MANAGING SECURITY AND IDENTITY

MODULE OVERVIEW

- SECURITY & MONITORING &DATA SECURITY
- APPLICATION SECURITY WITH AZURE ACTIVE DIRECTORY
  - Azure AD
  - Hybrid Identity
  - Azure AD Application Integration

SECURITY & MONITORING

SECURITY & MONITORING

- AZURE PLATFORM SECURITY UNDER THE HOOD
- SECURITY FEATURES BUILT INTO AZURE PLATFORM

PLATFORM SECURITY

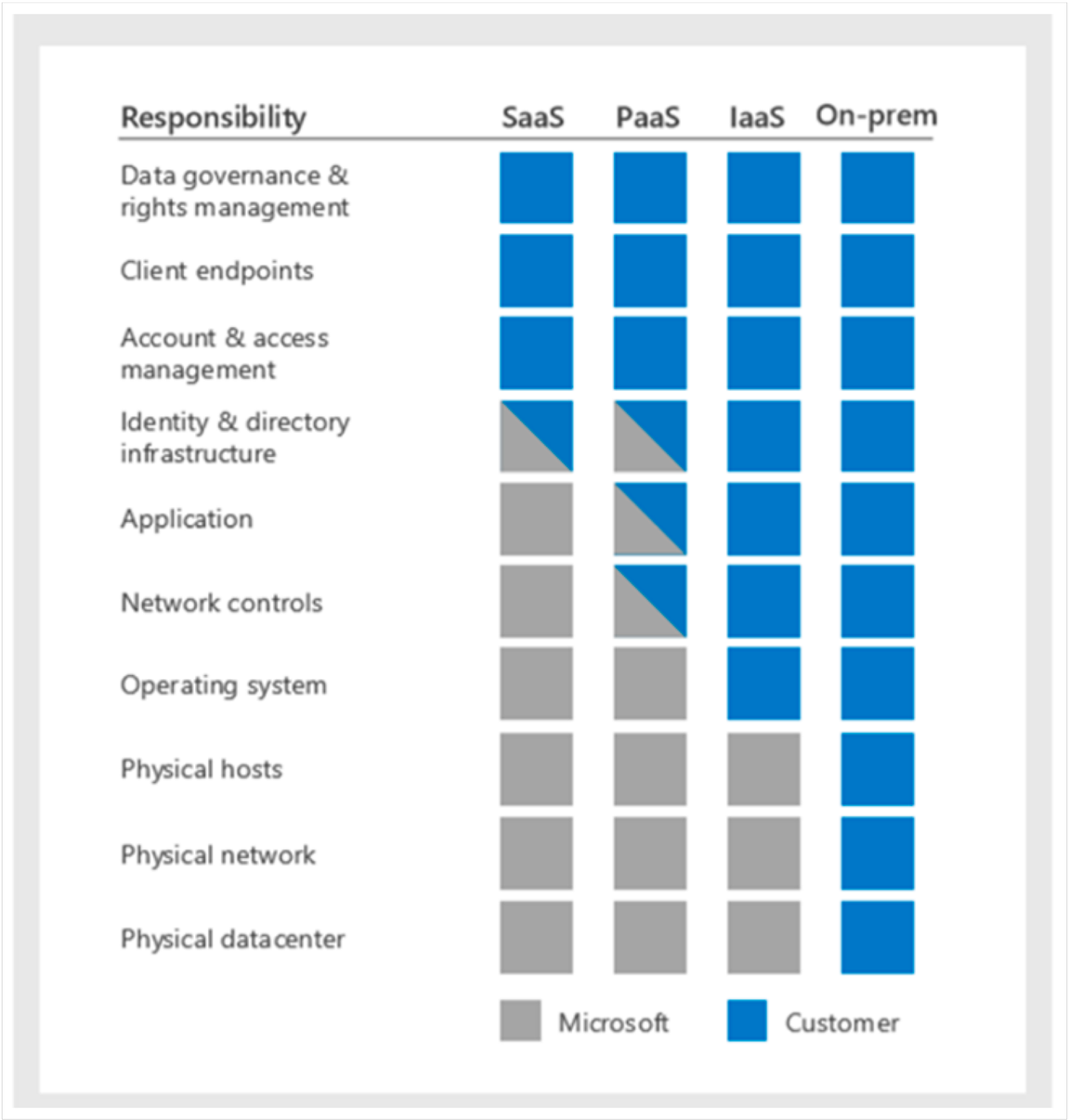
SECURITY RESPONSIBILITY IS SHARED

- AZURE IS BUILT WITH END-TO-END SECURITY IN MIND.
- MICROSOFT GIVES YOU A SECURE FOUNDATION, AS WELL AS THE TOOLING TO CONTROL YOUR ENVIRONMENT
- CERTIFICATION SHOWS THE VENDOR COMMITMENT TO MAKE THIS PLATFORM SECURE FROM SCRATCH.

- CUSTOMERS OWN RESPONSIBILITY OF THEIR SUBSCRIPTION GOVERNANCE
- DATA, IDENTITIES, AND HOW TO PROTECT THOSE.
- IN IAAS, CUSTOMER OWNS MORE CONTROL THAN IN PAAS OR SAAS
- CLOUD IS IN A CONSTANT DEVELOPMENT PROCESS SO THE SET OF TOOLS IS CHANGING

PLATFORM SECURITY

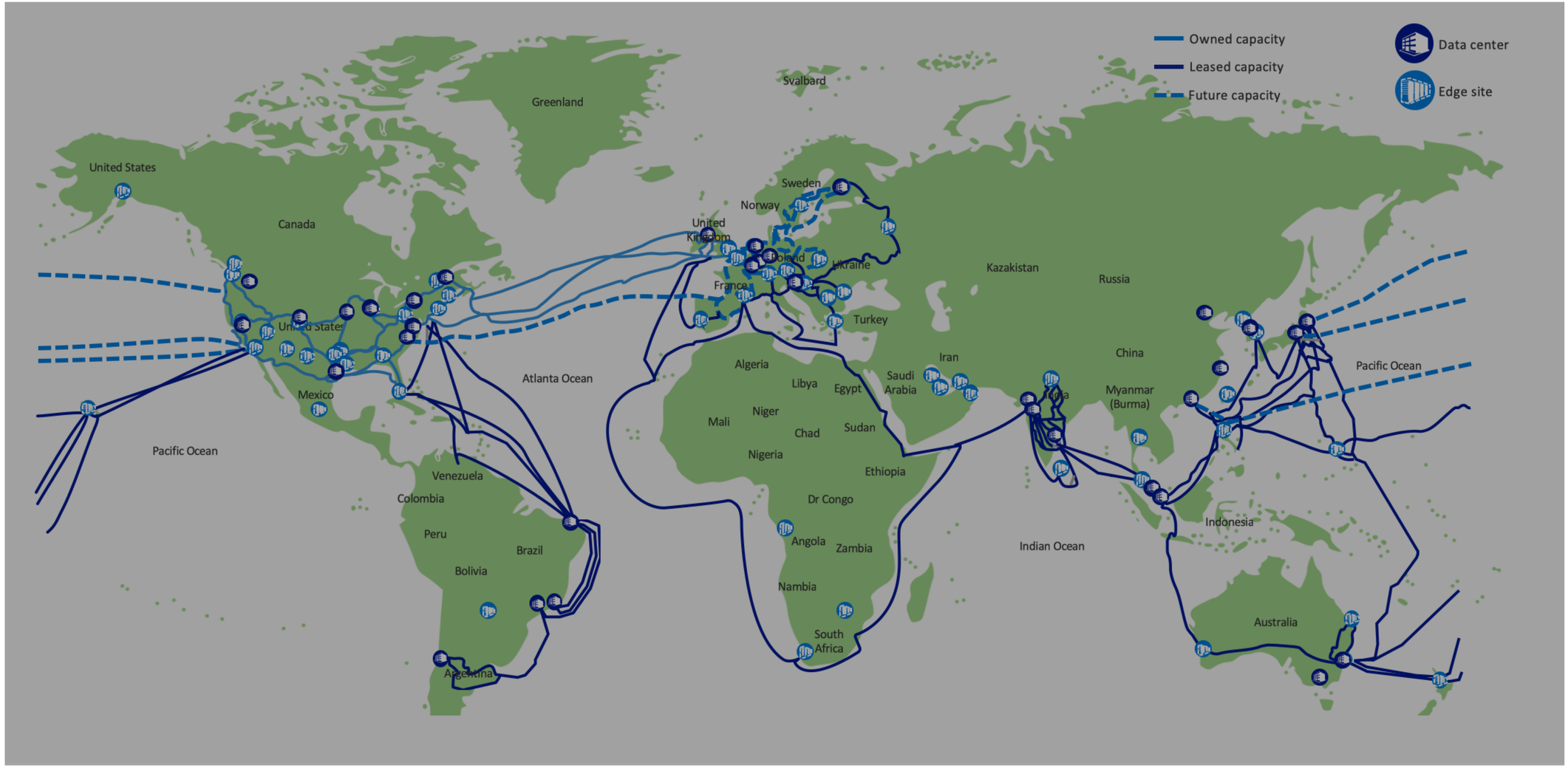
- DIFFERENT WORKLOADS HAVE VARIOUS POSSIBILITIES AND TOOLS OFFERED
- AMONG 120+ SERVICES THOSE GENERAL RULES MAY DIFFER, YOU BETTER UNDERSTAND YOUR WORKLOAD
- SECURITY IS CONSTANT WORK – IT NEVER STOPS AND IT IS NEVER PERFECT



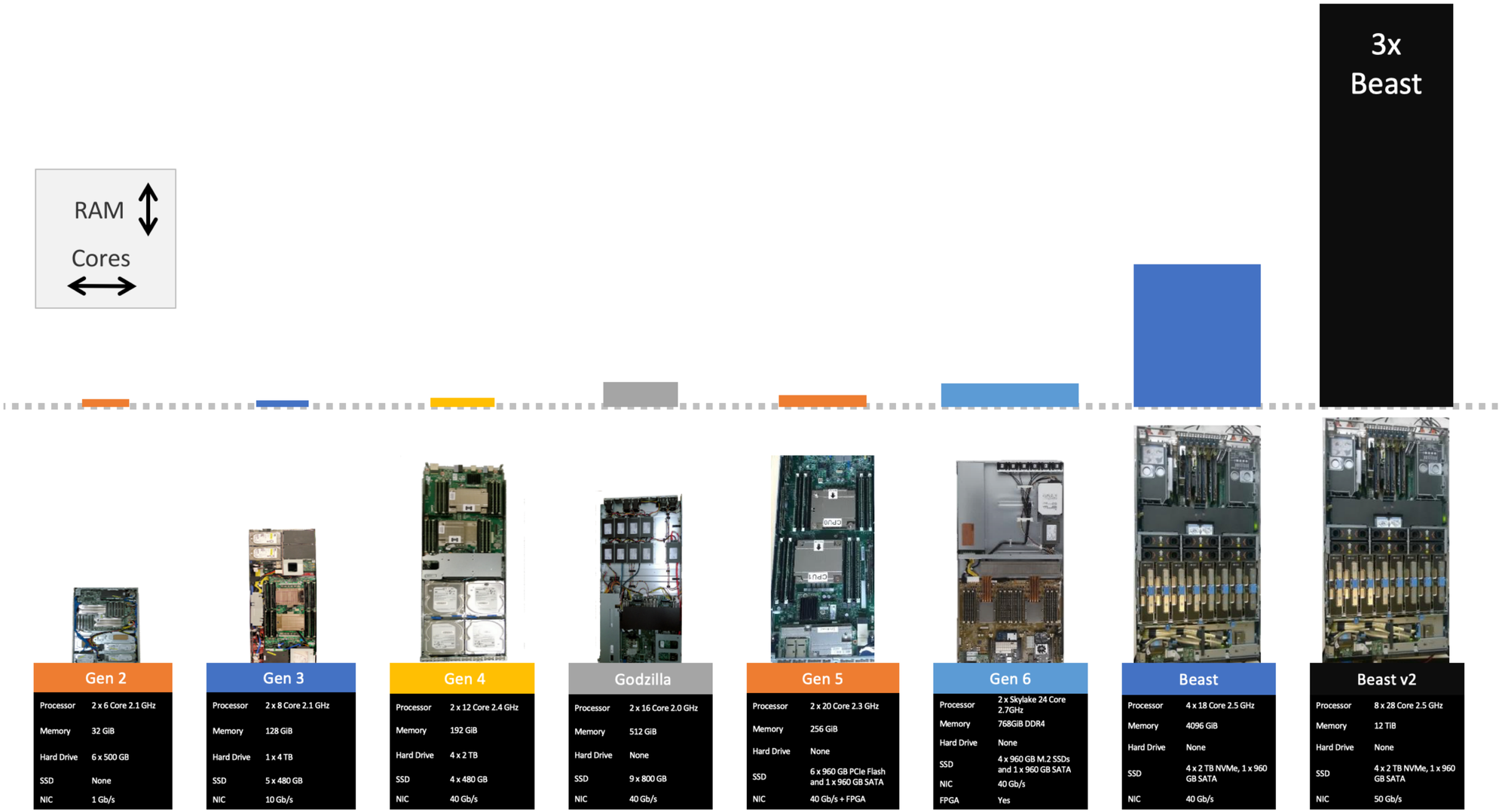
REGIONAL DATACENTERS

REGIONAL DATACENTERS

NETWORK SCALE AND FOOTPRINT

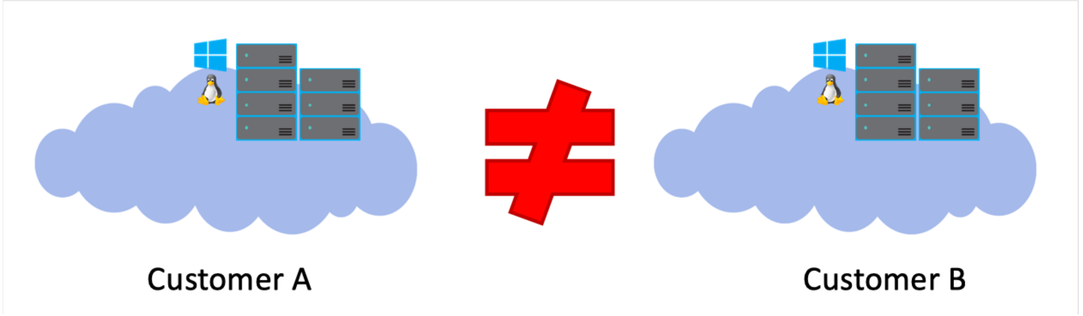


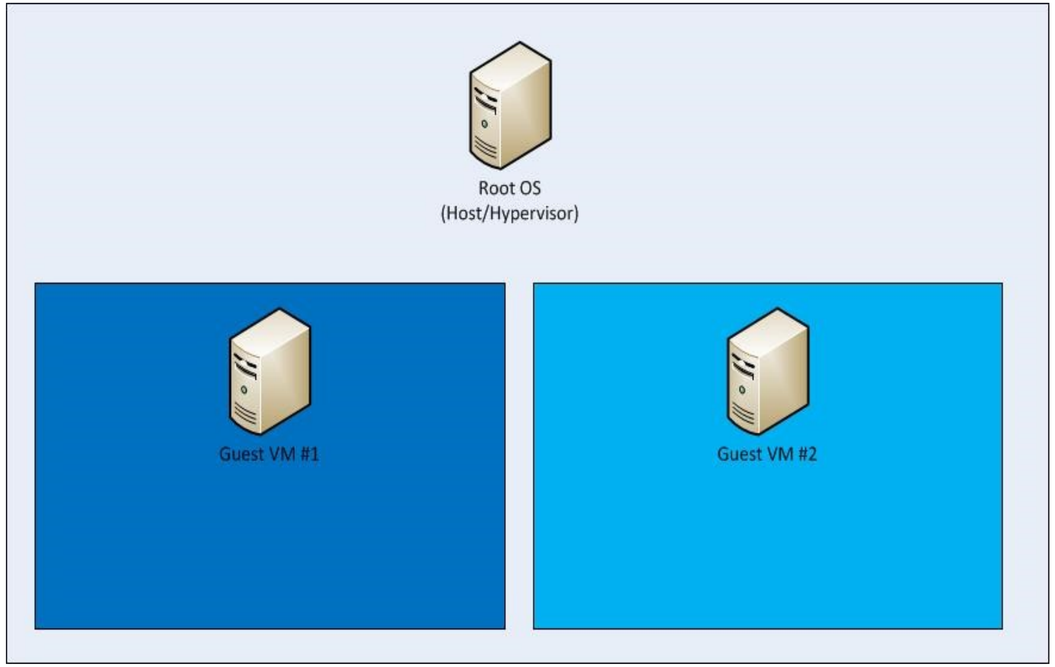
HARDWARE USED IN DATACENTER



DATACENTER SECURITY

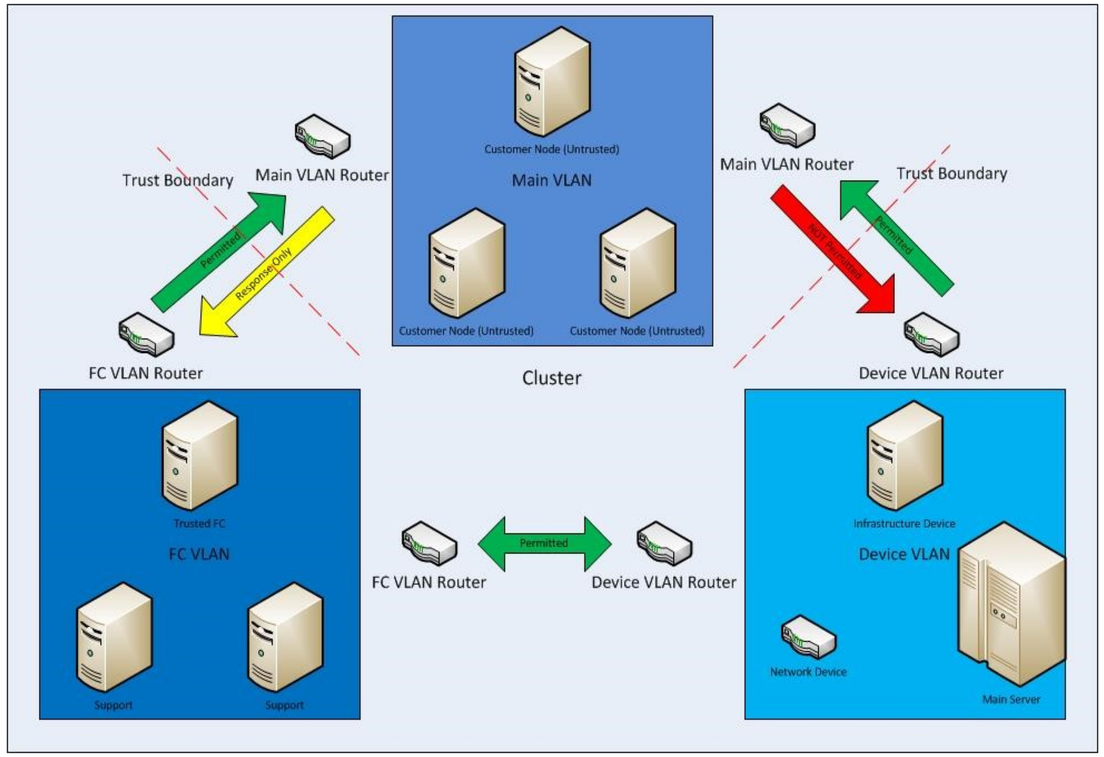
- CUSTOMERS ARE HIGHLY ISOLATED BETWEEN EACH OTHER ON THE TENANT LEVEL
- ALL COMMUNICATION BETWEEN WORKLOADS GOES THOUGH AZURE FABRIC CONTROLLER
- DATACENTERS ARE BASED ON CUSTOM HARDWARE (AS PRESENTED PREVIOUSLY) AND CUSTOMIZED VERSION OF HYPER-V VIRTUALIZATION





ENCRYPTION IN BUILT

- LOT'S OF ISOLATION ON THE NETWORK LEVEL BETWEEN CUSTOMERS, AZURE MANAGEMENT AND ADMINISTRATION TRAFFIC
- ALL SESSIONS ARE ENCRYPTED, ALL DATA AT REST ARE ENCRYPTED
- ON TOP THERE ARE PLENTY OF POSSIBILITIES TO ADD ADDITIONAL ENCRYPTION
- IN MANY SCENARIOS, THERE IS A POSSIBILITY TO ADD APP LEVEL SOLUTIONS

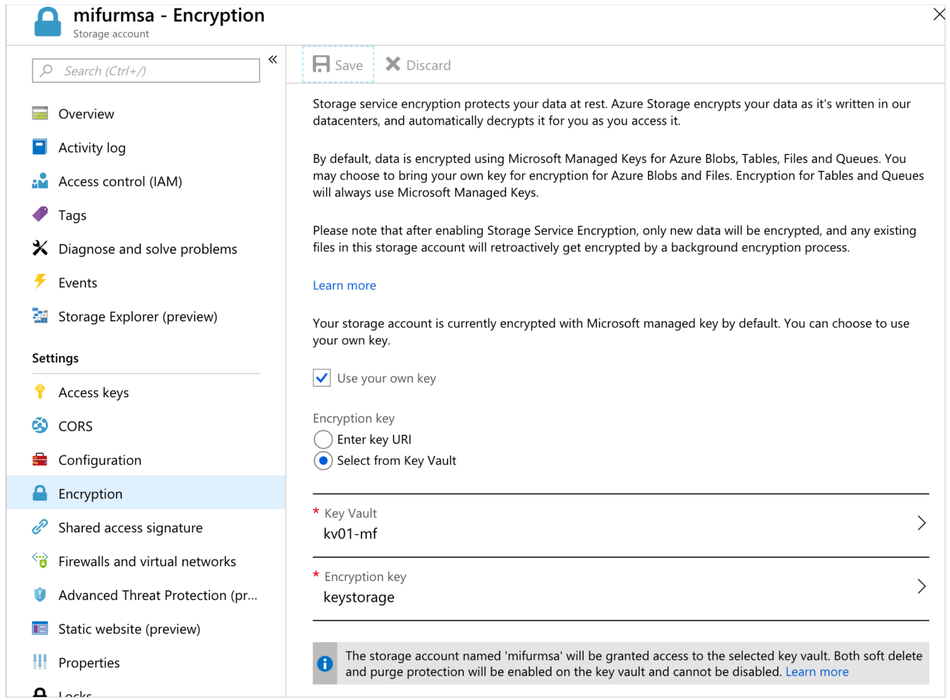


CUSTOM ENCRYPTION SCENARIOS ARE POSSIBLE

ON TOP OF THE AZURE PLATFORM PROVIDED ENCRYPTION, CUSTOMERS HAVE LOTS OF CUSTOM POSSIBILITIES:

- OFFLINE DISK SHIPMENT: ONLY ENCRYPTED DISKS ARE ACCEPTED
- SQL AZURE PROVIDES DATABASE CONTENT ENCRYPTION (SQL DB TDE)
- AZURE STORAGE ACCOUNTS CAN BE ENCRYPTED USING KEY VAULT
- AZURE VMS (GUESTS) ALLOW KIND OF BITLOCKER ENCRYPTION (FOR WINDOWS / LINUX)
- AZURE BACKUP, AZURE RECOVERY VAULT DATA IS STORED ENCRYPTED
- ARCHIVE DATA (DATA AT REST) ALLOWS ENCRYPTION

- AT THE APP LEVEL YOU HAVE PLENTY OF OTHER OPTIONS



COMPLIANCE

Global	US Government	Industry	Regional
CSA-STAR-Attestation	CJIS	23 NYCRR Part 500	BIR 2012 (Netherlands)
CSA-Star-Certification	DoD DISA L2, L4, L5	APRA (Australia)	C5 (Germany)
CSA-STAR-Self-Assessment	DoE 10 CFR Part 810	CDSA	CCSL/IRAP (Australia)
DFARS	EAR (US Export Administration Regulations)	CFTC 1.31	CS Gold Mark (Japan)
ISO 20000-1:2011	FDA CFR Title 21 Part 11	DPP (UK)	Cyber Essentials Plus (UK)
ISO 22301	FedRAMP	FACT (UK)	DJCP (China)
ISO 27001	FERPA	FCA (UK)	EN 301 549 (EU)
ISO 27017	FIPS 140-2	FFIEC	ENISA IAF (EU)
ISO 27018	IRS 1075	FINRA 4511	ENS (Spain)
ISO 9001	ITAR	FISC (Japan)	EU-Model-Clauses
SOC 1, 2 and 3	NIST 800-171	GLBA	EU-U.S. Privacy Shield
WCAG 2.0	NIST Cybersecurity Framework (CSF)	GxP	GB 18030 (China)
	Section 508 VPATS	HIPAA/HITECH	GDPR (EU)
		HITRUST	IDW PS 951 (Germany)
		MARS-E	IT Grundschutz Workbook (Germany)
		MAS + ABS (Singapore)	LOPD (Spain)
		MPAA	MeitY (India)
		NEN-7510 (Netherlands)	MTCS (Singapore)
		NHS IG Toolkit (UK)	My Number (Japan)
		OSFI (Canada)	NZ CC Framework (New Zealand)
		PCI DSS	PASF (UK)
		SEC 17a-4	PDPA (Argentina)
		Shared Assessments	PIPEDA (Canada)
		SOX	TRUCS (China)
			UK-G-Cloud

Security

- Services are built from the ground up, to help safeguard customer data

Privacy

- Policies and processes help keep customer data private and in their control

Compliance

- Industry-verified compliance conformity and certifications

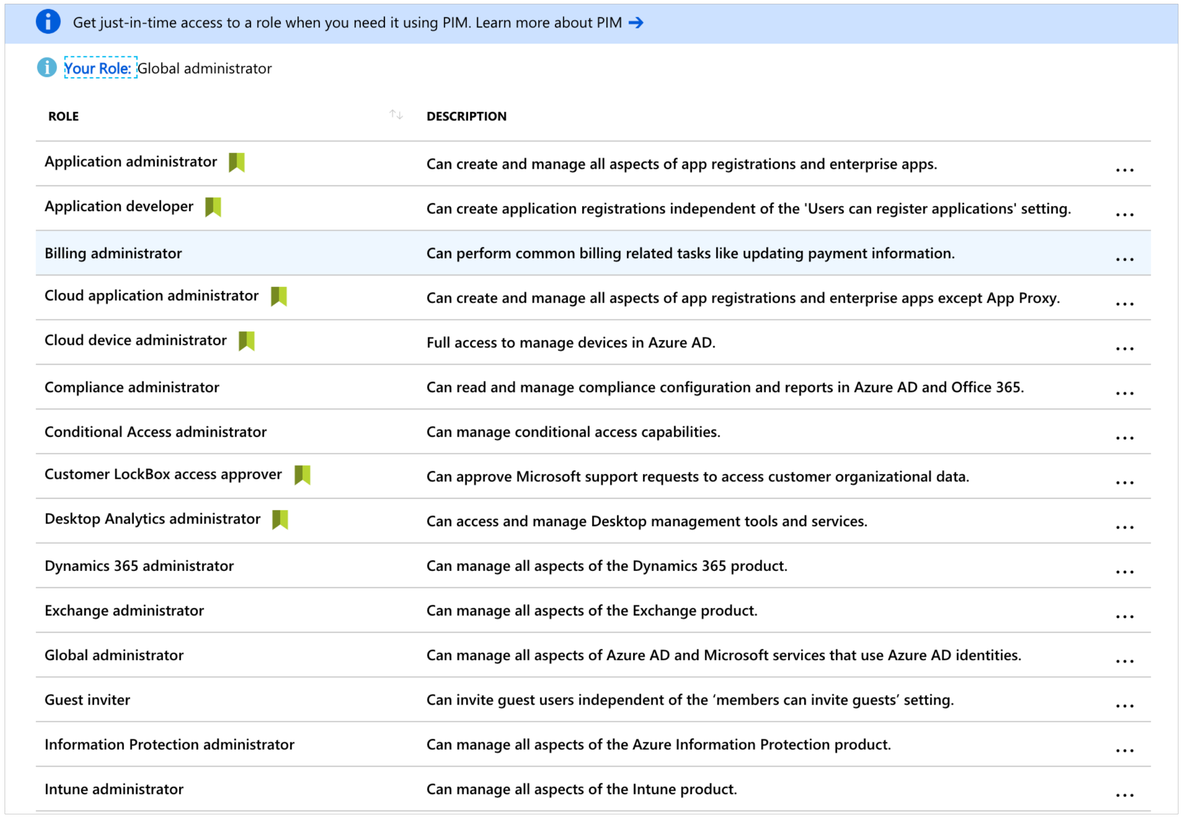
Transparency

- Azure practices, policies and guidelines are public, clear and accessible

SECURING SUBSCRIPTION

AZURE SUBSCRIPTION GOVERNANCE

- LIMIT ADMIN ACCESS USING RBAC (ROLE BASED ACCESS CONTROL)
- LIMIT VM ADMIN ACCESS USING JIT (JUST IN TIME) ACCESS OR PRIVILEGED IDENTITY MANAGEMENT
- ENABLE (FORCE) MULTI-FACTOR AUTHENTICATION FOR
  AZURE ADMIN ACCOUNTS, HOWEVER, KEEP ALSO "ENVELOPE" BASED ADMIN ACCOUNTS FOR THE SAKE OF MFA NOT WORKING PROPERLY
- CUSTOMIZE RBAC ROLES WHERE NEEDED FOR YOUR
  ORGANIZATIONAL COMPLIANCE
- VERIFY IF PEOPLE HAVE PROPER ROLES ASSIGNED
- KEEP IN MIND THAT ROLES FOR AZURE ACTIVE DIRECTORY ARE DIFFERENT FROM RBAC



ROLE	DESCRIPTION
Application administrator	Can create and manage all aspects of app registrations and enterprise apps.
Application developer	Can create application registrations independent of the 'Users can register applications' setting.
Billing administrator	Can perform common billing related tasks like updating payment information.
Cloud application administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
Cloud device administrator	Full access to manage devices in Azure AD.
Compliance administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.
Conditional Access administrator	Can manage conditional access capabilities.
Customer LockBox access approver	Can approve Microsoft support requests to access customer organizational data.
Desktop Analytics administrator	Can access and manage Desktop management tools and services.
Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 product.
Exchange administrator	Can manage all aspects of the Exchange product.
Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.
Guest inviter	Can invite guest users independent of the 'members can invite guests' setting.
Information Protection administrator	Can manage all aspects of the Azure Information Protection product.
Intune administrator	Can manage all aspects of the Intune product.

SECURING PLATFORM - STORAGE

AZURE STORAGE ACCOUNTS:

- ENABLE STORAGE ACCOUNT ENCRYPTION:
  - USING YOUR ENCRYPTION KEYS (BY IMPORTING THEM TO KEY VAULT)
  - USING KEYS STORED IN KEY VAULT
- ACCESS KEYS:
  - KEY1/KEY2 -> REGENERATE PERIODICALLY
  - ALL SAS ARE SIGNED USING KEYS
- SHARED ACCESS SIGNATURES (SAS) TO NARROW APPLICATION SERVICE ACCESS TO THE STORAGE OBJECT AND DATA
- STORAGE ACCESS POLICIES:
  - TIMESTAMP
  - PERMISSIONS
- FOR FILE SHARES – YOU CAN INTEGRATE ACCESS WITH AZURE AD DS
- **NEW FEATURES**: SOFT DELETE, RETENTION POLICY OF DATA, ADVANCED THREAT PROTECTION

SECURING PLATFORM – AZURE SQL DATABASE

AZURE SQL-AS-A-SERVICE:

- APPLY RBAC TO LIMIT SQL RESOURCES ADMIN-LEVEL ACCESS
- BE CAUTIOUS WITH THE “ALLOW AZURE SERVICES” ACCESS
- THINK ABOUT SERVICE ENDPOINTS AND NETWORKS
- MONITORING THROUGH LOG ANALYTICS IS THE KEY
- ADD ACCESS TO ACCOUNTS FROM AZURE AD, NO LOCAL ACCOUNTS APPROVED

FEATURES:

- SQL DATABASE ENCRYPTION AT REST (TDE)
- SQL DATABASE ENCRYPTION IN TRANSIT
- SQL AUDITING & THREAT DETECTION
- SQL DYNAMIC DATA MASKING
- SQL ROW LEVEL SECURITY
- SQL VULNERABILITY ASSESSMENT

SECURING PLATFORM – AZURE NETWORKING

AZURE NETWORKING

- ISOLATE VM TRAFFIC BY DEPLOYING MULTIPLE VNETS AND SEPARATE SUBNETS WITHIN
- USE HUB & SPOKE ARCHITECTURE TO LIMIT THE VPN CONNECTIONS, USE SERVICE TAGS AND ENDPOINTS TO LIMIT ACCESS FROM IAAS SERVICE TO PAAS OFFERING
- USE NETWORK SECURITY GROUPS TO LIMIT TRAFFIC ALLOW/DENY, USE APPLICATION SECURITY GROUPS TO MAKE SEGEMENTATION EASIER AND MORE PARTICULAR
- INTEGRATE FORCED TUNNELING, USER DEFINED ROUTING TO CONTROL TRAFFIC OUTSIDE FROM THE DEFAULT AZURE ROUTES – BE CAREFUL, IT MAY IMPACT YOUR CHARGES
- EXPLORE AZURE MARKETPLACE VIRTUAL APPLIANCES:
  - LOAD BALANCERS
  - FIREWALLS

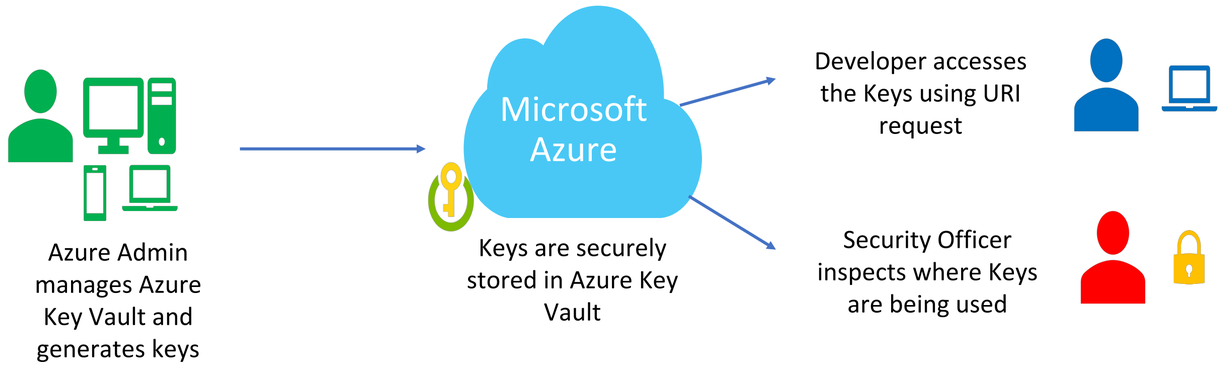
USE

- AZURE LOG ANALYTICS WITH SERVICE MAP
- NETWORK WATCHER
- TRAFFIC ANALYTICS

SECURING PLATFORM – KEY VAULT

AZURE KEY VAULT:

- SECURITY KEYS ARE STORED IN A VAULT AND INVOKED BY URI WHEN NEEDED
- KEYS ARE SAFEGUARDED BY AZURE, USING INDUSTRY-STANDARD ALGORITHMS, KEY LENGTHS, AND HARDWARE SECURITY MODULES (HSMS)
- KEYS ARE PROCESSED IN HSMS THAT RESIDE IN THE SAME AZURE DATACENTERS AS THE APPLICATIONS.
- MOST VENDORS CURRENTLY ON THE MARKET HAS A SUPPORT TEAM.



DEMO

SECURITY & MONITORING SUMMARY

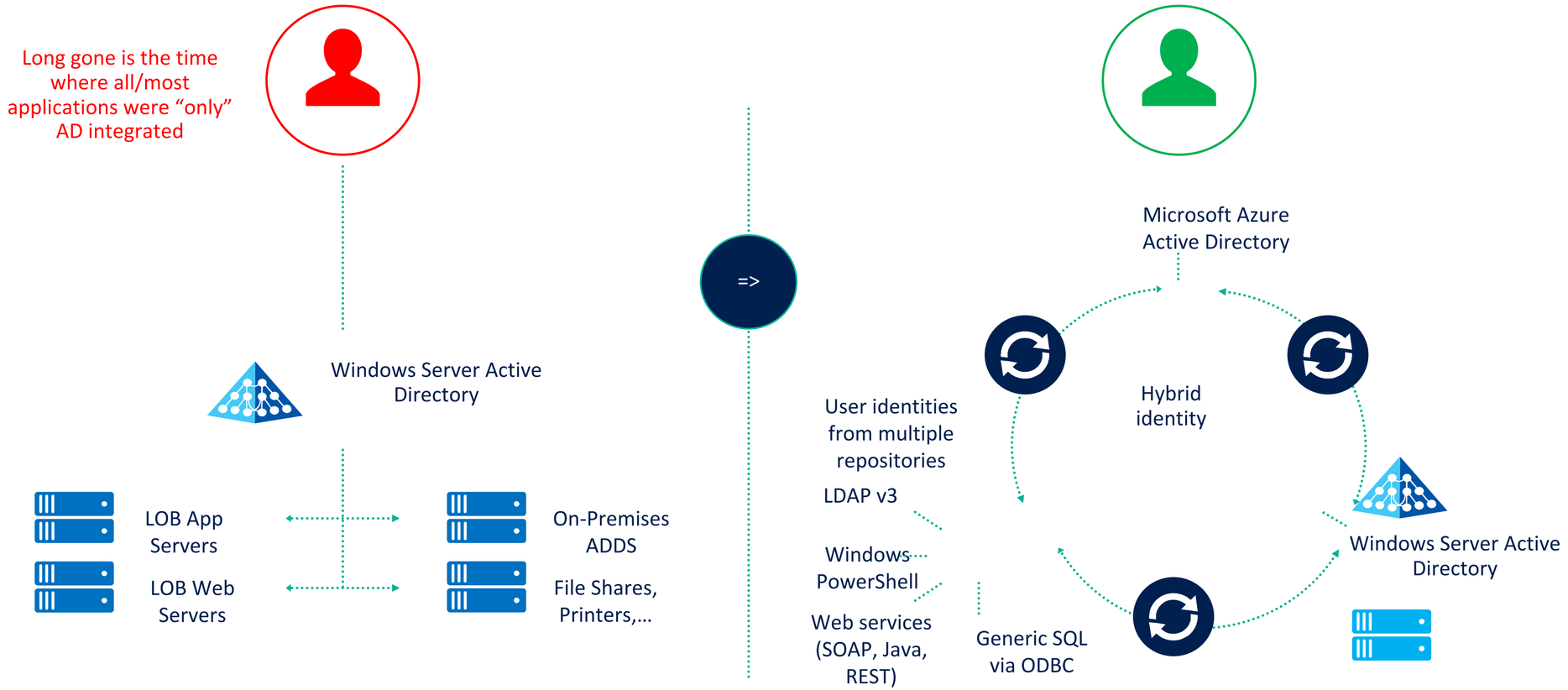
- AZURE PLATFORM SECURITY UNDER THE HOOD
- SECURITY FEATURES BUILT INTO AZURE PLATFORM

APPLICATION SECURITY WITH AZURE ACTIVE DIRECTORY

APPLICATION SECURITY WITH AZURE ACTIVE DIRECTORY

- AZURE ACTIVE DIRECTORY
- AZURE AD AUTHENTICATION STRATEGIES
- AZURE AD B2B & B2C
- AZURE AD IDENTITY PROTECTION
- AZURE AD DOMAIN SERVICES

APPLICATION SECURITY WITH AZURE ACTIVE DIRECTORY - OVERVIEW



APPLICATION SECURITY WITH AZURE ACTIVE DIRECTORY - OVERVIEW

- AZURE ADCONNECT USING PASSWORD HASH SYNC
- AZURE ADCONNECT USING FEDERATION (ADFS)
- AZURE ADCONNECT USING AZURE AD PASSTHROUGH AUTHENTICATION AGENT

AZURE ACTIVE DIRECTORY – CLOUD WAY OF AUTHENTICATION

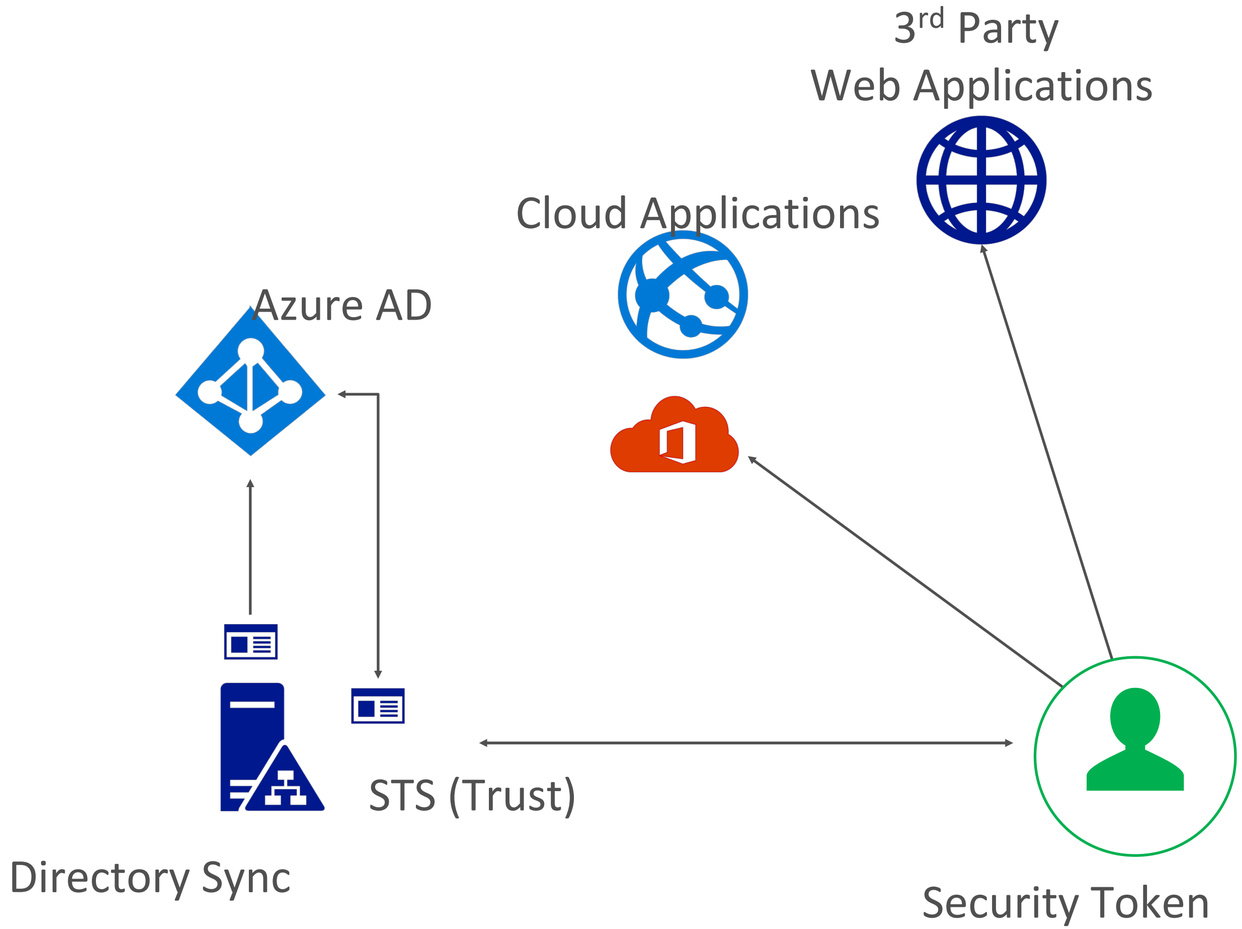
Application management	Manage your cloud and on-premises apps using Application Proxy, single sign-on, the My Apps portal (also known as the Access panel), and Software as a Service (SaaS) apps. For more information, see How to provide secure remote access to on-premises applications and Application Management documentation.
Authentication	Manage Azure Active Directory self-service password reset, Multi-Factor Authentication, custom banned password list, and smart lockout. For more information, see Azure AD Authentication documentation.
Business-to-Business (B2B)	Manage your guest users and external p control over your own corporate data. F Active Directory B2B documentation.
Business-to-Customer (B2C)	Customize and control how users sign u profiles when using your apps. For mor Directory B2C documentation.
Conditional access	Manage access to your cloud apps. For more information, see Azure AD Conditional Access documentation.
Azure Active Directory for developers	Build apps that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or custom APIs. For more information, see Microsoft identity platform (Azure Active Directory for developers).
Device Management	Manage how your cloud or on-premises devices access your corporate data. For more information, see Azure AD Device Management
Privileged identity management (PIM)	Manage, control, and monitor access within your organization. This feature includes access to resources in Azure AD, Azure resources, and other Microsoft Online Services, like Office 365 or Intune. For more information, see Azure AD Privileged Identity Management.
Reports and monitoring	Gain insights into the security and usage patterns in your environment. For more information, see Azure Active Directory reports and monitoring.
Domain services	Join Azure virtual machines to a domain without using domain controllers. For more information, see Azure AD Domain Services documentation.
Enterprise users	Manage license assignment, access to apps, and set up delegates using groups and administrator roles. For more information, see Azure Active Directory user management documentation.
Hybrid	Use Azure Active Directory Connect and Connect Health to provide a ity for authentication and authorization to all resources, ation (cloud or on-premises). For more information, see ocumentation.
	ganization's identity through employee, business service, and app access controls. You can also perform or more information, see Azure AD identity governance and Azure AD access reviews.
Identity protection	Detect potential vulnerabilities affecting your organization's identities, configure policies to respond to suspicious actions, and then take appropriate action to resolve them. For more information, see Azure AD Identity Protection.
Managed identities for Azure resources	Provides your Azure services with an automatically managed identity in Azure AD that can authenticate any Azure AD-supported authentication service, including Key Vault. For more information, see What is managed identities for Azure resources?.

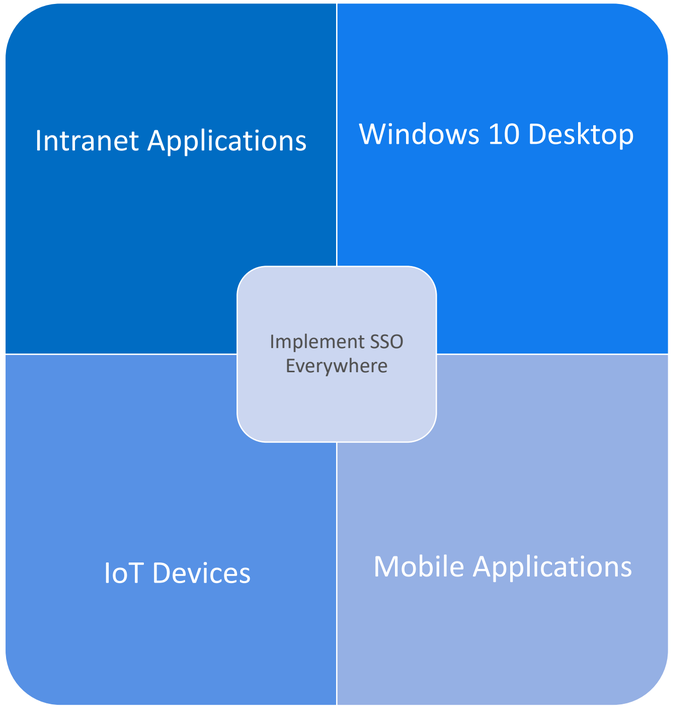
AZURE ACTIVE DIRECTORY – CLOUD WAY OF AUTHENTICATION

Authentication Protocols Articles and Reference

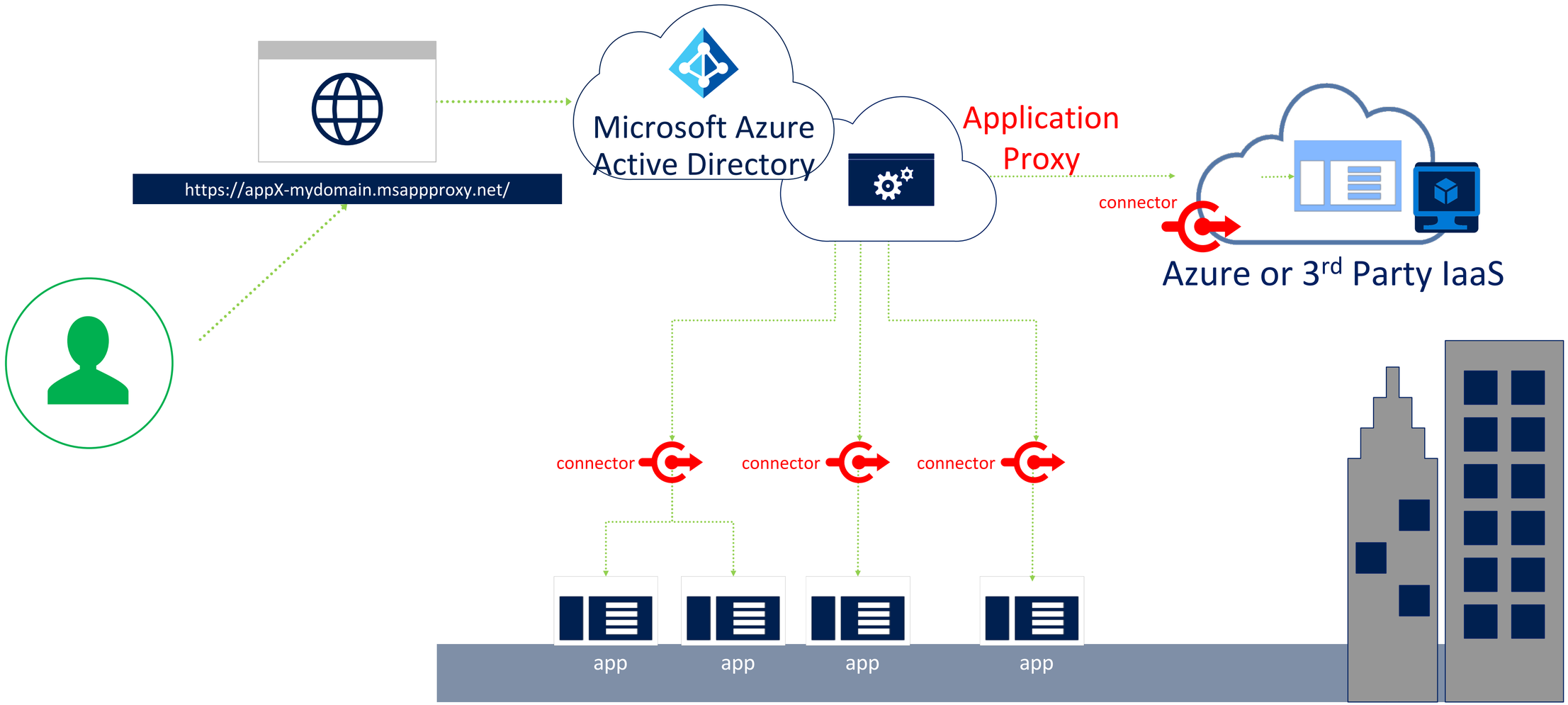
- Important Information About Signing Key Rollover in Azure AD – Learn about Azure AD's signing key rollover cadence, changes you can make to update the key automatically, and discussion for how to update the most common application scenarios.
- Supported Token and Claim Types - Learn about the claims in the tokens that Azure AD issues.
- Federation Metadata - Learn how to find and interpret the metadata documents that Azure AD generates.
- OAuth 2.0 in Azure AD - Learn about the implementation of OAuth 2.0 in Azure AD.
- OpenID Connect 1.0 - Learn how to use OAuth 2.0, an authorization protocol, for authentication.
- Service to Service Calls with Client Credentials - Learn how to use OAuth 2.0 client credentials grant flow for service to service calls.
- Service to Service Calls with On-Behalf-Of Flow - Learn how to use OAuth 2.0 On-Behalf-Of flow for service to service calls.
- SAML Protocol Reference - Learn about the Single Sign-On and Single Sign-out SAML profiles of Azure AD.

AZURE ACTIVE DIRECTORY – CLOUD WAY OF AUTHENTICATION

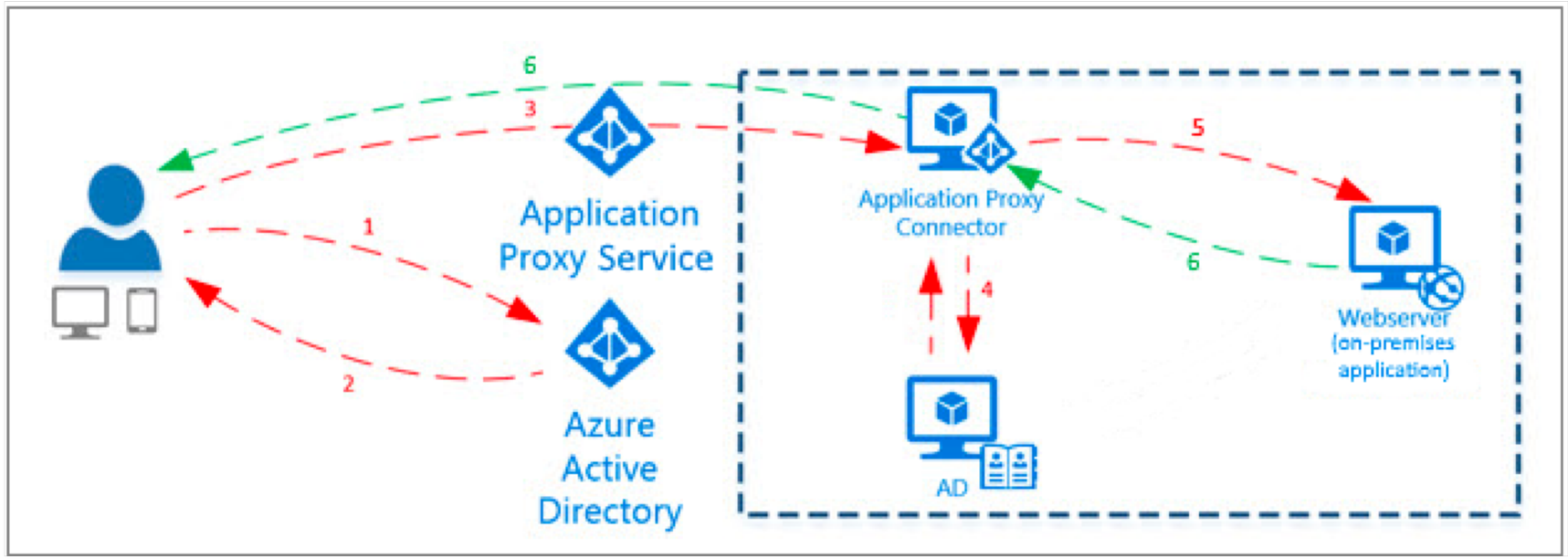




AZURE APPLICATION PROXY



AZURE APPLICATION PROXY



AZURE AD AUTHENTICATION SCENARIOS

IN ANY OF THE “CLOUD” SCENARIOS, AD CONNECT USER/GROUP OBJECT SYNC IS REQUIRED

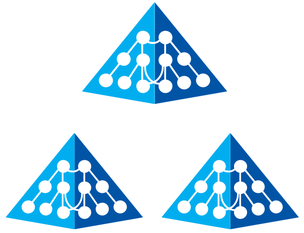
- REPLACES LEGACY TOOLS => **DIRSYNC, ADSYNC, FIM WITH AD CONNECTOR**
- BENEFITS
- ALLOWS FOR WRITE-BACK (PASSWORDS, DEVICES, GROUPS) TO ON-PREMISES AD
- BUILT-IN DEPLOYMENT WIZARD FOR ON-PREMISES ADFS INFRASTRUCTURE
- AZURE AD CONNECT SYNCHRONIZATION SERVICES DASHBOARD
- MANAGED USER SIGN-IN OPTIONS

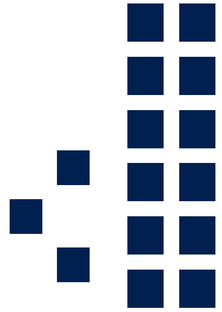
AZURE AD AUTHENTICATION SCENARIOS – PASSWORD (HASH)

1st option: Identity + Password (Hash) synchronization

Identity +
Password Hash
synchronization

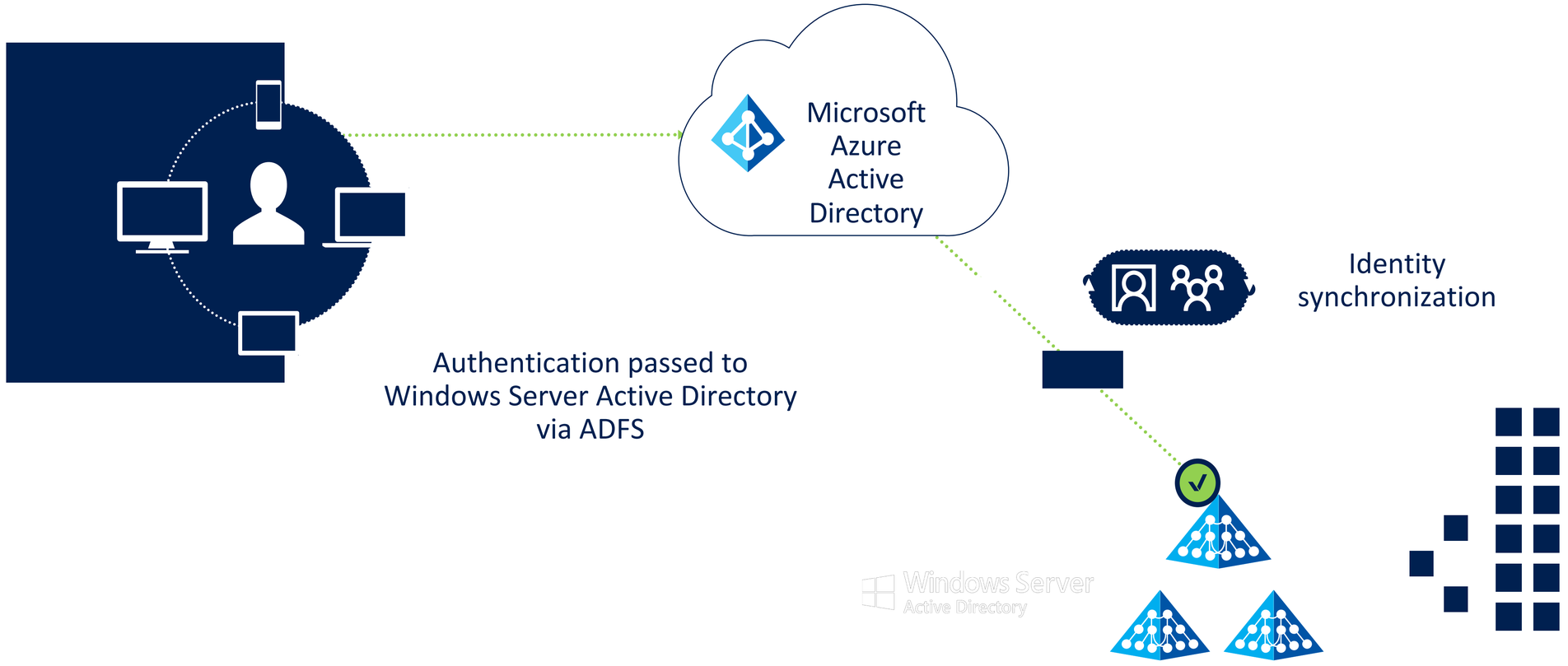
Azure Active Directory
authenticates user





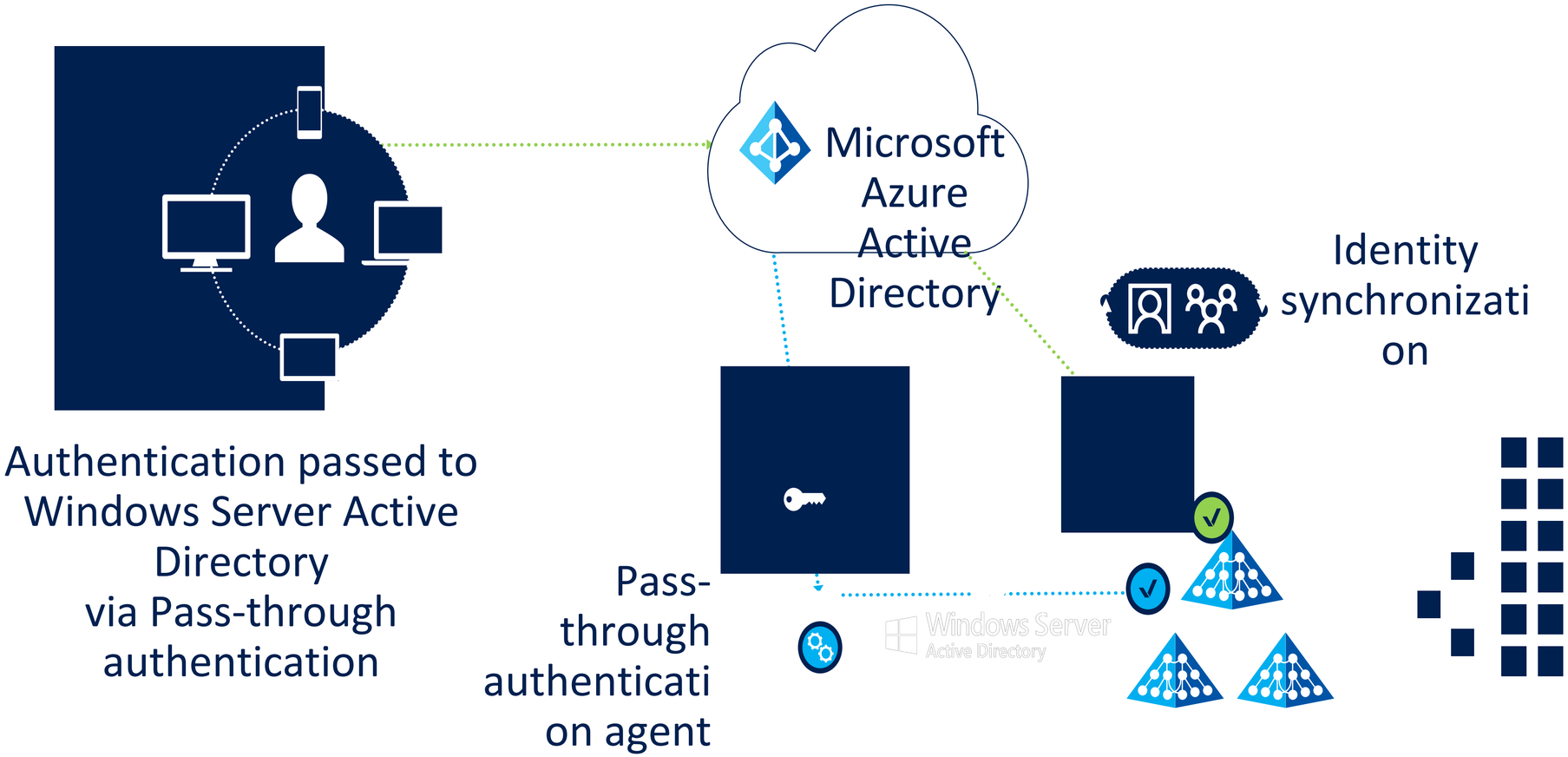
AZURE AD – IDENTITY SYNC. + PASS THROUGH WITH SSO

2nd option: Identity synchronization + ADFS



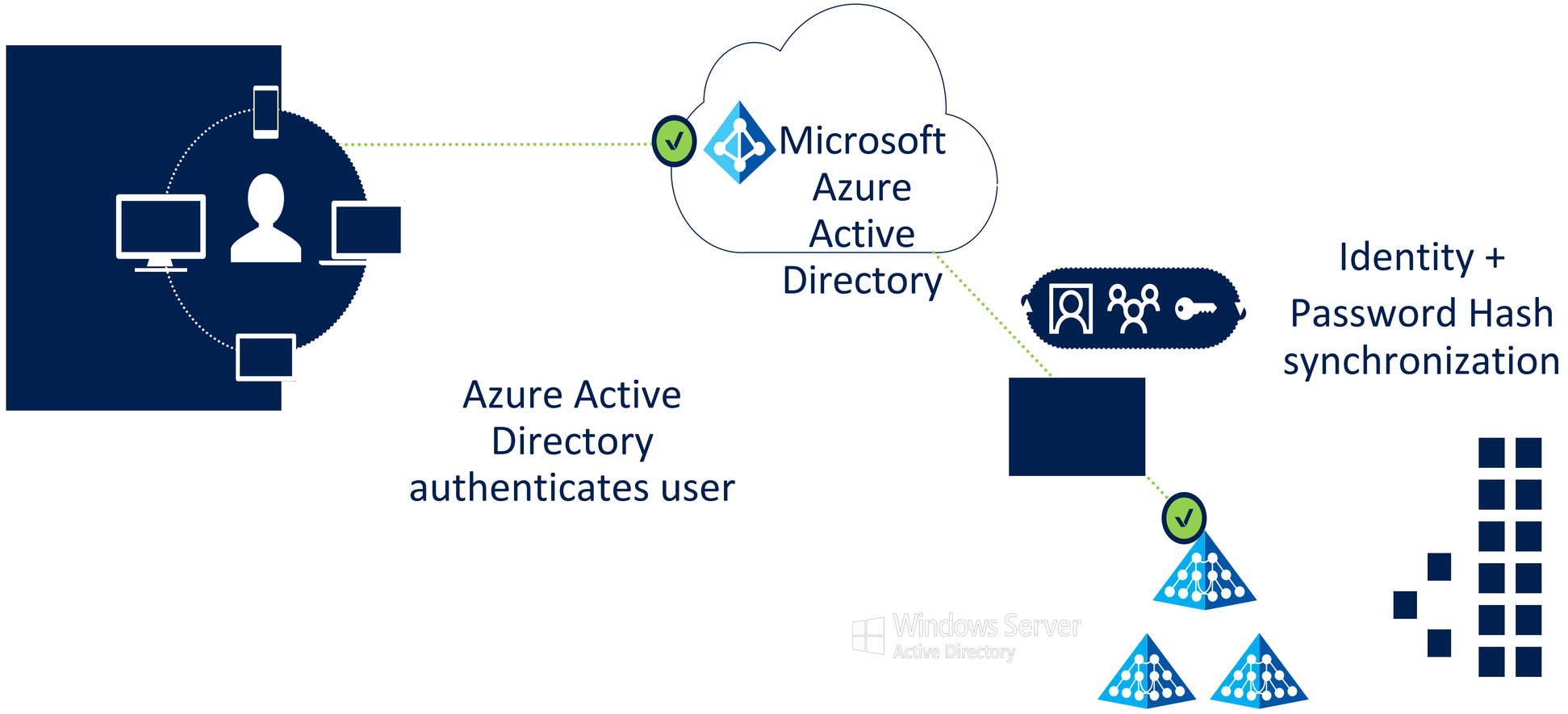
AZURE AD – PASS-THROUGH AUTHENTICATION WITH SEAMLESS SSO

New option: Identity synchronization + Pass-through authentication with Seamless SSO



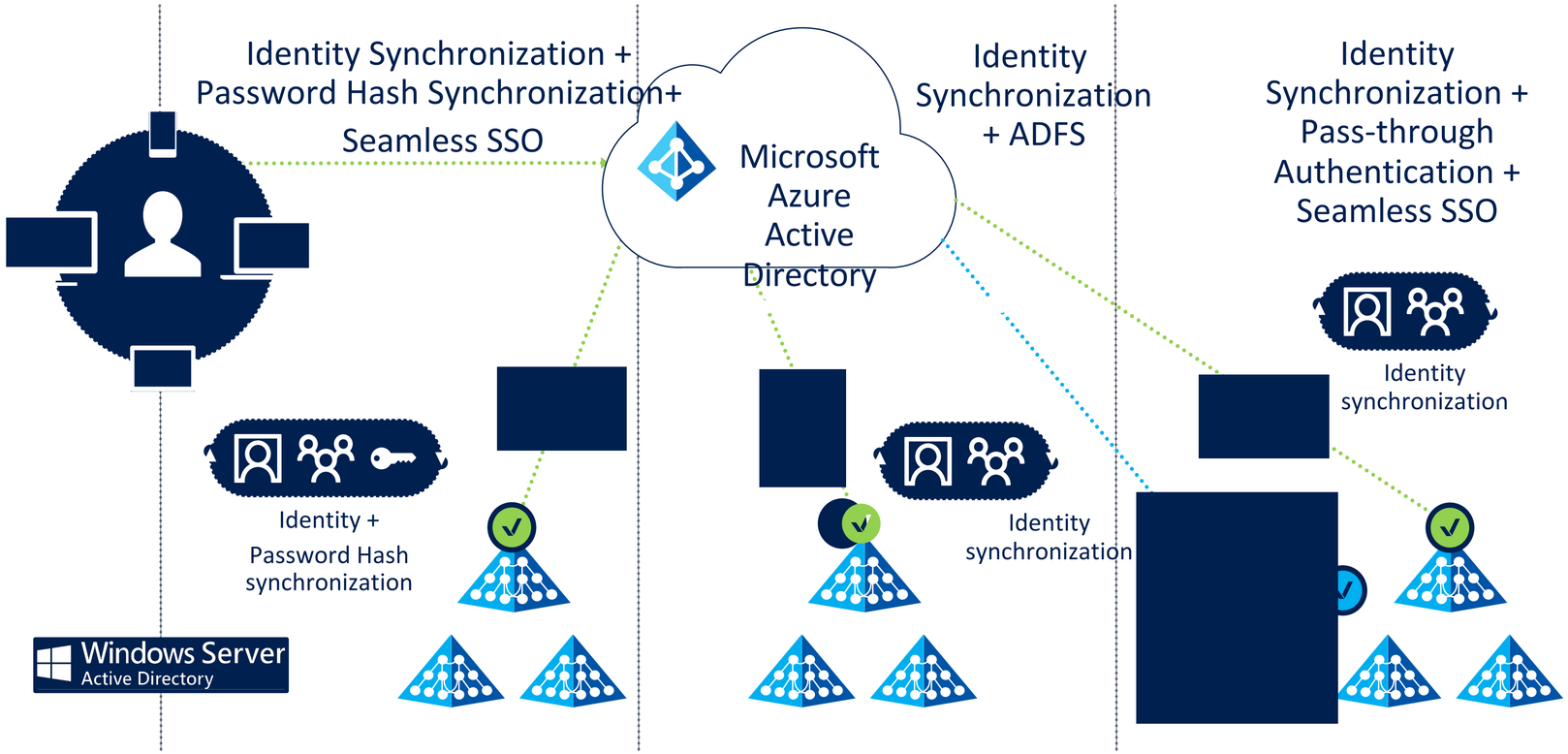
AZURE AD – IDENTITY SYNC. + PASS THROUGH WITH SSO

Seamless SSO is now enabled for the 1st option, too: Identity + Password (Hash) synchronization



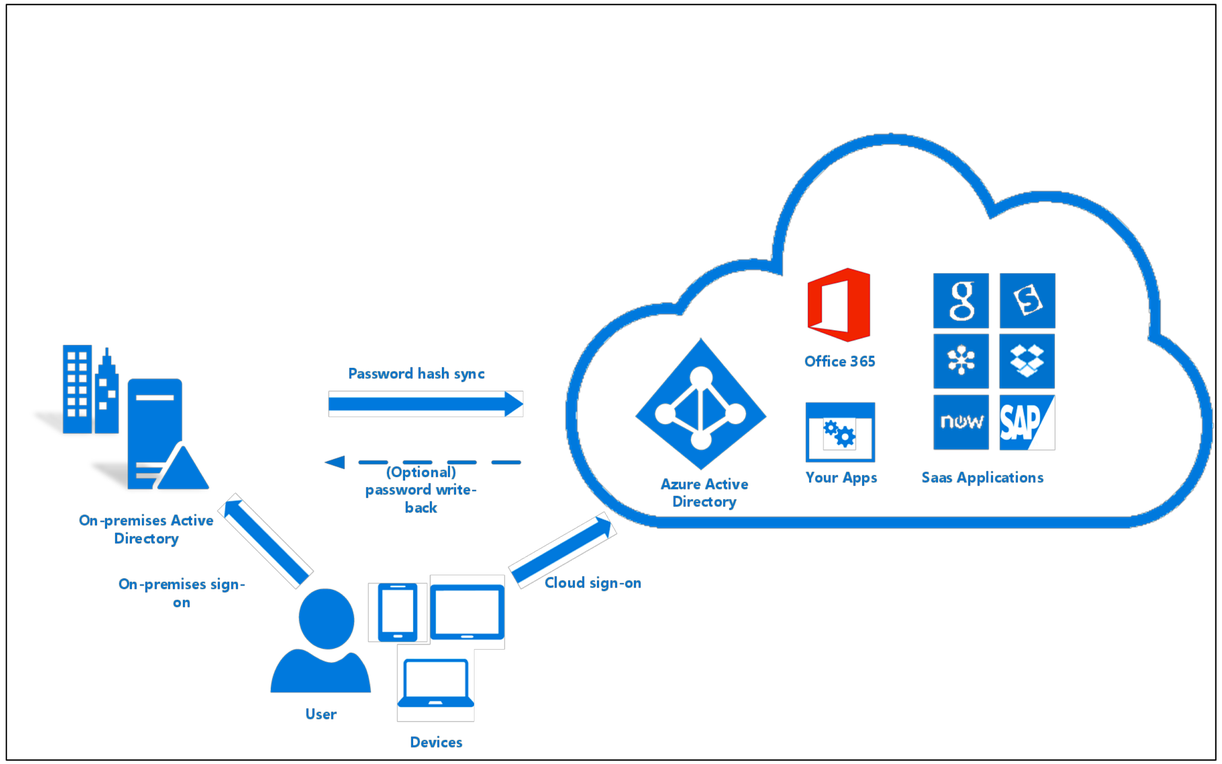
AZURE AD – OVERVIEW OF SERVICES

More options than ever!



AZURE AD – HYBRID IDENTITY

- CONSOLIDATED DEPLOYMENT ASSISTANT FOR YOUR IDENTITY BRIDGE COMPONENTS
- AD CONNECT – DEDIDCATED SOLUTION AT THE MOMENT FOR USER / PASS SYNC
- ASSISTED DEPLOYMENT OF ADFS WILL BE AVAILABLE THROUGH AZURE ACTIVE DIRECTORY CONNECT
- ADFS IS AN OPTIONAL COMPONENT FOR AUTHENTICATION IN HYBRID IMPLEMENTATION. PASSWORD SYNC CAN REPLACE ADFS FOR MORE SCENARIOS



AZURE AD – OTHER POSSIBILITIES

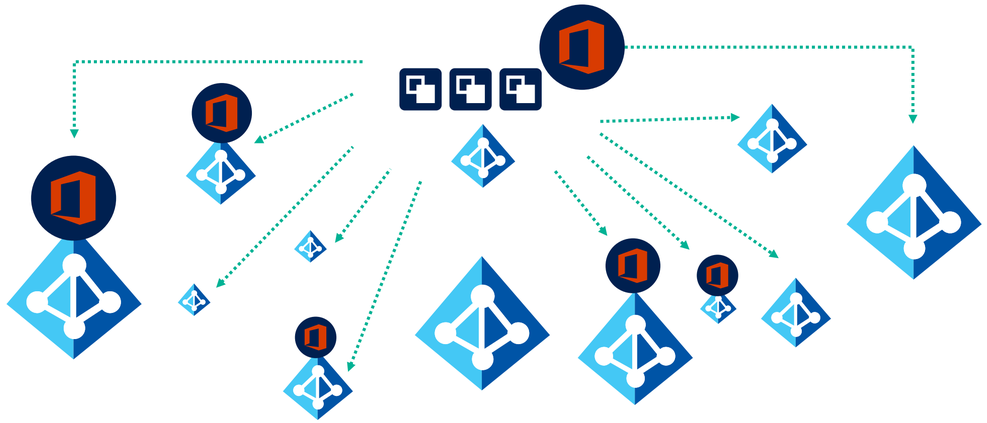
- **B2B (BUSINESS TO BUSINESS)**
  - COLLABORATE BETWEEN ORGANIZATIONS
  - AVOID FEDERATION AND EXTRA SERVERS
  - ADD OTHER AAD USERS TO THE ONE, YOU HAVE ACCESS TO

- **B2C (BUSINESS TO CUSTOMER)**
  - USE THEIR EXISTING IDENTITIES FROM EXTERNAL, CONSUMER SOURCES
  - AVOID CREATING ADDITIONAL IDENTITIES

- **MFA (MULTI-FACTOR AUTHENTICATION)**
  - FURTHER AUTHENTICATE USERS
  - AVOID COMPROMISES DUE TO SIMPLE PASSWORD CONSTRAINTS

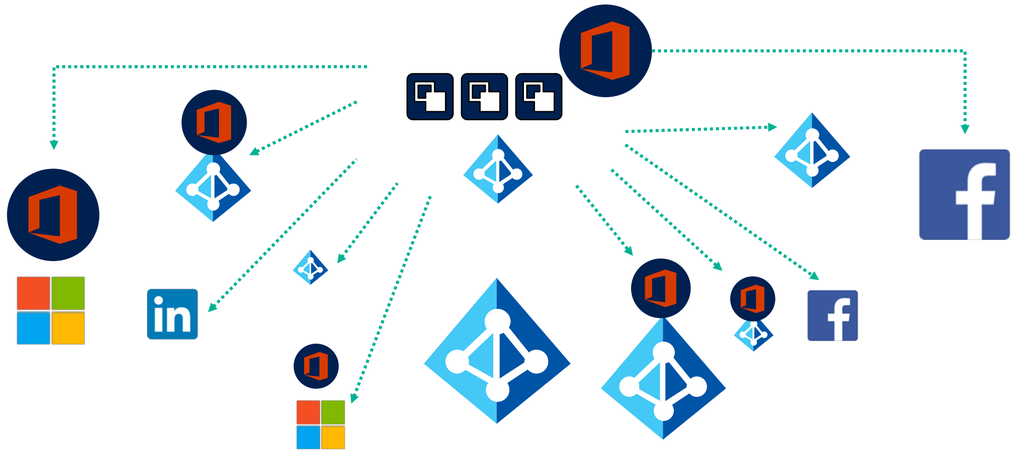
AZURE AD B2B

- **B2B (BUSINESS TO BUSINESS)**
  - INVITING USERS FROM OTHER AZURE AD TENANTS INTO YOUR OWN ORGANIZATION TENANT
  - USER PROVISIONING IS DONE BY THE INVITED PARTY
  - YOU AS AN ORGANIZATION ARE IN CONTROL TO INVITE THE OTHER SIDE'S USER



AZURE AD B2C

- **B2C (BUSINESS TO CONSUMER)**
  - INVITING USERS FROM OTHER SOCIAL MEDIA IDENTITY TENANTS (E.G. FACEBOOK, TWITTER, GOOGLE, LINKEDIN, MICROSOFT ACCOUNT) INTO YOUR OWN ORGANIZATION TENANT
  - USER PROVISIONING IS DONE BY THE INVITED PARTY
  - YOU AS AN ORGANIZATION ARE IN CONTROL TO INVITE THE OTHER SIDE'S USER



AZURE AD MULTI-FACTOR AUTHENTICATION

WHAT IS IT?:

- AN AUTHENTICATION METHOD, WHICH REQUIRES AN ADDITIONAL VALIDATION ITEM, BESIDES YOUR USERNAME AND PASSWORD COMBINATION:
- TEXT MESSAGE
- AZURE AUTHENTICATION APP
- HOW DOES MFA WORK?
- REQUIRES 2 OR MORE (CONFIGURABLE) ACCOUNT VALIDATION OPTIONS:
  - SOMETHING YOU KNOW (TYPICALLY USER/PASSWORD COMBINATION)
  - SOMETHING YOU HAVE (MOBILE AUTHENTICATOR APP)

AZURE AD IDENTITY PROTECTION

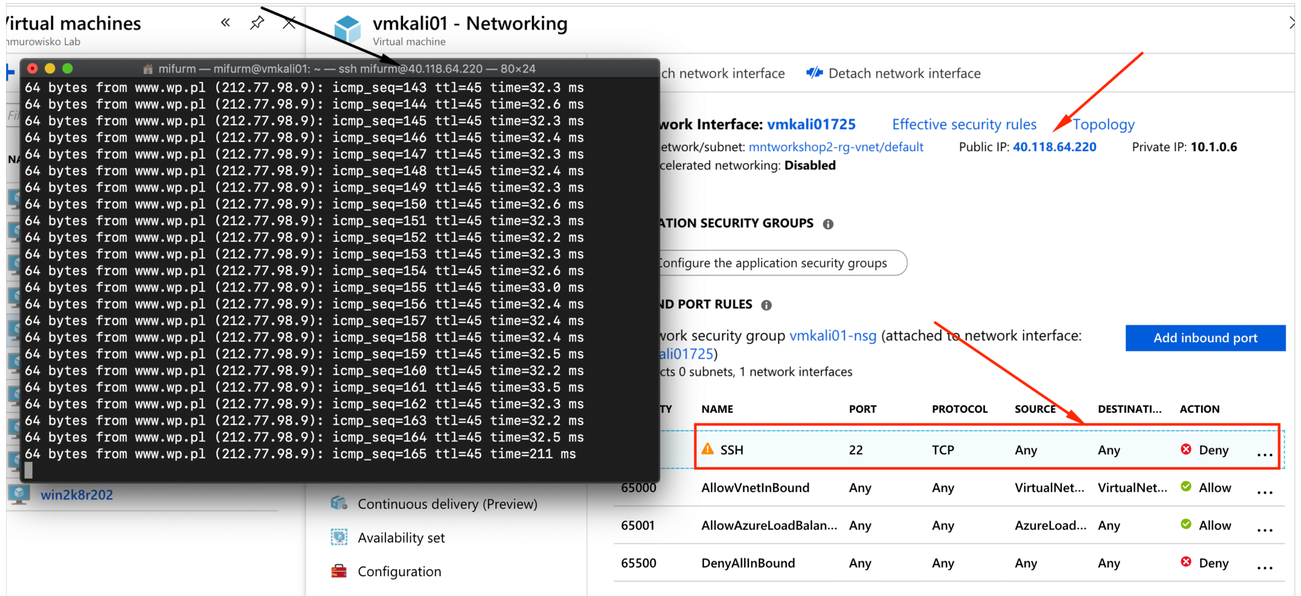
WHAT IS IT?:

- AUTOMATIC DETECTION OF VULNERABILITIES IN YOUR ORGANIZATION'S IDENTITY OBJECTS (E.G., COMPROMISED USER ACCOUNTS)
- DEFINE CONFIGURATION ALERTS AND AUTOMATIC RESPONSES (RUNBOOKS), TO DETECTED SUSPICIOUS AND MALICIOUS ACTIONS THAT OCCUR IN YOUR ORGANIZATION'S IDENTITY SOLUTION
- RECOGNIZE, AUDIT AND INSPECT SUSPICIOUS ACTIVITY, AND TAKE APPROPRIATE ACTION TO RESOLVE THEM

AZURE AD PRIVILEGED IDENTITY MANAGEMENT

WHAT IS IT?:

- DETECT PRIVILEGED USERS IN AZURE ACTIVE DIRECTORY
- ENABLE “JUST-IN-TIME” ADMINISTRATIVE LEVEL ACCESS TO MICROSOFT CLOUD SERVICES
- DETAILED REPORTING RELATED TO WHO GOT WHAT ADMINISTRATIVE ACCESS LEVEL
- AUTOMATICALLY GIVE USERS PERMISSION TO HAVE PERMANENT ADMIN-LEVEL RIGHT ACCESS, OR ALLOW FOR SELF-SERVICE GROUP MEMBERSHIP



AZURE AD DOMAIN SERVICES

SOME APPLICATIONS DON'T "SPEAK" CLOUD:

- THE APPLICATION RELIES ON ACTIVE DIRECTORY PROTOCOLS (LDAP, KERBEROS,…)
- AZURE AD DOESN'T PROVIDE GROUP POLICIES
- AZURE AD DOESN'T PROVIDE ORGANIZATIONAL UNITS
- YOU CANNOT "JOIN" SERVERS INTO AN AZURE AD TENANT

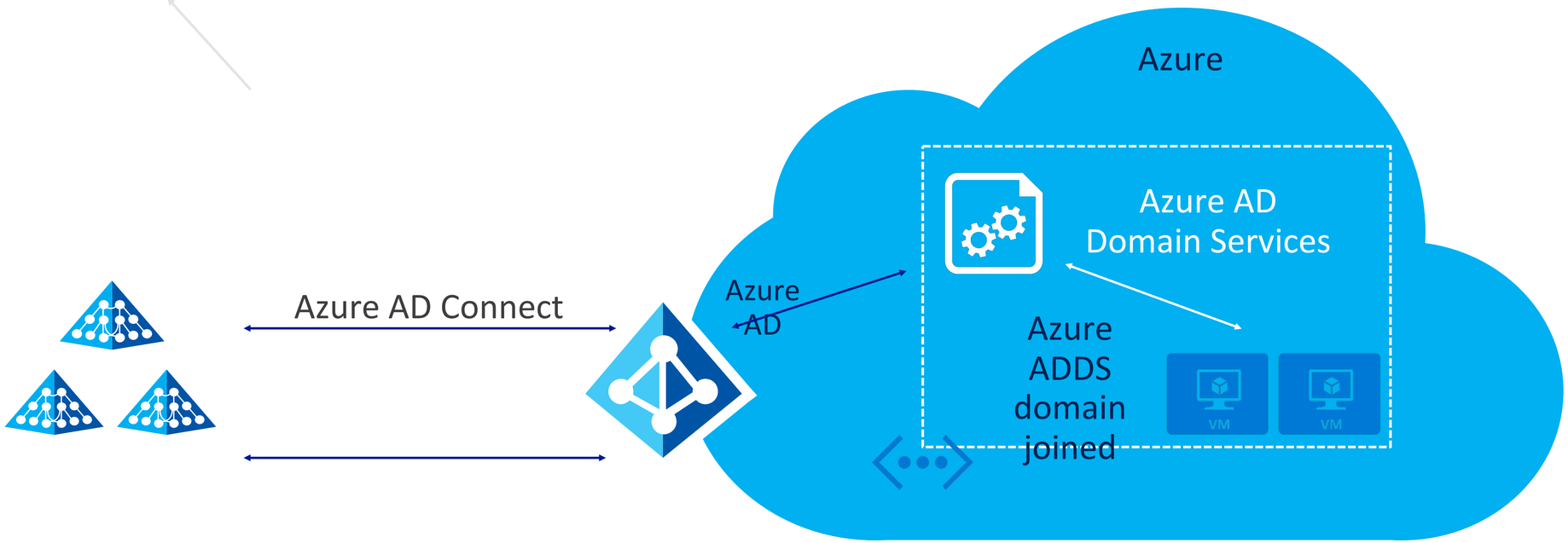
Feature	Azure AD Domain Services	'Do-it-yourself' AD in Azure VMs
Managed service	✓	✕
Secure deployments	✓	Administrator needs to secure the deployment.
DNS server	✓ (managed service)	
Domain or Enterprise administrator privileges	✕	
Domain join	✓	
Domain authentication using NTLM and Kerberos	✓	
Kerberos constrained delegation	resource-based	resource-based & account-based
Custom OU structure	✓	✓
Schema extensions	✕	✓
AD domain/forest trusts	✕	✓
LDAP read	✓	✓
Secure LDAP (LDAPS)	✓	✓
LDAP write	✕	✓
Group Policy	✓	✓
Geo-distributed deployments	✕	✓

AZURE AD DOMAIN SERVICES

KEY CHARACTERISTICS

- PROVIDES A COMPATIBILITY LAYER FOR ACTIVE DIRECTORY INTEGRATED APPLICATIONS, ON TOP OF AZURE AD
- TAKES RESOURCES FROM AZURE AD TO “EMULATE” AN ACTIVE DIRECTORY DOMAIN (USERS, GROUPS, MEMBERSHIPS, PASSWORDS, LIMITED GPOS)
- ONE AAD DS PER AZURE AD
- HIGH AVAILABILITY BUILT-IN

AZURE AD DOMAIN SERVICES



APPLICATION SECURITY WITH AZURE ACTIVE DIRECTORY - SUMMARY

- AZURE ACTIVE DIRECTORY
- AZURE AD AUTHENTICATION STRATEGIES
- AZURE AD B2B & B2C
- AZURE AD IDENTITY PROTECTION
- AZURE AD DOMAIN SERVICES

AZURE TOOLS TO MONITOR AND SECURE THE ENVIRONMENT