Aprio

CMMC PNW

Hybrid Environment

Cloud + On Premises

What is a Hybrid Environment?

Part of your CUI environment is in the cloud, and part remains at your physical location.

Cloud: Microsoft 365 GCC, GCC-High, AWS, GCP, FR SaaS apps

On-premises: CAD, workstations, file servers, manufacturing systems, scanners, printers, CNC equipment, or engineering applications.

Controlled connections allow approved identities and data to **move between** the two.

Logically or physically separate the rest of the corporate environment from the CUI environment.

Aprio

Hybrid Use Cases

MANUFACTURING
CNC machines, shop-floor systems & production equipment

ENGINEERING
CAD, large design files, high-performance workstations & licensing

LEGACY SYSTEMS
Business critical apps that cannot move or would be costly to rebuild in the cloud

PERFORMANCE LIMITATIONS
Moving large design or manufacturing files back and forth may create delays that interfere with production.

Cloud or On-Prem

REASONS FOR ON-PREM

- Legacy equipment
- GPU requirements / Latency
- Software compatibility
- Large file sizes
- Production availability
- Security
- Licensing
- Disconnected operations (reliability)
- Not FR authorized/equivalent

REASONS FOR CLOUD

- Cost for on-site management (operations)
- Some workloads are more efficient in the cloud
- Inexpensive storage
- VDI/AVD/Cloud PCs – smaller scope
- Cloud admin centers are user friendly

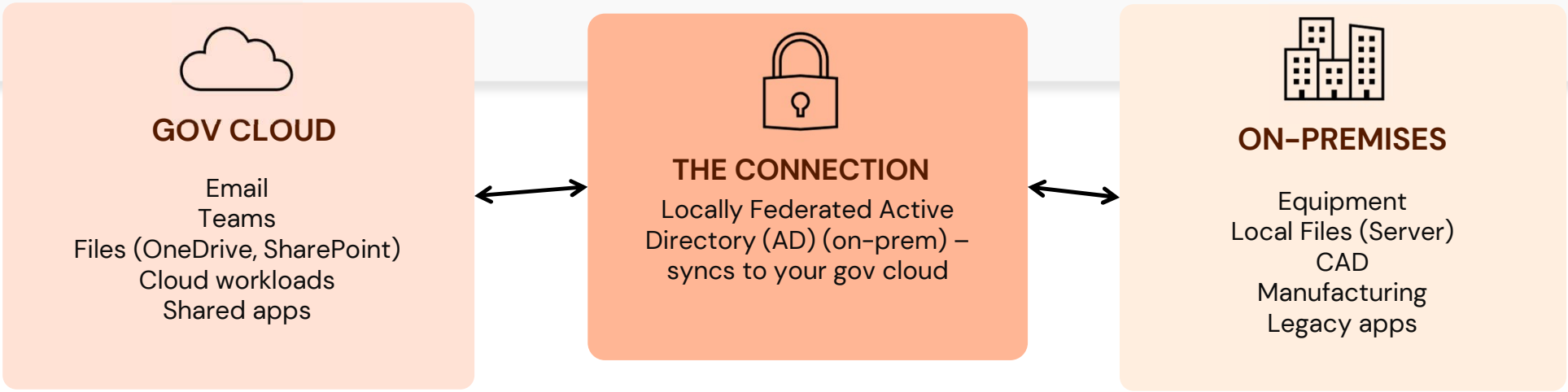
REMEMBER:

Physical Scope Introduces Physical Controls. Make sure you address these for your physical boundary:

- Controlled areas
- Visitor access
- Server rooms
- Workstation placement
- Screen visibility
- Printed material
- Media storage
- Equipment disposal
- After-hours access (Cleaning and maintenance personnel)

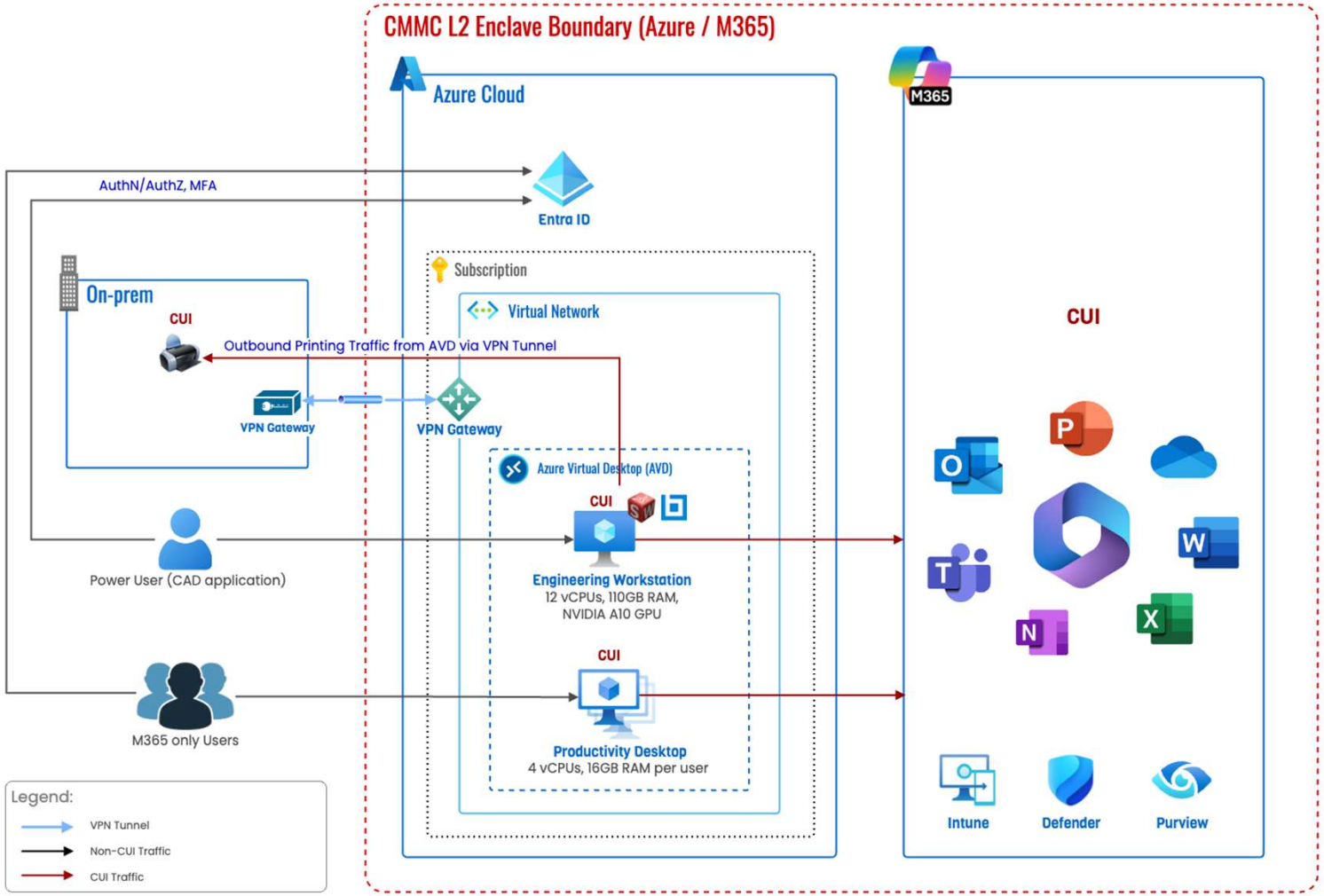
Aprio

How Cloud & On-Prem Meet



Aprio

Sample - Greenfield Architecture Diagram



How do I connect on-premises to GCC or GCC High without exposing CUI?

First segregate (logically, physically) on-prem compute from commercial environment to include in boundary.

Use managed endpoints, virtual sessions, firewall restrictions, MFA, conditional access, centralized monitoring, and synchronize identities.

Ensure physical controls are in place that meet CMMC requirements (server rooms are secure)

1. **Who** can access?
2. **What** information is allowed through?
3. **Which** device or system may receive it?
4. Is the **movement** encrypted and monitored?
5. Can we **show** an assessor **evidence**?

Will a hybrid setup make my assessment harder?

Not necessarily harder, but there is more to explain.

Physical controls are in place.

Ensure you understand your boundary very well and the security controls in place to protect it.

Contact:

Ashley Lex

Senior Manager,
Security & Compliance Services

ASHLEY.LEX@APRIO.COM

www.linkedin.com/in/ashley-lex

Thank you!

Q&A

Basic Scoping – Follow your CUI

01

What is it, and how is it received?

Files, drawings, email, print jobs or security information.

Contracts, data > Email, customer portals, file sharing or physical delivery.

02

Where is the work being done?

Cloud applications, shop floor, workstations, CAD, servers, manufacturing, backups, print or scan, USB, shared folders, remote access.

03

Who has access?

Employees, engineers, administrators, vendors, subcontractors or service providers.

Follow the whole lifecycle of CUI. Where it's created, received, stored, processed, transmitted, printed, destroyed and the people, processes, applications that interact with it along the way.

Will Hybrid Make My Assessment Harder?

01

Inventory the CUI, not the network

Start from contracts and data. Interview engineering, quality, PM, and the shop floor.

02

Draw the data flows across planes

Trace CUI origin to disposal across on-prem, GCC High, and Azure Gov.

03

Categorize every asset

Into one of five buckets, asset by asset. Write down the reasoning.

04

Apply separation only where you want out-of-scope

If it's not worth the cost, accept the asset into scope instead.

05

Settle inheritance & shared responsibility

A CRM for every ESP and CSP. Unassigned is yours by default.

06

Set the re-baseline triggers

Architectural changes need reassessment; routine ones are covered by annual affirmation.

REMEMBER:

Not harder — different. It requires the architecture and the evidence to match. This six-step method is how you get there.

What DIB Contractors Should Do Now

01

Update Your SPRS Score

Submit or refresh your self-assessment. A stale or inflated score is **more** exposed now, not less. NIST 171 vs. CMMC record.

02

Keep Affirmations Current

The Affirming Official's annual affirmation must stay up to date. Lapses create immediate contractual risk.

03

Don't Stop C3PAO Prep

Treat it as a mock assessment to support SPRS. It's the best path to validate your score.

04

Maintain Your Evidence Package

SSP, POA&Ms, and artifacts — keep them as if an assessor arrives tomorrow.

05

Train Employees

Continue CUI handling and identification training. Workforce awareness is a scored NIST 800-171 practice.

06

Manage Subcontractors

Expect prime flowdowns to continue or tighten regardless of DoD's posture. Audit your supply chain now.

REMEMBER:

Your Business Risk Did Not Change

- A stale or inflated SPRS score is more exposed now, not less. DIBCAC and DOJ's Civil Cyber-Fraud Initiative (False Claims Act) enforcement doesn't pause with CMMC.

Five Categories CUI Assets

01 **CUI Asset** Creates, stores, processes, or transmits CUI. Fully in scope, fully assessed.

02 **Security Protection Asset** Provides a security capability. In scope wherever it runs.

03 **Specialized Asset** OT, IoT, GFE, test equipment. Documented and risk-managed.

04 **Contractor Risk Managed Asset** Can reach CUI, kept away from it by policy, not architecture.

05 **Out-of-Scope Asset** No path to CUI at all — and you can demonstrate it.

REMEMBER:

Separation is only required to push assets out of scope. In-scope categories don't have to be separated from each other.