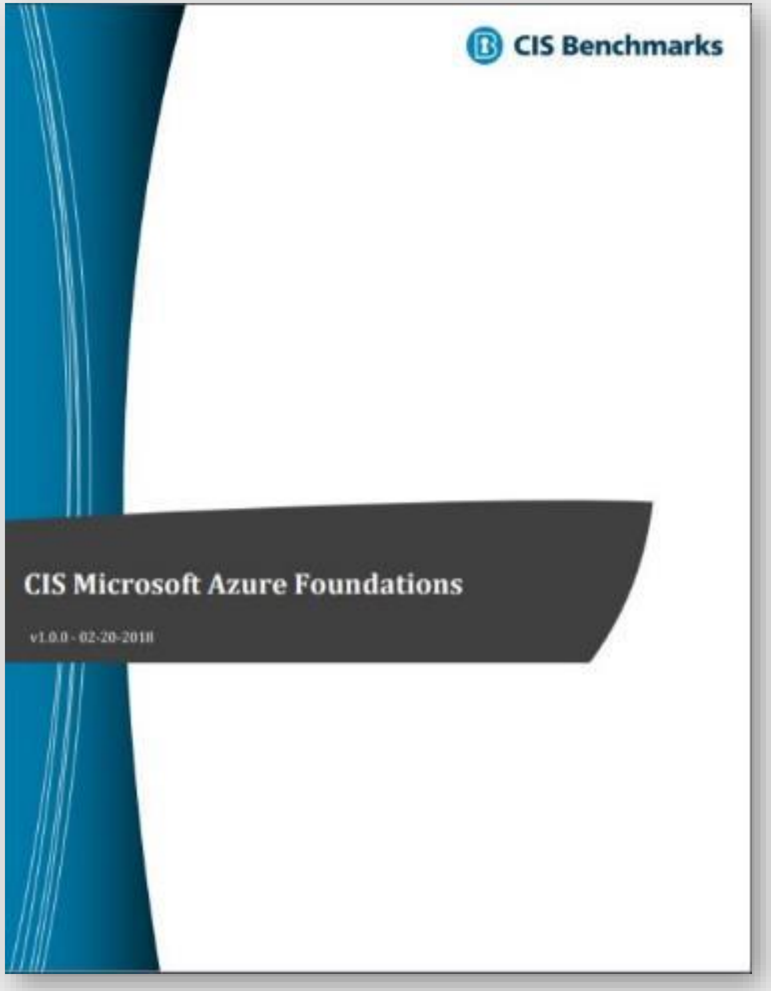
Consensus Based Best Practices

Over 100 benchmarks covering 14 technology groups

Examples:

- Ensure Multi-factor Auth is Enabled
- Ensure SSH access is restricted
- Ensure that 'Data disks' are encrypted

https://azure.microsoft.com/en-us/resources/cis-microsoft-azure-foundations-security-benchmark/



CIS Benchmarks

CIS Microsoft Azure Foundations

v1.0.0 - 02-20-2018

What's inside a CIS benchmark?

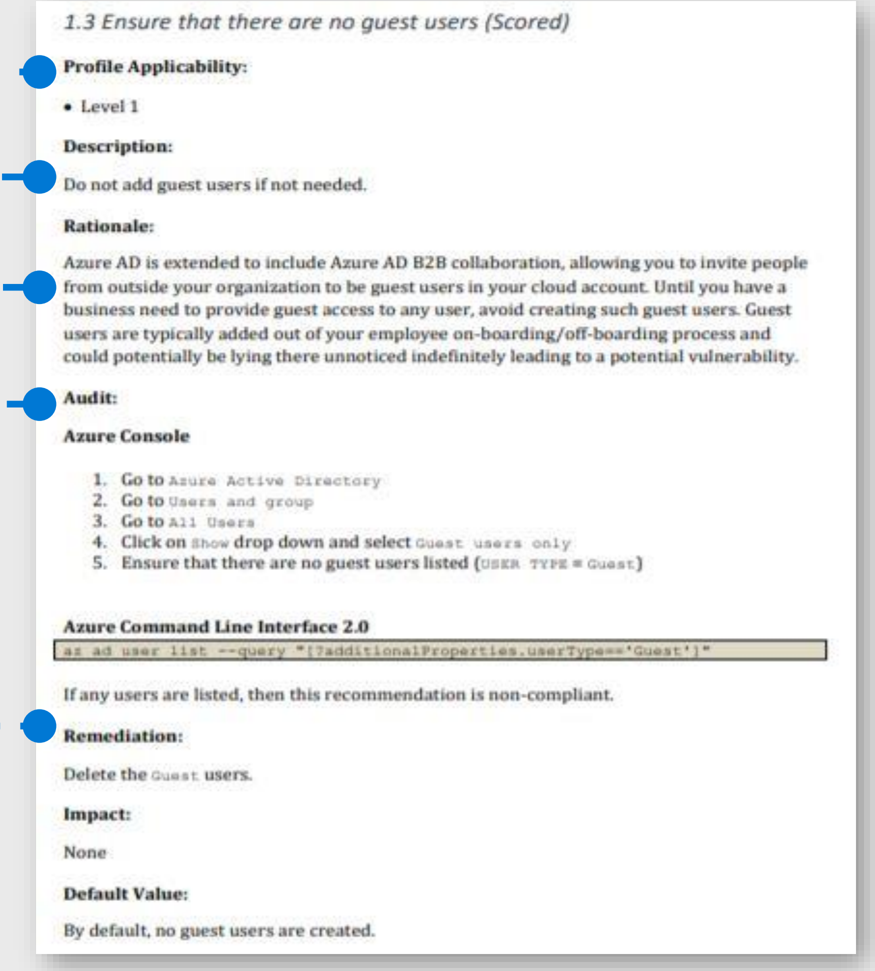
What it applies to...

What to do...

Why to do it...

How to audit...

How to fix...



1.3 Ensure that there are no guest users (Scored)

Profile Applicability:

- Level 1

Description:

Do not add guest users if not needed.

Rationale:

Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account. Until you have a business need to provide guest access to any user, avoid creating such guest users. Guest users are typically added out of your employee on-boarding/off-boarding process and could potentially be lying there unnoticed indefinitely leading to a potential vulnerability.

Audit:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Show` drop down and select `Guest users only`
5. Ensure that there are no guest users listed (`USER TYPE = Guest`)

Azure Command Line Interface 2.0

```
az ad user list --query "[?additionalProperties.userType=='Guest']"
```

If any users are listed, then this recommendation is non-compliant.

Remediation:

Delete the `Guest` users.

Impact:

None

Default Value:

By default, no guest users are created.

Summary of CIS Controls v1.0

MAIN MENU

Section	Recommendations	Control Count
Identity & Access Mgmt.	Setting the appropriate IAM policies	23
Azure Security Center	Configuration and use of Azure Security Center	19
Storage Accounts	Setting storage account policies	7
Azure SQL Services	Securing Azure SQL Servers	8
Azure SQL Databases	Securing Azure SQL Databases	8
Logging/Monitoring	Setting logging & monitoring policies on Azure subscriptions	13
Networking	Securely configuring Azure networking settings and policies	5
Virtual Machines	Setting security policies for Azure compute services, specifically virtual machines	6
Other	General security and operational controls, including those related to Azure Key Vault and Resource Locks	3
	Total Recommendations	**92**