



Reimagining The Future of Work with Microsoft technologies

Alan Fong
Microsoft Account Technology Strategist
Public Sector



The New Normal

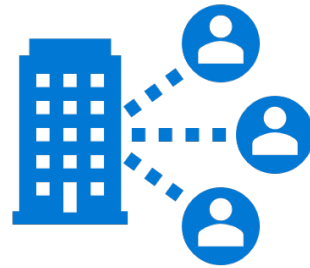




Future of Work



Collaboration



Remote Access

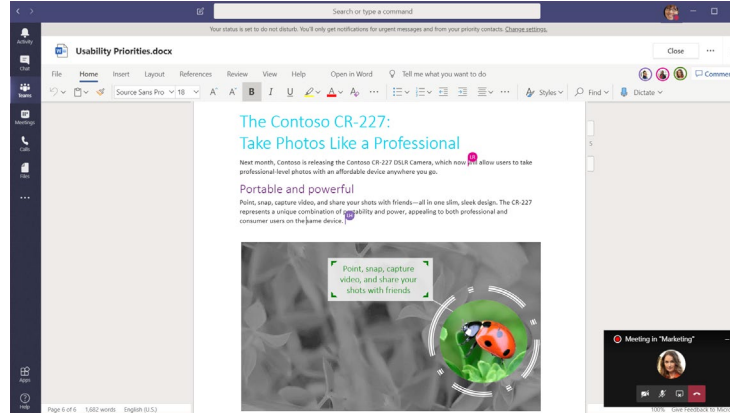


Workstations

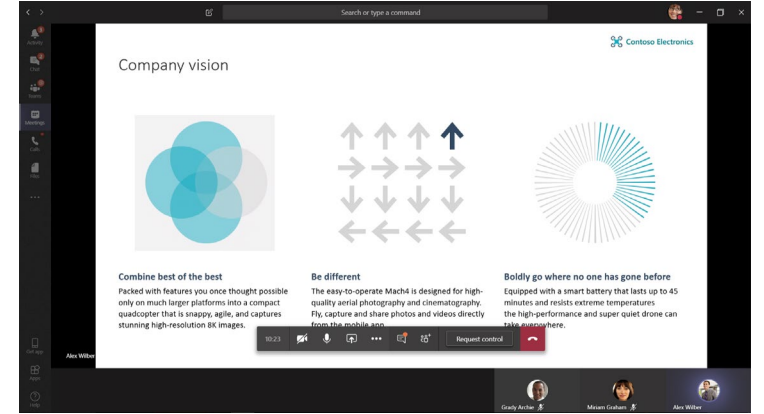
Collaboration Hub



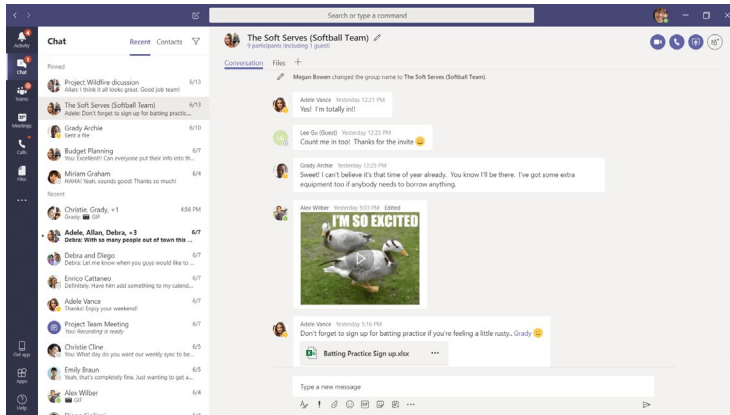
Have a conversation with a colleague or customer



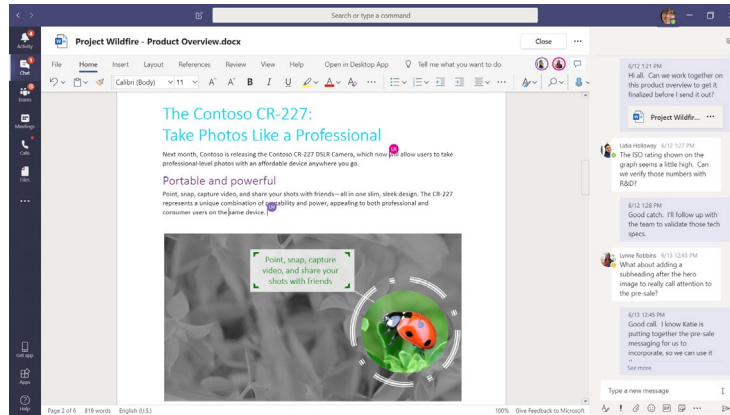
Hold a team update or brainstorming session



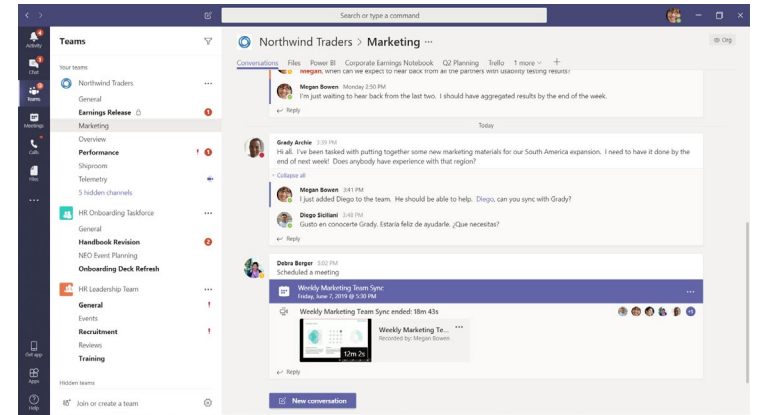
Deliver a training workshop



Do 1:1 and group chats



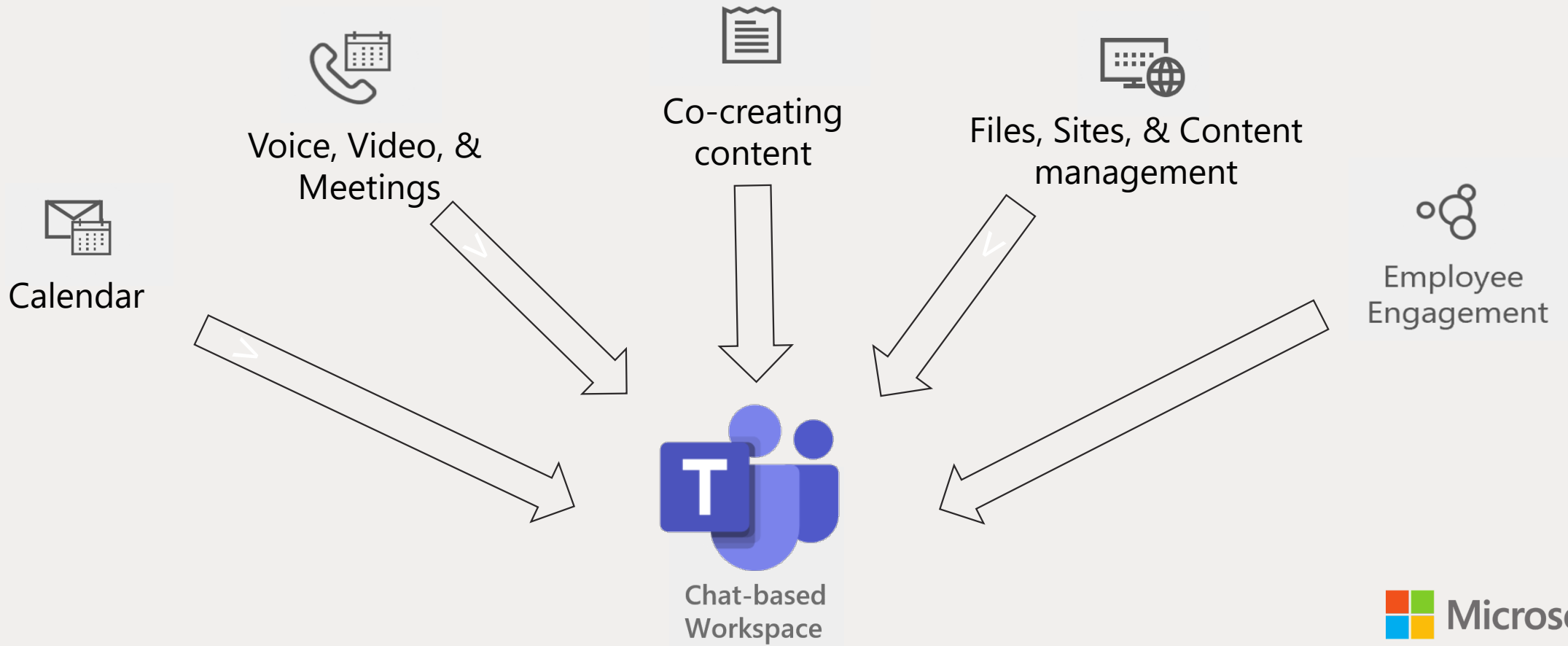
Co-author files and keep track of the conversation



Organize team projects by channel



Microsoft Teams



Security & Compliance

Compliance and Supervisory Controls

[Communication Compliance](#)

[Insider Risk Management](#)

[Auditing](#)

[Advanced Auditing](#)

[Advanced eDiscovery](#)

[Information Barriers](#)

Threat Management for Teams

[ATP Safe Links for Teams](#)

[ATP Safe Documents](#)

[ATP Safe Attachments for SPO, OneDrive and Teams](#)

Information Protection and Governance

[Sensitivity Labels for Teams Content](#)

[Retention Policies for Teams](#)

[Office365 DLP for Teams](#)

[Endpoint DLP for Teams](#)

[Cloud DLP – File Policies](#)

[Cloud DLP – Session Policies](#)



[Trustworthy by Design](#)

[Trustworthy by Default](#)

[How Teams Handles Common Security Threats](#)

[Security Framework for Teams](#)

[Addressing Threats to Teams Meetings](#)

Platform Protection

Identity and Device Protection for Teams

[Common identity and device access policies](#)

[Conditional Access](#)

[Identity Protection](#)

[Privileged Identity Management](#)

Membership, Access and Sharing

[Terms of use](#)

[Teams Classification – Modern \(Sensitivity Label\)](#)

[Privacy – Discovery of Private Teams](#)

[Private channels](#)

[Guest permissions](#)

[Access Reviews](#)

Lifecycle Management and Governance

[Group/Team Creation](#)

[Naming](#)

[Teams classification - Legacy \(public/private\)](#)

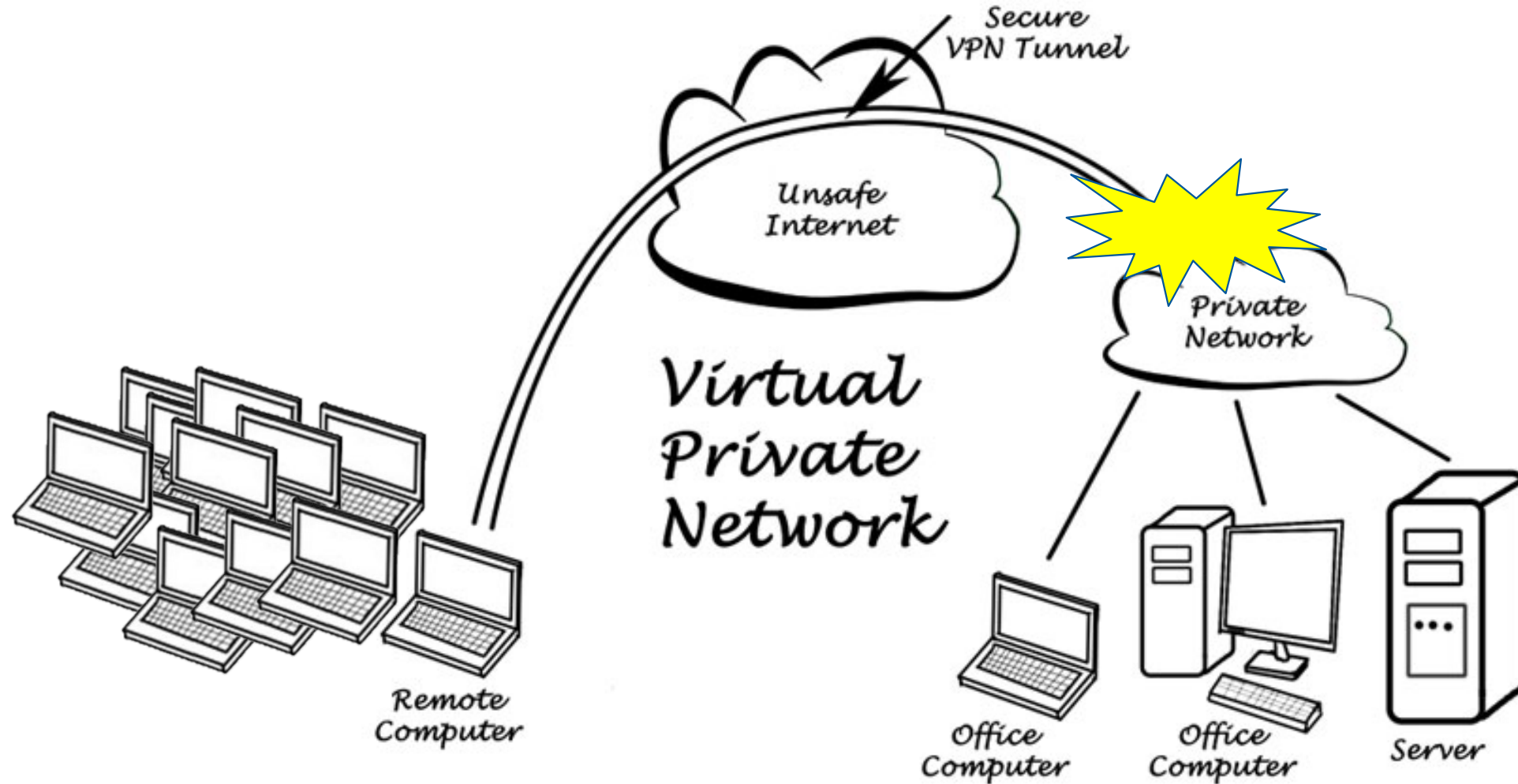
[Expiration](#)

Check list

Security & Compliance Evaluation	
<u>Audit & Compliance</u>	Security aspect
Content Search/ Legal Investigation	- Ability to place a hold on all electronic communication
	Text Messages
	Emojis
	Attachments
	Channel Messages
	Channel Files
	- Ability to apply retention policies
	to apply unique retention policies by Regions, departments
	- Ability to automatically (scheduled) destroy electronic communications that have reached their retention status of (seven) years
	- Ability to search and restore messages (text & files) for end users
Logs	- Ability to provide audit reports for Search, Retrieval, Supervision and administrative access activities and changes
	- Ability to fulfill international compliance standards
Enhanced Protection	
<u>Protect from malicious content sharing</u>	- Ability to provide an Isolated environment to protect all contents including URL, documents, attachment for collaboration
	Sandbox protection for URLs
	Sandbox protection for Documents
	Sandbox protection for Cloud Storages
<u>Data Governance</u>	- Ability to protect sensitive data leakage
	Content sensitivity classification- credit card numbers, social security numbers, health records, etc.
	Data loss prevention on private chat & channel conversations (text)
	Data loss prevention on private chat & channel conversations (files)
	Unique Retention policy applied to only retain content that contains sensitive information
<u>Secured Identity & Access</u>	- Ability to support for multi-factor authentication
	- Ability to offer a complete Privileged Identity Management (PIM)
	- Ability to apply Conditional Access by users' locations, managed devices to specific group of users
	- Ability to detect suspicious access pattern
<u>External Collaboration Controls</u>	- Fine grain B2B & B2C access control
	- only permit internal collaboration
	- Collaboration with external parties (i.e. business partners, vendors & agencies) is not permitted unless:
	- they are from whitelisted domain (federated users)
	- they are approved by administrator
	- they login with MFA
	- their devices fulfilled your device compliance policies (e.g. Windows/ iOS/ Android version)



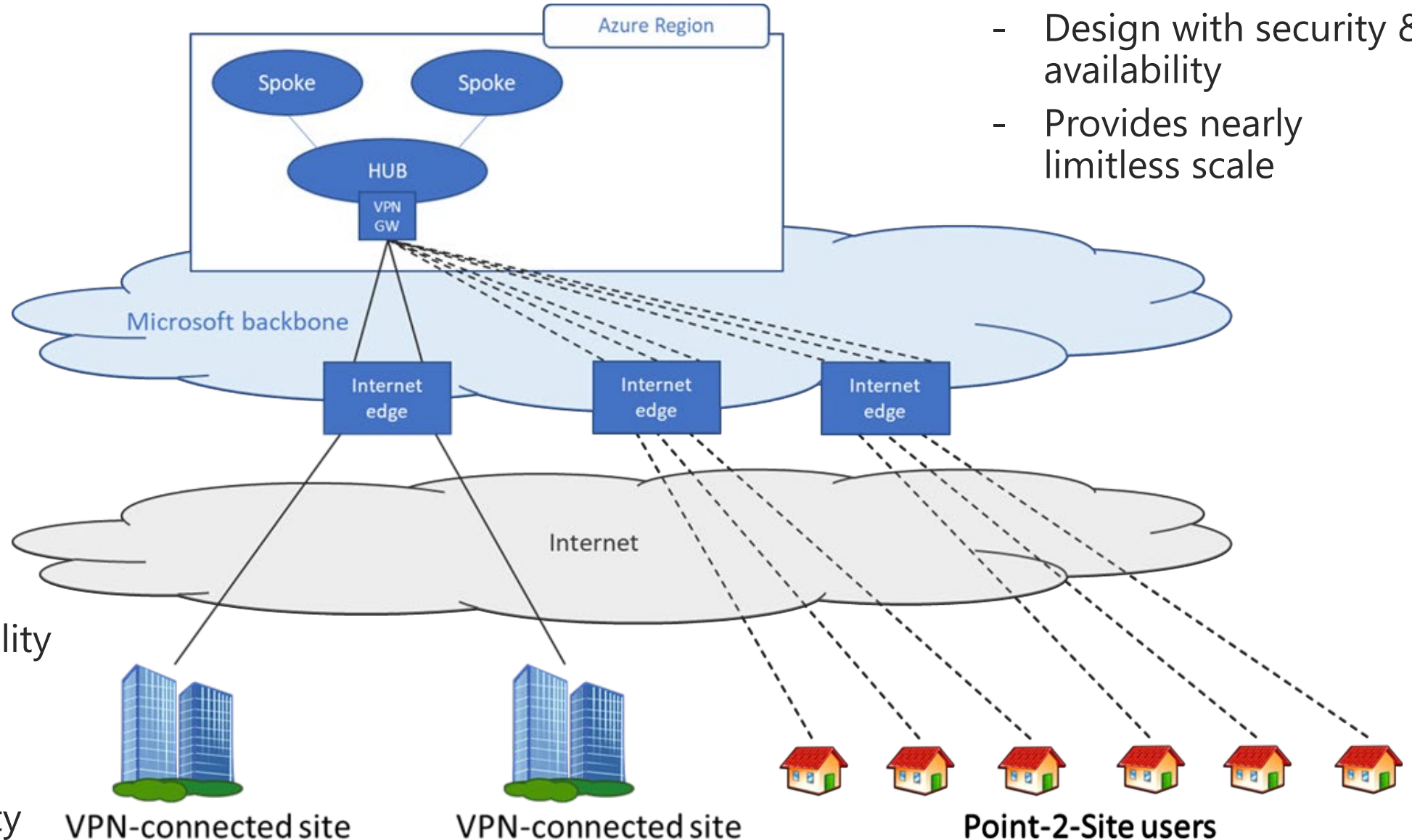
Remote Access to Premises Resources



Scale remote work with Azure

Point-2-Site VPN

- Leverage Microsoft network infrastructure
- Design with security & availability
- Provides nearly limitless scale



Site-2-Site VPN / ExpressRoute

- Eliminates availability & bandwidth challenge to on-premises network
- Private connectivity



VPN-connected site



VPN-connected site

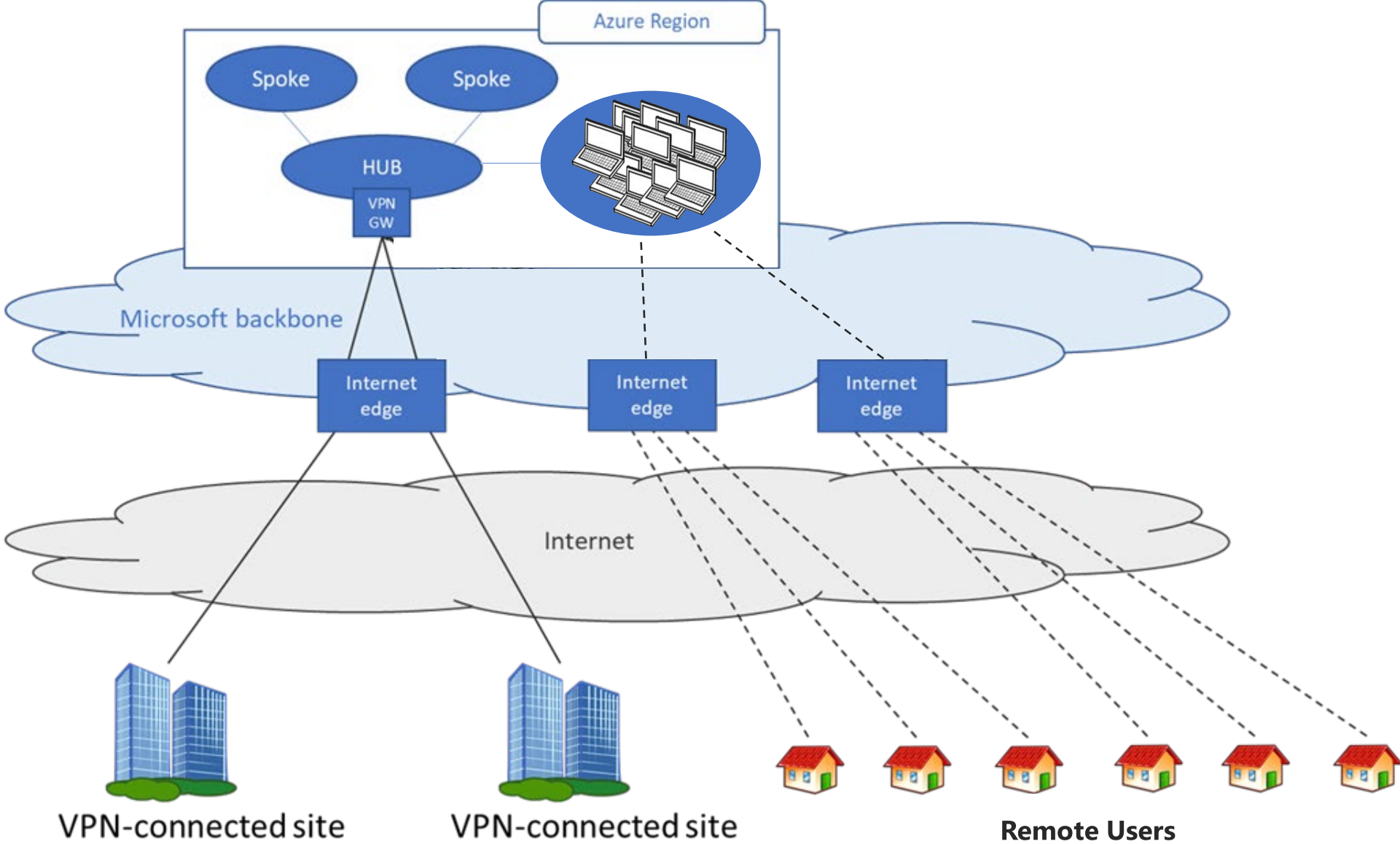


Point-2-Site users

Provision Remote Work devices



Virtual Desktop

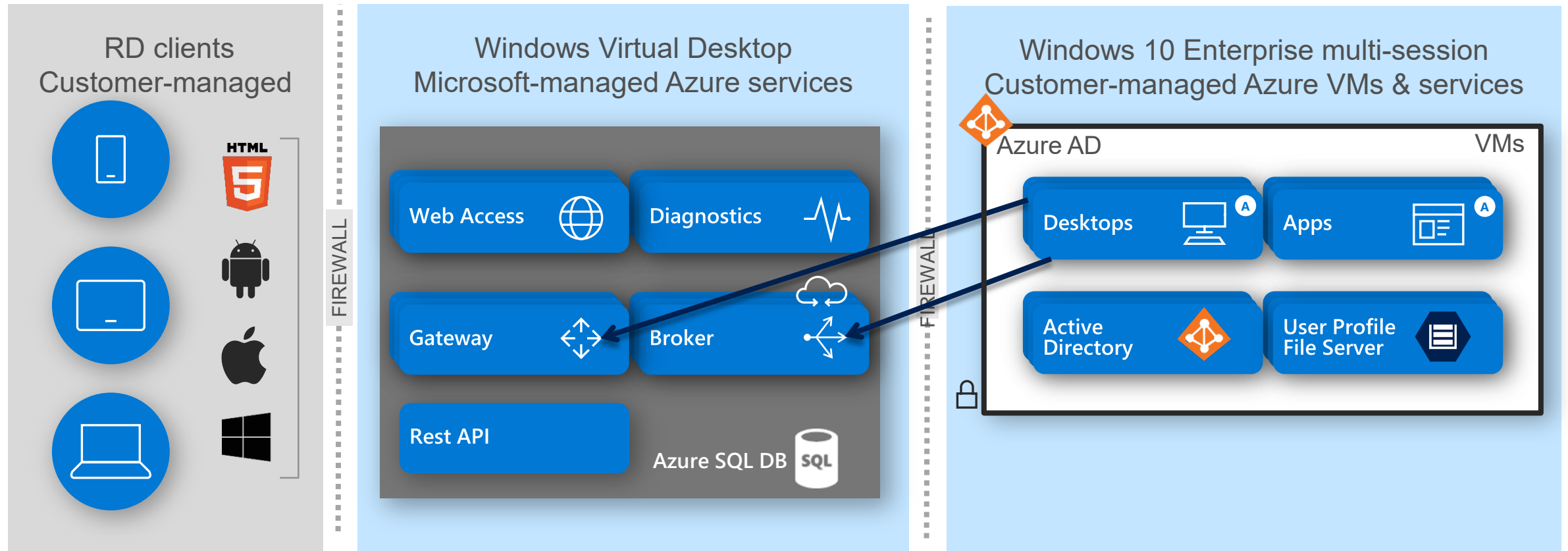


Improved Isolation: Reverse Connect

Outbound WebSocket connections from customer VMs to Broker and Gateway

Bidirectional communications between VMs and RD infra over https (443)

No inbound ports need be opened to the customer environment



Windows Virtual Desktop (WVD) on mobile devices

Full screen Windows 10 and Office 365 ProPlus experience mobile devices, providing the **Windows Virtual Desktop experience on an Android endpoint**

Enhanced mobility and productivity with **small and big screen experience**, allowing seamless switching from one application to another

Faster speeds and reduced latency with the support for 5G and Wi-Fi 6



Desktop-As-a Service

Windows Virtual Desktop (WVD) on Azure

- Securely access your desktop anywhere
- No client-side VPN required
- Most devices supported
- Require only Windows 10 Enterprise licenses

+ Unique Windows 10 Enterprise multi-session (share workload e.g. 3 VMs support 100 users)

+ Enable optimizations for Office 365 ProPlus

+ Deploy and scale in minutes

+ Charge only consumed workload





Secure
Collaboration

O365 Teams



Scalable
Remote Access

Azure VPN



On-demand
Workstations

WVD

Thank you.

Appendix



Teams overview



Access management

Integrated with your identity and access management system using Azure Active Directory

Take advantage of multi-factor authentication and conditional access

Unified identity and access management whether users sit inside or outside of your organization

Data security

Built on the Microsoft 365 hyperscale, enterprise cloud

Meets national and international standards, such as: ISO 27001, ISO 27018, SOC 1 and SOC2, HIPAA, GDPR

Many consumer-oriented data-sharing, chat, and video conferencing apps do not

Teams data is encrypted in transit and at rest

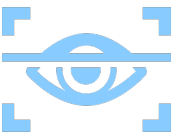
Meeting security: data and network transport

Core features:

- Network communications are encrypted using TLS, SRTP, and other industry standards, including 256-bit AES
- Media traffic uses SRTP both for client-to-client calls and multi-party meetings
- Files and other data are similarly encrypted on cloud storage
- All messages in Teams are archived for legal hold, compliance search, supervision, and retention (governed by policies)

Additional capabilities:

- Compliance recording APIs allows for third-party cloud or on-premises solutions to record all or selected calls and meetings
- Data loss prevention to block accidental or intentional leakage
- Sensitivity labels on teams and documents to control privacy and access
- Advanced threat protection to detect and block malware and unsafe links
- Key exchange (using PKI on Windows Server) is also done using TLS



Multi-factor authentication

81%

of breaches leverage stolen or weak passwords

MFA prevents

99.9%

of identity attacks



Microsoft Authenticator



Windows Hello



Hard Tokens OTP



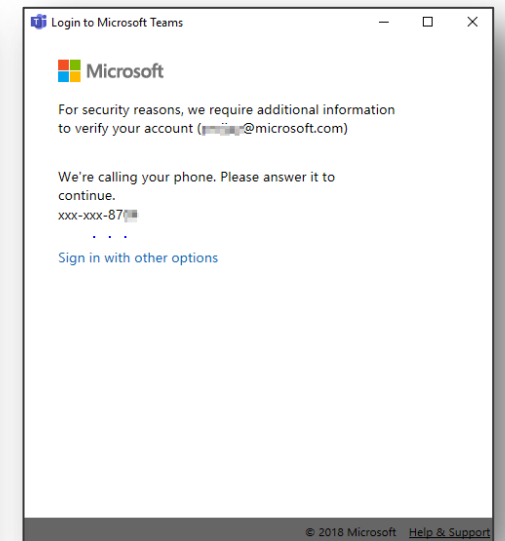
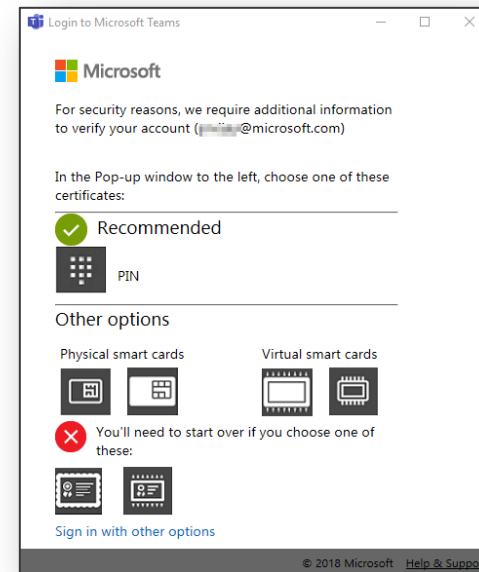
SMS, Voice



Push Notification






FIDO2 Security key

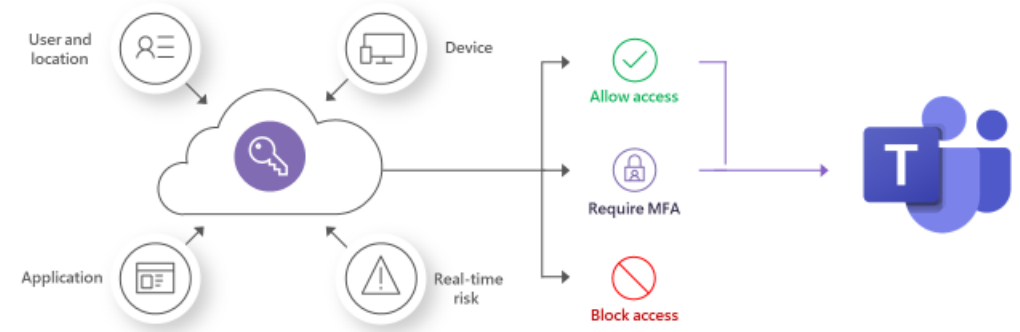


Identity and access




-  **MFA, conditional access, and SMS codes**
Enforce strong authentication and protect against unauthorized or atypical access risks
-  **Information Barriers**
Create different segments within the company and with guests to block discovery and communication
-  **Guests and secure cross-company access**
Securely manage how external individuals can access company resources and participate in chats and meetings

Conditional Access






Governance



-  **Management, roles, and reporting**
Manage and monitor Teams and dependent services using specialized admin roles
-  **Settings and policies**
Craft policies for different user populations governing messaging, meetings, apps, and more
-  **Teams and channels management**
Implement governance policies and lifecycle management to reduce security risk and "team sprawl"

Compliance and data security



-  **Compliance: archiving, retention, search, eDiscovery, supervision, audits**
Retain, review, and export sensitive content to monitor violations, and verify user behaviors
-  **Data loss prevention**
Monitor content sharing, detect violations, and block distribution of sensitive or private information in chats
-  **Secure access to data and apps**
Protect sensitive data by controlling and managing access to files and applications

Windows Virtual Desktop Supported OS

Windows 10 Enterprise Multi-session

Windows 10 Enterprise Single-Session

Windows 7 Single-Session

Windows Server 2019

Windows Server 2016

Windows Server 2012 R2

[VMs in customer's Azure subscription](#)



Native Windows Virtual Desktop

High Level Architecture

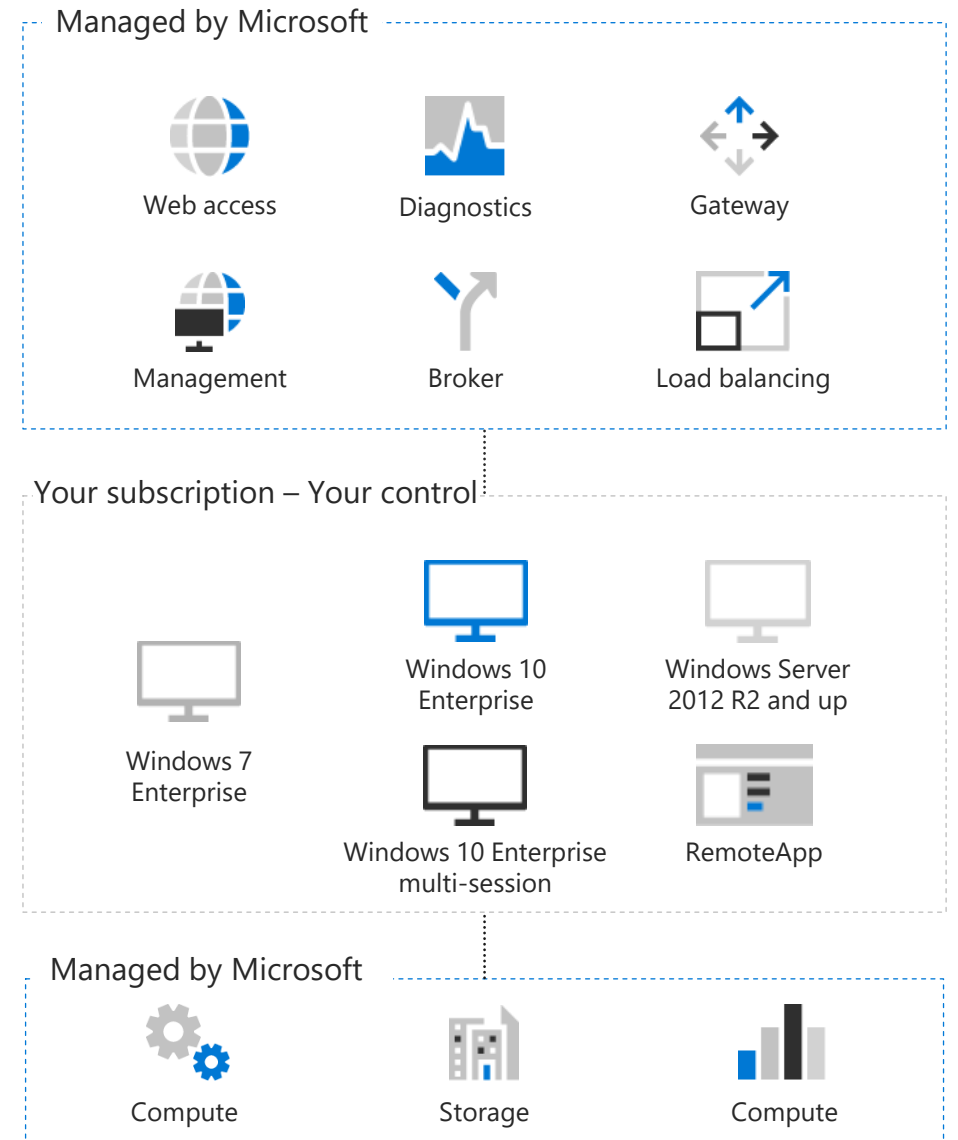
Use Azure Active Directory identity management service

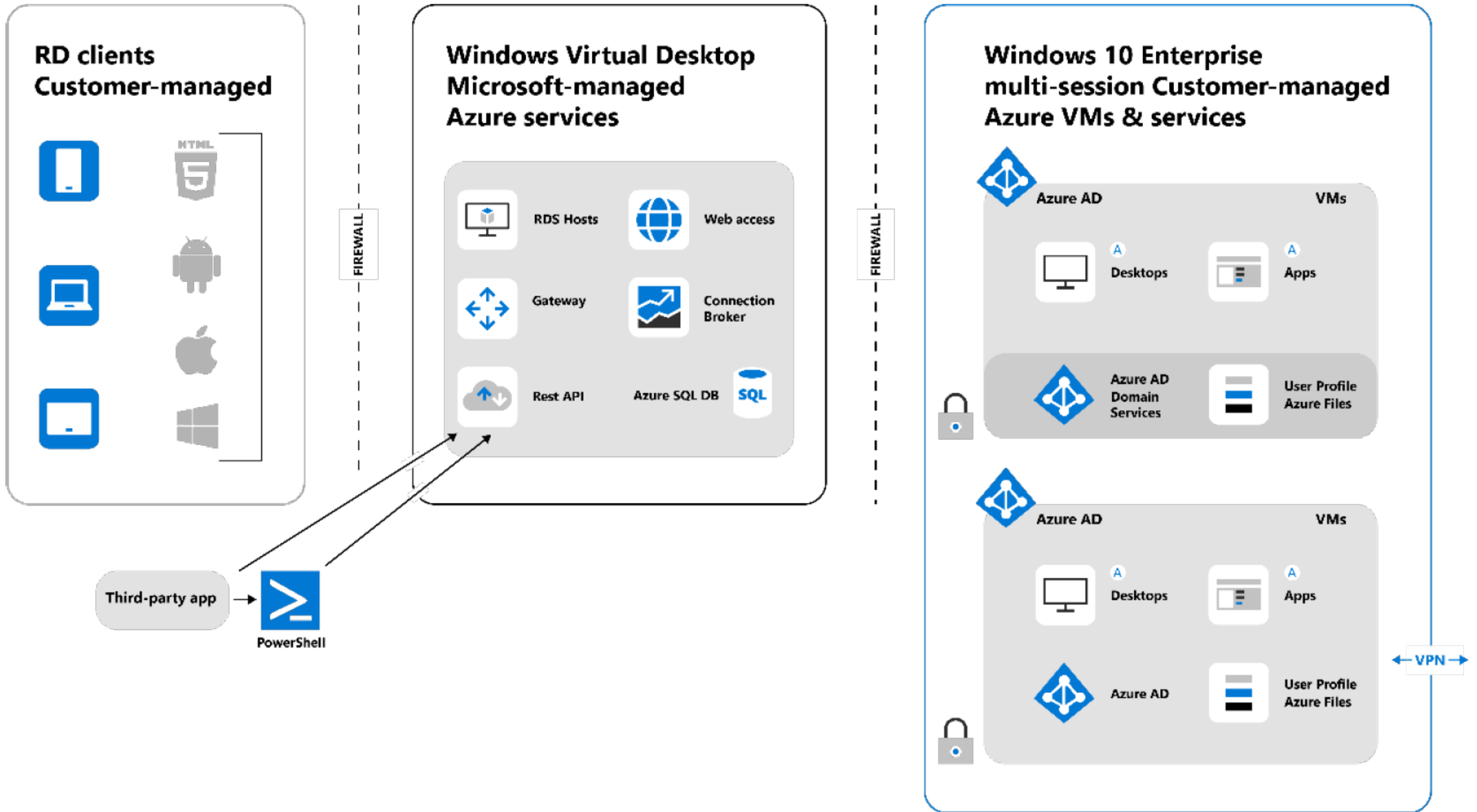
Provide virtualization infrastructure as a managed service

Deploy and manage virtual machines in Azure subscription

Manage using existing tools like Configuration Manager or Microsoft Intune

Connect easily to on-premises resources





Recommended identity setup for hybrid organizations

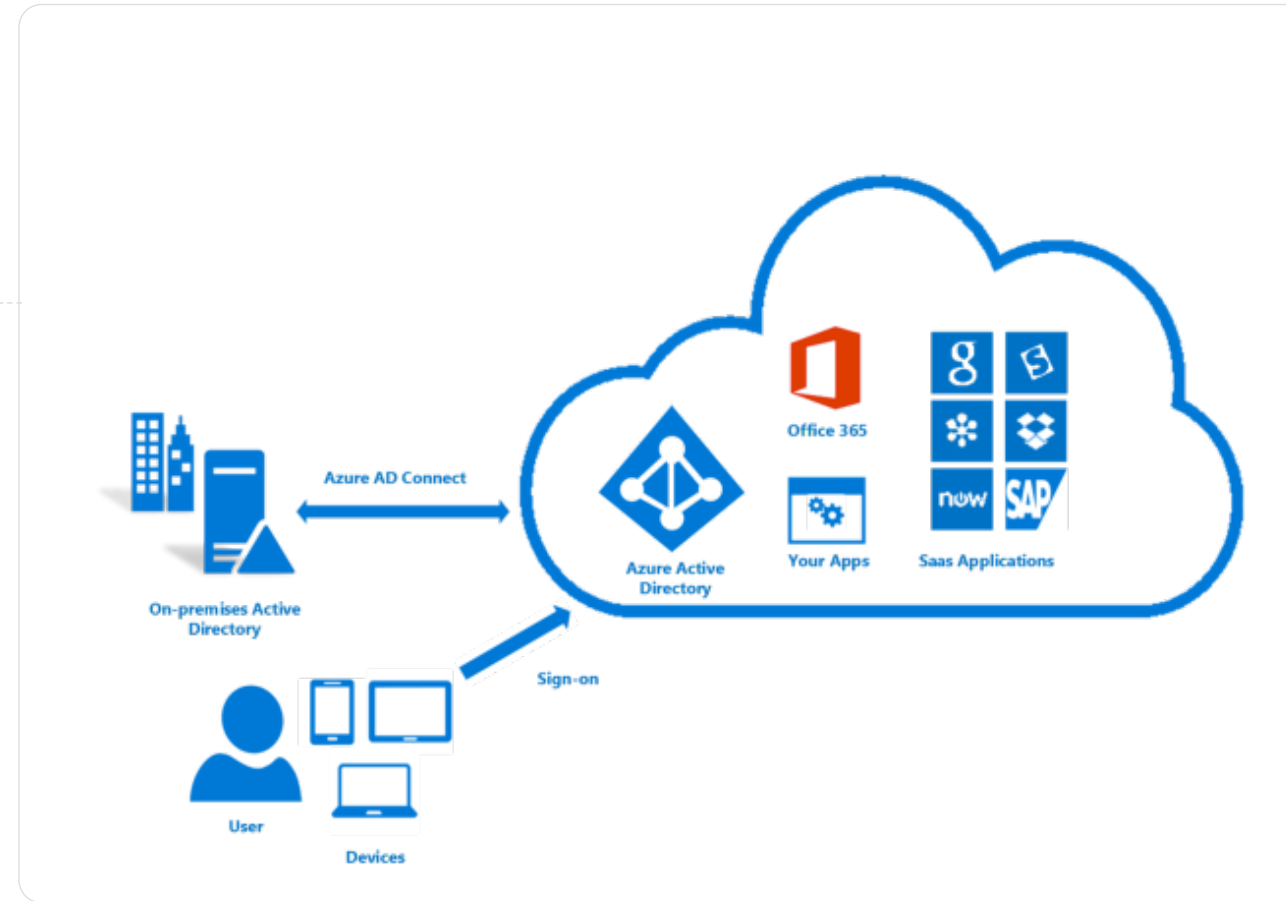


Azure AD



Windows Server AD on-prem connected to Azure

- ExpressRoute or site-to-site VPN to Azure
- Azure AD Connect to synchronize identities



Many customers are already eligible for WVD

WVD Licensing Requirements



Client

Customers are eligible to access Windows 10 single and multi session and Windows 7 with Windows Virtual Desktop (WVD) if they have one of the following licenses*:

- Microsoft 365 E3/E5
 - Microsoft 365 A3/A5/Student Use Benefits
 - Microsoft 365 F1
 - Microsoft 365 Business
 - Windows 10 Enterprise E3/E5
 - Windows 10 Education A3/A5
 - Windows 10 VDA per user
-



Server

Customers are eligible to access Server workloads with Windows Virtual Desktop (WVD) if they have one of the following licenses:

- RDS CAL license with active Software Assurance (SA)

Customers pay for the virtual machines (VMs), storage, and networking consumed when the users are using the service

*Customers can access Windows Virtual Desktop from their non-Windows Pro endpoints if they have a Microsoft 365 E3/E5/F1, Microsoft 365 A3/A5 or Windows 10 VDA per user license.