Microsoft

Microsoft Identity platform Developer training

Irina Kostina

Irina.Kostina@Microsoft.com

Cloud Solution Architect

Bojan Magusic

Bojan.Magusic@microsoft.com

Cloud Solution Architect

Microsoft

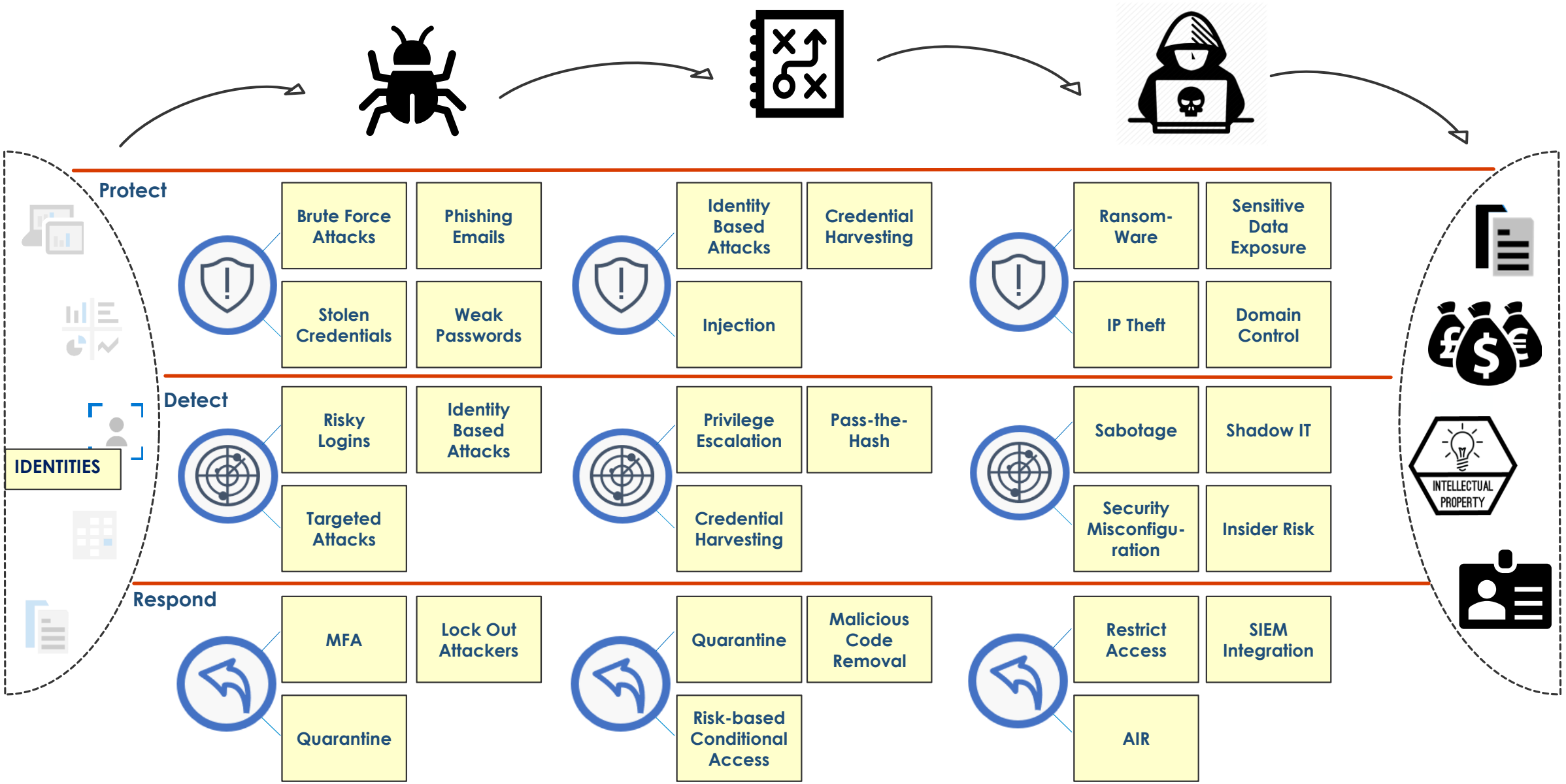
Modern Identity – 6 – Best practices for securing your services

Irina Kostina, Bojan Magusic

Why is this important?

On May 13, 2017, attackers began a cyberattack on Equifax. The attack lasted for 76 days. The attackers dropped "web shells" (a web-based backdoor) to obtain remote control over Equifax's network. They found a file containing unencrypted credentials (usernames and passwords), enabling the attackers to access sensitive data outside of the ACIS environment. The attackers were able to use these credentials to access 48 unrelated databases.

https://web.archive.org/web/20181219201616/https:/oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf


Protect
Brute Force Attacks
Phishing Emails
Stolen Credentials
Weak Passwords
Identity Based Attacks
Credential Harvesting
Injection
Ransom-Ware
Sensitive Data Exposure
IP Theft
Domain Control
Detect
Risky Logins
Identity Based Attacks
Targeted Attacks
Privilege Escalation
Pass-the-Hash
Credential Harvesting
Sabotage
Shadow IT
Security Misconfigu-ration
Insider Risk
Respond
MFA
Lock Out Attackers
Quarantine
Quarantine
Malicious Code Removal
Risk-based Conditional Access
Restrict Access
SIEM Integration
AIR
IDENTITIES
INTELLECTUAL PROPERTY

Microsoft

Front protection

5 https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview

Azure Front Door Service

Global secure entry-point to the cloud

- Application acceleration at Microsoft's edge
- Global HTTP load balancing with fast failover
- Massive SSL offload, integrated static caching
- Global WAF at edge, secure, protect services
- Free domain and certificate management
- Global app dashboard, service insights

Global HA, BCDR

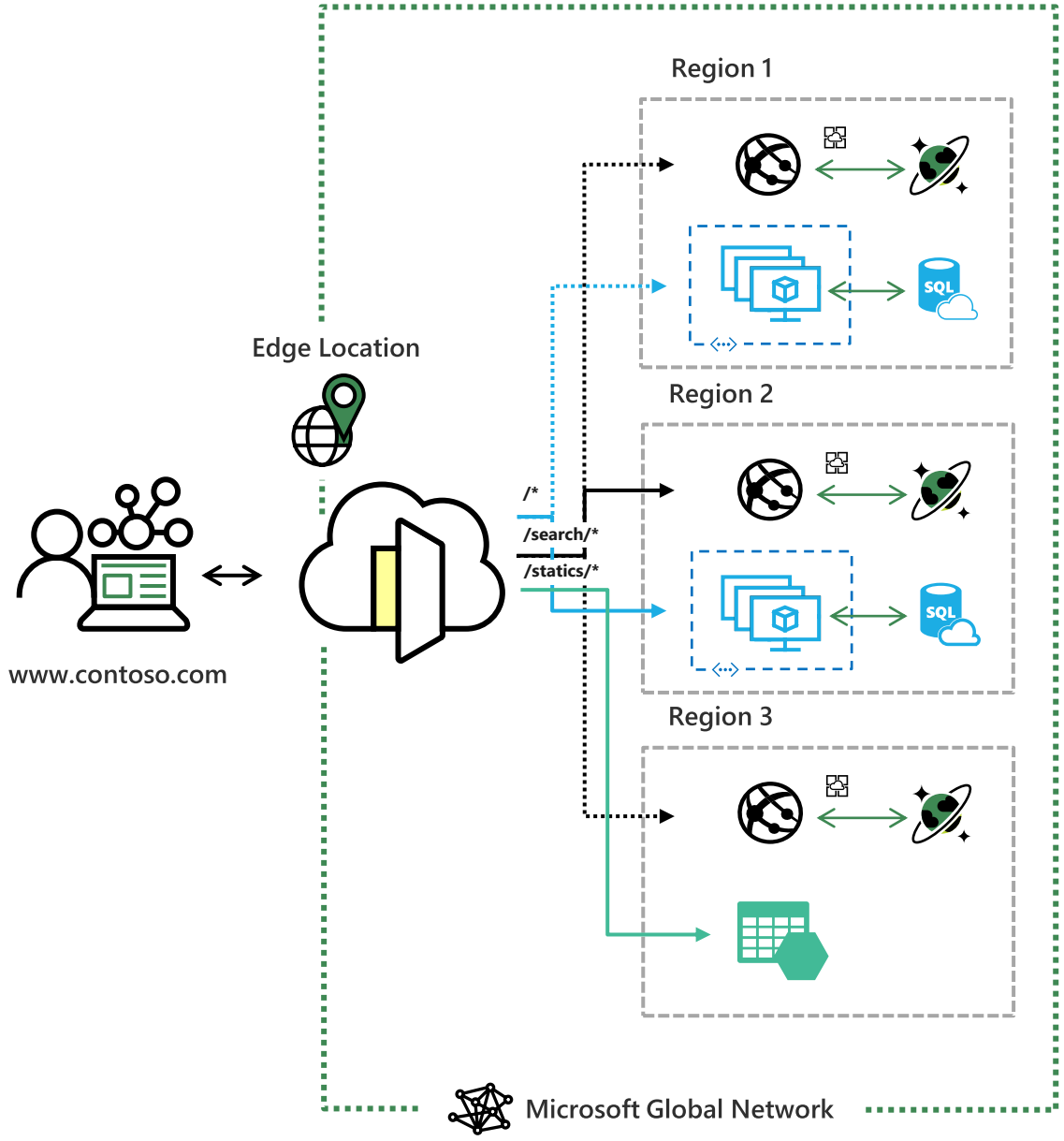
Enable fast-failover for regional services, microservices at the Edge with active path monitoring

Security at the Edge

Stop threats where they come from at the Edge with DDoS protection and customizable WAF

Faster apps

Reduce latency and increase throughput for apps by offloading SSL at the Edge and accelerating requests



Stop global attacks with WAF at edge

Scalable, best practice WAF on demand

- ✓ Always on inline protection, usage-based meters
- ✓ Stops attack close to the sources
- ✓ DDoS resilient
- ✓ Best practice OWASP top 10

Stopped at the edge

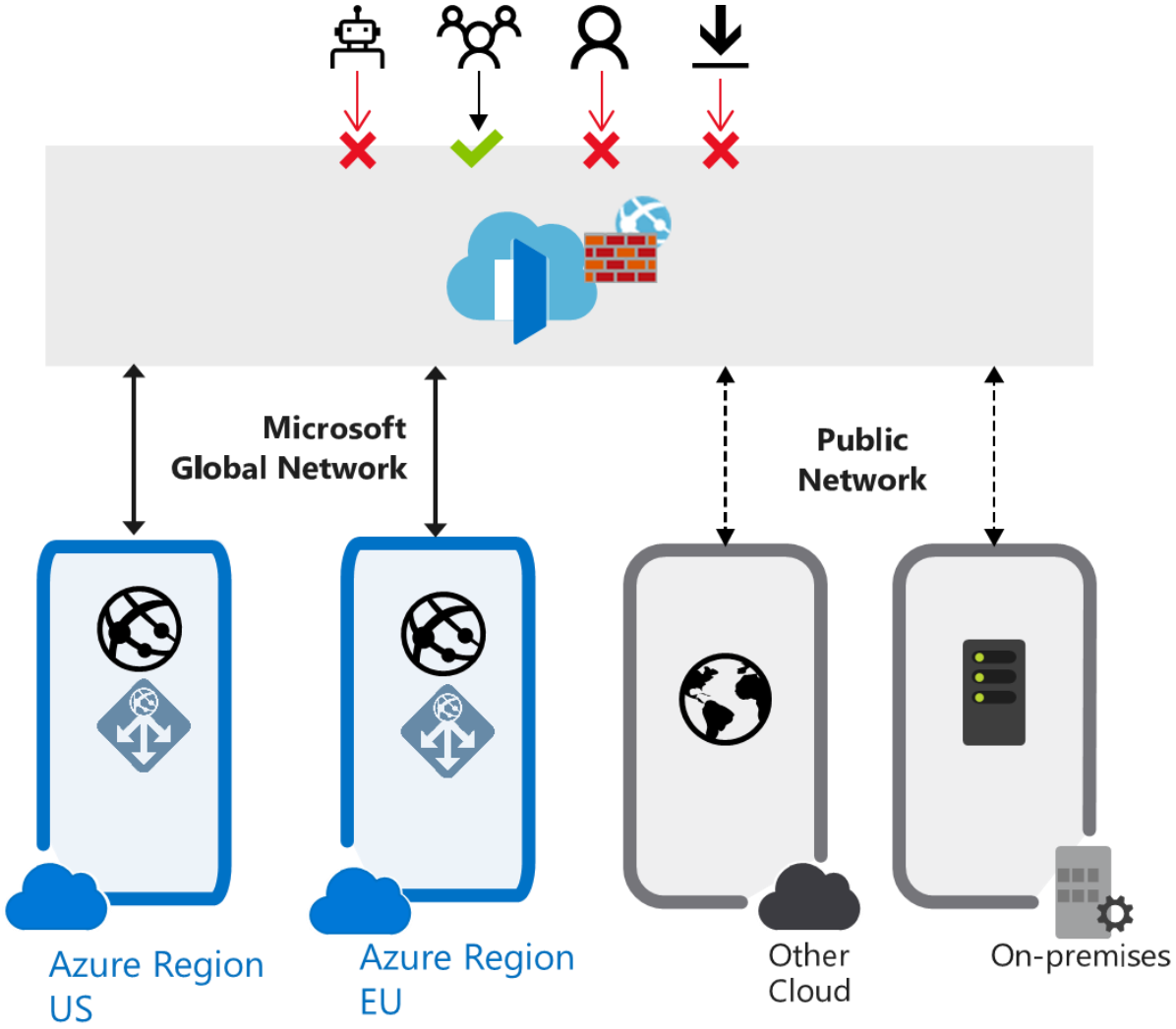
Maximize availability while saving on cost by protecting global services at the edge with unified rules and global actions.

Robust, real-time apps

Quickly add-on WAF to improve service reliability through best practice patterns, bot detection and custom rules.

Understand attacks

Get detailed attack logs for each blocked request; understand the who, when and why in detail or globally track block statistics.



WAF at Front Door feature list

Global, network DDoS defense at edge

Customizable access control

IP allow or block list

Geo filtering

Http parameters matching

Request methods restriction

Size constraint

Preconfigured OWASP TOP 10 ruleset

Conditional rate limiting

Match condition

Rate threshold

Bot manager basic

Detect malicious bots based on Microsoft Threat Intelligence feeds

Flexible Actions

Allow, Block, Monitor, or Redirect

Custom response code and message

DevOps integration

API, PS, Azure CLI and Portal

WAF logs integrated with Azure monitoring

Near real time dashboard

Customer storage account, Event hub, log analytics

Microsoft

Backend protection

API management solves API-related challenges

Discover
Learn
Get access
Try
SDKs and samples
Get help

Developers
(use APIs)

Connected experiences

Consume | Mediate | Publish

Services and data

Abstract
Secure and protect
Manage lifecycle
Monitor and measure
Onboard developers
Monetize

Publishers
(provide APIs)

There is a policy for that

Encapsulate common API management functions

Access control, Protection, Transformation, Caching, …

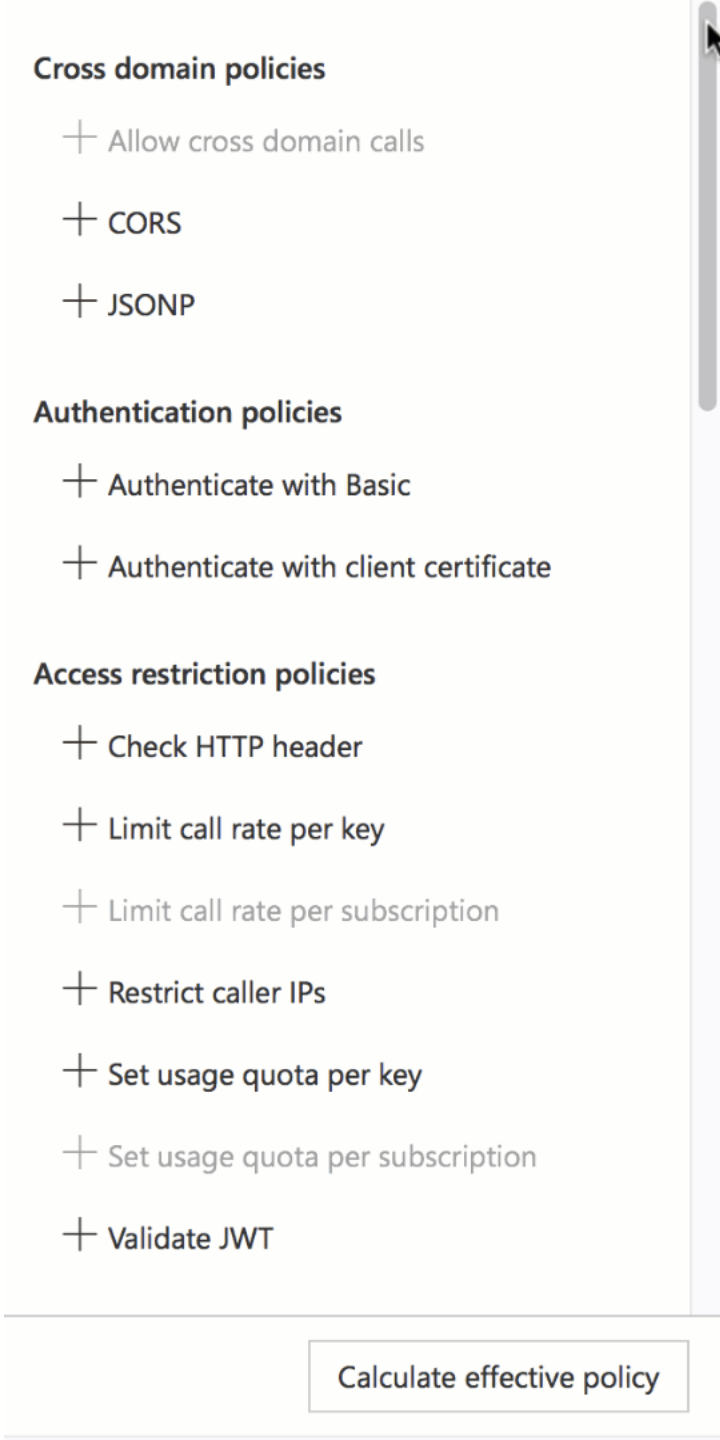
Chained together into a pipeline

Mutate request context or change API behavior

Set in the inbound and outbound directions

Can be triggered on error

Applied at a variety of scopes



 http://aka.ms/apimpolicyexamples

Demo

API Management:
JWT validation policy to pre-authorize requests

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

Microsoft

SPN/ MSI/ Credentials

Client Credentials

- Identity of the application
  - Secrets
  - Certificate – best practice

- Use the Confidential Client in MSAL
  - MSAL .NET Daemon sample

- Avoid using a “Service Account”
- Use Managed Identity for Azure Resources - Supporting Resources

Service Principals

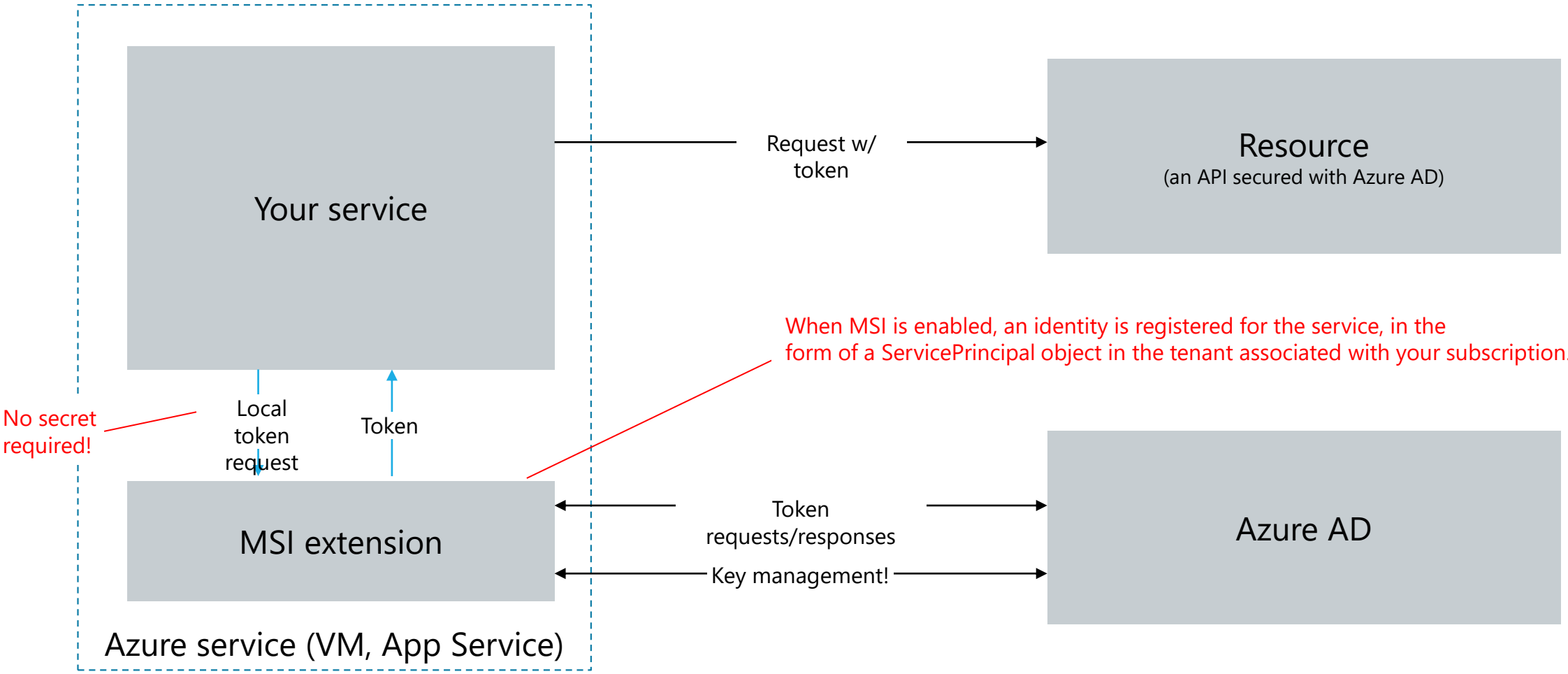
- a **security identity** used by user-created apps, services, and automation tools to access specific Azure resources
  - Think of it as a 'user identity' (login and password or certificate)
    - with a specific role
    - tightly controlled permissions
- Capable of :
  - **Password-based authentication (and if you forget -> Reset Credentials)**
  - **Certificate-based authentication**

Managed identities for Azure resources

Formerly known as "Managed Service Identities"

- Gives your Azure *service* an identity
- Available for many Azure resource types (and more coming)
- System-assigned vs. user-assigned
  - System assigned identities, tied to a given resource only
  - User assigned identities, can be assigned to different resources
- No secrets in code!

Managed identities for Azure resources



What services support managed identity?

Preview/Available now…

- Virtual Machines
- Machine Learning Services
- Functions
- Azure SQL
- Stream Analytics
- Storage
- App Service
- Azure Policy
- Azure Container Instances
- Data Factory
- API Management
- Data Lake Storage
- Virtual Machine Scale Sets
- Azure Blueprints
- Logic Apps
- HDInsight
- Container Registry
- Azure Search

Coming soon…

Service Fabric
Preview

Batch
Preview

AKS
Cluster Identity:
Preview tbd

Pod Identity:
Preview tbd

Find the latest list at: aka.ms/AzureManagedIdentityStatus

Difference SPN /MSI

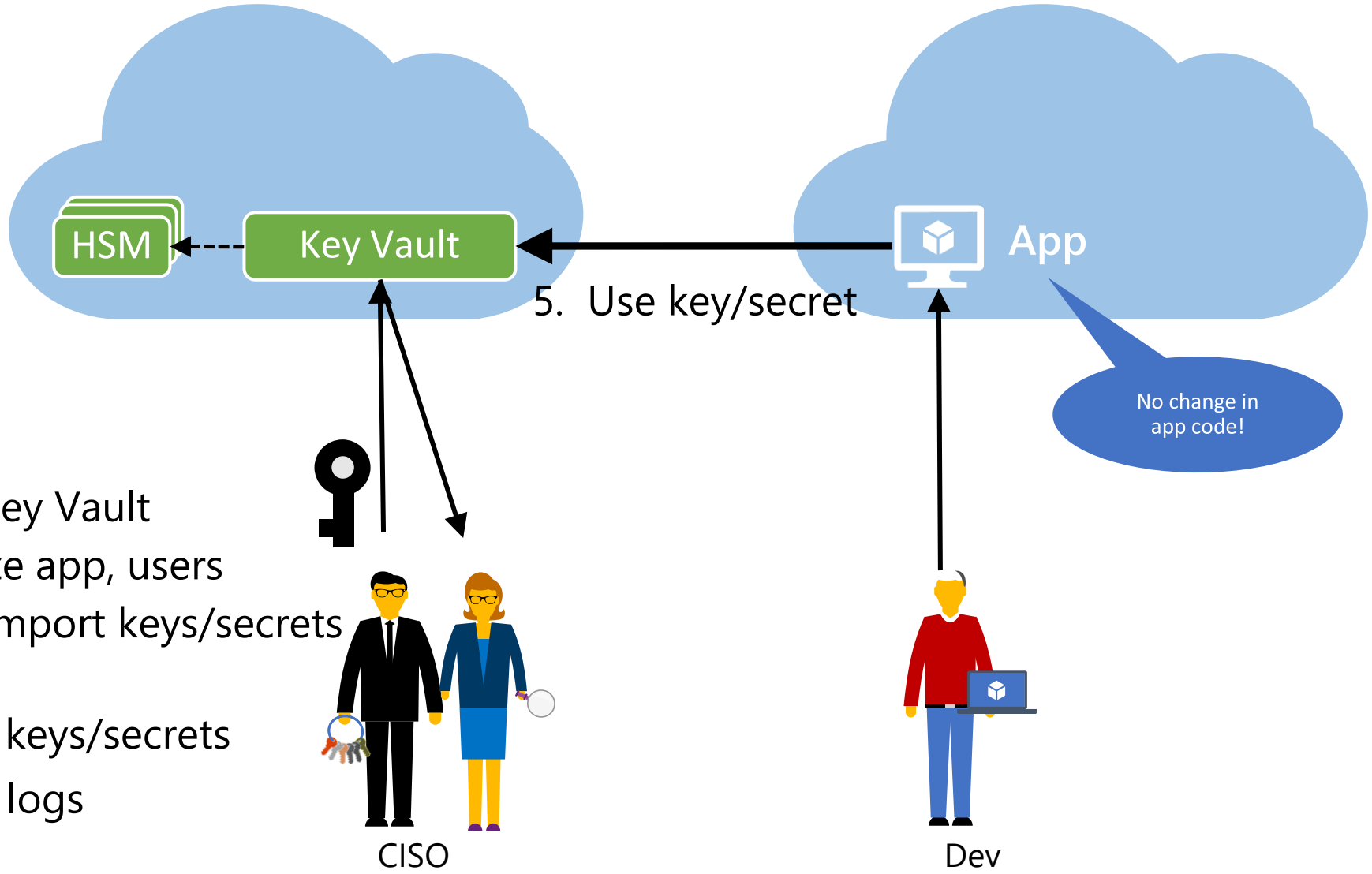
Traditional way of giving an app an identity (SP)

With Managed identities for Azure resources

Microsoft

Demo: Key Vault with MSI

Store differently : KeyVault or Designated HSM

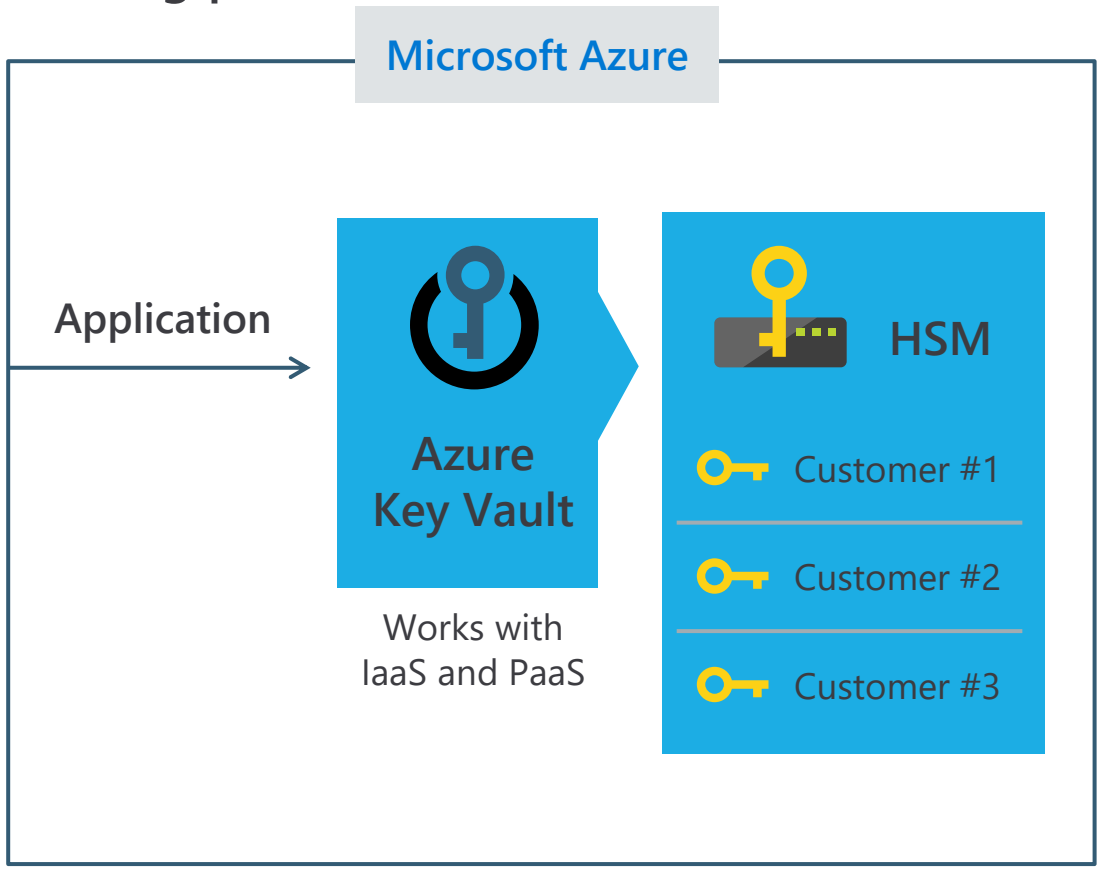


1. Create Key Vault
2. Authorize app, users
3. Create/import keys/secrets

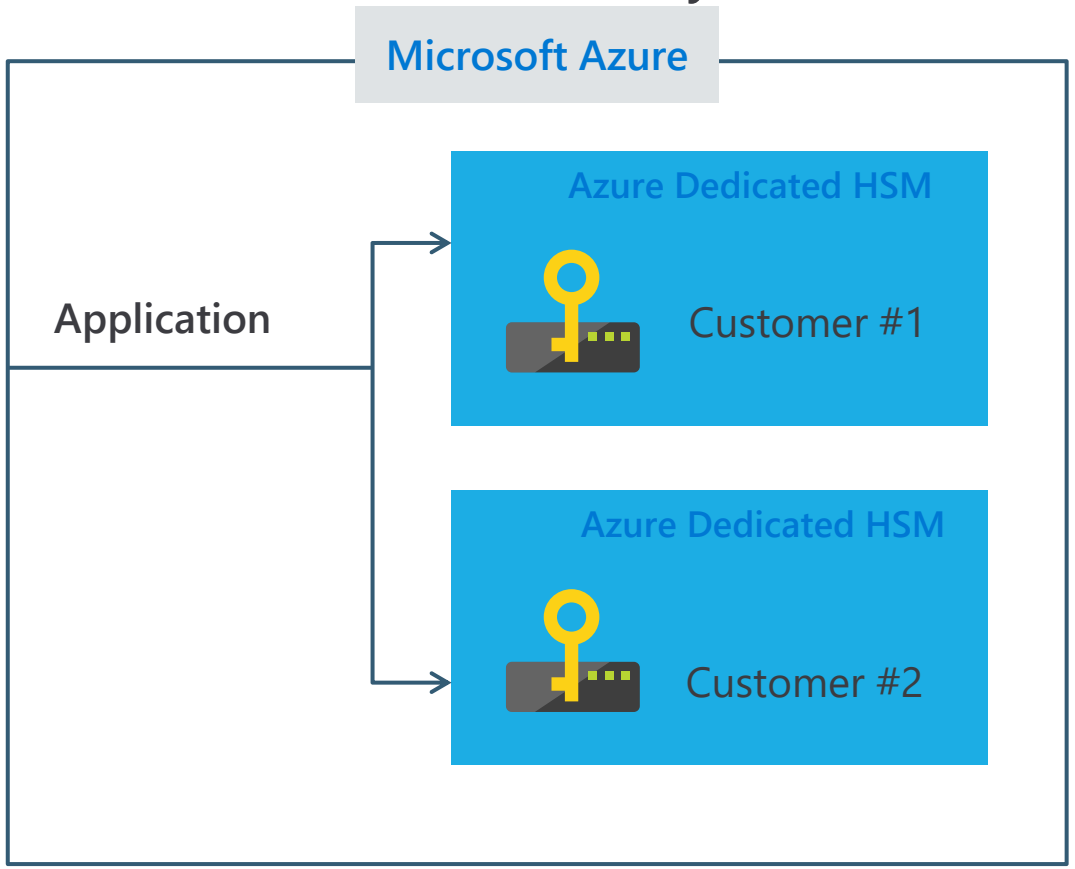
6. Manage keys/secrets
7. Monitor logs

Key management offers

Existing public offer



New offer to address industry needs



When to use Azure Key Vault or Azure Dedicated HSM?

Azure Key Vault:

Scenario 1: Industry customers that need key management that is FIPS 140-2 Level 2 validated

Scenario 2: Applications that are running in the cloud, and need its keys need to be in an HSM

Scenario 3: Store keys that work with first-party or third-party PaaS and SaaS services running in Azure

Azure Dedicated HSM:

Scenario 1: Customers in highly-regulated industries that need key management that is FIPS 140-2 Level 3 validated

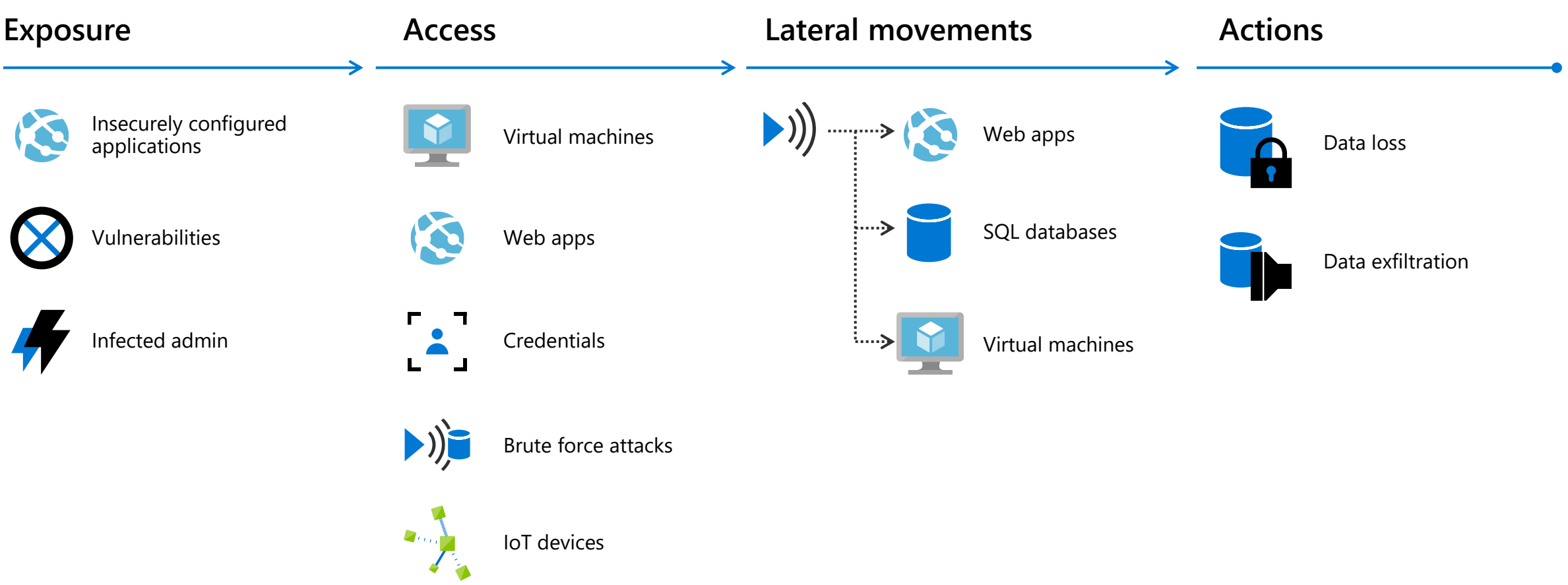
Scenario 2: Migrating applications from on-premises or from other clouds to Azure

Scenario 3: Store keys for homegrown or legacy applications that are running in Azure

Microsoft

The Last Mile

The cloud kill chain model



Azure Security Center

Strengthen security posture

Cloud security posture management

Secure Score | Policies and compliance

Protect against threats

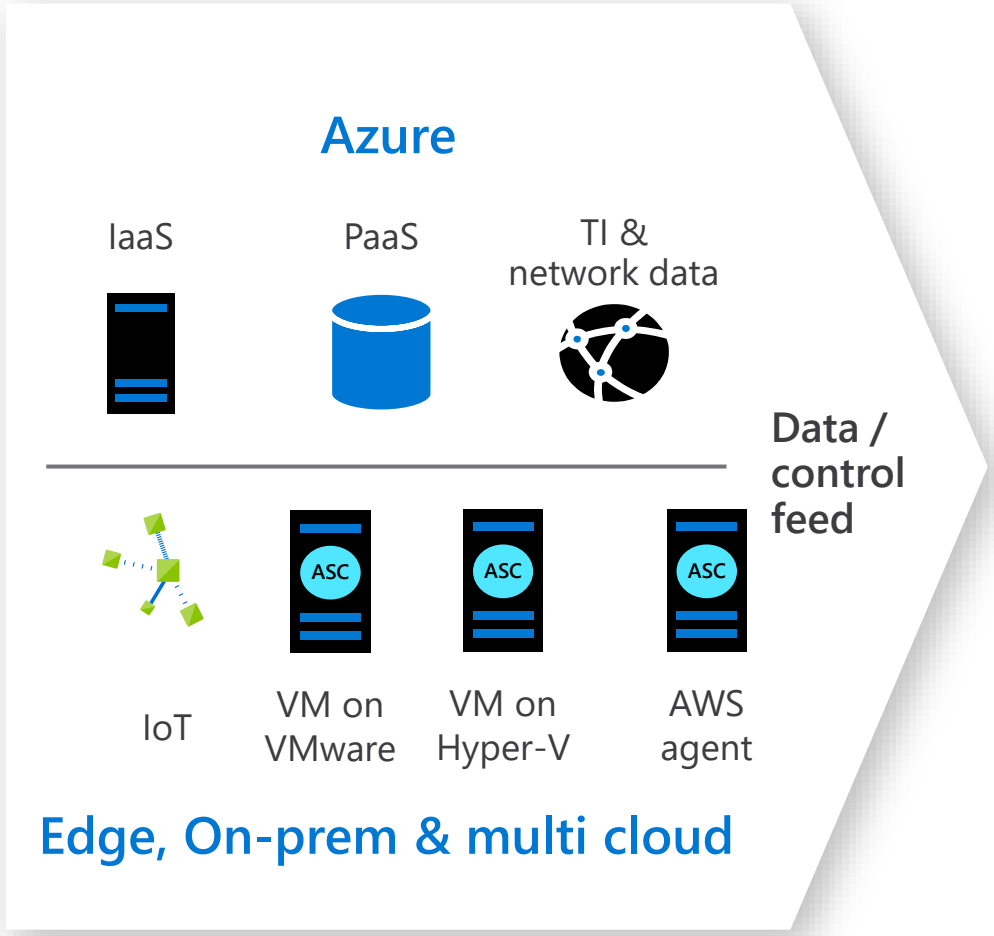
For servers

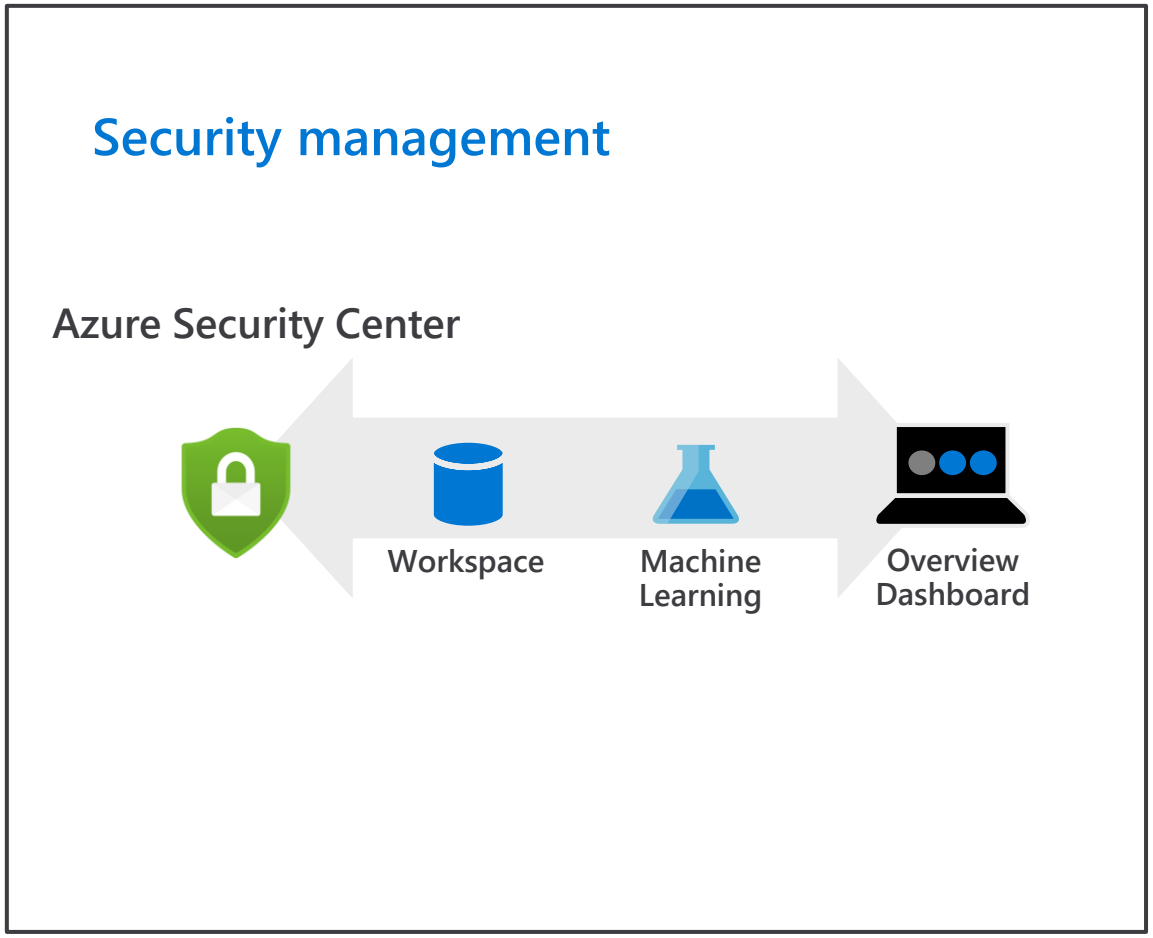
For cloud native workloads

For databases and storage

Get secure faster

Azure Security Center Architecture





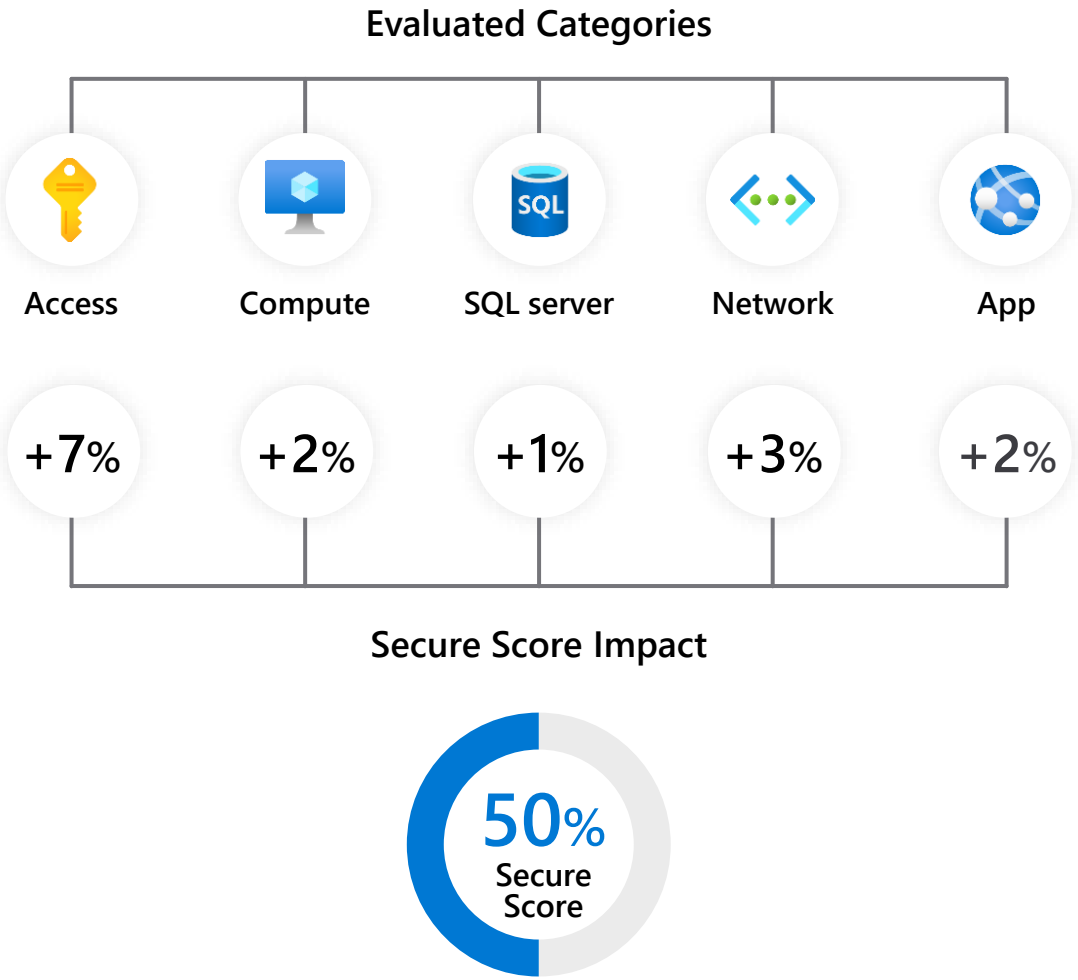
Security posture management with Secure Score

Gain instant insight into the security state of your cloud workloads

Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

Speed up regulatory compliance

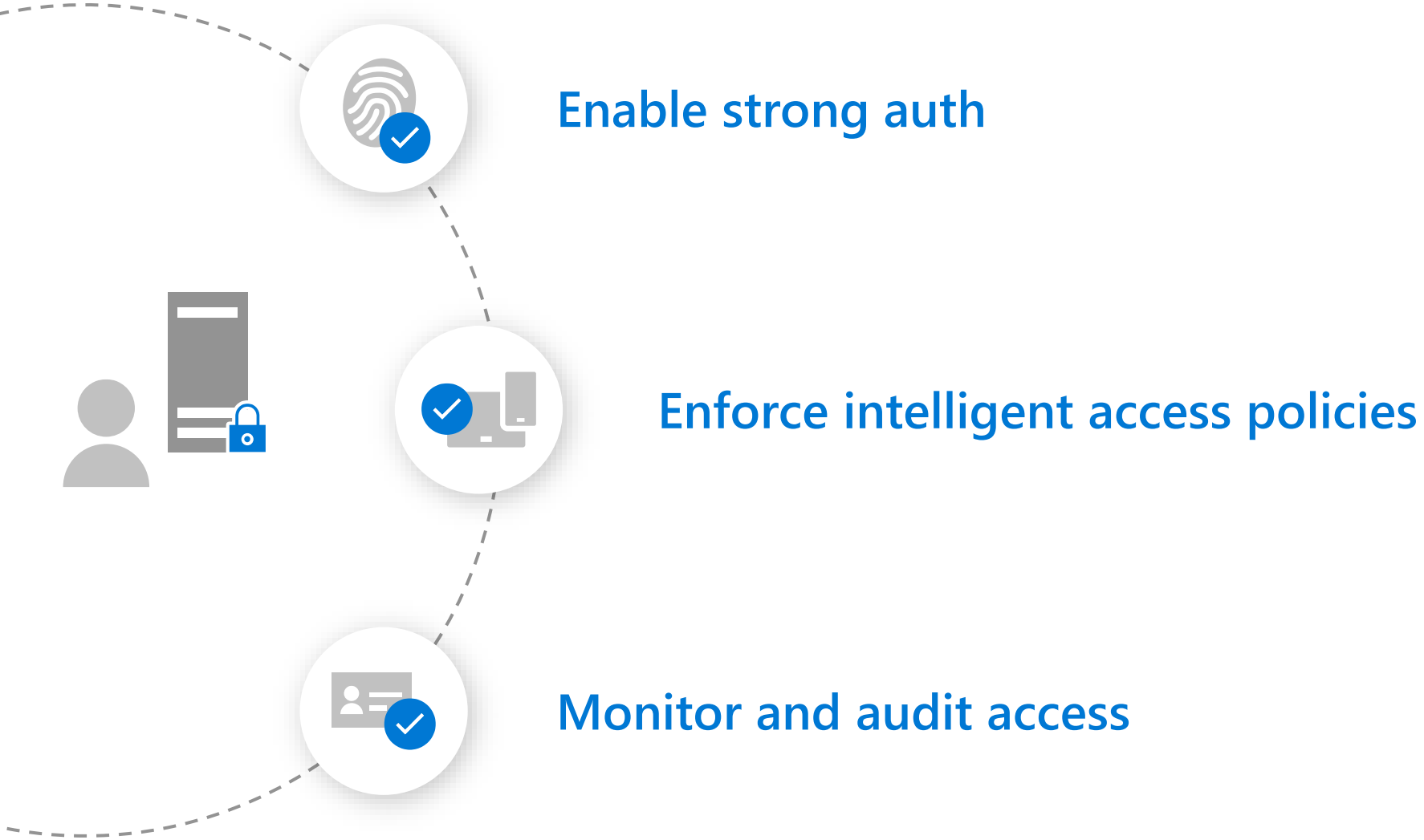


Microsoft

Demo: Azure Security Center

Protect and govern access

Network walls have come down but your security doesn't have to



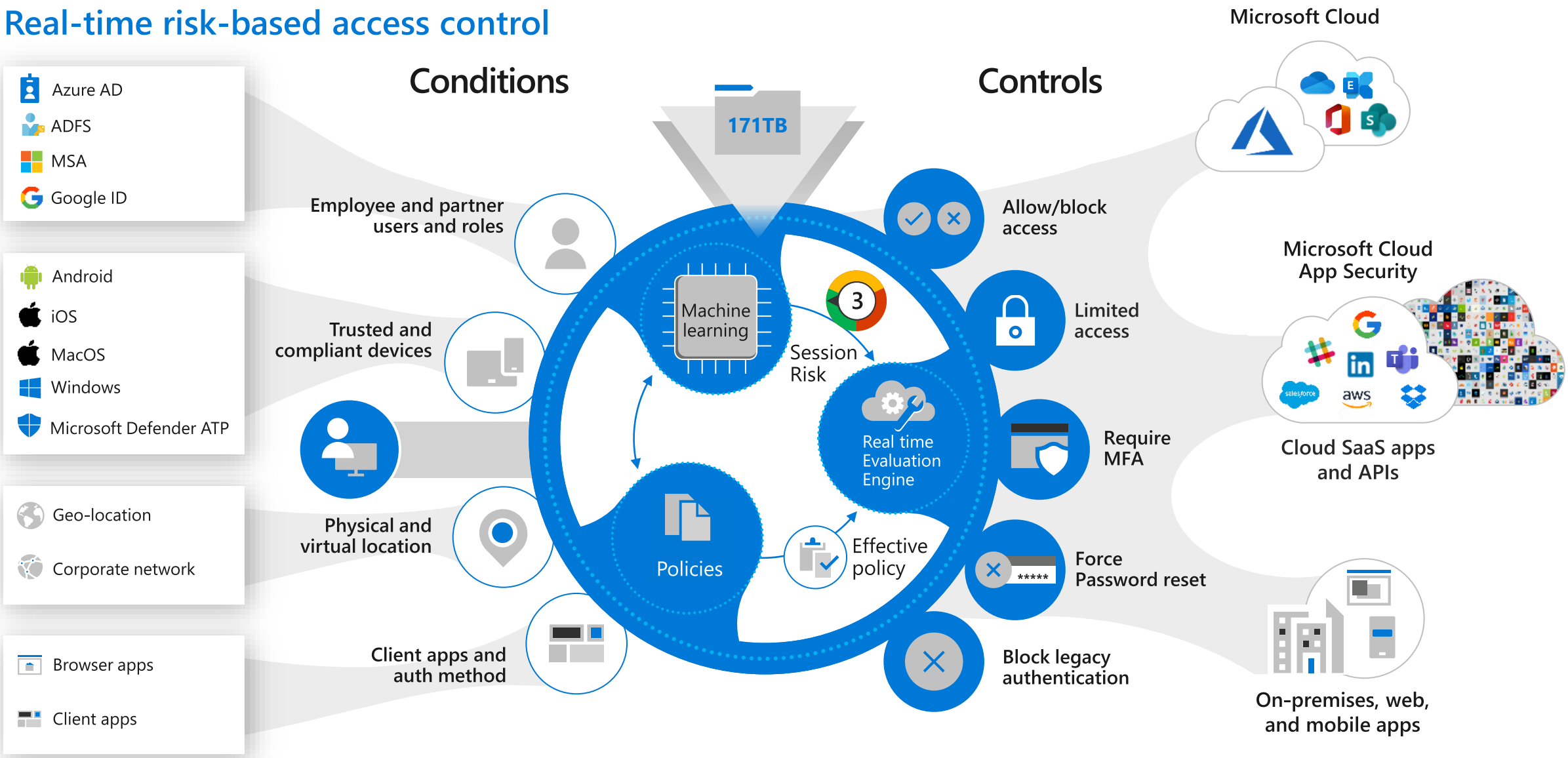
Enable strong auth

Enforce intelligent access policies

Monitor and audit access

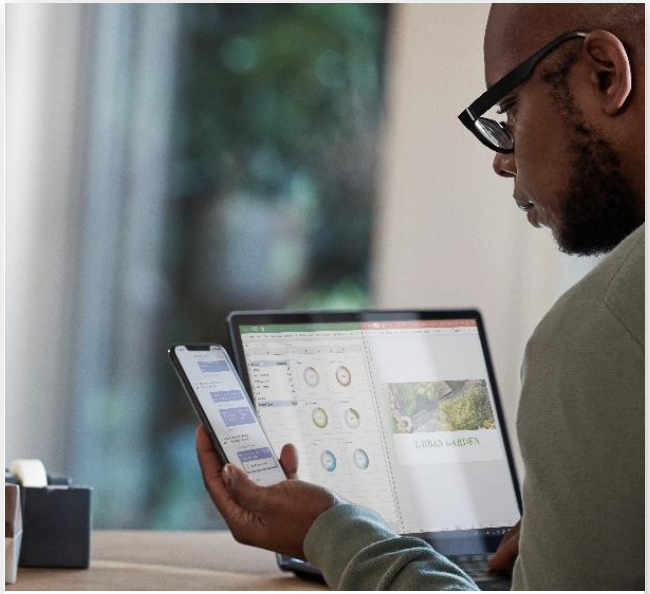
Azure Active Directory Conditional Access

Real-time risk-based access control



Protect and govern access

Verify user identities with strong authentication to establish trust



We support a broad range of multi-factor authentication options

Including passwordless technology

- Microsoft Authenticator
- Windows Hello
- FIDO2 Security key
- Biometrics

- Push Notification
- Soft Tokens OTP
- Hard Tokens OTP
- SMS, Voice

Multi-factor authentication prevents 99.9% of identity attacks

Microsoft

Demo: Azure AD Conditional Access

Microsoft

Conclusions

Conclusion: Rules of thumb

- Try to rule out man in the middle

→DON’T DO SECRETS IN CONFIGS – USE Keyvault

- Principle of least privilege

→ MINIMUM SET OF PERMISSIONS

- System-assigned vs. user-assigned
  - System assigned identities, tied to a given resource only
  - User assigned identities, can be assigned to different resources

- No secrets in code!

Microsoft

What questions do you have for us?