Windows Virtual Desktop for CMMC

[Your name here]
[Presentation date here]

SUMMIT7

DIB challenges:
The pursuit of secure, compliant, and productive remote work

SUMMIT7

Provide a Managed User Experience and **Prevent Download or Exfiltration of CUI**

CMMC
DFARS
ITAR

Security and compliance

Meeting compliance requirements for CUI and ITAR data necessitates secure network access, access control for users and administrators of the environment, proper logging, and mature authentication practices.

Budget and resource constraints

Additional investment in securing on-premises systems and hardware can be expensive and time-consuming, and puts pressure on available IT budgets as well as on human capital.

Scaling and capacity issues

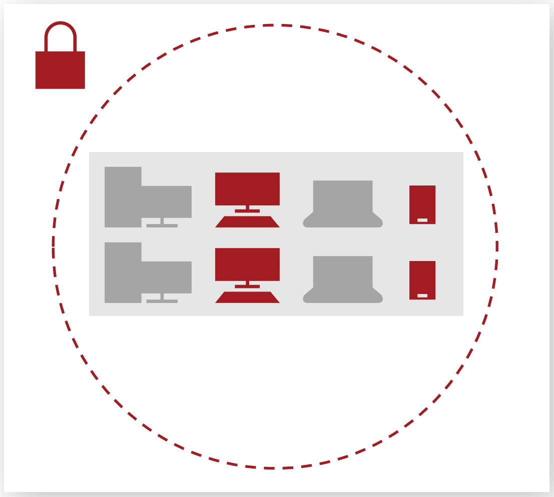
Contractors in the DIB need to adapt to consistent onboarding with contracts won and lost, as well as accommodate back office users and heavy engineering workloads alike. Organizations also need to scale quickly and handle the variable server load.

Enabling remote work

With more being accomplished outside of the workplace than ever before, there is an immediate need to enable secure, remote IT practices that are simple, efficient, and can be done from anywhere on any device.

WVD Pooled Model

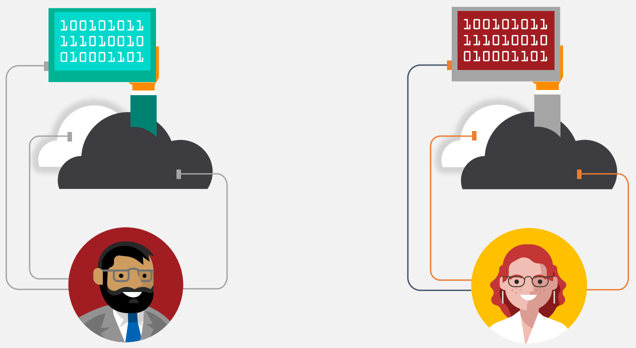
Multiple user sessions each with their individual Windows 10 Desktop Profile



WVD

Containerized profiles

User profiles

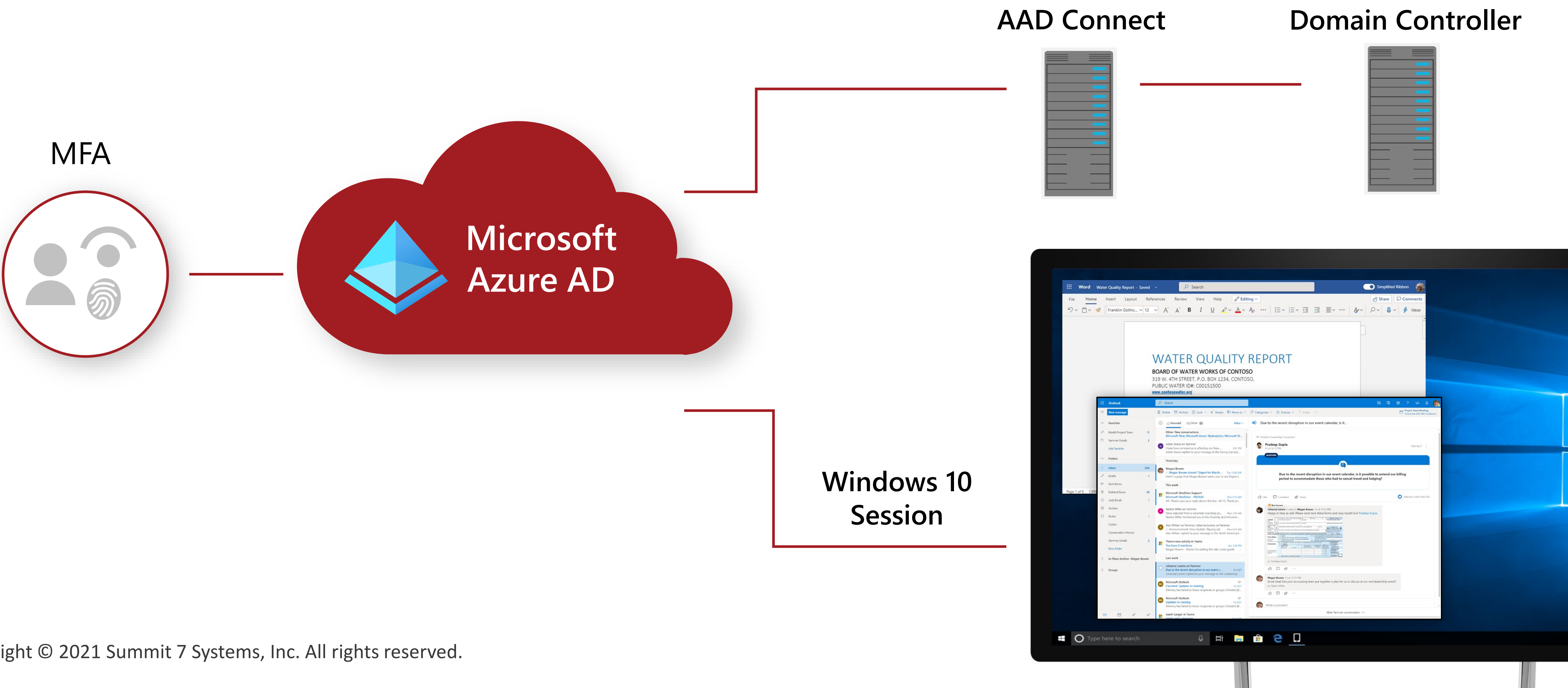


Placed into a VHD container stored on Azure Government

- Dynamically attached at user logon
- Content appears to be in its native location

Windows 10
+
Office 365
Windows
Server
Microsoft Azure

Enable CMMC Compliant Remote Access



WVD Solution Standard Deliverables

- Azure Government Tenant Configuration
- Prepare and Configure Azure AD
- Configure Secure Profile Storage
- Configure Azure File Share
- WVD Image Creation for Pool
- Secure VMs

+ *More Deliverables and Detail in SOW*

SUMMIT7

Windows Virtual Desktop Licensing

Client

Customers are eligible to access Windows 10 single and multi-session with Windows Virtual Desktop if they have one of the following licenses:

- Microsoft 365 E3/E5
- Microsoft 365 F1
- Windows 10 Enterprise E3/E5
- Windows 10 VDA per user

Server

Customers are eligible to access server workloads with Windows Virtual Desktop if they have one of the following licenses:

RDS CAL license with active Software Assurance

SUMMIT7

Why Windows Virtual Desktop for CMMC?

SUMMIT7

Domains Addressed in CMMC via WVD Solution

- Access Control (AC)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Media Protection (MP)
- Recovery (RE)
- System and Information Integrity (SI)

SUMMIT7

CMMC
DFARS
ITAR

Improve security with built-in and integrated Microsoft security offerings

With the widest portfolio of security offerings, Windows Virtual Desktop keeps business applications and user data both secure and compliant.

Windows Virtual Desktop:

- Limit the compliance and security scope on end points (no CUI residing on personal machines)
- Includes built-in Azure security capabilities and is integrated with the security and management of Microsoft 365
- Helps keep users, devices, and data safe with multifactor authentication and conditional access
- Increases protection for our infrastructure with configurable security tools such as Azure Security Center and Microsoft Endpoint Manager.

Deliver the best user experience, on every device

Windows Virtual Desktop offers the best virtualized experience, within the only solution that is fully optimized for Windows 10 and Microsoft 365.

Windows Virtual Desktop:

- Provides the only fully-optimized Windows 10 and Windows Server desktop and application virtualization, for personal devices from any internet-connected location.
- Offers seamless integration with Microsoft 365 Apps for enterprise and Microsoft Teams, so employees enjoy the same benefits they expect of desktop experiences.
- Azure Government ensures data residency and access requirements are maintained while serving up quick access to users with dedicated data centers

Avoid capacity constraints—deploy and scale in minutes

Windows Virtual Desktop simplifies the deployment and management of infrastructure, and quickly scales based on business demands.

Windows Virtual Desktop:

- Is always up to date, because Microsoft and Azure manage the entire VDI (*not the security*)
- Reduces the need for hardware inventory and maintenance per CMMC, freeing IT team to focus on users, apps, and OS images
- Quickly gets users up and running and leverages the cloud to instantly scale in response to business needs

Reduce costs and modernize

With Windows Virtual Desktop organizations can save by using existing licenses, leveraging a cloud-based VDI to pay only for what is used, and modernizing infrastructure using the products that are already in the toolkit.

Windows Virtual Desktop:

- Accessed through existing Windows and Microsoft 365 eligible licenses.
- Provides consumption-based pricing down to the minute
- Uses Windows 10 multi-session to add more users and increase utilization of Virtual Machines (VMs)
- Limits compliance scope within CMMC Domains: Asset Management (AM), Physical Protection (PE) and Media Protection (MP)

Why Summit 7?

SUMMIT7

Cloud Compliance Focus
Exclusively DIB

Summit 7 is a CMMC AB accredited RPO specializing in configuring Microsoft 365 GCC High and Azure Government to CMMC specifications. Since 2017 the company has implemented NIST 800-171 controls and CMMC practices in hundreds of tenants, many of which that have received perfect assessments from DCMA.

Microsoft
US Partner Award 2020
Security and Compliance

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

Microsoft Partner
Microsoft

- Gold Security
- Gold Cloud Productivity
- Gold Cloud Platform
- Gold Enterprise Mobility Management
- Gold Collaboration and Content
- Gold Messaging
- Gold Data Analytics
- Gold Small and Midmarket Cloud Solutions
- Gold Application Development
- Gold Datacenter
- Gold Windows and Devices
- Silver Communications

SUMMIT7