

It's 10 PM, Do You Know Where Your MSP Is?

Presented by: Ryan Bonner and Daniel Akridge



MSPs want to know how CMMC applies to them.

CMMC applicability isn't easy to determine based on rule language.

A simple "D.A.R.E." model can help.



Data

- CUI: Controlled Unclassified Information. Subject to DFARS 252.204-7012.
- SPD: Security Protection Data. Loosely defined as "system logs, configuration data."



Data



Data

FedRAMP “Direct Impact” data. “...security data revealing the current security posture of the system, vulnerability information, active incident response information and communications, active threat assessment, penetration test or security investigation information and communications.” FedRAMP® Authorization Boundary Guidance v 3.0 (Draft) 3/15/2022



Data

Merging these two sources looks something like this:

- System logs (3.3.1)
- Configuration data (3.4.2)
- Vulnerability scan data or reports (3.11.2)
- Security incident tickets or reports (3.6.2)
- Threat intelligence analysis (3.11.1e) 800-172
- Internal security directives (3.14.3)
- Penetration tests or red team reports (3.12.1e) 800-172
- Security control assessment reports (3.12.1)
- Team communications (emails, messages) during incidents (3.6.2)



Data

- CUI: Controlled Unclassified Information. Subject to DFARS 252.204-7012.
- SPD: Security Protection Data. Loosely defined as "system logs, configuration data."



Asset Type

- CUI Asset: processes, stores, or transmits CUI.
- ESP Asset: processes, stores, or transmits SPD.
- Security Protection Asset (SPA): Provides security protection for a CUI Asset.



Entity Type

- Internal Organization: simply part of the assessment scope
- External (Outsourced) Organization: requires standalone CMMC certification.



Asset Type

Data	Asset Type	Requirement	Entity	Certification
CUI	CUI Asset	800-171	Internal	OSA
CUI	Cloud CUI Asset	FedRAMP	Internal	OSA
SPD	ESP Asset	800-171	Internal	OSA
SPD	ESP Asset	800-171	External (MSP)	MSP
-	SPA	800-171	Internal	OSA
-	SPA	800-171	External (MSP)	MSP



MSPs use industry-specific tools to deliver services at scale

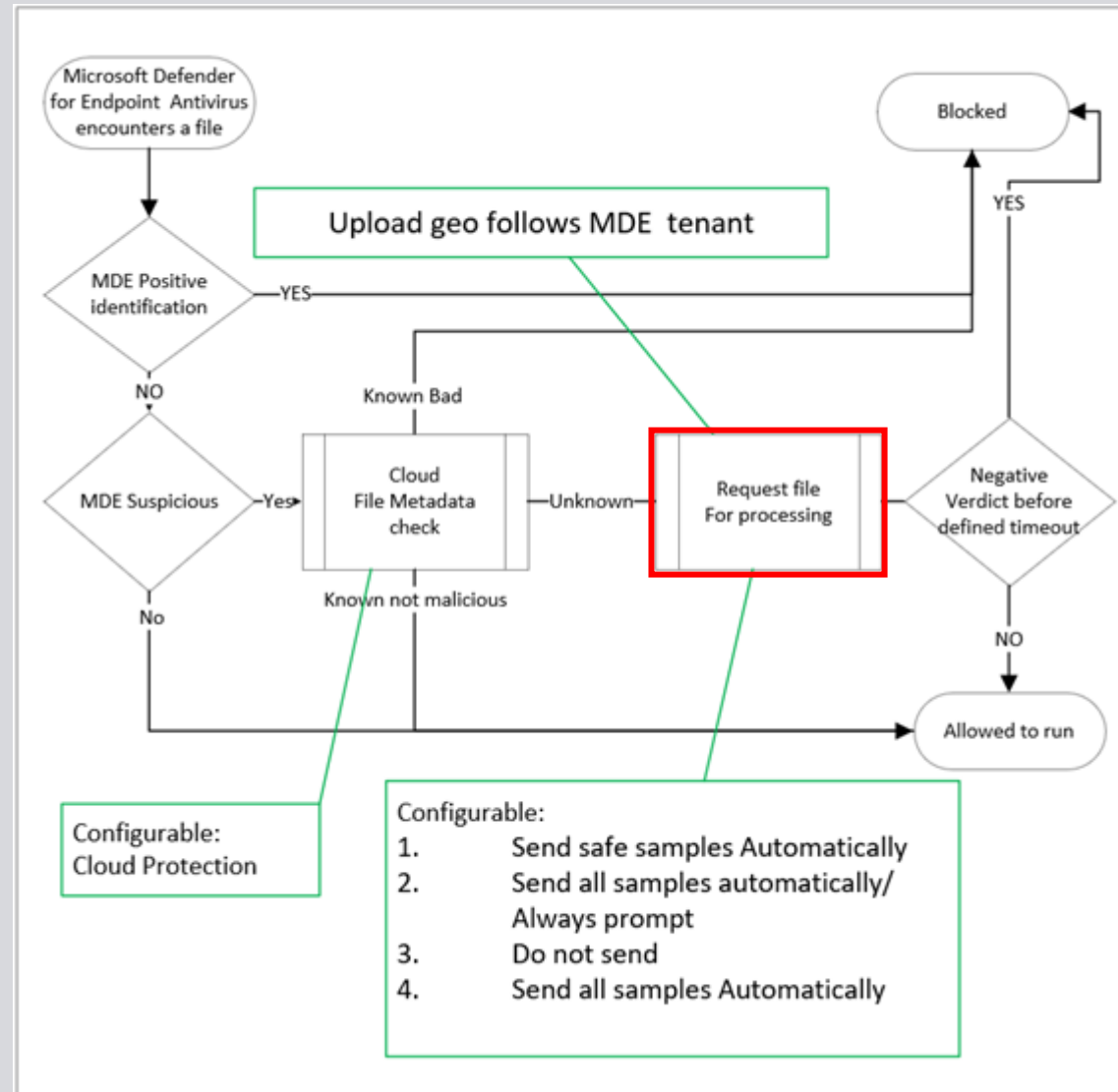
These specialized tools carry an elevated risk of unauthorized access and disclosure.

MSPs must realign their tech stack and service model.



EDR

Most EDR tools automatically upload files to the cloud for detonation and analysis.



EDR

Most EDR tools can launch a remote shell to collect files, memory dumps, and digital forensics data.

Collect a specific file and upload to Trend Vision One

Maximum file size: 4 GB

```
get  
<file_location_and_extension>
```

- To collect the file example.txt file in the current directory /Users/admin/Downloads :

```
Downloads> get  
example.txt
```

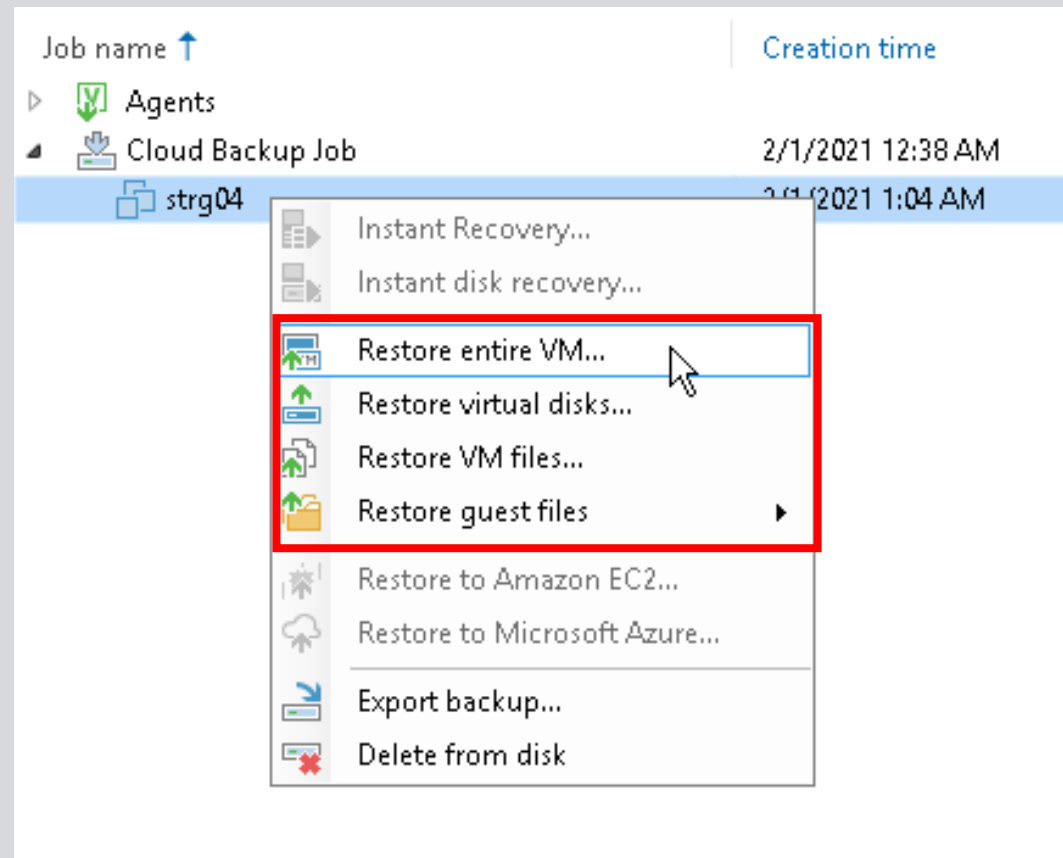
- To collect the file example.txt file located in the /tmp directory:

```
Downloads> get  
/tmp/example.txt
```



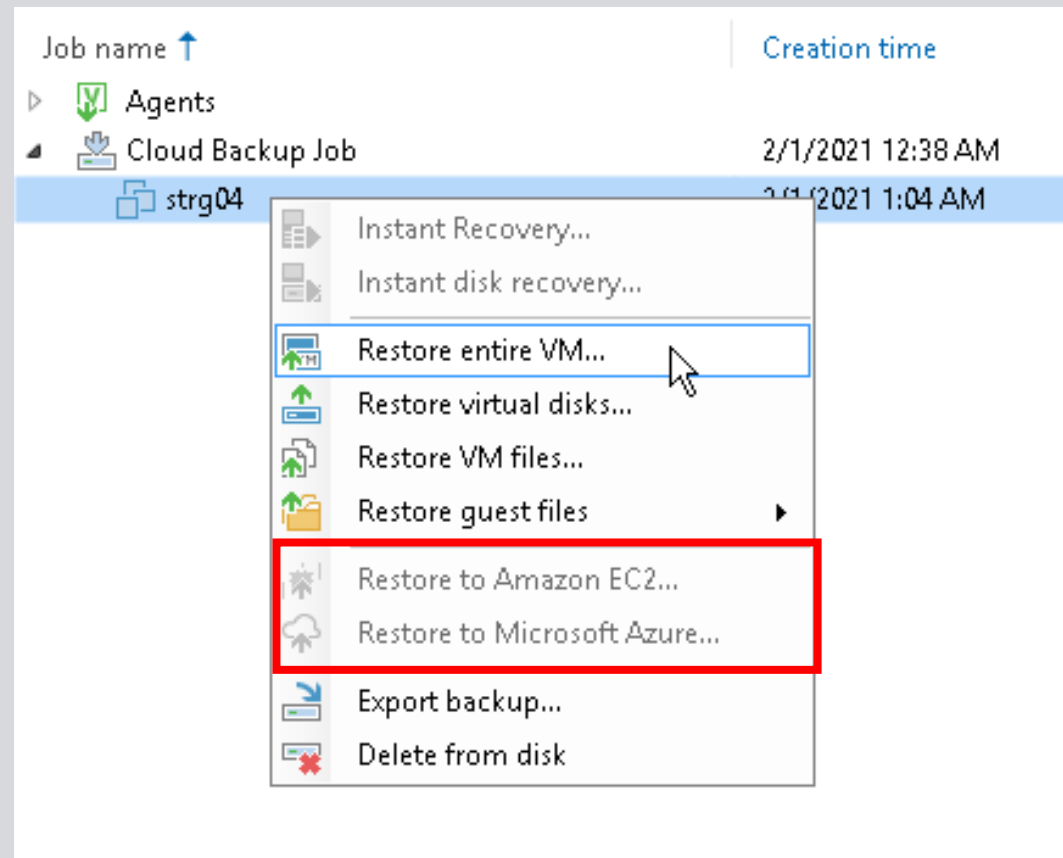
Data Backups

Many data backup services have the keys to decrypt and restore backup images or files.



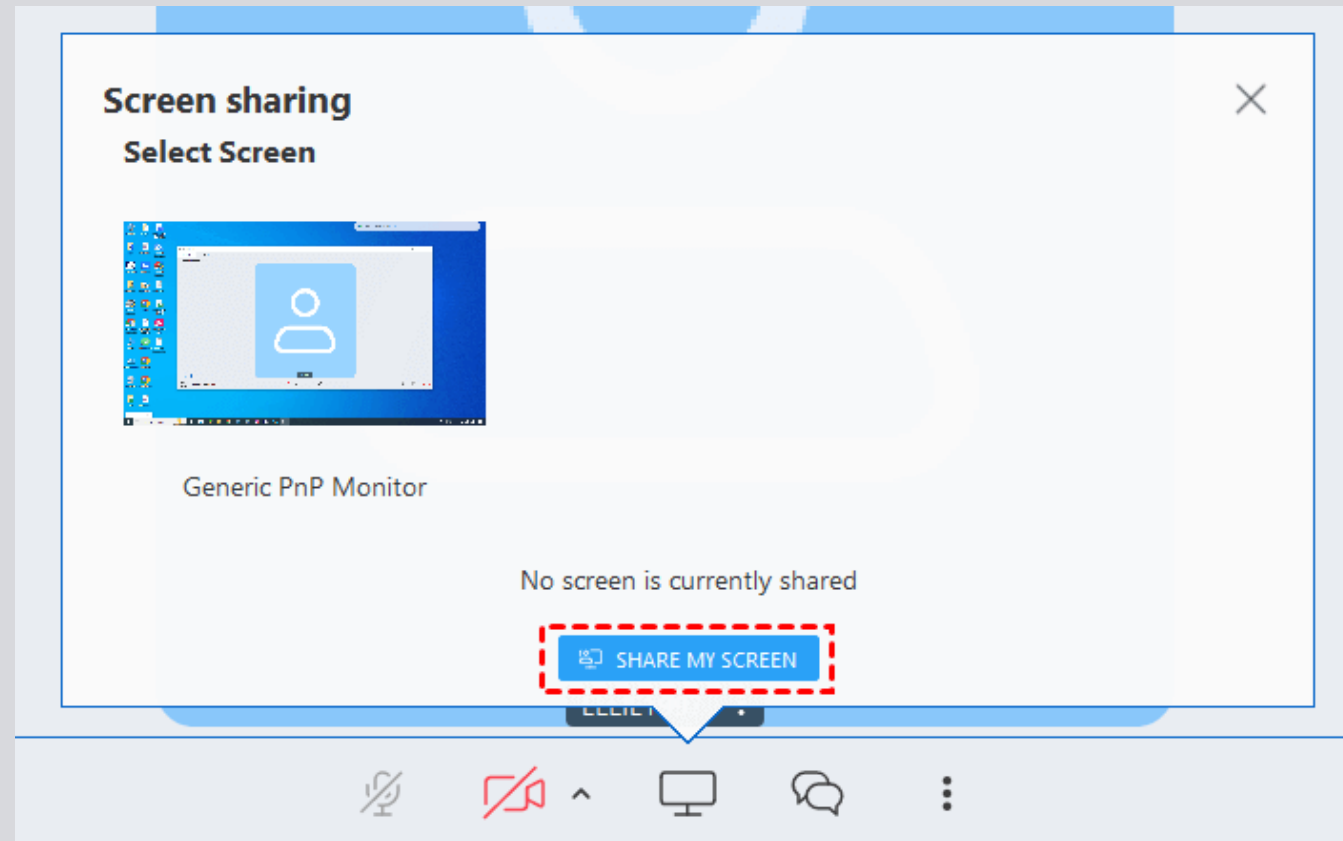
Data Backups

Some comprehensive business continuity and disaster recovery platforms can run recovered images as virtual machines.



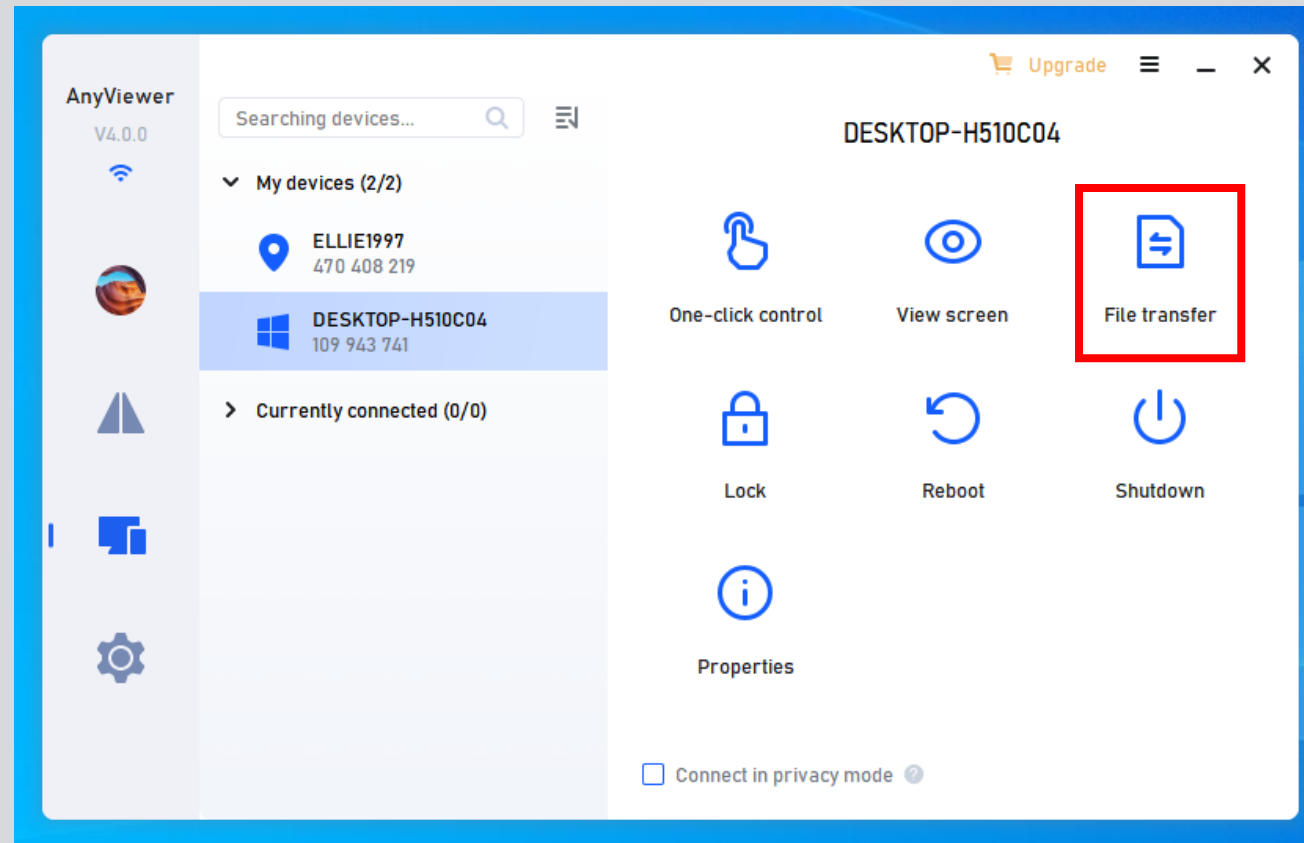
RMM

Screen-sharing tools provide access to user sessions, which could include visual observation of files open on the user's desktop.







RMM

Many RMM tools allow personnel to transfer files to helpdesk technicians.



RMM

Many RMM tools allow technicians to launch a remote shell and transfer files.

Servers	Workstations	Mixed	Mobile Devices	Network Devices	Services	Networks
Device ▾ Remote Control ▾						
Type	SSH	Site	Network Name	Name		
	 Hyper9	HQ	Hyper9 HQ Net	device_1		
	 8Visor	Office	8Visor Office Net	device_2		



ITAR Risks

22 CFR § 120.56 Release.

- a) Release.** Technical data is released through:
- 3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or
 - 4) The use of access information to cause technical data outside of the United States to be in unencrypted form.
- b) Provision of access information.** Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.



ITAR Risks

22 CFR § 120.56 Release.

- a) Release.** Technical data is released through:
- 3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or
 - 4) The use of access information to cause technical data outside of the United States to be in unencrypted form.
- b) Provision of access information.** Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data.



All Security Tools

- Disable vendor access to CUI/ITAR data and files or confirm CUI/ITAR data access is impossible.
- Set client expectations for adjusted or limited support.
- Explore US-based and American-staffed alternatives.



EDR

- Disable automatic file uploads into EDR consoles.
- Don't use a remote shell without clear rules of engagement.
- Save digital forensics to the local computer or an approved location.



Data Backups

- Fully encrypt backups using FIPS-validated modules before offsite replication.
- Don't provide decryption keys to unapproved BC/DR platforms.



RMM

- Establish screen sharing, file transfer, and remote shell usage rules.
- Respond to CISA security advisories regarding the use of Remote Access Software (RAS) and RMM as part of attacker Tactics, Techniques, and Procedures (TTPs).



The CMMC Proposed Final Rule requires CMMC L2/L3 certification for contractors and MSPs.

Individual CMMC Certifications are expensive.

OSAs and MSPs should pursue certification together.



Embrace "Co-Certification"

MSPs can't provide an ill-defined service; they must provide:

- Policy (rules)
- Processes (participation)
- Proof (critical)



Embrace "Co-Certification"

Contractors can't be customers; they must become:

- Content Creators
- Collaborators
- "Checkers"



Embrace "Co-Certification"

For each Assessment Objective:

- Identify Primary Responsible Party
- Jointly Approve Governing Document(s)
- Collect Proof in Both Self-Assessment Packages



Embrace "Co-Certification"

Joint C3PAO Assessment

- Agree on Cost-Share
- Identify Joint Requirements (Cooperative) and Independent Requirements (Org-Specific)
- Create a Readiness Schedule



**I'm sure you have questions,
let them begin.**

Ryan.Bonner@defcert.com

Daniel.Akridge@summit7.us

