

Bezbedonosni inženjering

Uroš Babić

Security Architect at Crayon, Microsoft Security MVP, MCT

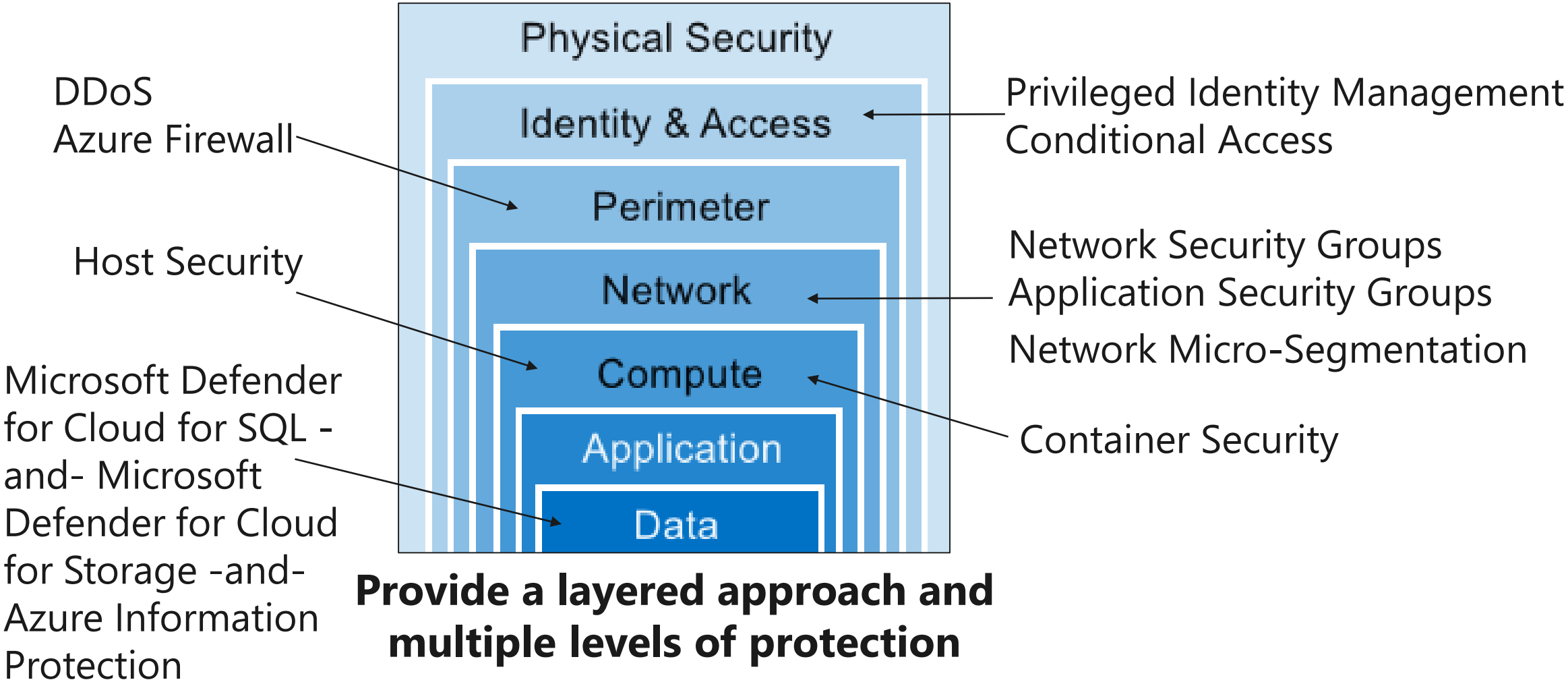
uros.babic@crayon.com



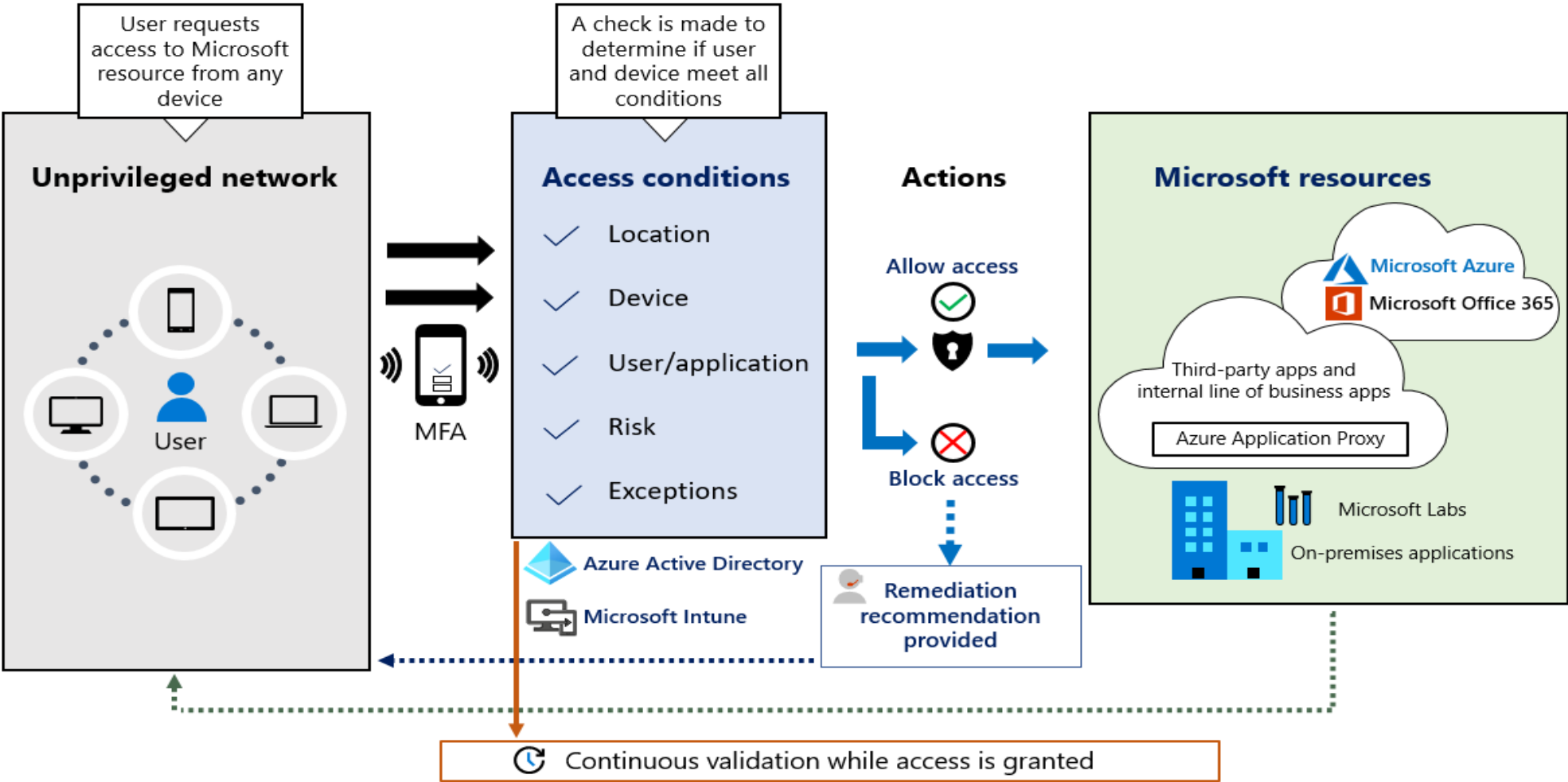
Agenda:

- ❑ Modeli bezbednosti: dubinska odbrana, Zero trust okvir
- ❑ Bezbedonosne prakse:
 - network security,
 - endpoint security,
 - email security
- ❑ Upravljanje identitetima i dozvolama za pristup
- ❑ Autentifikacija, autorizacija, višefaktorska autentifikacija (MFA)
- ❑ Single sign-on
- ❑ Upravljanje privilegovanim identitetima

Defense in Depth



Microsoft's Zero Trust Model



Microsoft's Zero Trust Model

Pre-Zero Trust	Verify identity	Verify device	Verify access	Verify services
 ✗ Device management isn't required ✗ Single factor authentication to resources ✓ Capability to enforce strong identity exists ✓ Data classification and information protection exists	 ✓ Strong identity is verified and enforced ✓ Passwords are eliminated in favor of biometrics ✓ Access to applications and data is limited to minimum required to perform job function	 ✓ Client device health is enforced ✓ Unmanaged devices have secure alternative access methods ✓ Users don't have administrative permissions on client devices	 ✓ Internet is the default network in all Microsoft office locations ✓ Network segmentations are built based on role and function	 ✓ Applications and conditions are enforced using conditional access ✓ Applications and services are accessible directly from the internet
Pervasive telemetry				

Microsoft's Zero Trust Model

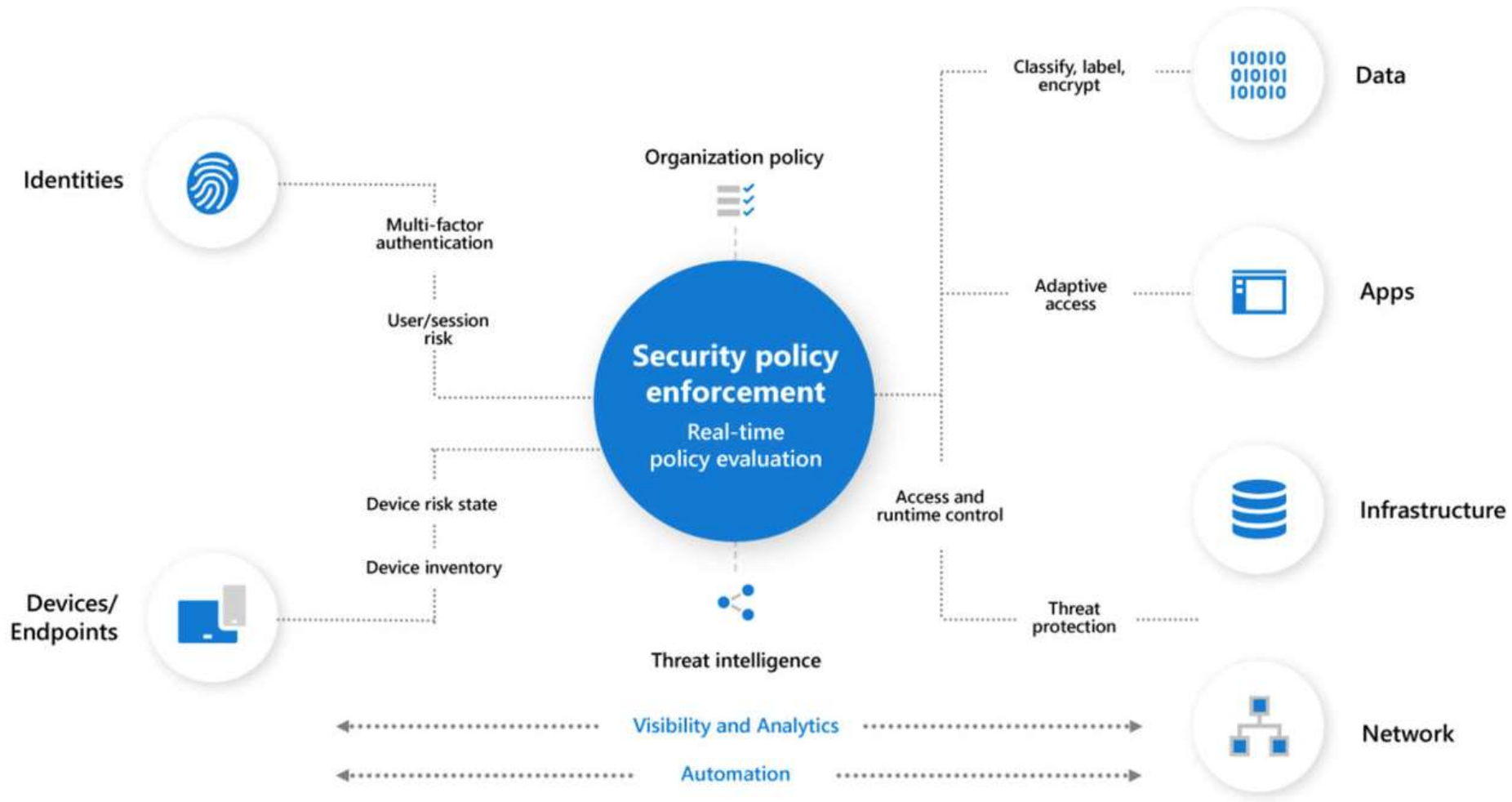
Modernized security architecture principles, defined by The Open Group
Embraced by Microsoft and many other vendors in their reference architectures

The Zero Trust Security Architecture principles are:

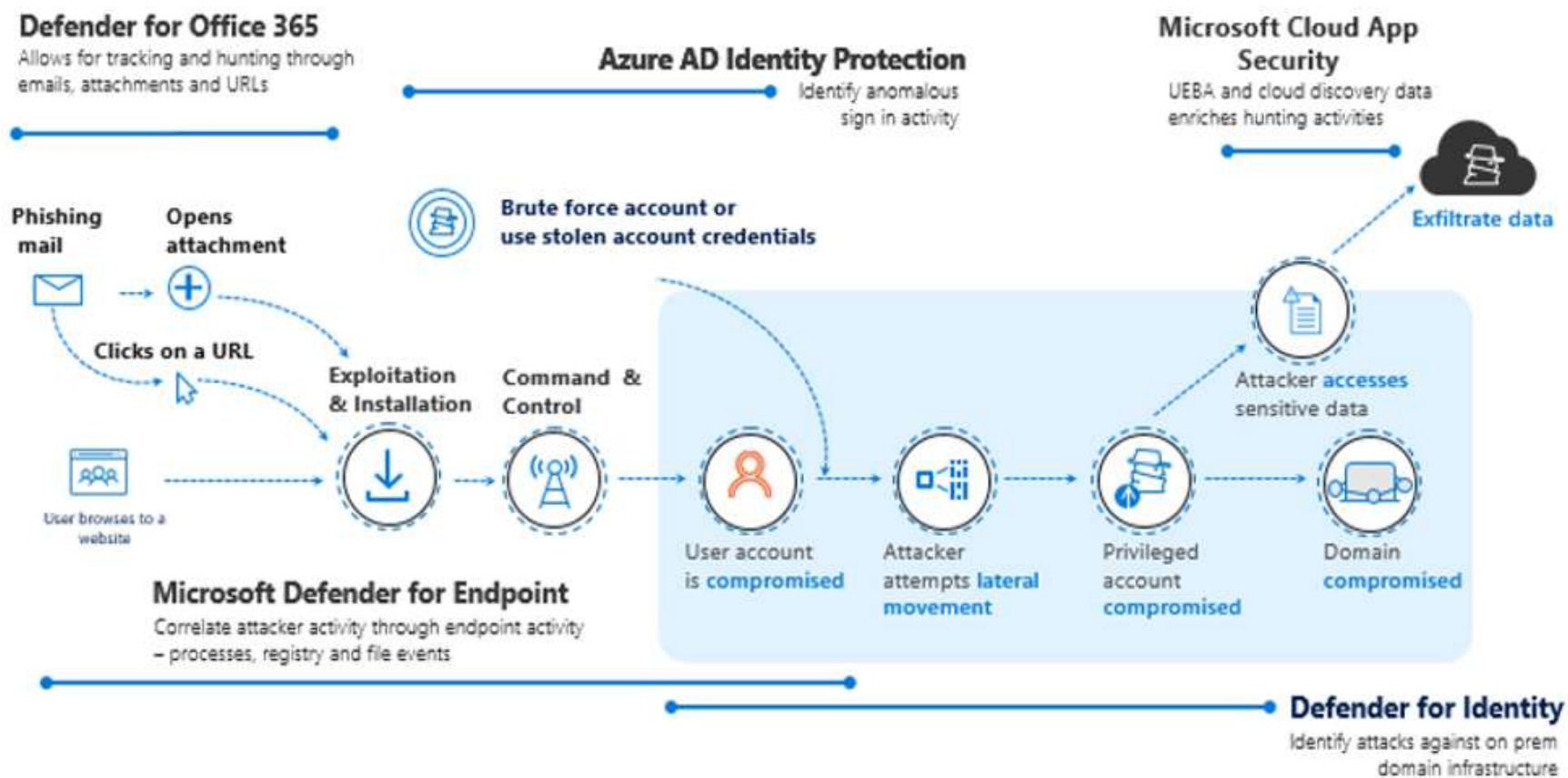
- 1. Verify explicitly**
Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.
- 2. Use least privileged access**
Limit user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive policies, and data protection to help secure both data and productivity.
- 3. Assume breach**
Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and app awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defenses.

Microsoft's Zero Trust Model

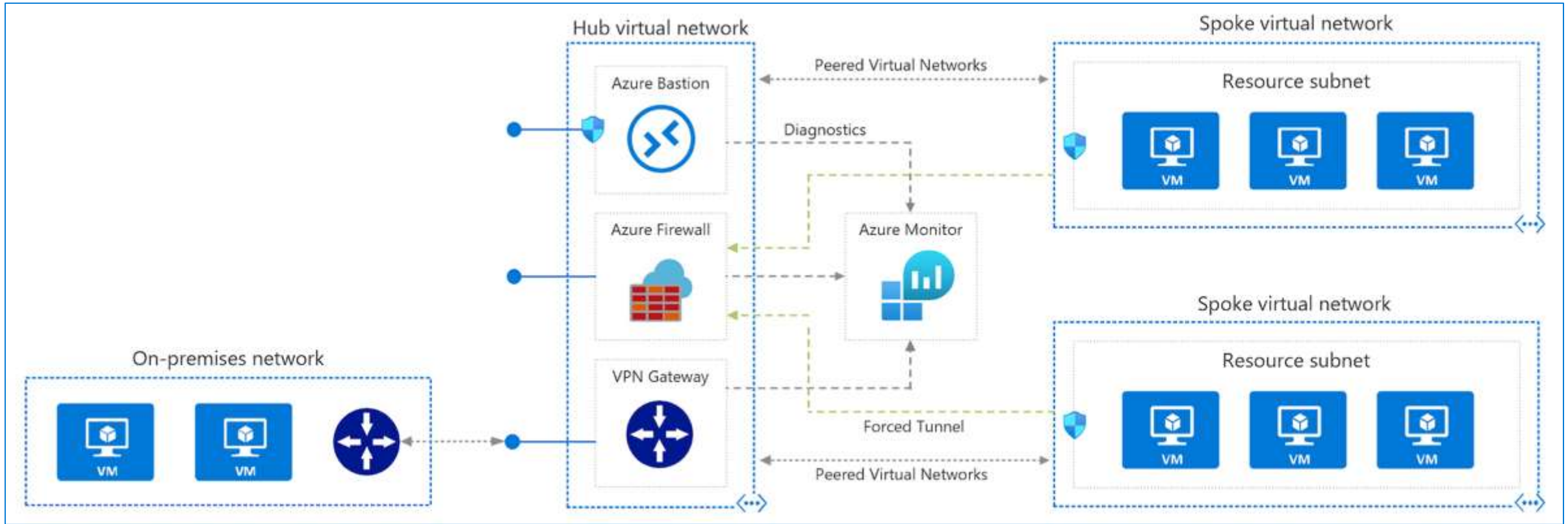
Assume breach and verify each request as though it originates from an open network



Hunting through attack chain



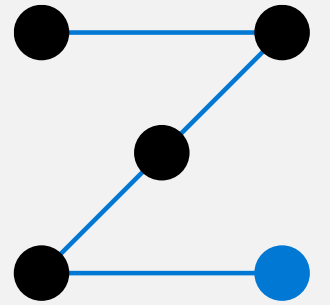
Hub and Spoke topology with Azure



Hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network.

Spokes are virtual networks that peer with the hub and can be used to isolate workloads.

Network Security



Network Security



Network Security Groups (NSG)



NSG Implementation



Application Security Groups



Service Endpoints



Private Endpoints



Azure Application Gateway



Web Application Firewall



Azure Front Door



ExpressRoute

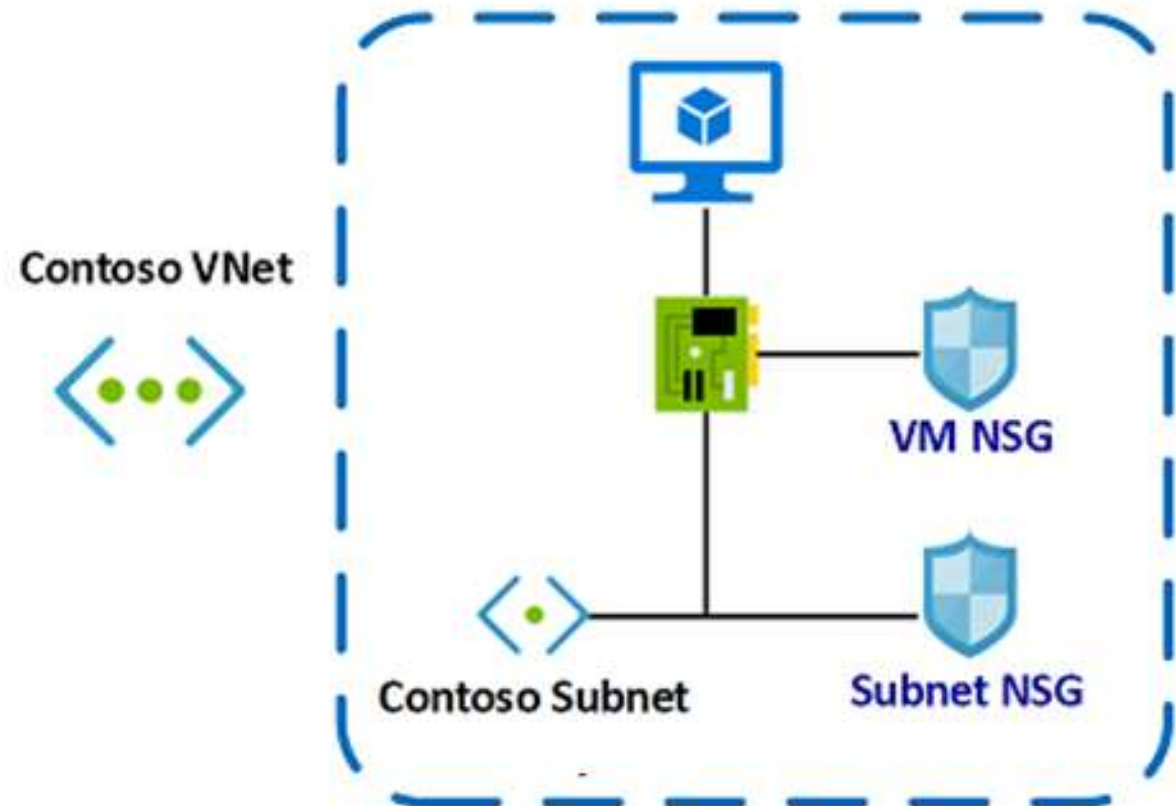
Network Security Groups (NSG)

Limit virtual network traffic

Can be associated to a subnet or a network interface

Uses security rules to allow or deny network traffic

Default inbound and outbound rules allow virtual network and load balancers – all other traffic denied



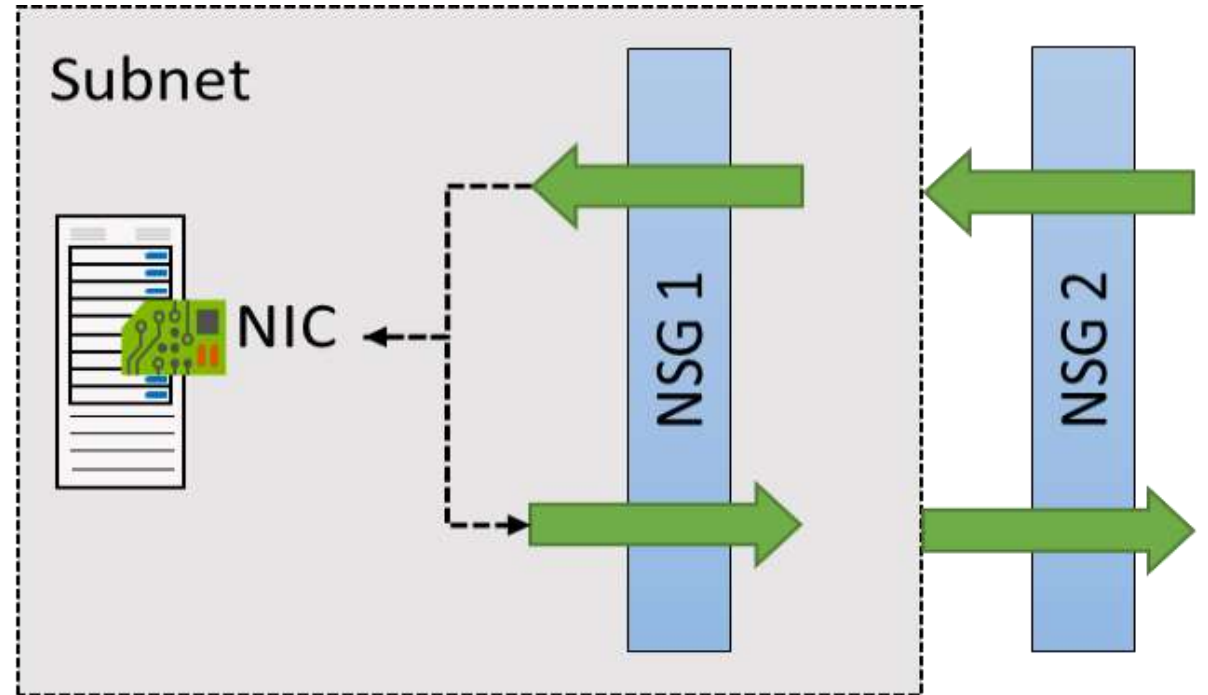
NSG Implementation

NSGs are evaluated independently for the subnet and NIC

An “allow” rule must exist at both levels for traffic to be admitted

You can add more rules – many preconfigured selections (SSH, RDP, FTP...)

Troubleshoot with the Effective Security Rules link



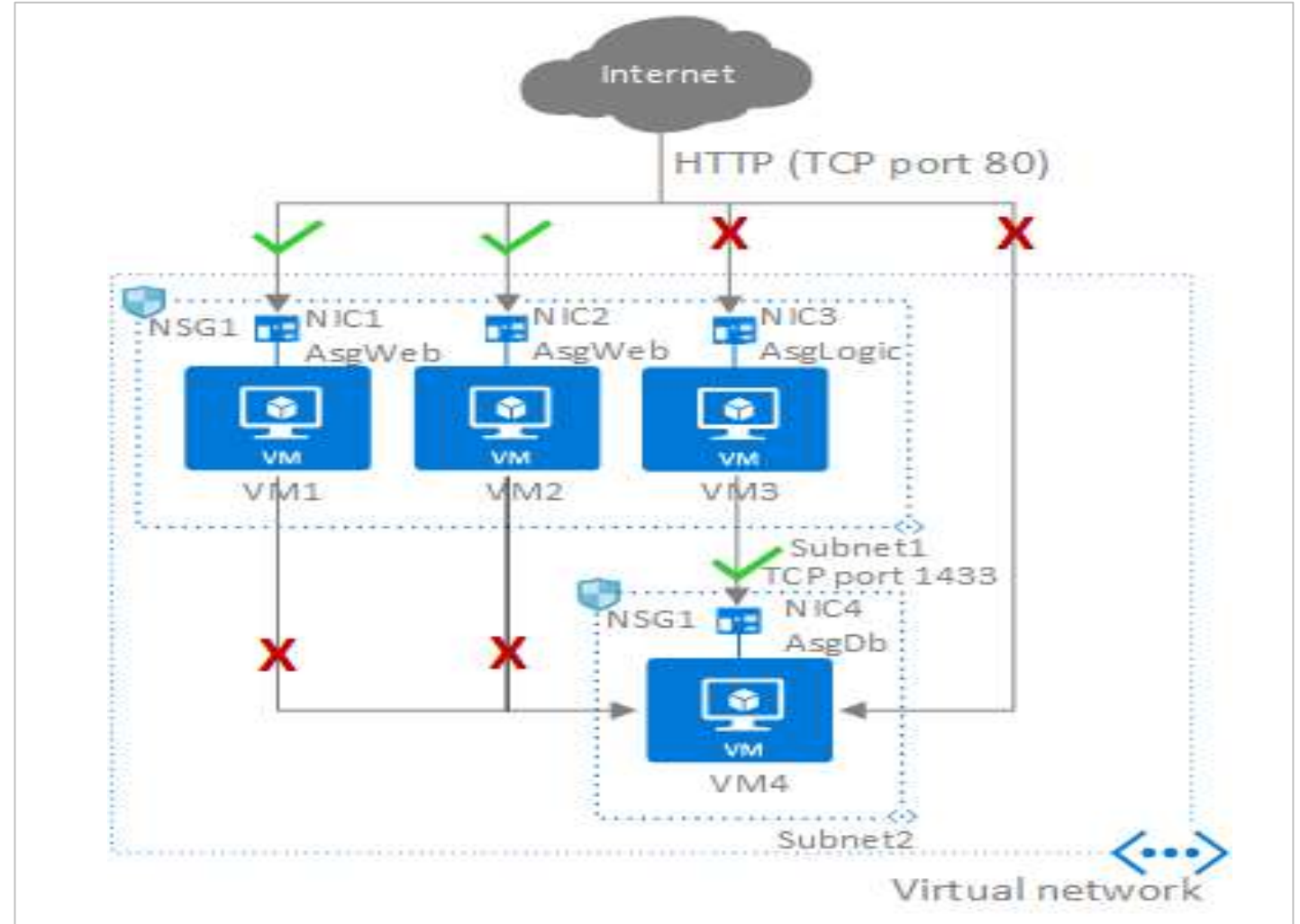
Application Security Groups (ASGs)

Extends your application's structure

ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

Wrap the ASG with an NSG for added security



Service Endpoints

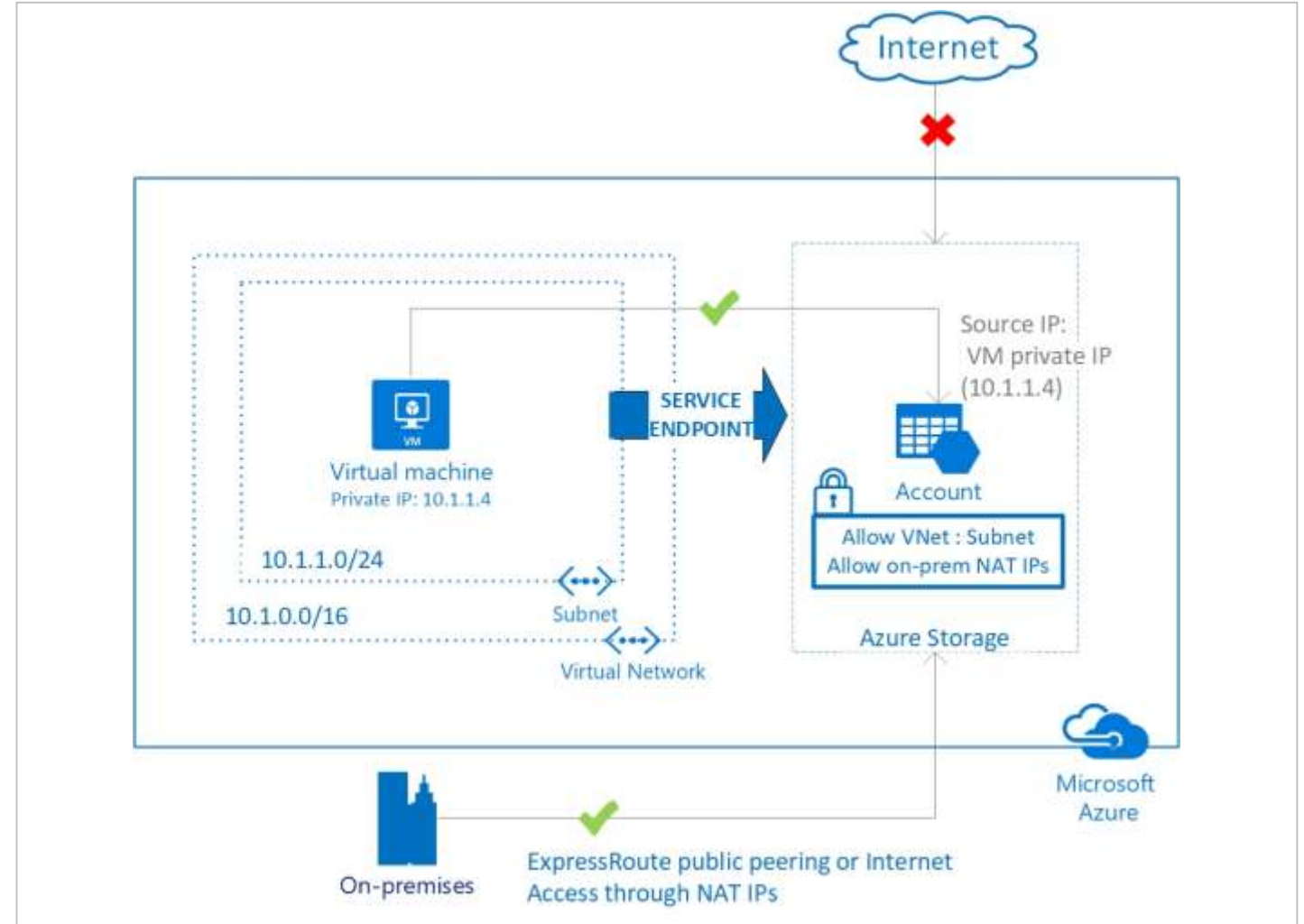
Endpoints limit network access to specific subnets and IP addresses

Improved security for your Azure service resources

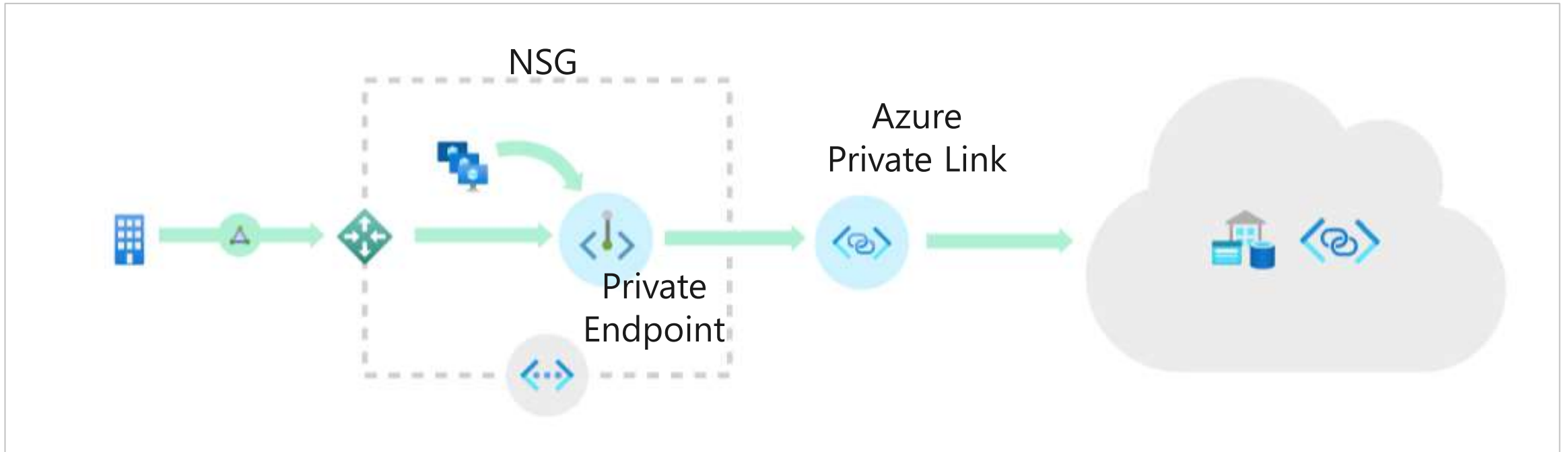
Optimal routing for Azure service traffic from your virtual network

Endpoints use the Microsoft Azure backbone network

Simple to set up with less management overhead



Private Endpoint



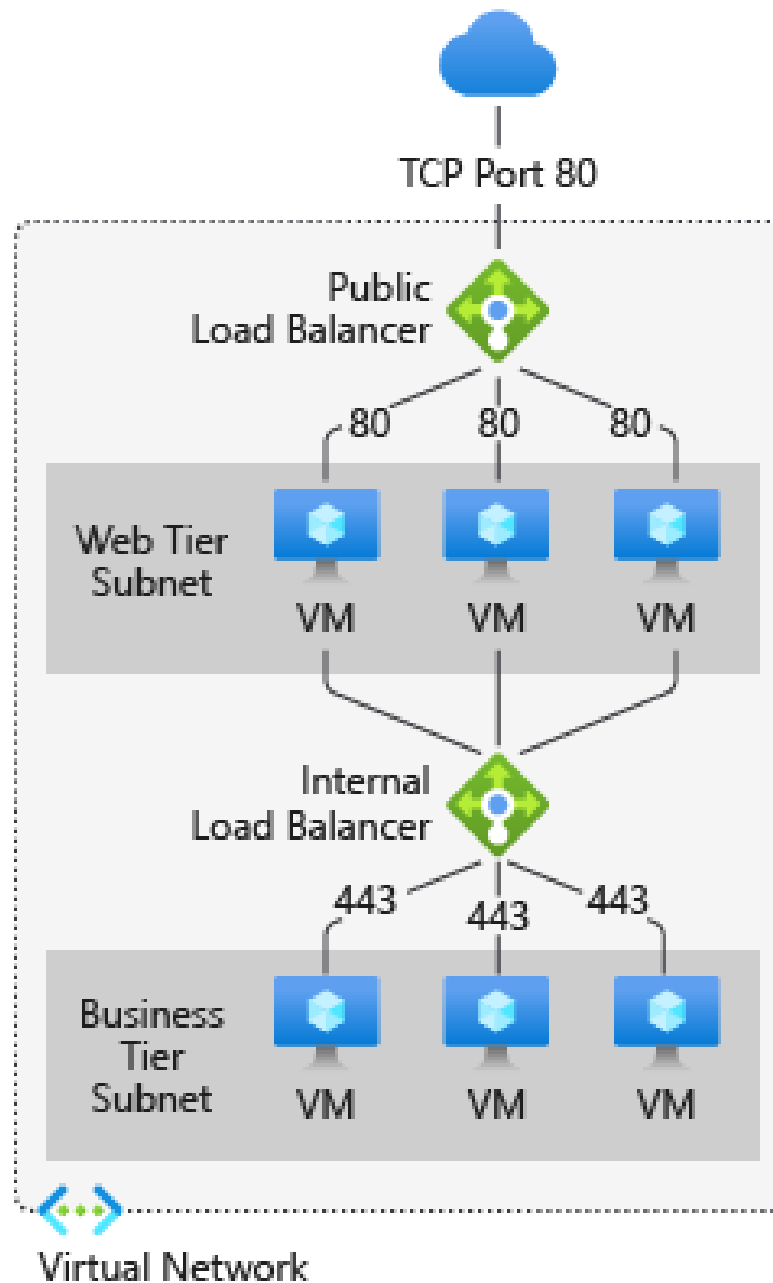
Private connectivity to services on Azure

Integration with on-premises and peered networks

Traffic remains on the Microsoft network, with no public internet access

During a security incident within your network, only the mapped resource would be accessible

Load Balancer



Balancing multi-tier applications by using both **public** and **internal** Load Balancer

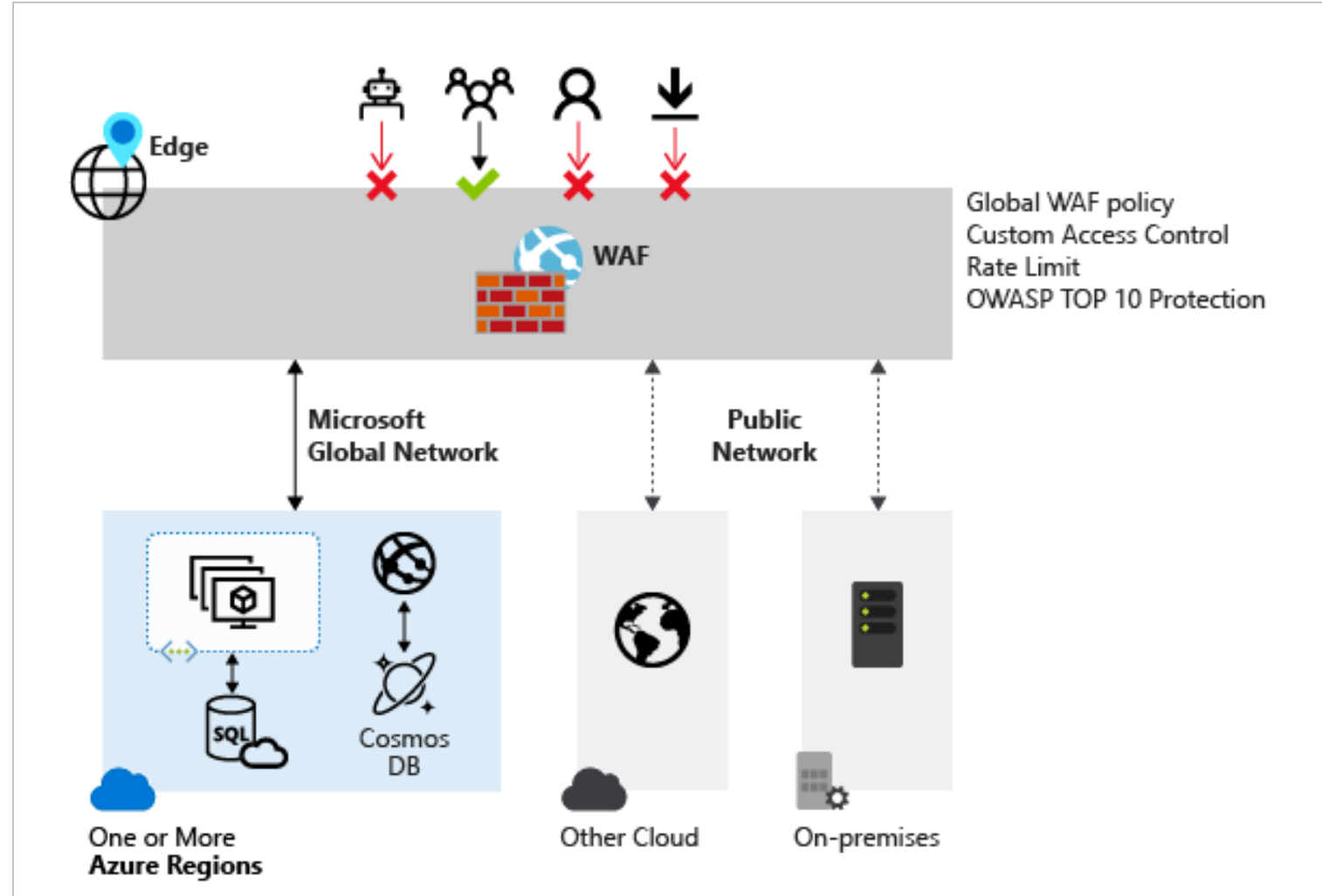
Web Application Firewall

Protects against cross site scripting and SQL injection

OWASP Core Rule sets 3.1, 3.0, 2.29

Custom access control

Supports Azure Front Door, Azure Application Gateway, and CDN (preview)



Azure Front Door

Layer 7 global routing

Accelerate application performance with anycast and split TCP

URL-based routing and session affinity

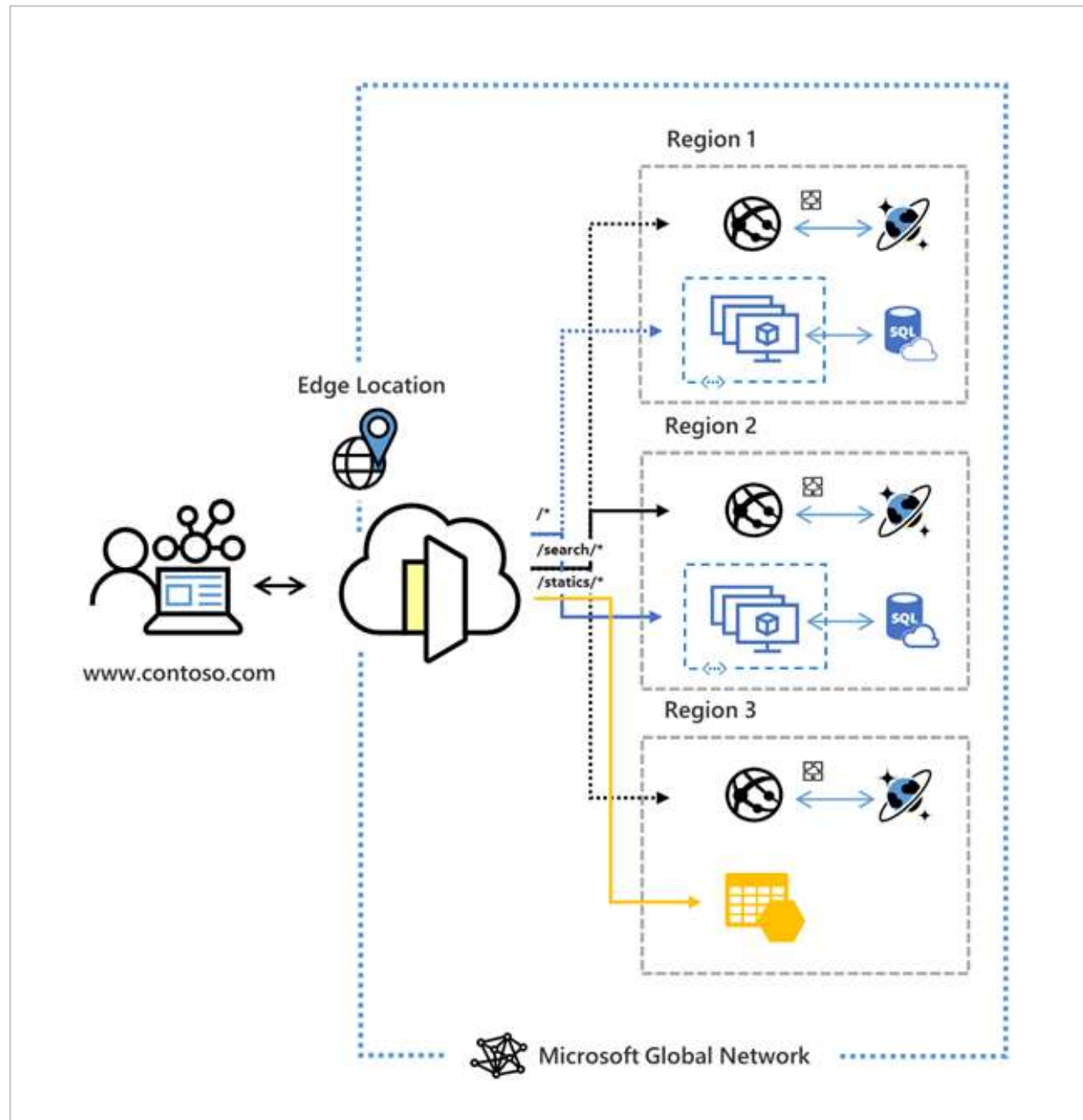
Multi-site hosting

Custom domains and certificate management

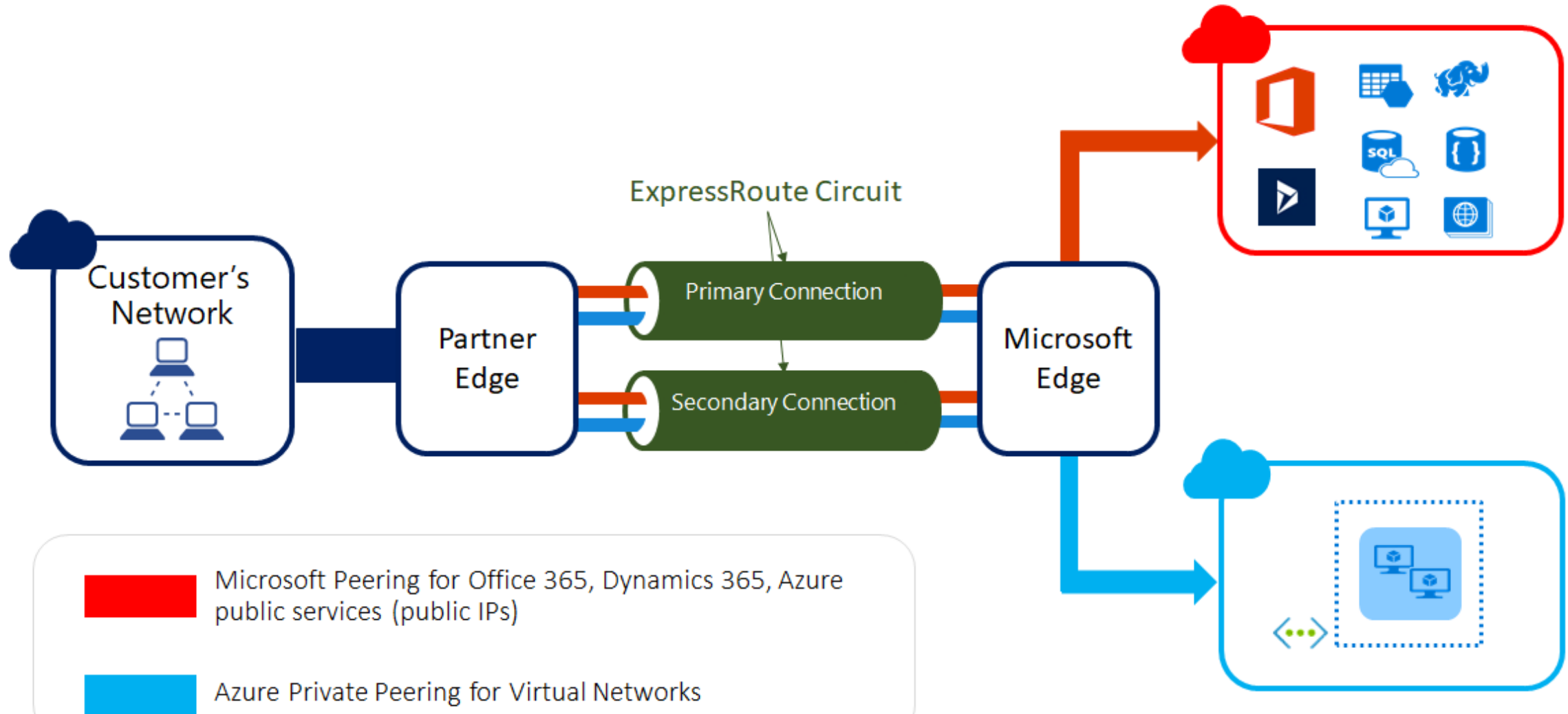
Application layer security - WAF

URL redirection and URL rewrite

Protocol support – IPv6 and HTTP/2 traffic



ExpressRoute



Host Security



Host Security



Endpoint Protection



Privileged Access Workstations



Virtual Machine Templates



Remote Access Management



Update Management



Disk Encryption



Microsoft Defender



Microsoft Defender for Cloud Recommendations



Securing Azure Workloads

Endpoint Protection



Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks **prevent, detect, investigate, and respond** to advanced threats.



Core Defender
Vulnerability
Management



Attack surface
reduction



Next-generation
protection



Endpoint detection
and response



Automated investigation
and remediation



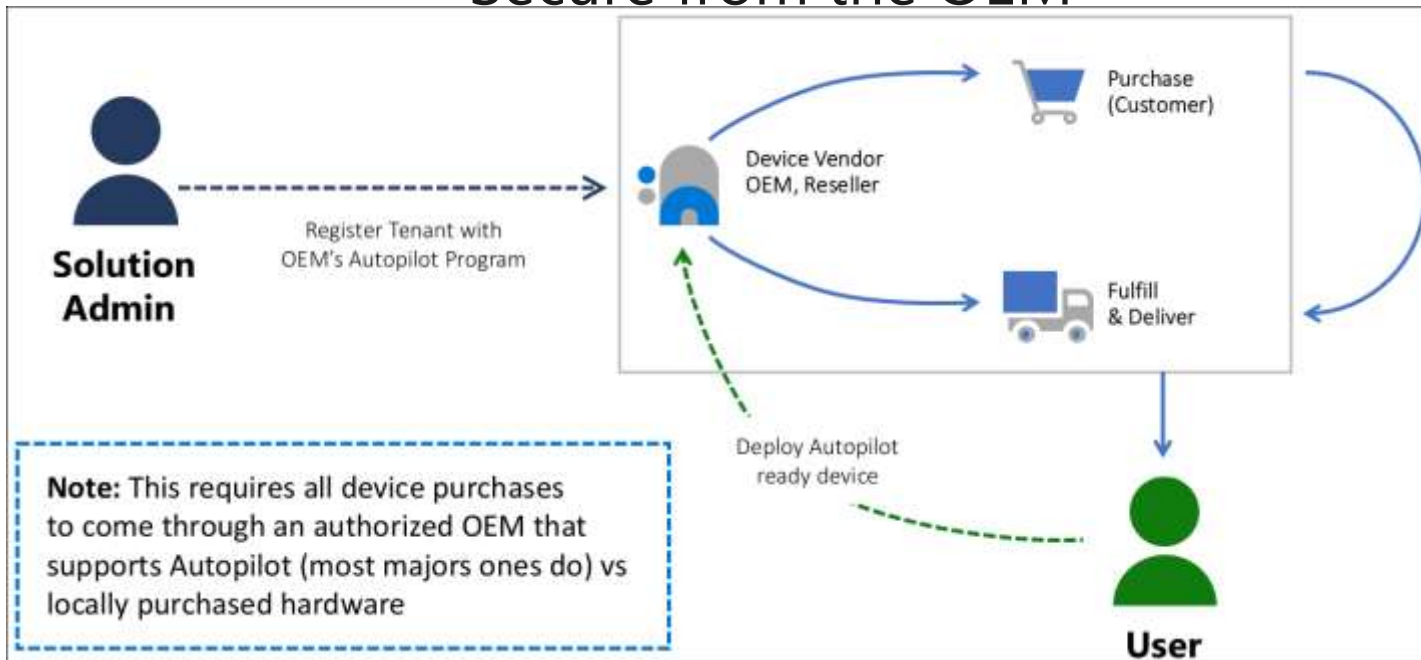
Microsoft
Threat Experts



Microsoft Defender for Endpoint is available in two plans, Defender for Endpoint Plan 1 and Plan 2.

Privileged Access Device Strategy

Secure from the OEM



Hardware Root-of-Trust

- Trusted Platform Module (TPM) 2.0
- BitLocker Drive Encryption
- UEFI Secure Boot
- Drivers and Firmware Distributed through Windows Update
- Virtualization and HVCI Enabled
- Drivers and Apps HVCI-Ready
- Windows Hello
- DMA I/O Protection
- System Guard
- Modern Standby

Privileged Access Workstations



Separate dedicated administrative accounts and workstations.

Protects from Internet attacks and threat vectors phishing attacks, application and OS vulnerabilities, and credential theft attack

Appropriate for accounts with access to high value assets -Administrators and High Sensitivity Information Workers

Virtual Machine Templates

Improves consistency

Express complex deployments

Reduce manual, error prone tasks

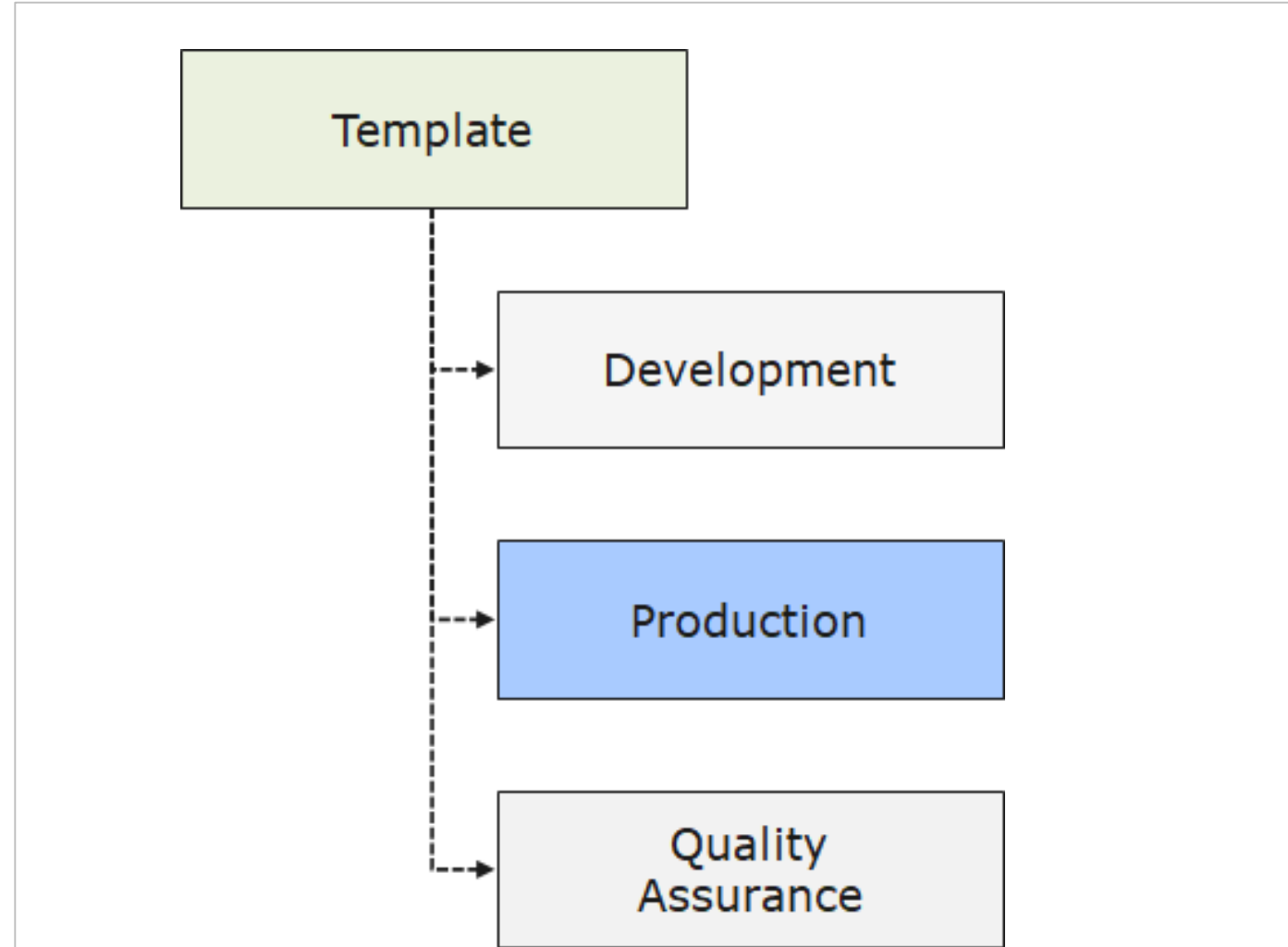
Express requirements through code

Promotes reuse

Modular and can be linked

Simplifies orchestration

Enforces security concerns

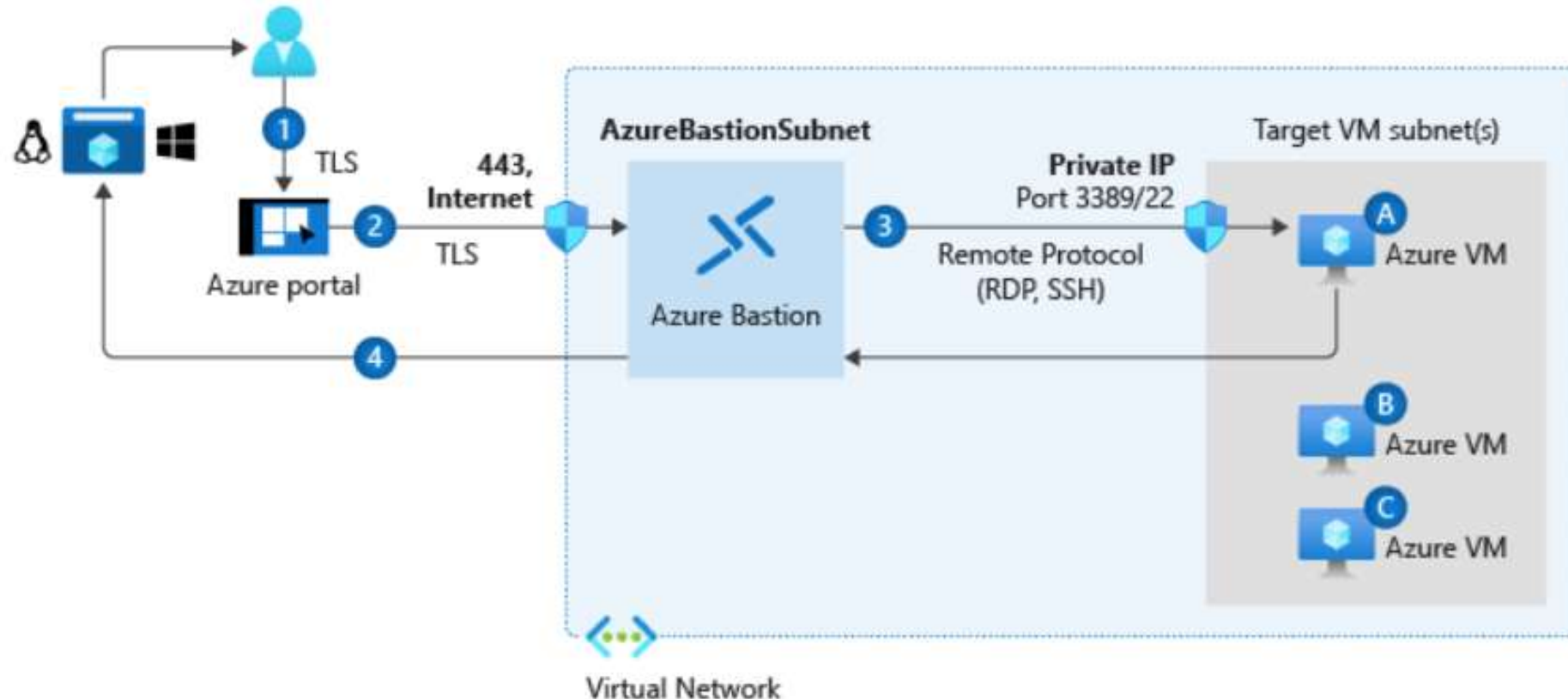


Remote Access Management

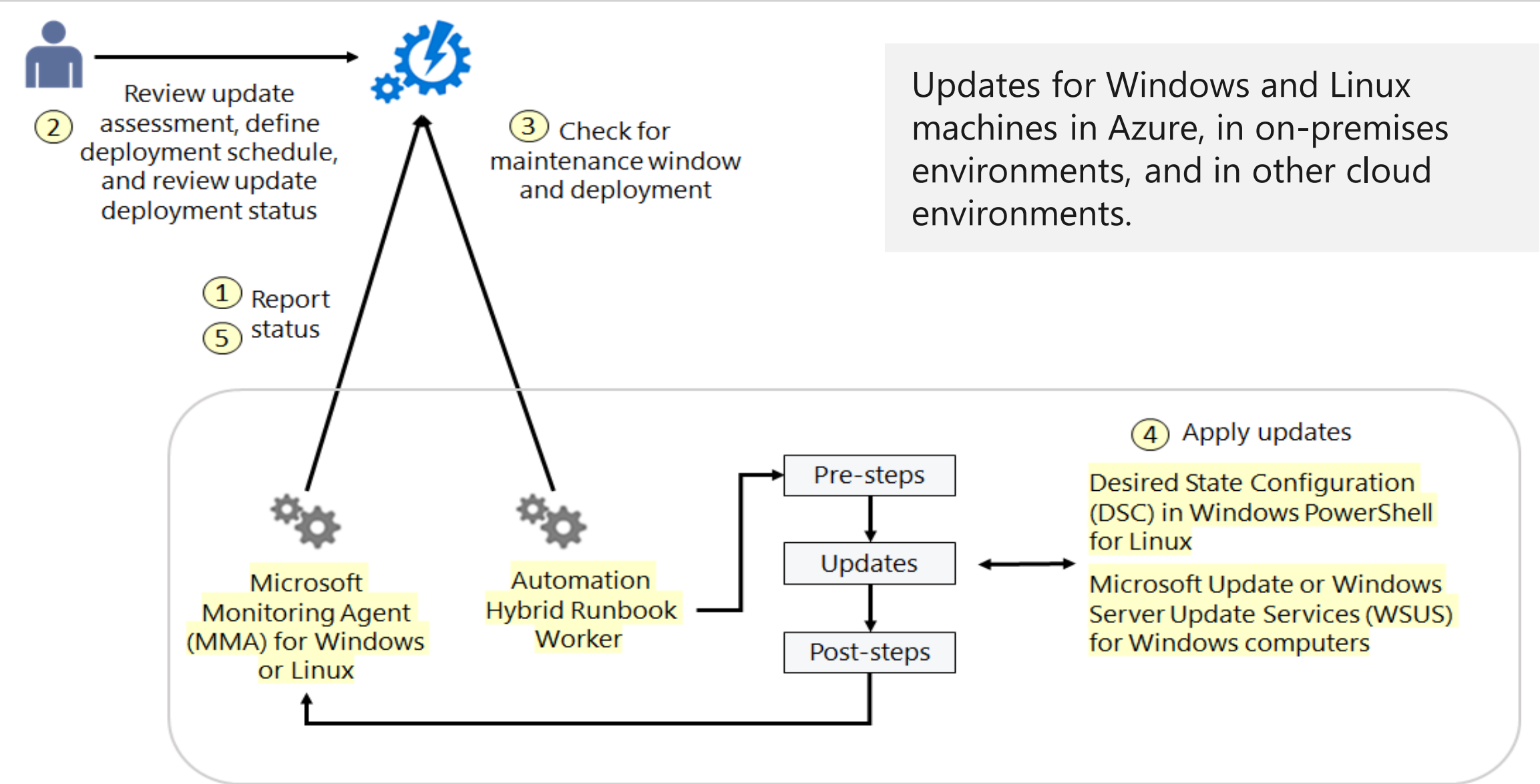
Remote Desktop Protocol (RDP) for Windows-based virtual machines

Secure Shell Protocol (SSH) for Linux based virtual machines

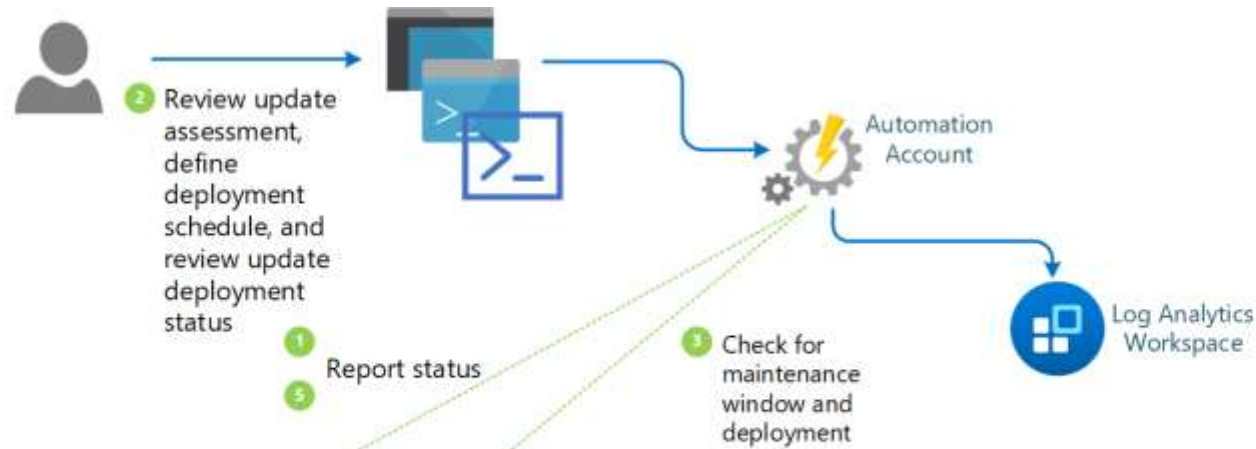
Bastion Subnet for RDP/SSH through the Portal over SSL



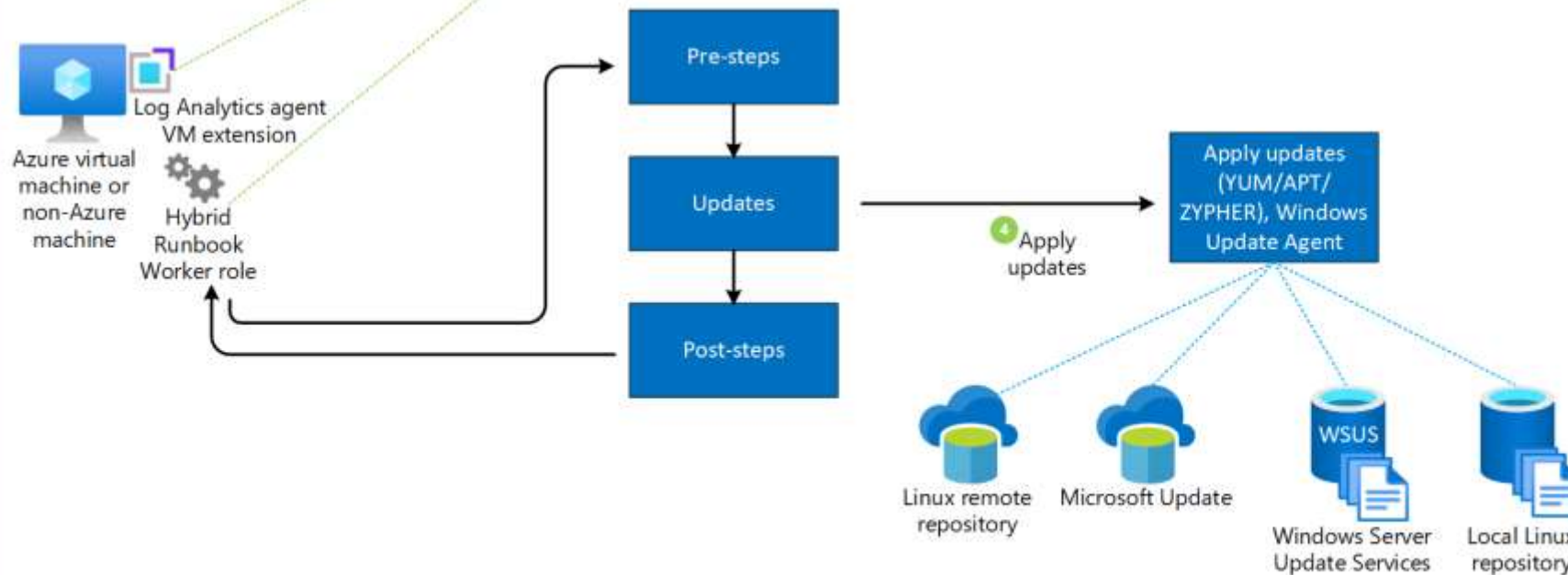
Update Management



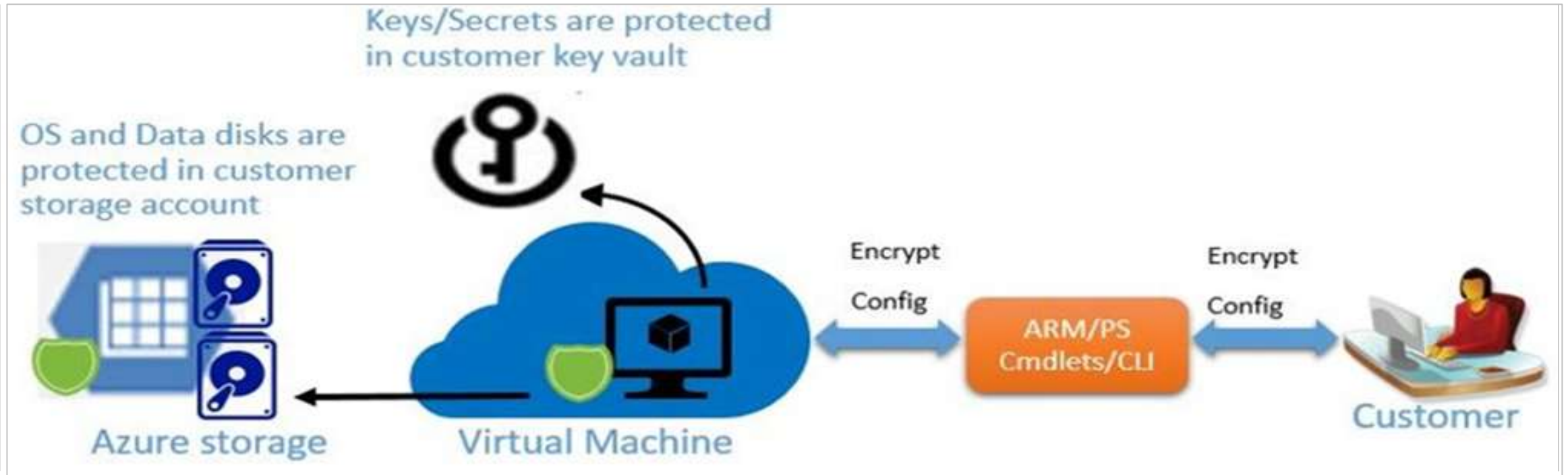
Azure Automation Update Management Overview



Updates for Windows and Linux machines in Azure, in on-premises environments, and in other cloud environments.



Disk Encryption



Provides encryption of the operating system and data disks

Windows VMs (BitLocker) and Linux VMs (DM-Crypt)

Stores encryption keys in a customer-managed key vault

Microsoft Defender for Endpoint – Supported Operating Systems

Supported Windows versions

Windows 11	Enterprise, Education, Pro, Pro Education
Windows 10	Enterprise, Enterprise LTSC: 2016 (or later), Enterprise IoT, Enterprise Education, Windows 10 Pro, Windows 10 Pro Education
Windows 8.1	Enterprise, and Pro
Windows 7 SP1	Enterprise (Requires ESU for support.), and Pro (Requires ESU for support.)
Windows Server	2008 R2 SP1 (Requires ESU for support), 2012 R2, 2016, version 1803 or later, 2019 and later, 2019 core edition, and 2022
Windows	Virtual Desktop
Windows	365

Other Operating Systems

macOS
Linux
Android
iOS

Microsoft cloud security benchmark in Defender for Cloud

- The Microsoft cloud security benchmark (MCSB) provides best practices and recommendations, with input from a set of holistic Microsoft and industry security guidance that includes:



Cloud Adoption Framework: Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.



Azure Well-Architected Framework: Guidance on securing your workloads on Azure.



The Chief Information Security Officer (CISO) Workshop: Program guidance and reference strategies to accelerate security modernization using Zero Trust principles.



Other industry and cloud service providers security best practice standards and framework: Examples include the Amazon Web Services, Center for Internet Security (CIS) Controls, National Institute of Standards and Technology, and the Payment Card Industry Data Security Standard.

Recommendations

Using the policies, Defender for Cloud periodically analyzes the compliance status of your resources to identify potential security misconfigurations and weaknesses.

It then provides you with recommendations on how to remediate those issues.

Recommendations result from assessing your resources against the relevant policies and identifying resources that aren't meeting your defined requirements.

Secure score recommendations

All recommendations

<



77%

Secure score ⓘ



7/38

Active recommendations

 Search recommendations

Recommendation status == **None** ✕

Email Security



Email Security

Email security defined

Email security is the practice of protecting email accounts and communications from unauthorized access, loss, or compromise. Organizations can enhance their email security posture by establishing policies and using tools to protect against malicious threats such as malware, spam, and phishing attacks. Cybercriminals target email because it is an easy entry point to other accounts and devices—and it relies in large part on human error. All it takes is one misguided click to cause a security crisis for an entire organization.

Why is email security important?

Email has been a primary communication tool in the workplace for more than two decades. More than 333 billion emails are sent and received daily worldwide—and employees get an average of 120 emails a day. This spells opportunity for cybercriminals who use business email compromise attacks, malware, phishing campaigns, and a host of other methods to steal valuable information from businesses. Most cyberattacks—94 percent—begin with a malicious email. Cybercrime cost more than \$4.1 billion in 2020, with business email compromise causing the most damage, according to the [FBI's Internet Crime Complaint Center \(IC3\)](#). The consequences can be severe, leading to significant financial, data, and reputational losses.

The benefits of email security

Businesses of all sizes are realizing the importance of prioritizing email security. An email security solution that safeguards employee communication and reduces cyberthreats is important because it helps to:

- Protect a company's brand, reputation, and bottom line. Email threats can lead to devastating costs, operational disruption, and other severe consequences.
- Enhance productivity. With a robust email security solution in place, businesses can reduce potential disruptions to operations and downtime because of a cyberattack. An effective solution helps security teams streamline response and stay ahead of increasingly sophisticated threats.
- Ensure compliance with data protection laws such as the General Data Protection Regulation (GDPR) and help circumvent the many intangible costs of a [cyberattack](#) such as business disruption, legal fees, regulatory fines.

Email Security

Types of email threats

Organizations face a number of complex email threats from account takeover and [business email compromise](#) to spear phishing and vishing. Generally, email threats fall into these group types:

Data exfiltration

Data exfiltration is the unauthorized transfer of data from an organization either manually or through malicious programming. Email gateways help make sure businesses avoid sending sensitive data without authorization, which could lead to a costly data breach

Malware

Malware is short for malicious software, and its primary aim is to damage or disrupt computers and computer systems. Common types of malware include viruses, worms, ransomware, and spyware.

Spam

Spam is an unsolicited message sent in bulk and without the recipient's consent. Businesses use spam email for commercial purposes. Scammers use spam to spread malware, trick recipients into divulging sensitive information, or extort money.

Impersonation

Impersonation occurs when cyber criminals pretend to be a trusted person or organization to secure money or data via email. Business email compromise is one example in which a scammer impersonates an employee to steal from the company or its customers and partners.

Phishing

Phishing is the practice of pretending to be a trusted person or organization to trick victims into disclosing valuable information such login credentials and other types of sensitive data. Different types of phishing include spear phishing, vishing, and whaling.

Email Security

Types of email security services

Email security services help companies protect email accounts and communication from cyberthreats. The best way for companies to implement email security is to create and maintain a policy for using email and share that with employees so they are aware of email security best practices. Common email security services available for individuals, schools, communities, and organizations include:

- Detonation capabilities that scan incoming, outgoing, and internal email for malicious links and attachments.
- Data encryption to secure mail communications from being intercepted by cybercriminals.
- Image and content control capabilities to scan attached or embedded images and content for malware and blocks them from being downloaded.
- Spam filters that filter unwanted email like bulk and spam messages.
- Authentication systems to evaluate the validity of senders.

Email security best practices

In response to the fast-changing email threat landscape, enterprises have established email security best practices to support communication and guard against threats. Top email security best practices include:

- Educate employees with periodic training to minimize the risk of human error and ensure that employees—often considered a company's first line of defense—understand the importance of email security.
- Invest in user awareness training so users can learn how to recognize the signs of a phishing attack and other indicators of malicious intent.
- Upgrade to an email security solution that provides advanced threat protection.
- Implement [multifactor authentication \(MFA\)](#) to prevent account compromise. Asking users to provide more than one way to sign into accounts is an easy way to help secure organizational data.
- Review protections against business email compromise attacks through methods like spoofing and impersonation.
- Move high-risk processes and transactions to more authenticated systems.

Identity and Access Management



Azure Active Directory



Hybrid Identity



Azure AD Identity Protection



Azure AD Privileged identity Management



Enterprise Governance



Application Security



Module Labs

Entra ID



Azure Active Directory (Azure AD)



Azure AD features



Azure AD versus Active Directory Domain Services (AD DS)



Roles for Azure AD



Azure AD Domain Services



Azure AD Users



Azure AD Groups

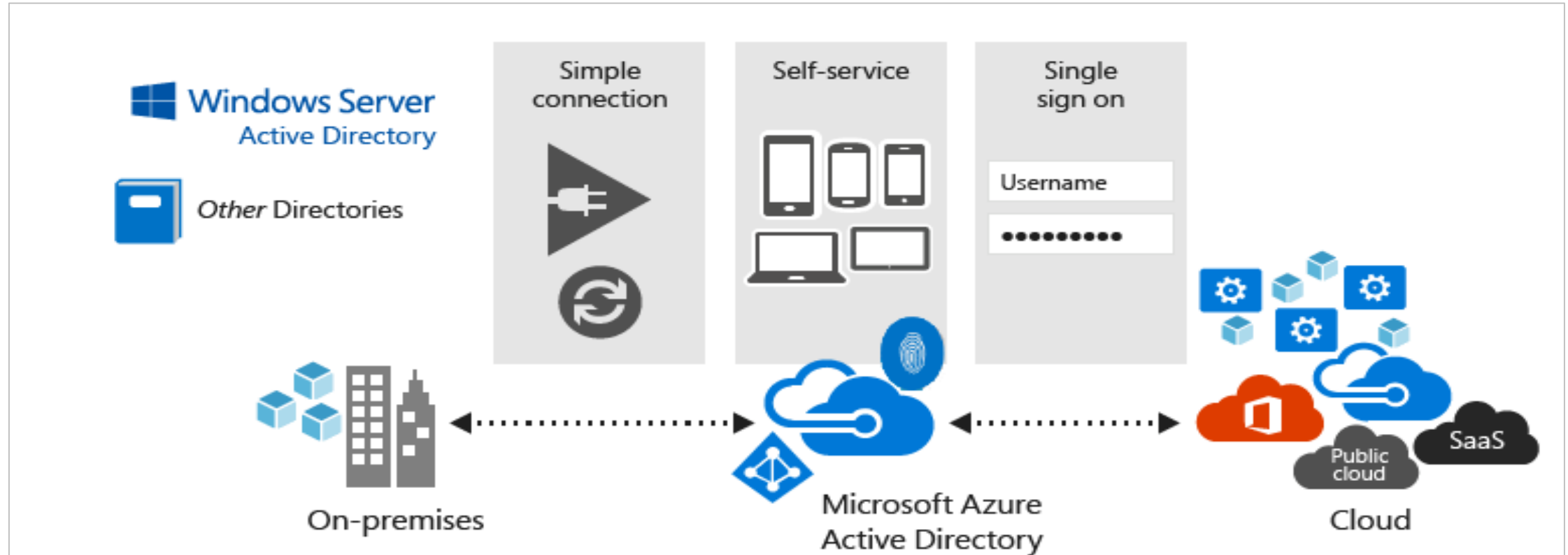


Administrative Units



Passwordless

Azure Active Directory Features



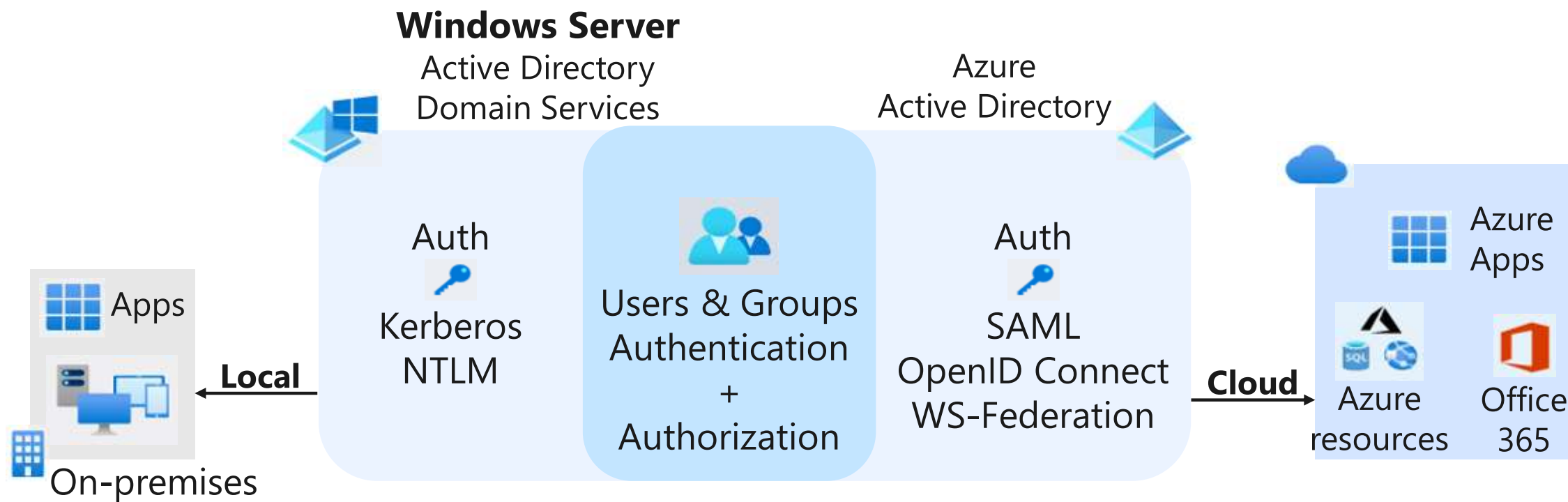
Microsoft's multi-tenant cloud-based directory and identity management service

Identity management capabilities and integration

Integrates with Windows Server Active Directory

Provides SSO access

Azure AD versus Active Directory Domain Services (AD DS)

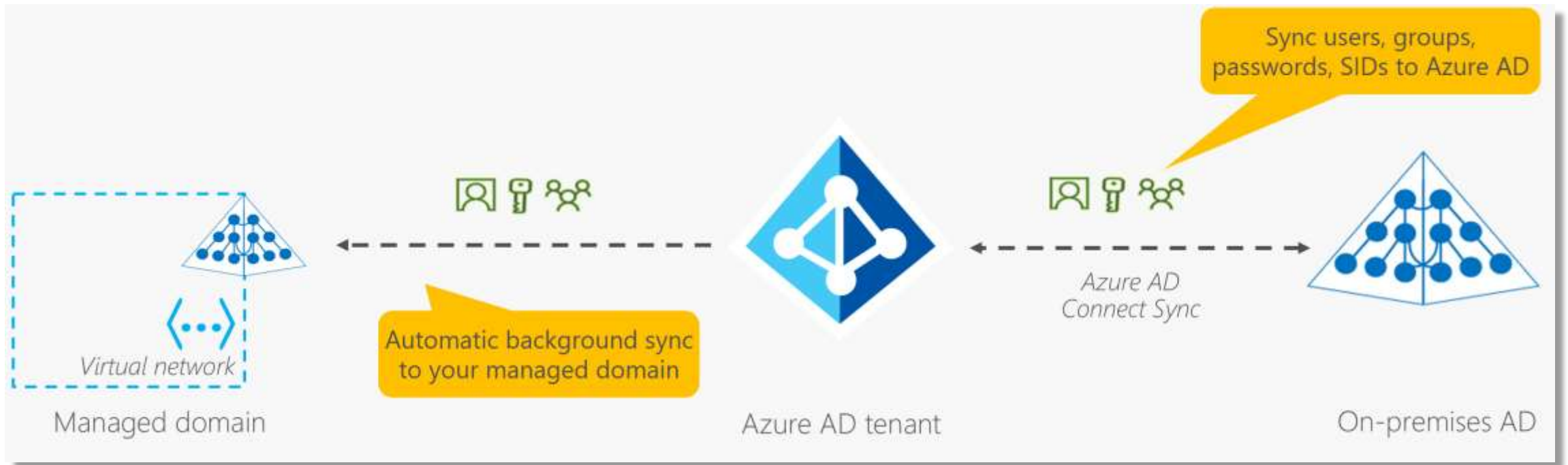


Service	Authentication	Structure	What it's used for
Azure Active Directory	Includes SAML, OpenID Connect (based on OAuth), WS-Federation	Tenants	Internet-based services and applications like Office 365, Azure services, and third-party SaaS applications
Active Directory Domain Services	Kerberos, NTLM	Forests, domains, organizational units	Authentication and authorization for on-premises printers, applications, file services, and more

Roles for Azure AD (sample)

Built-in Role	Description
Global Administrator	Users with this role have access to all administrative features in Azure Active Directory
Security Administrator	Users with this role have permissions to manage security-related features in the Microsoft 365 Security Center, Security Center, Azure Active Directory Identity Protection, Azure Information Protection, and Office 365 Security & Compliance Center
Billing Administrator	Makes purchases, manages subscriptions, manages support tickets, and monitors service health
Global Reader	Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions.

Azure Active Directory Domain Services



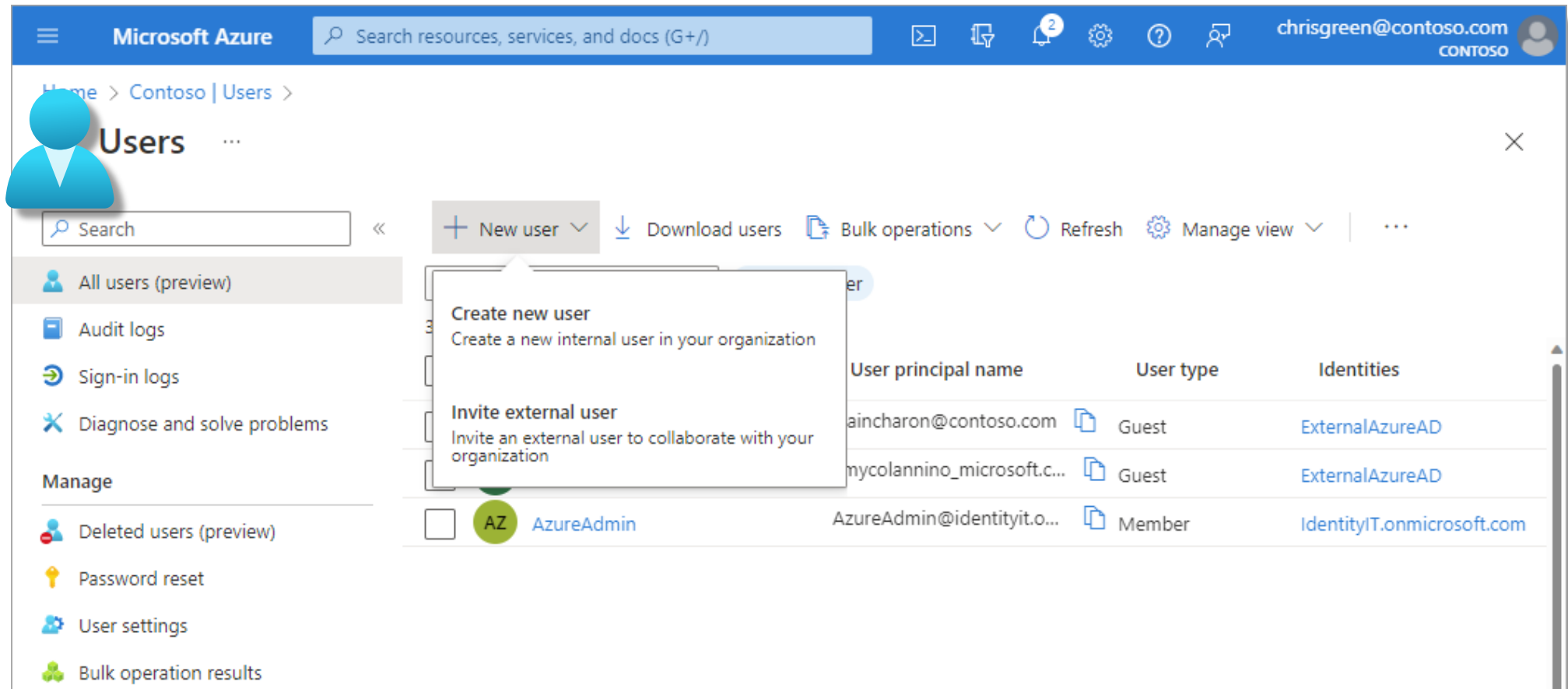
- Azure Active Directory Domain Services (Azure AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/New Technology LAN Manager (NTLM) authentication.



You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

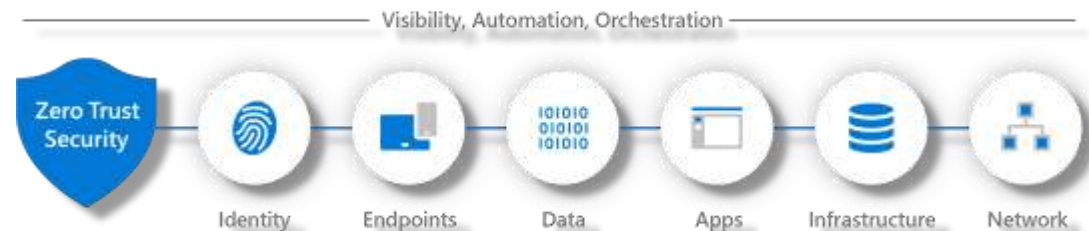
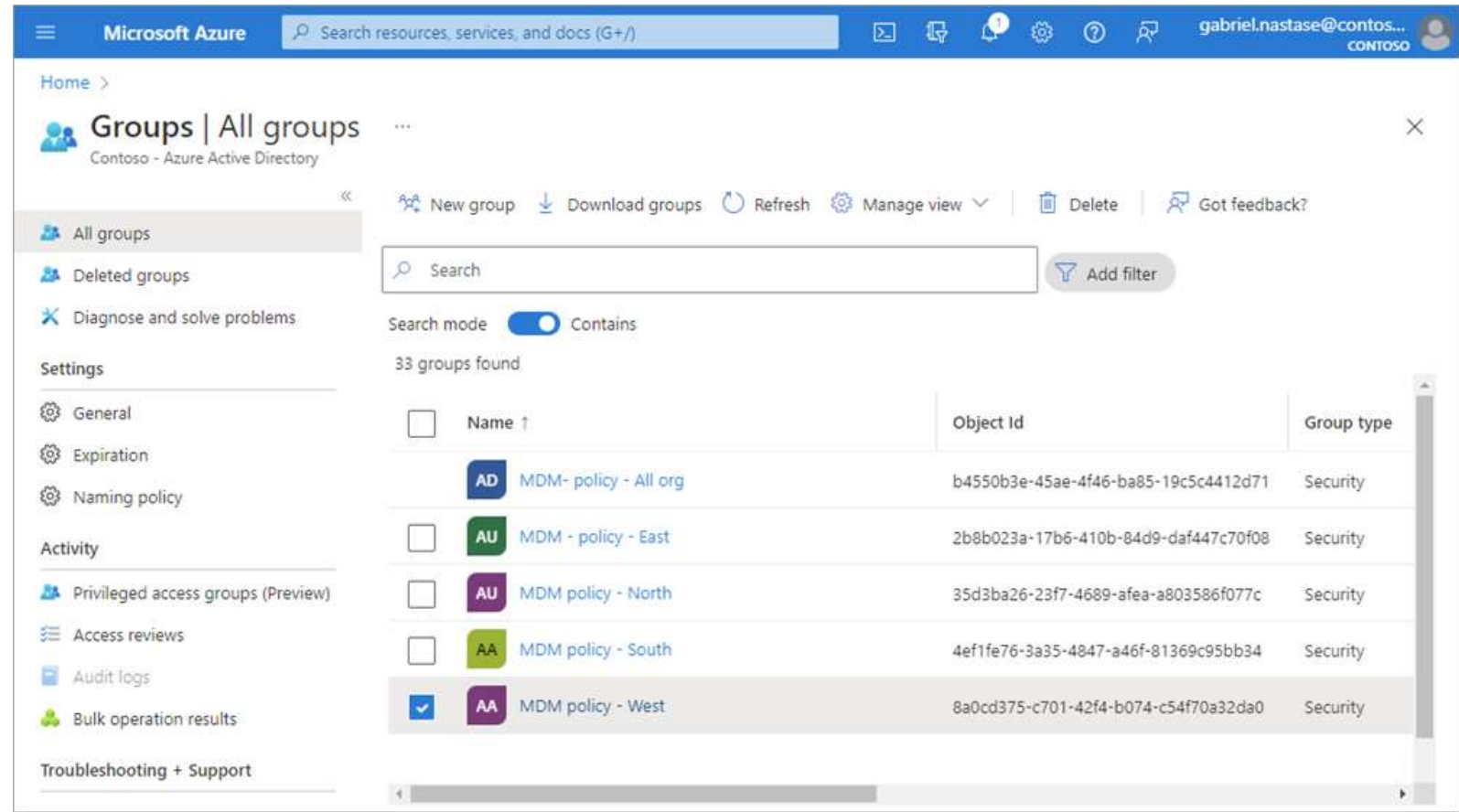
Azure AD Users

- Add new users or delete existing users from your Azure Active Directory (Azure AD) tenant.
 - To add or delete users, you must be a User Administrator or Global Administrator.



Azure AD Groups

- Azure Active Directory (Azure AD) provides several ways to manage access to resources, applications, and tasks.
- With Azure AD groups, you can grant access and permissions to a group of users instead of each individual user.
- Limiting access to Azure AD resources to only those users who need access is one of the core security principles of Zero Trust.



Passwordless

Home > Default Directory > Security >

 **Authentication methods | Policies** ...

Default Directory - Azure AD Security

Search (Ctrl+ /)

<<

Got feedback?

Manage

 Policies

 Password protection

Monitoring

 Activity

 User registration details

 Registration and reset events

Method

Target

Enabled

FIDO2 Security Key

No

Microsoft Authenticator

No

Text message (preview)

No

Temporary Access Pass (preview)

No

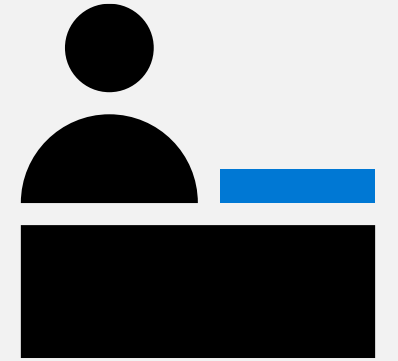
Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need to enable your users for the enhanced registration preview so they can register these authentication methods and use them to sign in.

Click here to enable users for the combined security info registration experience. →

Log in without using a password, ever.

- Increased security
- Better user experience
- More insights with logs and audits

Hybrid Identity



Hybrid Identity

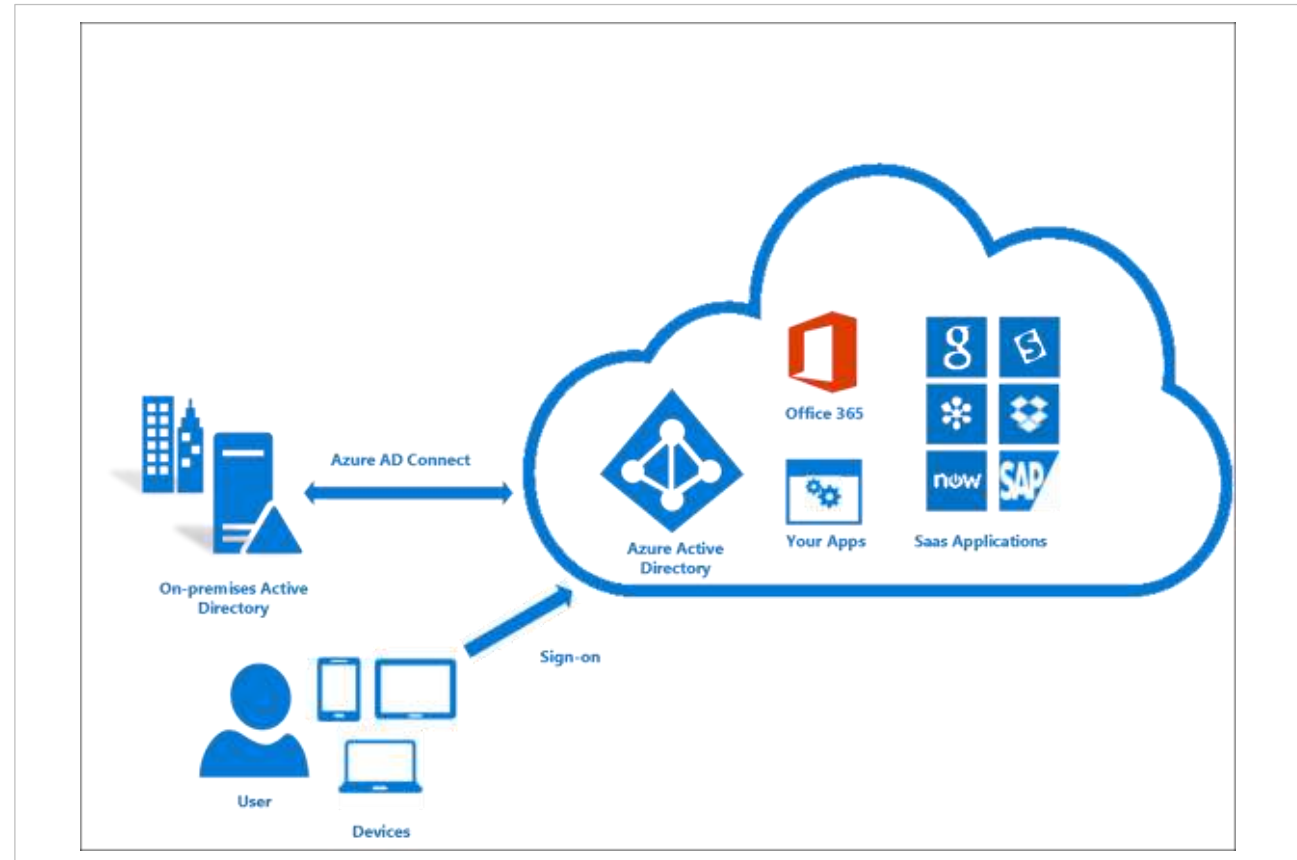
-  Azure AD Connect
-  Azure AD Connect cloud sync
-  Authentication Options
-  Password Hash Synchronization (PHS)
-  Pass-through Authentication (PTA)
-  Federation with Azure AD
-  Authentication Decision Tree
-  Password Writeback

Azure AD Connect

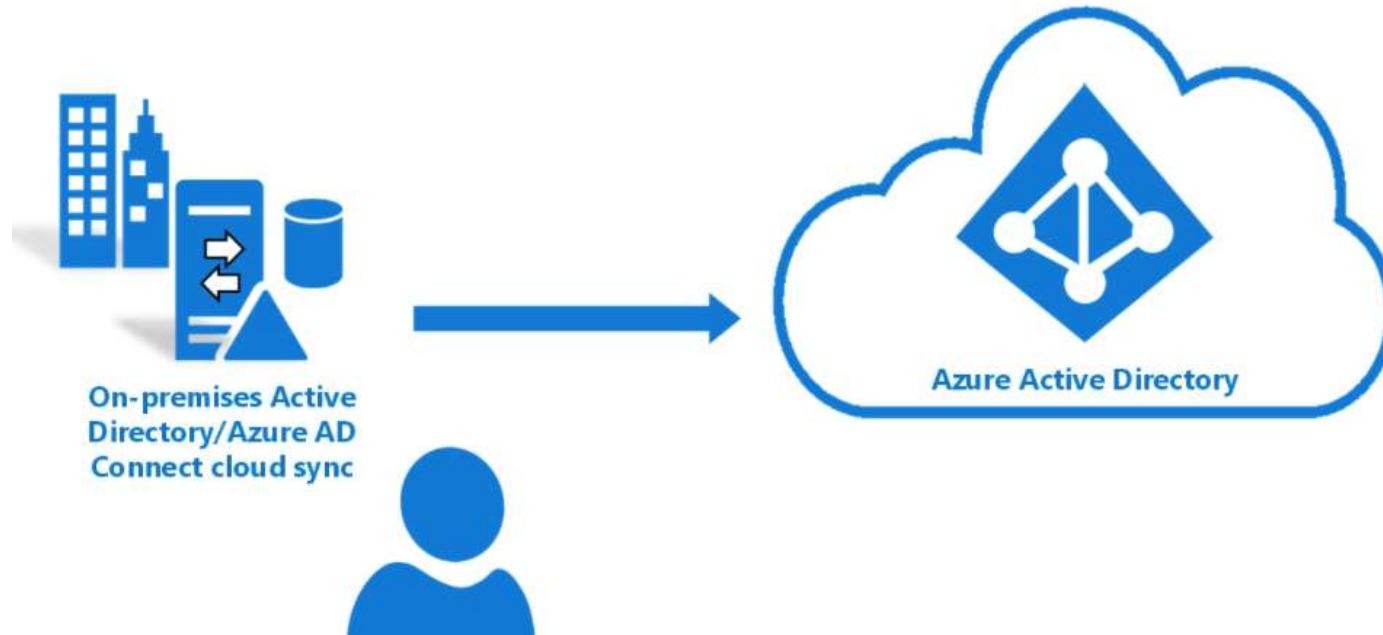
Integrate your on-premises directories with Azure Active Directory

Provides a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD

There are several authentication options to enable hybrid identity



Azure AD Connect Cloud Sync



Alternate method to integrate your on-premises directories with Azure Active Directory

Uses the Azure AD cloud provisioning agent

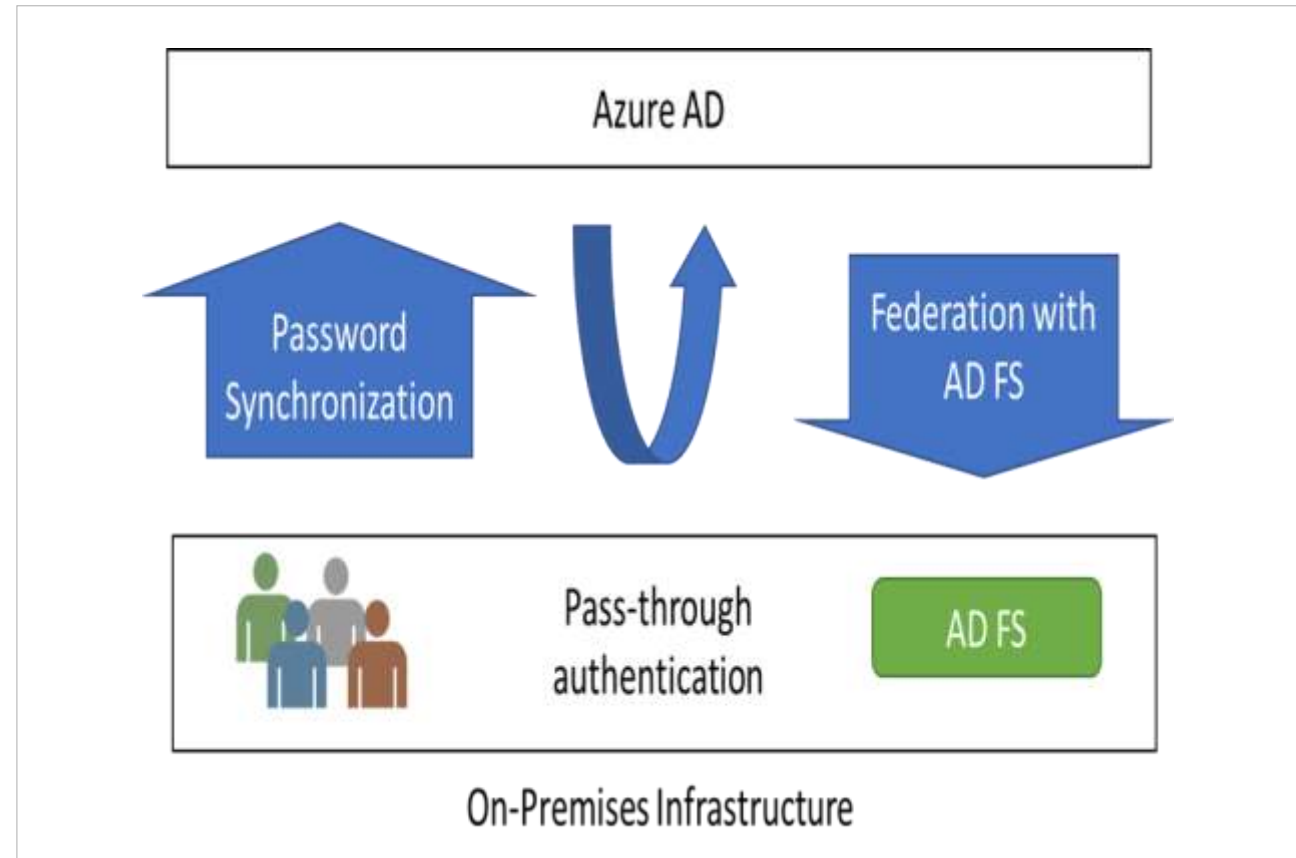
Runs stand-alone or along-side Azure AD Connect

Authentication Options

Password Hash Synchronization (PHS) can synchronize an encrypted version of the password hash for user accounts

Pass-through authentication (PTA) authenticates the username and password with the on-premises domain controllers

AD FS is the Microsoft implementation of an identity federation solution that uses claims-based authentication

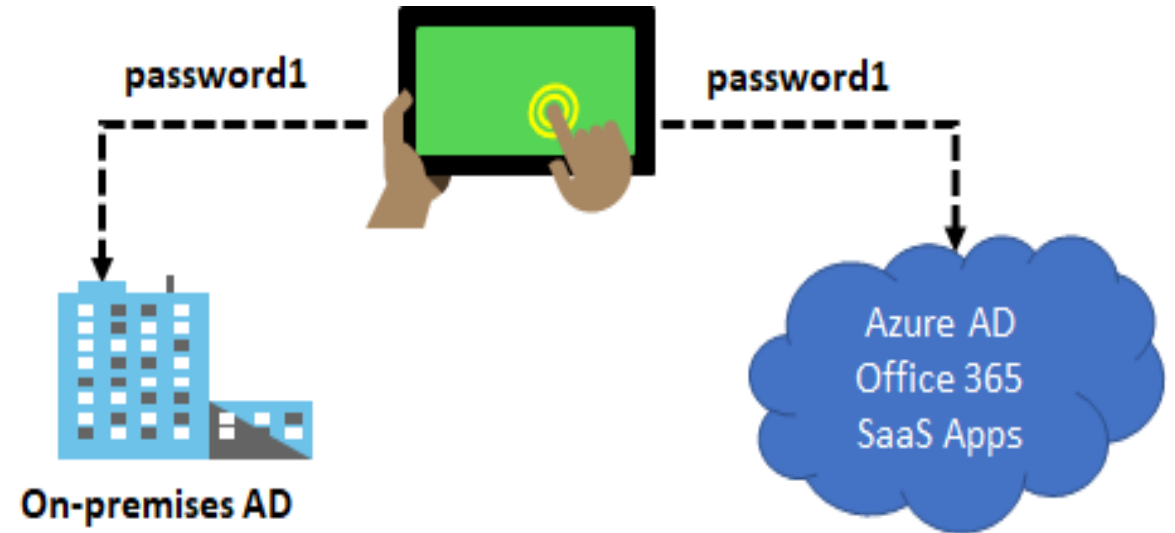


Password Hash Synchronization

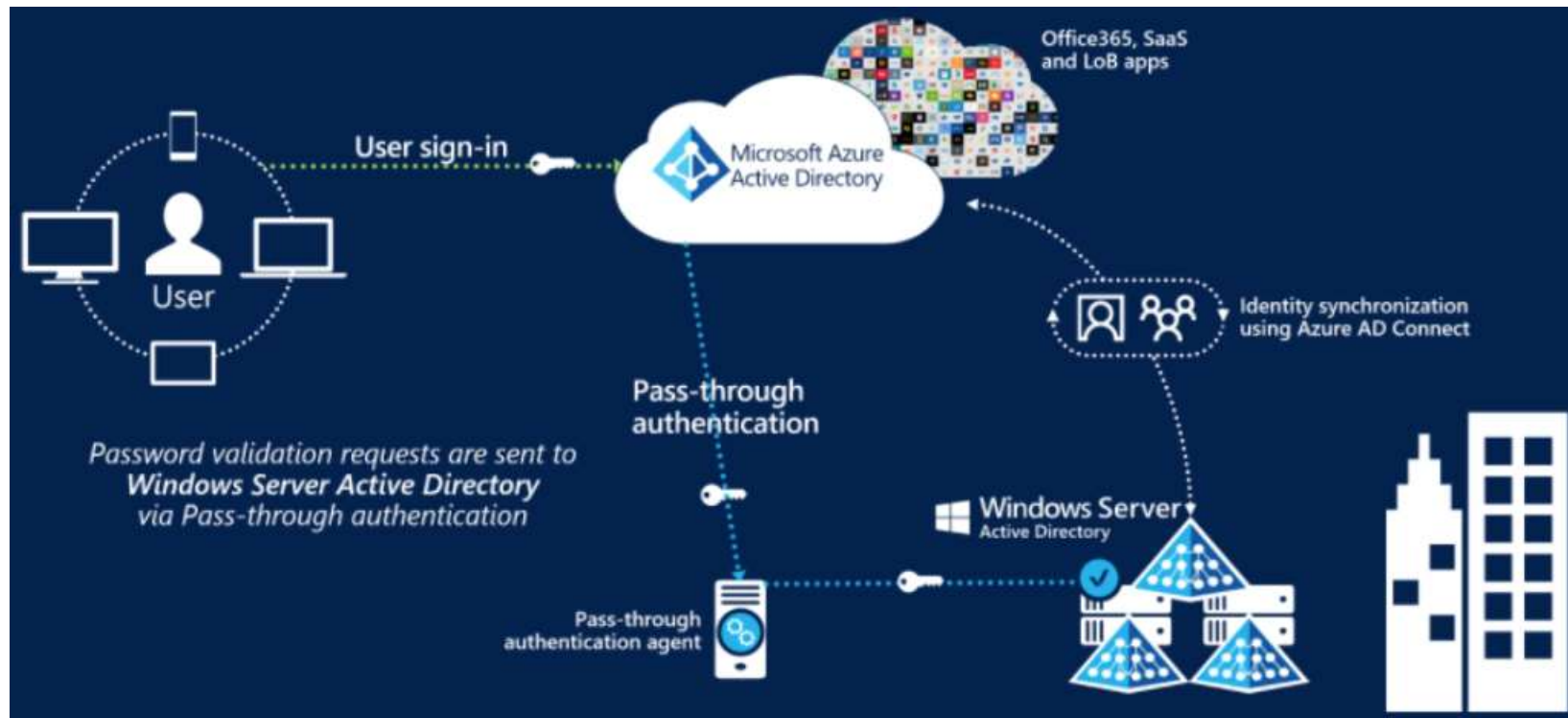
Password hash synchronizes user passwords from on-premises Active Directory to cloud-based Azure AD

Sign into Azure AD services using the on-premises password

Improve the productivity of your users and reduce your helpdesk costs



Pass-through Authentication



Supports user sign-in into all web browser-based applications and into Microsoft Office client applications

Is a free feature and can be enabled via Azure AD Connect

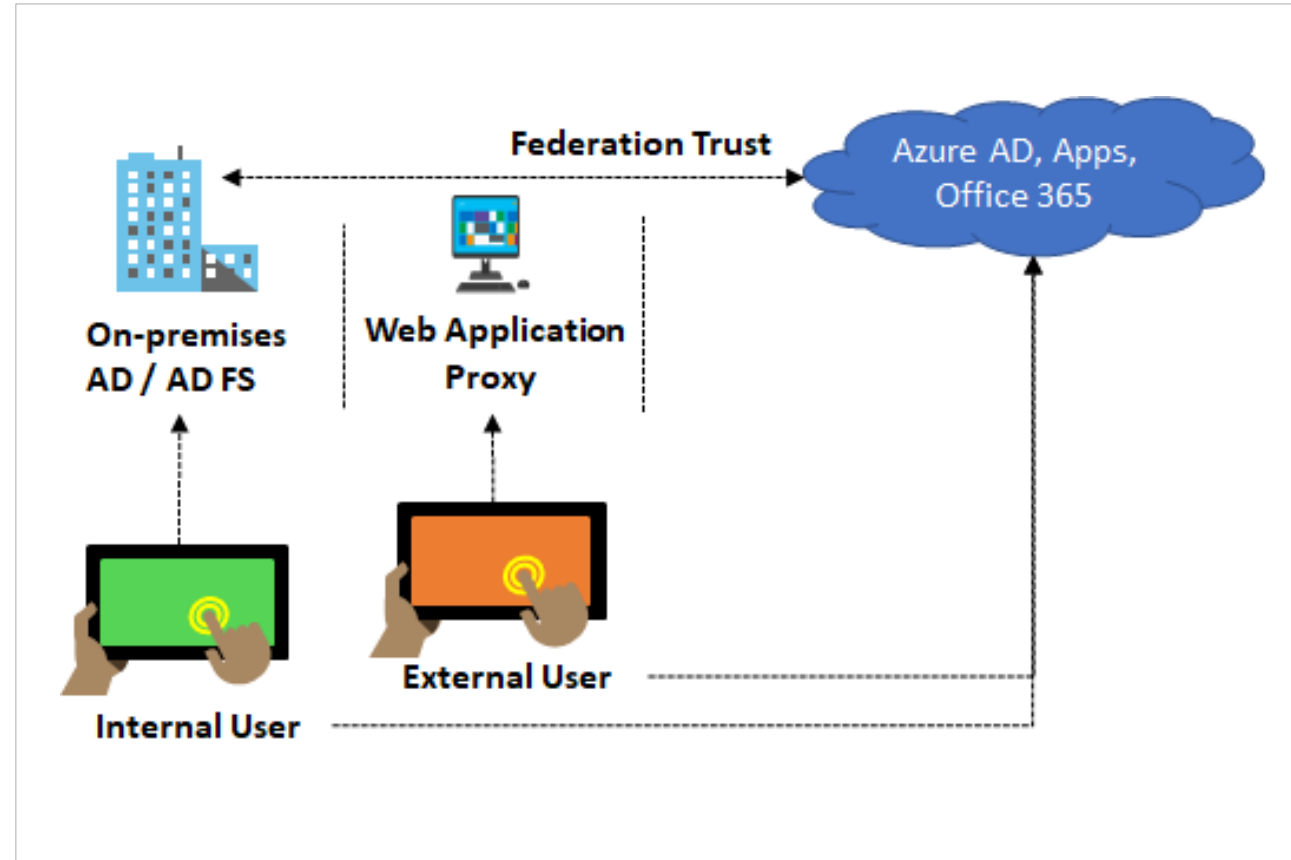
Is not only for user sign-in but allows an organization to use other Azure AD features – MFA and Self-Service Password Reset

Federation with Azure AD

Federation is a collection of domains that have established trust

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization

This sign-in method ensures that all user authentication occurs on-premises



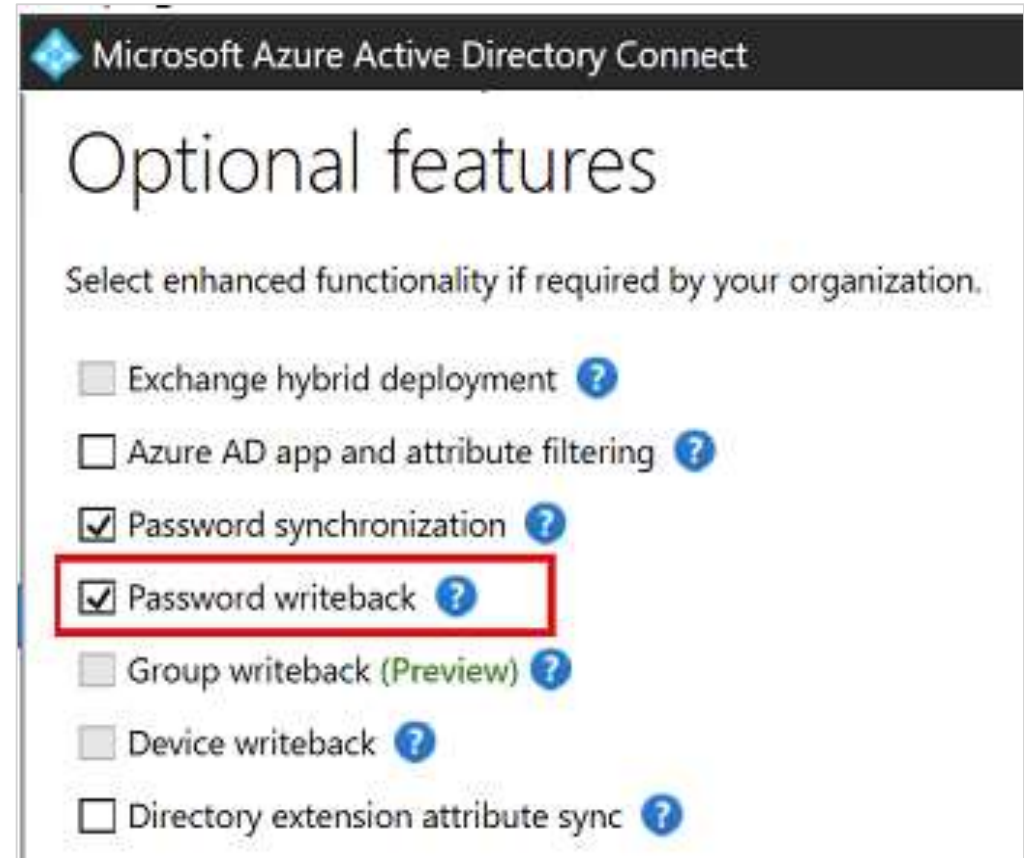
Password Writeback

Use Password Writeback to configure Azure AD to write passwords back to your on-premises Active Directory

A component of Azure AD Connect

Available to subscribers of Premium Azure Active Directory editions

Removes the need to set up and manage an on-premises SSPR solution



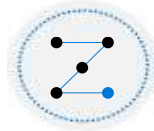
Azure AD Identity Protection



Azure AD Identity Protection



Azure AD Identity Protection



Risk Events



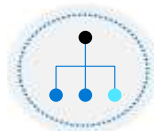
User Risk Policy



Sign-in Risk Policy



Azure MFA concepts



Azure AD Conditional Access



Conditions

Azure AD Identity Protection Features

Policy name Multi-factor authentication registration policy Assignments Users ⓘ All users > Controls Access ⓘ Require Azure MFA registration > ⓘ MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected. Enforce Policy ☒ On ☐ Off	Policy name User risk remediation policy Assignments Users ⓘ All users > Conditions ⓘ User risk > Controls Access ⓘ Require password change > Review Estimated impact ⓘ Number of users impacted > Enforce Policy ☒ On ☐ Off	Policy name Sign-in risk remediation policy Assignments Users ⓘ All users > Conditions ⓘ Sign-in risk > Controls Access ⓘ Require multi-factor authentication > Review Estimated impact ⓘ Number of sign-ins impacted > Enforce Policy ☒ On ☐ Off
--	--	---

Automate the detection and remediation of identity-based risks

Investigate risks using data in the portal

Export risk detection data to third-party utilities for further analysis

Azure Identity Protection Risk Events

Each detected suspicious action is stored in a record called a risk event

Leaked credentials

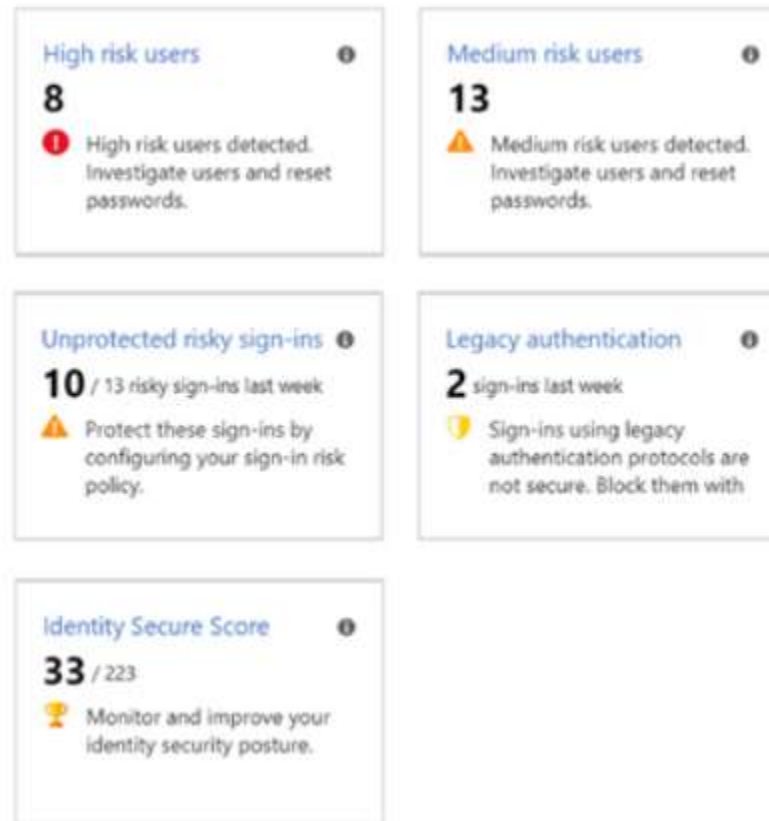
Sign in from anonymous IP addresses

Impossible travel to atypical locations

Sign in from unfamiliar locations

Sign in from infected devices

Sign in from IP addresses with suspicious activity



User Risk Policy



Applied to user sign-ins

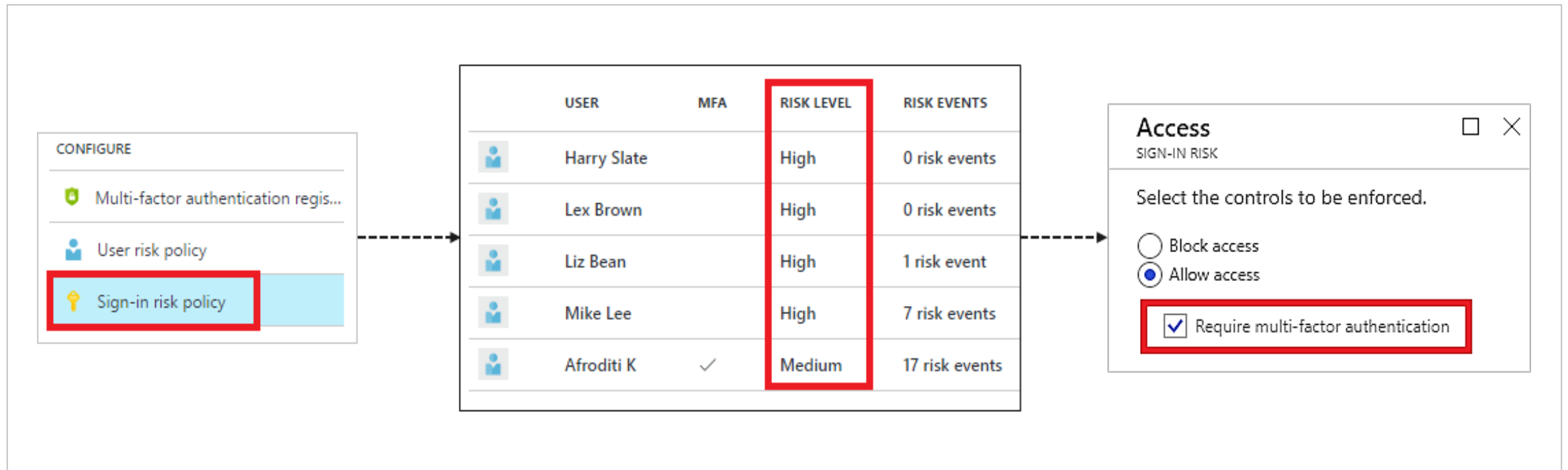
Automatically respond
based on a specific user's
risk level

Provide the condition (risk
level) and action (block or
allow)

Use a high threshold during
policy roll out

Use a low threshold for
greater security

Sign-in Risk Policy



Applied to all browser traffic and sign-ins using modern authentication

Provide the condition (risk level) and action (block or allow)

Automatically respond to a specific risk level

Target all policies to specific users – omit certain types of users

Azure MFA Concepts

The security of MFA two-step verification lies in its layered approach

Authentication methods include:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)
- Something you are (biometrics)

Username

test@xxx.com

Password



Enabling MFA

Select the users that you want to modify and enable for MFA

User states can be Enabled, Enforced, or Disabled

On first-time sign-in, after MFA has been enabled, users are prompted to configure their MFA settings

Azure MFA is included free of charge for global administrator security

contoso

admin@cms

multi-factor authentication

users

service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users

Multi-Factor Auth status: Any

bulk update

☐	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☒	Adam Barr	AdamB@contoso.com	Disabled
☒	Alice Ciccu	AliceC@contoso.com	Disabled
☐	Amy Rusko	AmyR@contoso.com	Disabled
☐	Ann Beebe	AnnB@contoso.com	Disabled
☒	Ben Smith	BenS@contoso.com	Disabled

3 selected

quick steps

Enable

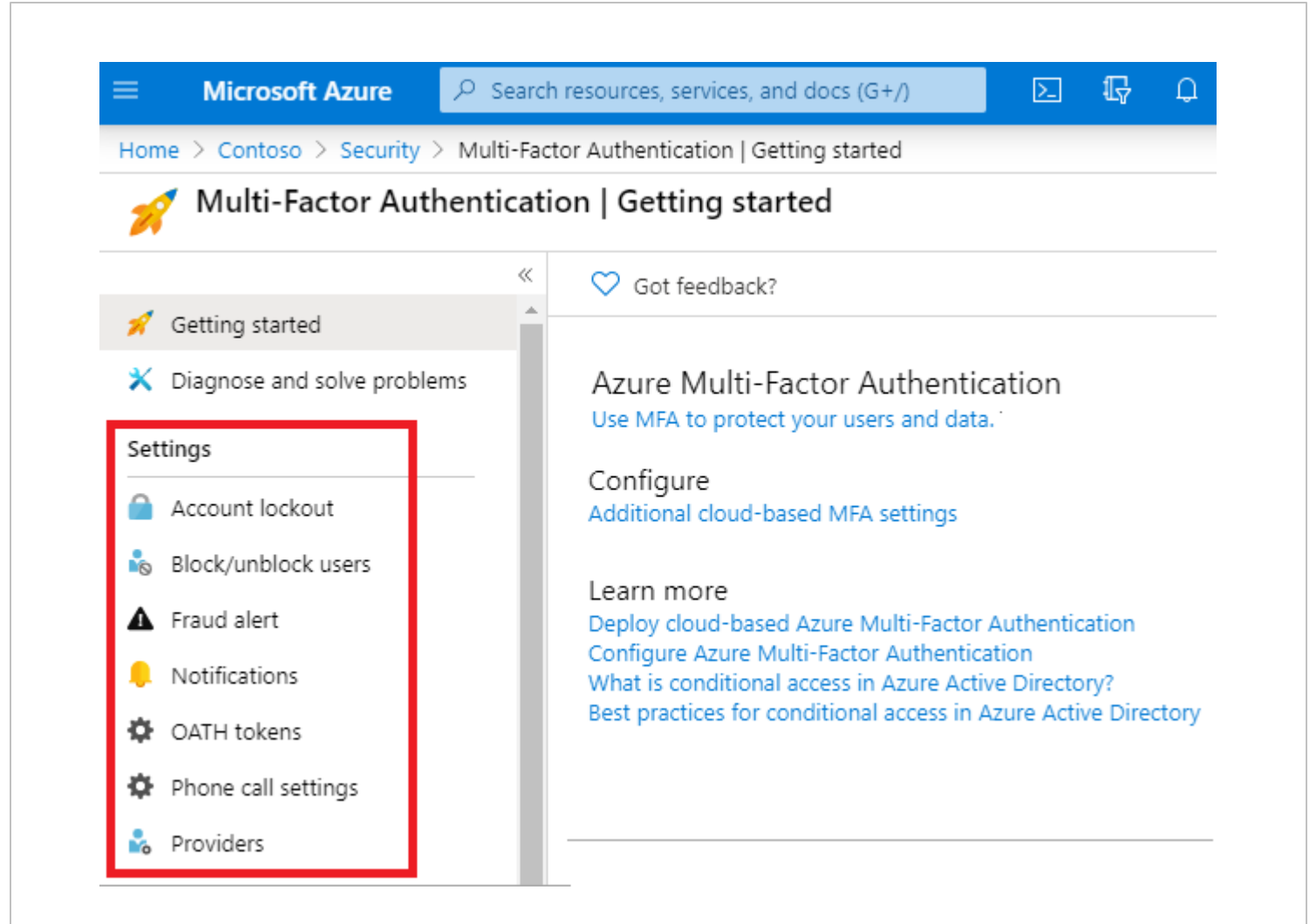
Manage user settings

MFA Settings

Account Lockout – temporarily lock accounts if too many denied authentication attempts occur.

Block/Unblock Users – block specific users from being able to receive MFA requests.

Fraud Alerts - Users can report fraudulent attempts to access their resources



The screenshot displays the Microsoft Azure portal interface for Multi-Factor Authentication (MFA) settings. The top navigation bar includes the Microsoft Azure logo, a search bar, and icons for mail, download, and notifications. The breadcrumb trail indicates the path: Home > Contoso > Security > Multi-Factor Authentication | Getting started. The main heading is 'Multi-Factor Authentication | Getting started'. The left sidebar contains a 'Getting started' section with links to 'Getting started', 'Diagnose and solve problems', and 'Settings'. The 'Settings' section is highlighted with a red box and lists the following options: Account lockout, Block/unblock users, Fraud alert, Notifications, OATH tokens, Phone call settings, and Providers. The main content area shows the 'Azure Multi-Factor Authentication' section with the subheading 'Use MFA to protect your users and data.' and a 'Configure' link labeled 'Additional cloud-based MFA settings'. Below this is a 'Learn more' section with links to 'Deploy cloud-based Azure Multi-Factor Authentication', 'Configure Azure Multi-Factor Authentication', 'What is conditional access in Azure Active Directory?', and 'Best practices for conditional access in Azure Active Directory'.

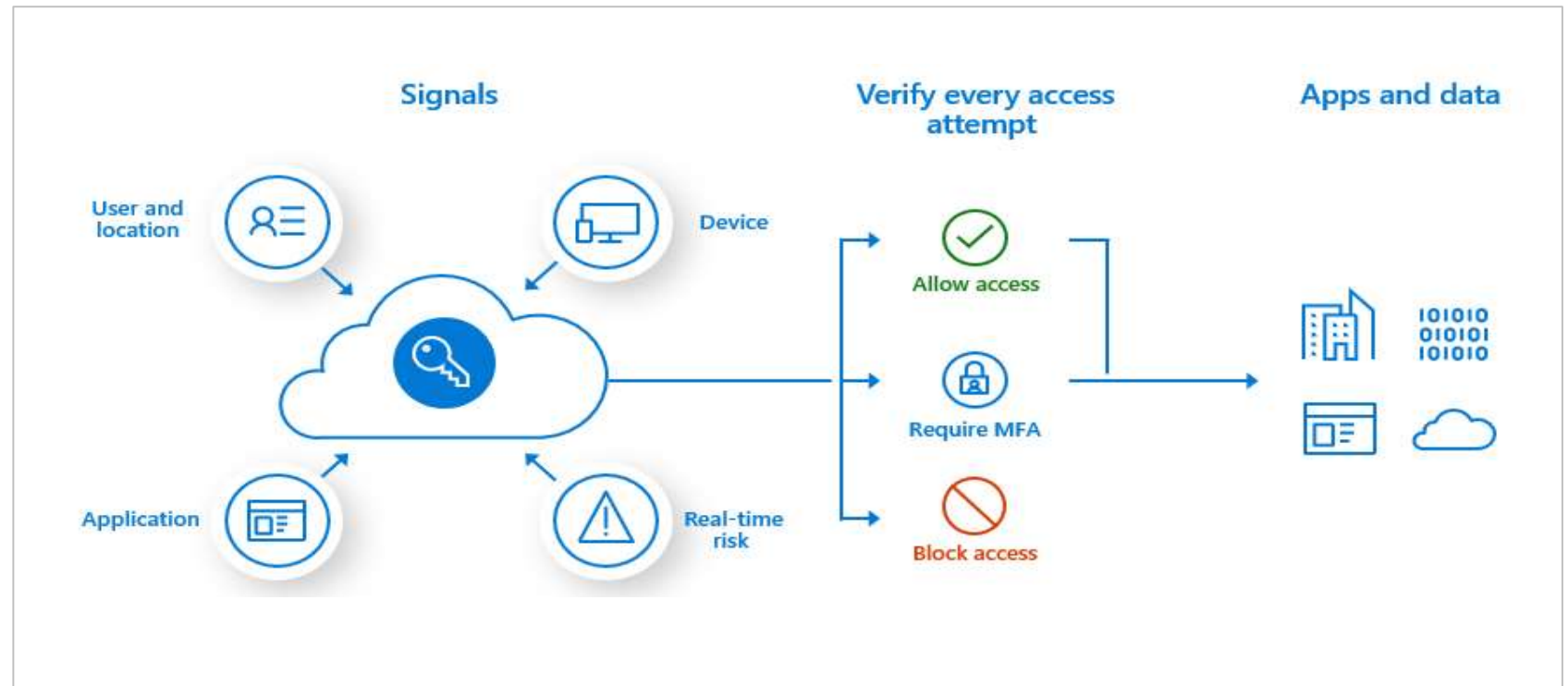
Azure AD Conditional Access

Identity management is the new control plane

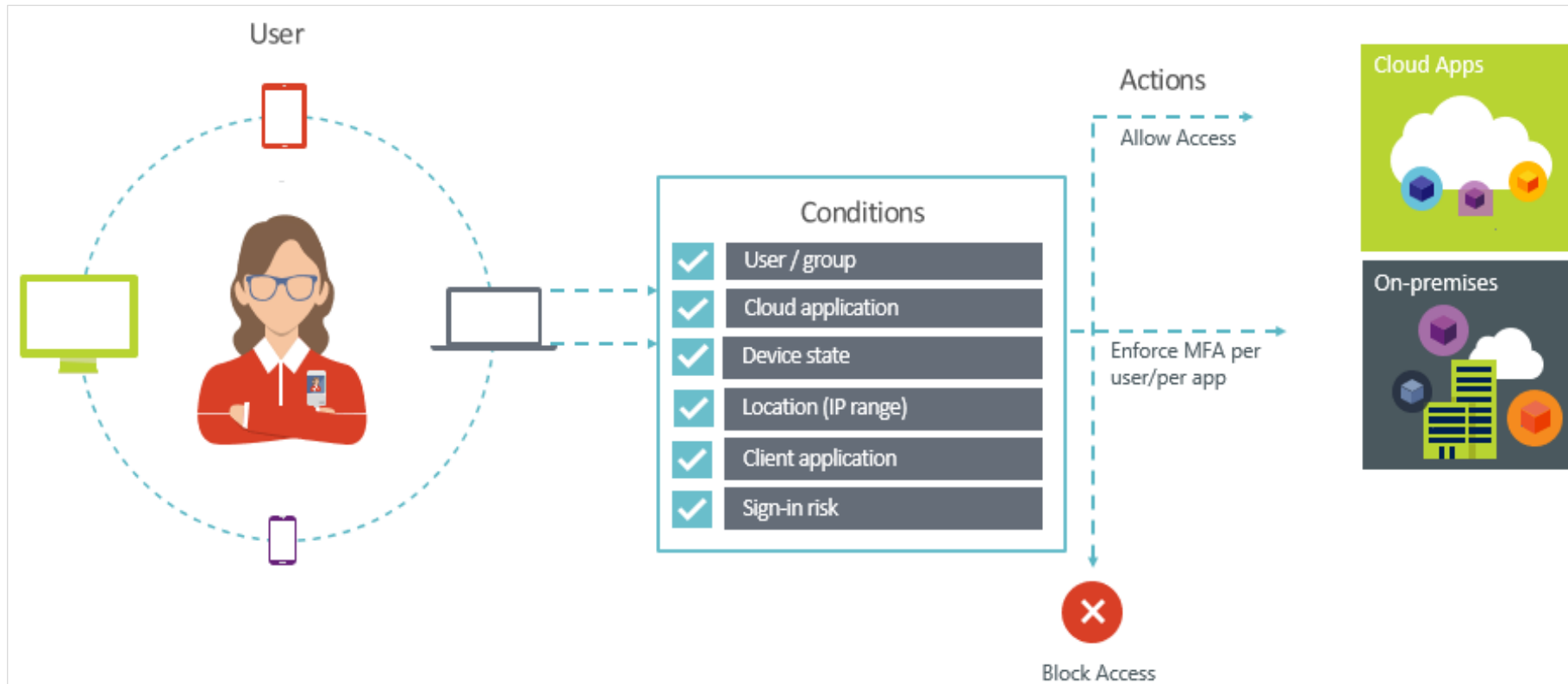
Use signals to make an informed decision

Base the decision on organizational policy

Enforce the decision across resources



Conditions



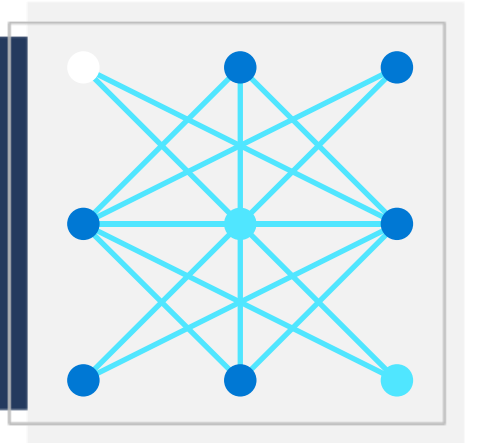
Conditions –
“When this
happens”

Access controls –
“Then do this”

Provides two step authentication verification

Lets you enforce controls on access to
apps based on specific conditions

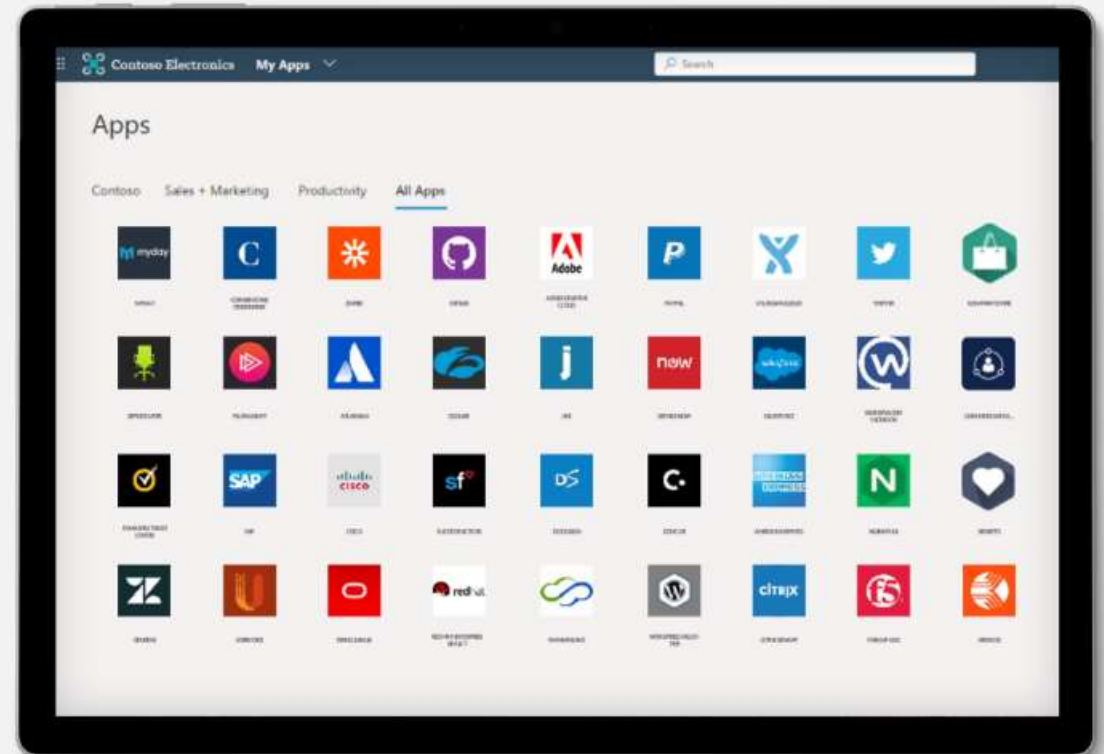
Single sign-on



Single sign-on

What is single sign-on?

With SSO, your teams can use just one set of credentials to conveniently access all their apps. No more memorizing multiple credentials or reusing passwords.



Single sign-on

What single sign-on provides



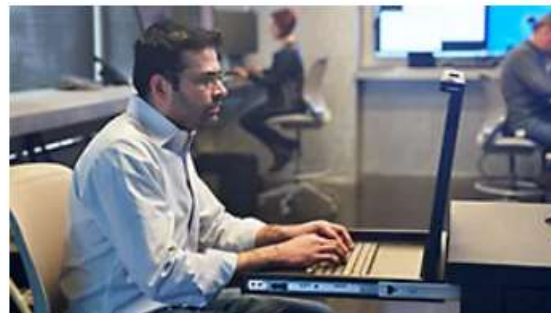
Streamlined sign-in experiences

Provide a superior sign-in experience by reducing or eliminating sign-in prompts.



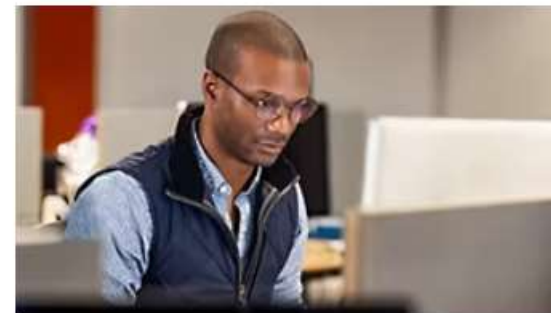
Increased employee productivity

Simplify access and app discovery with a quick, centralized app-launching experience.



Enhanced security

Reduce the reuse of usernames and passwords across apps to help minimize the risk of breaches.



Increased IT efficiency

Centralize user account management and automatically add or remove user access across apps based on group membership or roles.

Single sign-on

Single sign-on methods

Choose an SSO method based on how your application is configured for authentication.

[Learn more >](#)

Integrated single sign-on apps

Use our prebuilt integrations to connect to your cloud-enabled SaaS apps such as ServiceNow, Workday, and Box.

[Learn more >](#)

OpenID Connect single sign-on

Use OpenID Connect and OAuth for SSO when developing a new app.

[Learn more >](#)

SAML single sign-on

Choose Security Assertion Markup Language (SAML) whenever possible for existing apps that do not use OpenID Connect or OAuth.

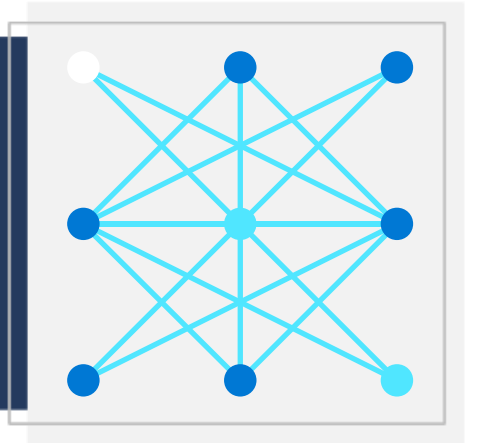
[Learn more >](#)

Single sign-on for on-premises apps

Use Microsoft Entra application proxy to provide SSO for on-premises apps that use authentication methods such as a header-based sign-on or integrated Windows authentication.

[Learn more >](#)

Privileged Identity Management



Privileged Identity Management (PIM)



Microsoft's Zero Trust Model



Microsoft Identity Management Evolution



PIM Features



PIM Scope



PIM Onboarding



PIM Configuration Settings



PIM Workflow

Microsoft Identity Management Evolution

We recommend Azure AD Privileged Identity Management as the service to help protect your privileged accounts

Traditional	Advanced	Optimal
• On-premises identity provider is in use • No SSO is present between cloud and on-premises apps • Visibility into identity risk is very limited	• Cloud identity federates with on-premises system • Conditional access policies gate access and provide remediation actions • Analytics improve visibility	• Password less authentication is enabled • User, device, location and behavior is analyzed in real time to determine risk and deliver ongoing protection • MFA is enforced

Azure AD Privileged Identity Management (PIM)

Time-based and approval-based role activation for privileged users

Just-in-time privileged access to Azure

Time-bound access to resources

Approval to activate privileged roles

Multi-factor authentication to activate any role



Justification to understand why users activate

Notifications when privileged roles are activated

Access reviews to ensure users still need roles

Audit history for internal or external audit

PIM Scope

Azure AD Roles

Assign users to a role – users must elevate to use the privileges granted by the role

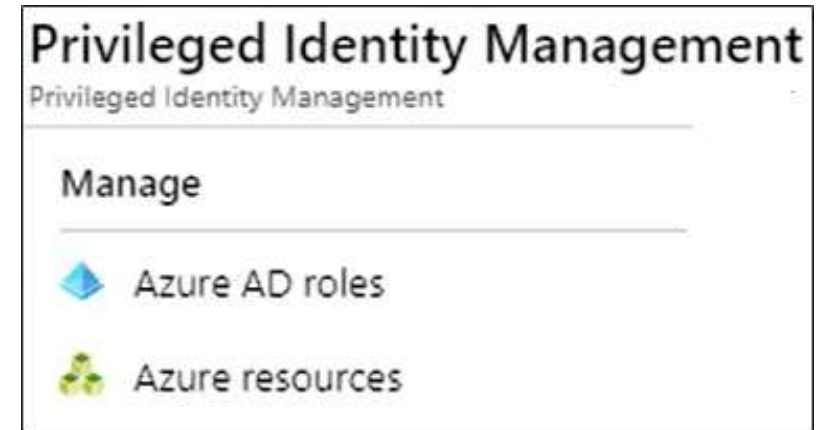
Prioritize protecting Azure AD roles that have the greatest number of permissions

Azure resources

Identify the management groups and subscriptions

Resources most vital for your organization or host the most sensitive data

Resources that core, customer-facing applications depend on - PIM will help you discover these resources



Which Azure AD roles and resources should be protected with PIM?

PIM Onboarding

PIM automatically enable when a privileged role goes into **PIM** or **Roles and Administrators**

The Global administrator (first user) who enables PIM gets write access

The first user can assign others to the Privileged Role Administrator

Global administrators (not first user), Security administrators, and Security readers have read-only access

Ensure there are always at least two Privileged Role Administrators

The screenshot shows the 'Add managed members' dialog box. The left pane has two sections: 'Select a role' with 'Privileged Role Administrator' and 'Select members' with 'No members were selected'. The right pane has a '+ Invite' button, a list of members, and a 'Select' button. The list includes 'Admin admin@' (checked) and 'Admin 2 admin2@'. Below the list is a 'Selected Admin' section.

PIM Configuration Settings

Settings can be different for Azure AD roles and Azure resources

Activation

Activation maximum duration (hours)

On activation, require ☒ Azure MFA ☐ None

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approver(s) >

No approver selected

Assignment

☒ Allow permanent eligible assignment

Expire eligible assignments after

1 Year

☒ Allow permanent active assignment

Expire active assignments after

6 Months

☐ Require Azure Multi-Factor Authentication

☒ Require justification on active assignment

Notifications

Send notifications when members are assigned as eligible to this role:

Role assignment alert	☒ Admin
Notification to the assigned user (assignee)	☒ Assignee
Request to approve a role assignment renewal/...	☒ Approver

Send notifications when members are assigned as active to this role:

Role assignment alert	☒ Admin
Notification to the assigned user (assignee)	☒ Assignee
Request to approve a role assignment renewal/...	☒ Approver

Send notifications when eligible members activate this role:

Role activation alert	☒ Admin
Notification to activated user (requestor)	☒ Requestor
Request to approve an activation	☒ Approver

PIM Workflow

PIM Administrator		PIM User	PIM Approver	PIM Administrator
 Plan	 Assign	 Activate	 Approve	 Audit
Determine users and roles that will be managed by PIM.	Assign users or current admins as eligible admins for specific Azure AD roles, so they only have access when necessary.	Activate your eligible admin roles so they can get limited access to the privileged identity.	View and approve all activation requests for specific Azure AD roles that you are configured to approve.	View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant.

End of presentation