


CMMC and CAD Files: Are You Leaving the Backdoor Open?

ankura 

SECUDE



Agenda

- CMMC level set
- Things just got real
- How CAD leaves the back door open
- How Secude closes the back door
- Q&A



Our Presenters



Simon Peel
Managing Partner



linkedin.com/in/simonlpeel
speel@gsvlimited.com



Alex Trafton
Managing Director



linkedin.com/in/alextrafton/
alex.trafton@ankura.com



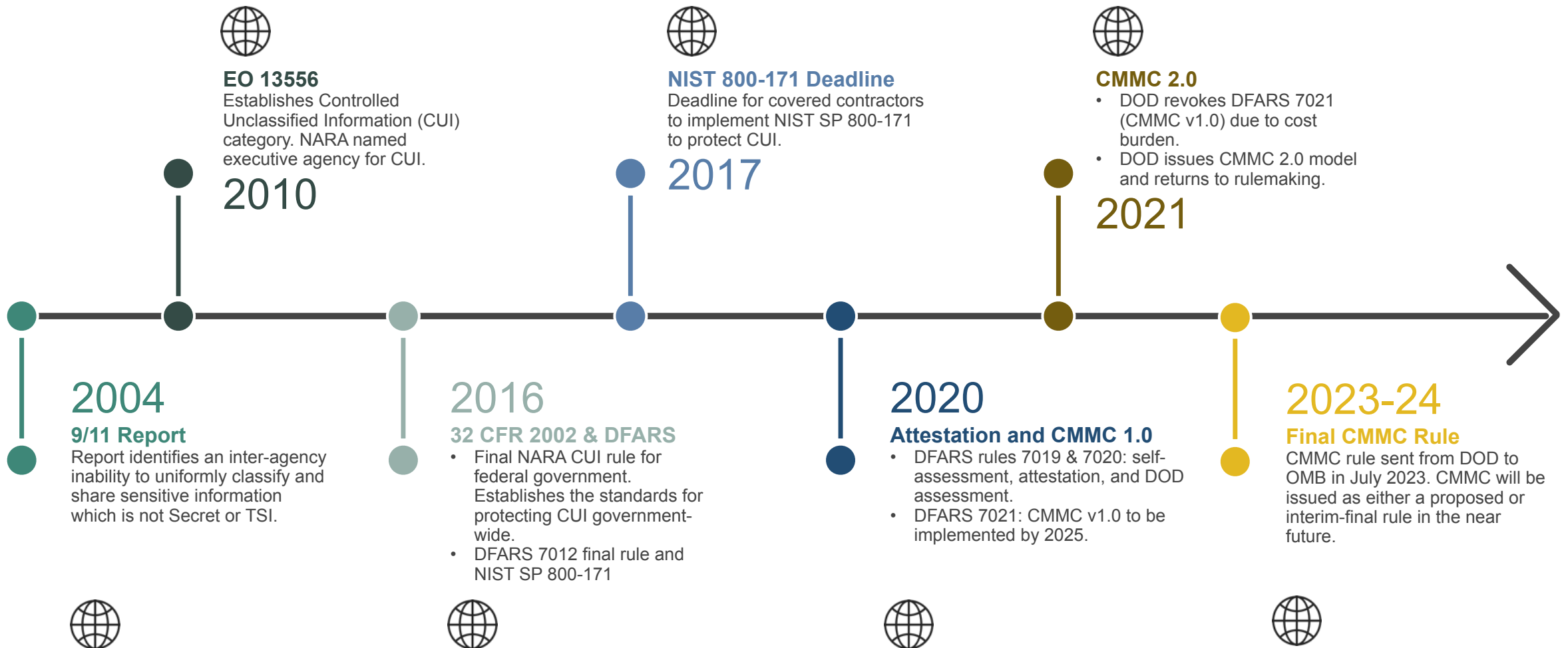
Jay Giunta, Sr. Software
Support Engineer



linkedin.com/in/jay-a-giunta/
jay.giunta@secude.com

CMMC Level-Set

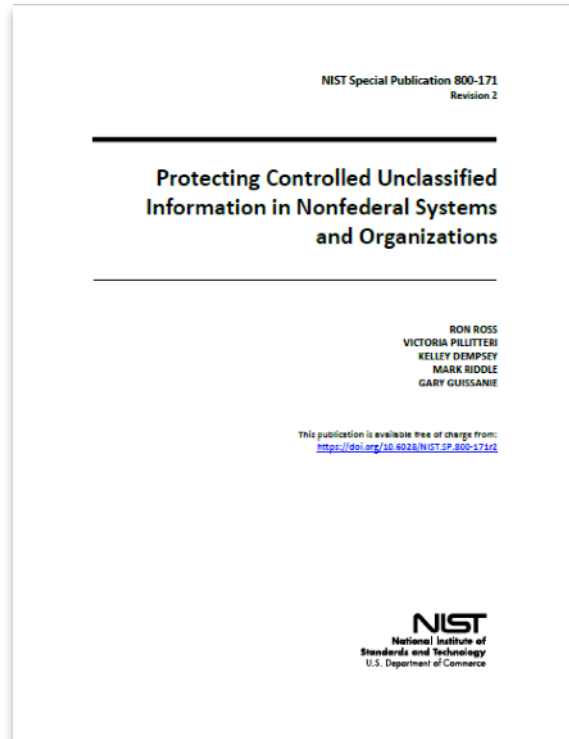
History of CUI Program – DFARS and CMMC



Govt. Solicitations Provisions & Contract Clauses Relating to Cybersecurity & CUI

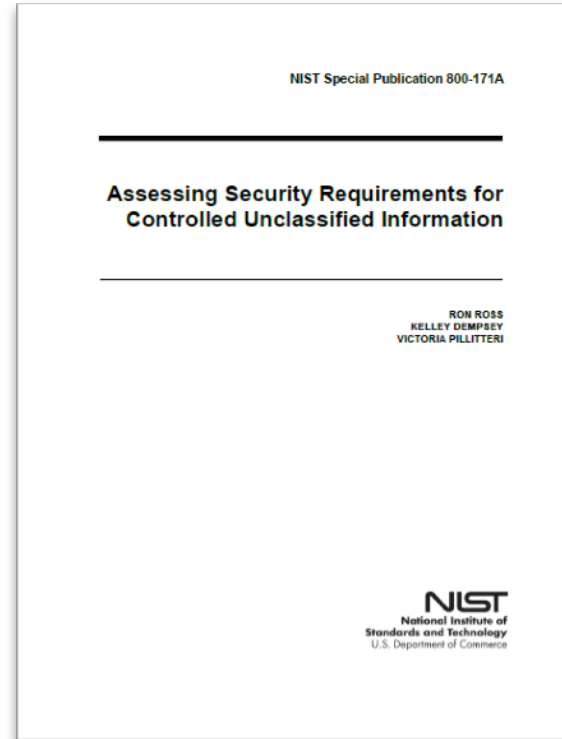
Clause/Provision	Data Type	Requirement	Standard
FAR 52.204-21	FCI	Basic safeguarding of covered contractor information systems	• CMMC Level 1 – 15 security controls
DFARS 252.204-7008	CUI	(Provision) Compliance with safeguarding covered defense information controls -	• NIST SP 800-171
DFARS 252.204-7012	CDI – CTI (CUI)	<ul style="list-style-type: none"> • [b] Implement NIST SP 800-171 + verify FedRAMP moderate controls on cloud providers • [c – g] Cyber incident reporting, preservation of evidence, DOD forensic access. 	<ul style="list-style-type: none"> • NIST SP 800-171 • DIBNet requirements • Provision requirements [c-g]
DFARS 252.204-7019	CUI	<ul style="list-style-type: none"> • Contractor self assessment of NIST SP 800-171 using the DOD Assessment Methodology • Submission of summary score in the SPRS system 	<ul style="list-style-type: none"> • NIST SP 800-171 • NIST SP 800-171A • DODAM
DFARS 252.204-7020	CUI	<ul style="list-style-type: none"> • DoD Medium Assessment of SSP • DoD High Assessment of SSP and all supporting evidence and artifacts 	<ul style="list-style-type: none"> • NIST SP 800-171 • NIST SP 800-171A • DODAM
DFARS 252.204-7021	FCI/CUI	CMMC v1.0 (withdrawn)	<ul style="list-style-type: none"> • FAR 52.204-21 • NIST SP 800-171 • “Delta 20” controls
DFARS 252.239.7010	DOD Data / CUI	Application of NIST RMF to cloud systems operated on behalf of the DOD – SRG requirements (DOD Impact Levels)	<ul style="list-style-type: none"> • NIST SP 800-53 • Cloud Computing Security Requirements Guide (SRG)
DFARS 252.227.7013	Technical Data (CTI)	DOD rights to technical data for non-commercial items.	

NIST SP 800-171 – Not a True Cybersecurity Framework



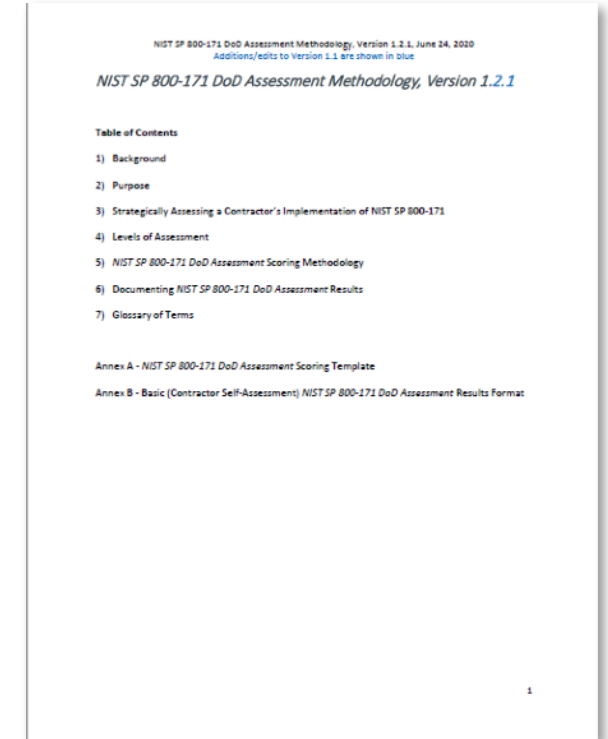
The framework is designed to protect the **confidentiality** of CUI and applies to nonfederal systems that process, store, or transmit CUI or that provide security protection for such components.

110 Security Requirements tailored from NIST SP 800-53 Moderate Baseline.



The companion assessment guide to NIST SP 800-171 which provides assessment procedures for evaluating implementation of the 110 requirements

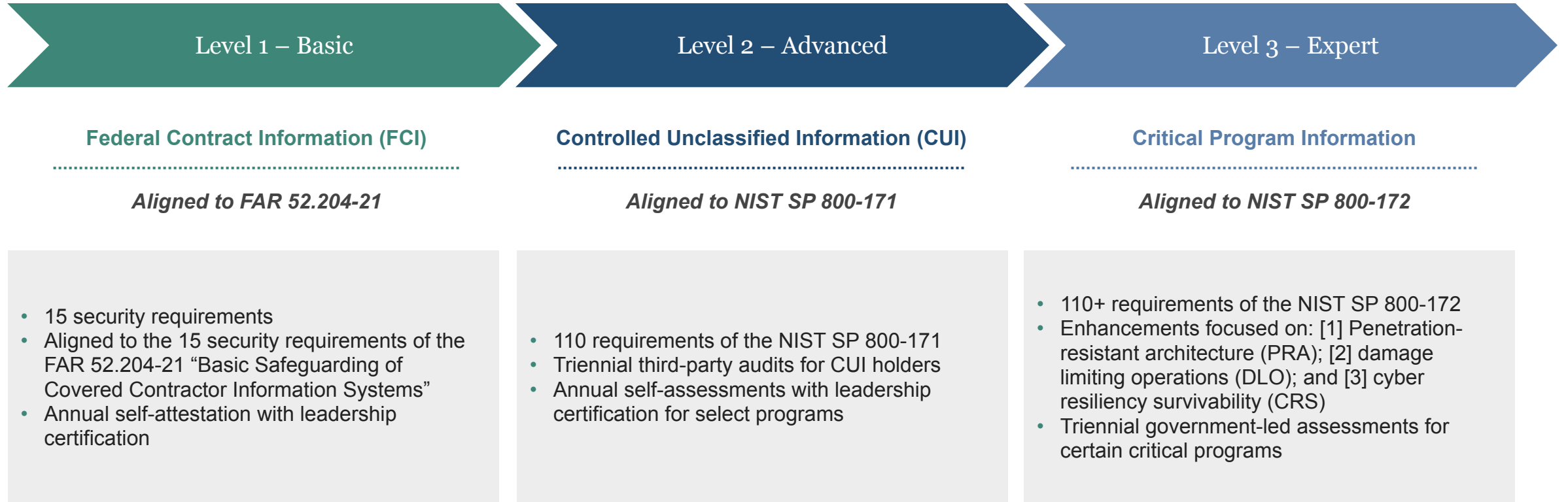
Contains **320 assessment objectives** across the 110 requirements, all of which must be satisfied for a security requirement to be considered satisfied.



Required methodology to calculate a summary score for input into the DOD SPRS systems.

- 44 controls worth 5 points
- 14 controls worth 3 points
- 52 controls worth 1 point

CMMC Program Basics



Things just got real...

DOJ Civil-Cyber Fraud Initiative

“We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards,”

-Deputy Attorney General Lisa Monaco.

The False Claims Act (FCA)

- Knowingly submit a false claims to the government **or** causes another to submit a false claim paid by the government.
- Mandatory damages of \$5,500-\$11,000 per claim **plus three times** the Government’s damages (can be reduced to double if violator provides fulsome information of the violations within 30 days of becoming aware of it).
- Qui Tam or Whistleblower mechanic – private attorneys general (15-25% of amount recovered by the Government through the qui tam action).
 - Anyone can be a whistleblower, but we usually think of employees, who have typically have greater access to relevant information.
- Distinct from Dodd-Frank whistleblowing incentives, which use a similar concept to reward individuals who provide information leading to an enforcement action in which over \$1,000,000 in sanctions are ordered.

The screenshot shows the official DOJ press release page for the Civil Cyber-Fraud Initiative. The page features the DOJ logo and navigation menu at the top. The main content includes the title "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative", the date "Wednesday, October 6, 2011", and a "FOR IMMEDIATE RELEASE" label. The text describes the initiative's goal to combat cyber threats and protect sensitive information. It also includes a list of key details such as building resilience, holding contractors accountable, and supporting government experts. A "Report Cyber-Fraud" section provides information on how to report potential fraud. The page concludes with metadata including the topic (Cyber Crime), component (Civil Division), and press release number (21-974).

FIPS Encryption: Compliant/Approved vs. Validated

The Cryptographic Algorithm Validation Program (**CAVP**) provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components. Cryptographic algorithm validation is a prerequisite of cryptographic module validation.

The Cryptographic Module Validation Program (**CMVP**) is a joint effort between the National Institute of Standards and Technology under the Department of Commerce and the Canadian Centre for Cyber Security, a branch of the Communications Security Establishment. The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

Cryptographic and Security Testing (CST) Laboratories are independent laboratories accredited by NVLAP. CST Labs verify each module meets a set of testable cryptographic and security requirements, with each CST laboratory submission reviewed and validated by CMVP.

An encryption algorithm can be labeled as “FIPS-compliant” but will not be sufficient for CUI protection. FIPS-validated encryption is only required where CUI is being encrypted – it is not required across the network or on devices which transmit encrypted CUI but do not themselves encrypt CUI.

How CAD leaves the back door open

Scope: CUI and CMMC

Assets According to CMMC

- CUI Assets
- Security Protection Assets
- Specialized Assets
- Contractor Risk-Managed Assets
- Out-of-Scope Assets

Contractor

Cloud Service Provider

External Service Provider

Subcontractor

Customer

Other Regulatory Considerations

ITAR

EAR

Are your CAD files CUI?

Are they encrypted to meet NIST SP 800-171 standards?

Are they marked as CUI?

Are your CAD files export-controlled

Are they ITAR or EAR? [Jurisdiction & Classification]

Are the files marked?

Do ESPs have file-level access to unencrypted data?

Are those ESP personnel US Persons?

Are your CAD files resident on public cloud systems?

Are those CAD files encrypted to meet NIST SP 800-171?

Are those cloud systems “sovereign”?

Are those cloud systems FedRAMP Moderate or equivalent?

Do you share CAD files with subcontractors?

Does the sub need technical data?

Are the CAD files securely shared using E2EE?

Do you share CAD files with customers?

Are those CAD files shared using E2SS?

How Secude closes that back door

Secude has been a proud member of MISA since the beginning.

Member of
Microsoft Intelligent
Security Association



Enabling Secude to Extend MPIP to CAD/PLM & SAP

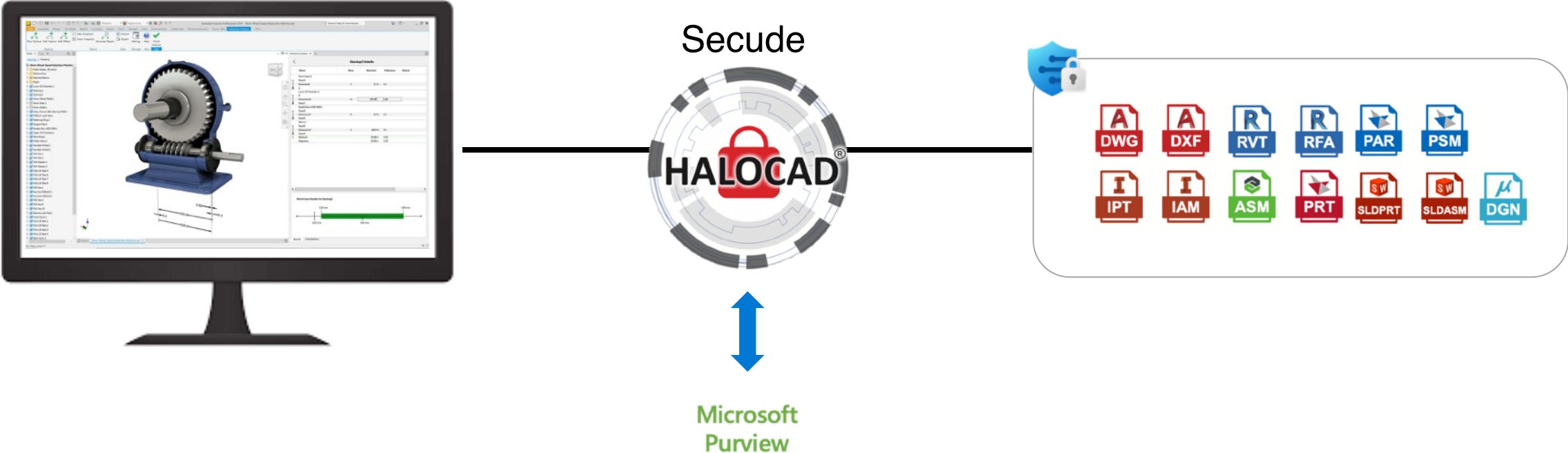
Default MPIP Protection



Secude-Extended MPIP Protection



Secude Plugs Directly into CAD & SAP Applications

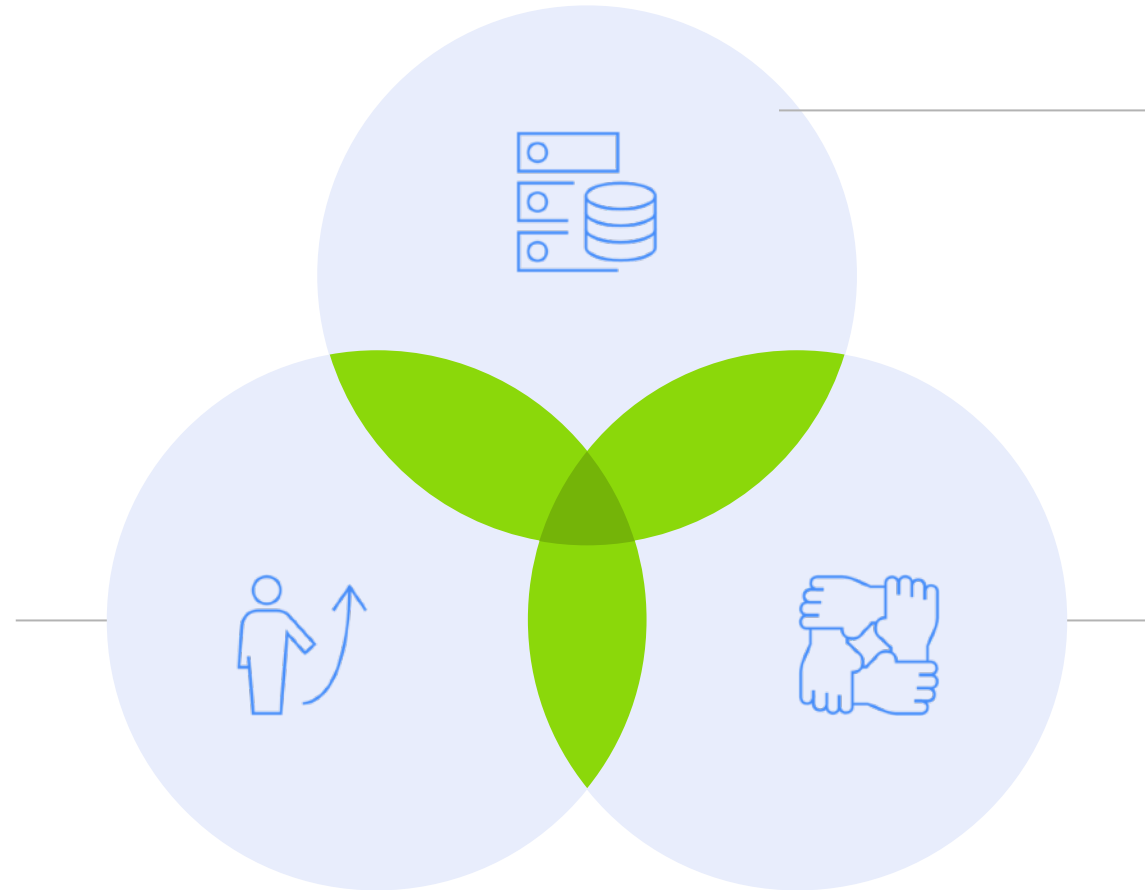


Why customers choose Secude

A

Greater MPIP Value

Extend the discovery, classification, labeling, and monitoring capabilities provided by Microsoft Purview Information Protection.



B

Data-Centric Protection

Monitor and protect sensitive SAP and CAD data beyond the security of the network.

C

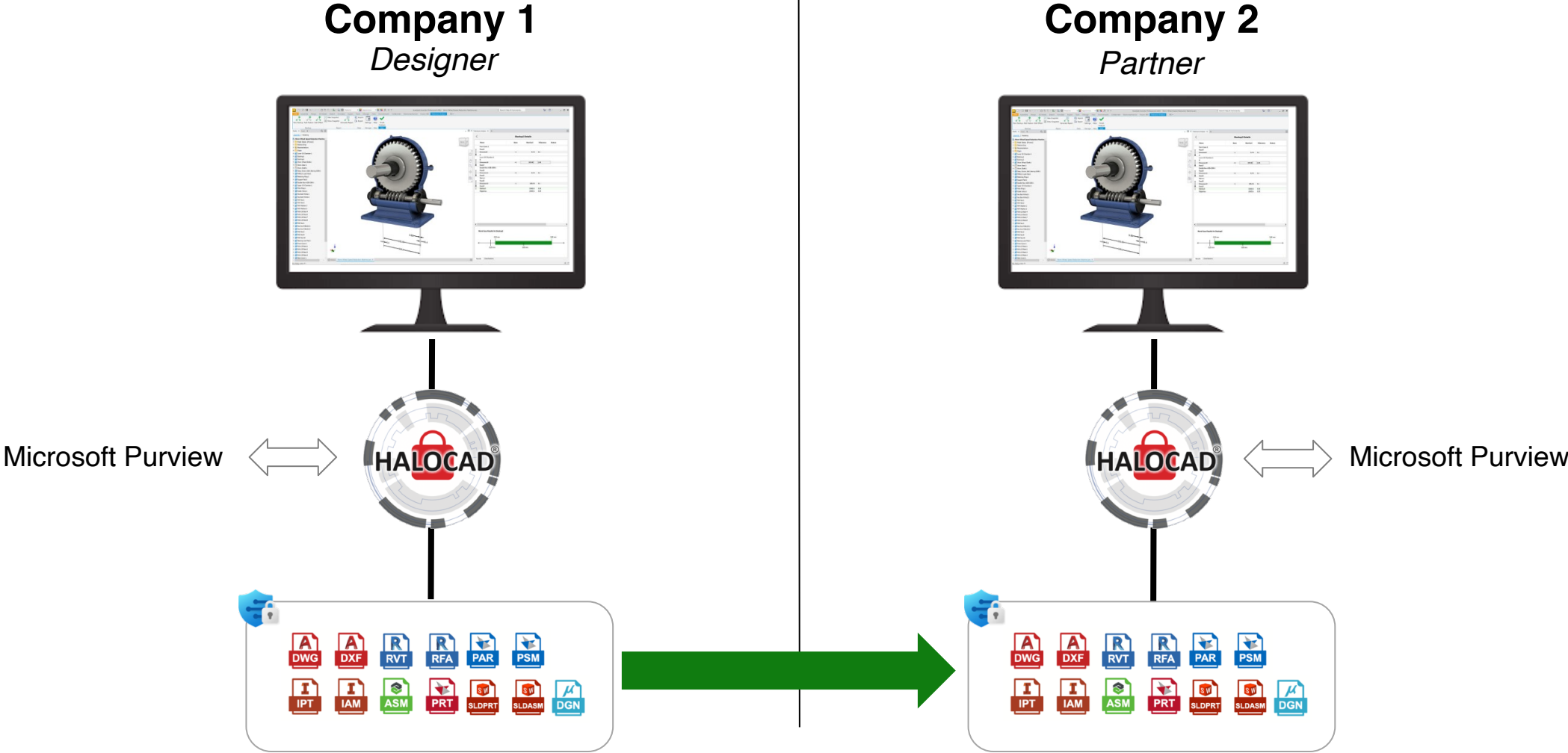
Secure Collaboration

Share data and collaborate with partners, suppliers, and others, knowing your sensitive data is protected.

Demonstration



Demo: Secure CAD Collaboration



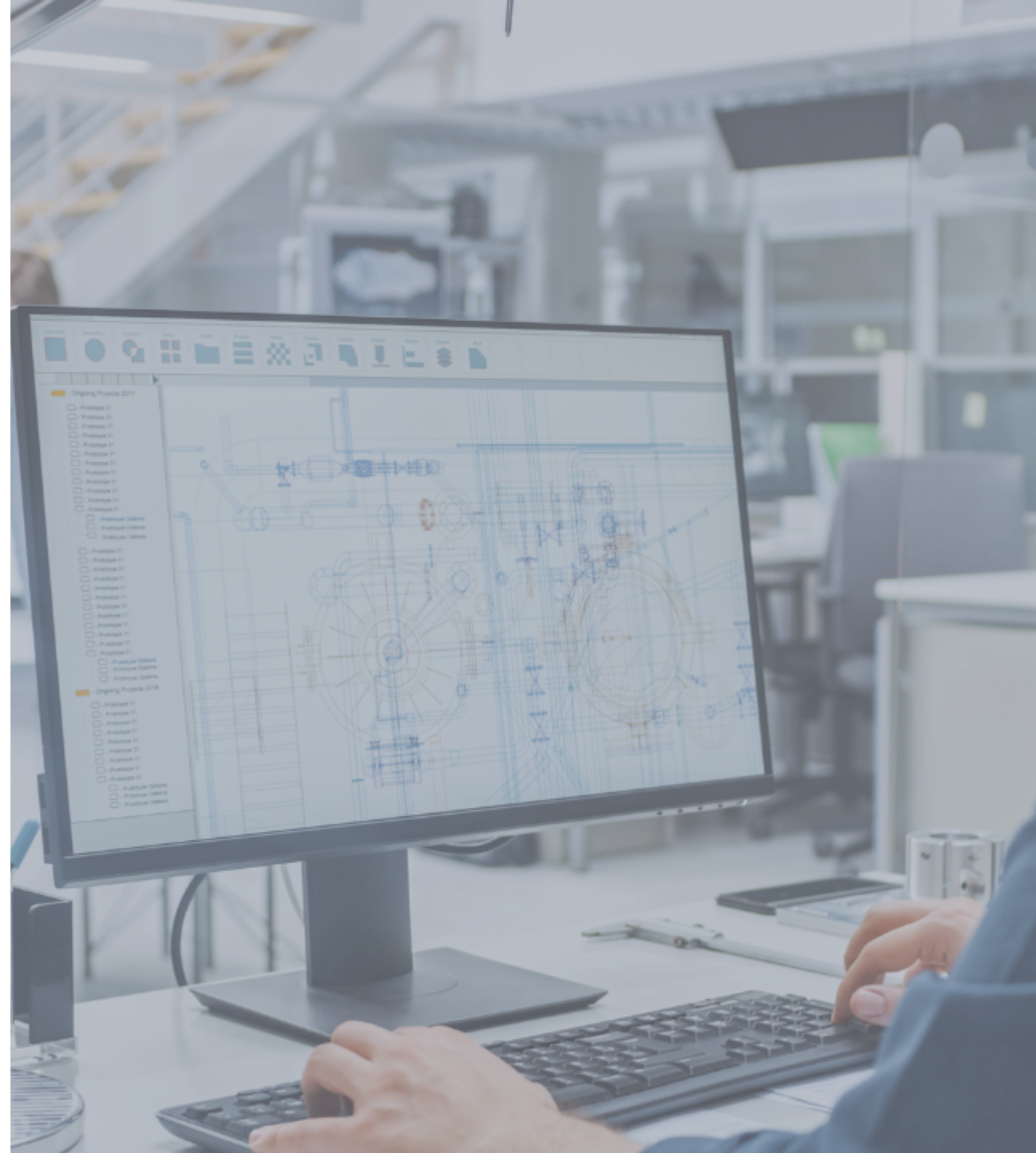
Q&A




Contact Jay Giunta (jay.giunta@secude.com) to learn more about Secude



Download our ebook to learn more about HaloCAD:
<https://bit.ly/halocad-ebook>



CMMC and CAD Files: Are You Leaving the Backdoor Open?

ankura 

SECUDE

