Secude

Case Study

How a US DoD Aerospace Contractor Uses Secude HaloCAD for CMMC Compliance

Background

With over 2,000 employees based worldwide, the Contractor provides design and engineering solutions for aviation, space and defense customers. In particular, the Aerospace Contractor delivers extensive manufacturing and design support for the US Department of Defense (DoD).

In November 2021, the DoD announced a new iteration of its Cybersecurity Maturity Model Certification (CMMC) model, outlining the DoD's cybersecurity requirements and updated standards for contractors handling Controlled Unclassified Information (CUI) - CMMC 2.0.

With CMMC 2.0 set to become a contract requirement for all members of the Defense Industrial Base (DIB) in Q1 2025, the Aerospace Contractor needed to implement security tools to speed up CMMC compliance and continue operating on DoD contracts.

The Challenge

The Aerospace Contractor was using Microsoft Azure Government GCC High, which provides more stringent security restrictions and default settings than its commercial Azure services. However, this protection did not extend to Computer-Aided Design (CAD) files, which the Aerospace Contractor used for DoD projects and were considered CUI.

At a Glance

Vertical
Government

Company
DoD Contractor

Employees
2000+

Location
Multiple locations worldwide

Highlights

The client needed to comply with CMMC 2.0's requirements around CUI.

HaloCAD protected, tracked and controlled access to the client's CAD files that were CUI without slowing down operations.

The client was able to simplify and speed up its CMMC 2.0 compliance process.

About Secude

Secude, a Microsoft and SAP Partner, is a global leader for Zero Trust data protection and data governance.

Secude has been protecting the data of Fortune 500 companies for over 25 years. Our Microsoft Purview Information Protection (MPIP) extension embeds Zero Trust protection and data governance into our customers sensitive files from creation, preventing data leakage, reputational damage and non-compliance. With branches in Europe, North America and Asia, Secude supports customers with the implementation of IT security strategies through a global network.

HaloCAD

Member of Microsoft Intelligent Security Association

Microsoft Security

CMMC 2.0 states that if you handle CUI, such as engineering drawings or design blueprints, you need to satisfy 110 security requirements and 320 assessment objectives aligned with NIST SP 800-171. This not only includes the protection of CUI at rest, but also requires contractors to prove access control of CUI (both internally and externally) and retain logs of where CUI travels.

The Aerospace Contractor didn't have sufficient CAD protection nor know where all its CAD files that were CUI lived. To simplify and speed up its CMMC compliance, the Aerospace Contractor decided to use Secude's HaloCAD to easily protect and track CAD files that were CUI.

The Solution

Secude customized the installation of HaloCAD to work with GCC High. Following a successful proof of concept and pilot program with its design engineers, the Aerospace Contractor then rolled out the use of HaloCAD across its engineering team.

HaloCAD enabled the Aerospace Contractor to:

- **Embed Zero Trust protection by default.** HaloCAD applied authorization tags to the client's CAD files at the application layer, ensuring CAD files that were CUI were encrypted from creation and only accessible by authorized users both inside and outside the company.
- **Track CAD files.** HaloCAD extended Microsoft Purview Information Protection (MPIP) access tracking to the Aerospace Contractor's CAD applications, enabling the company to track who had access to CAD files, where CAD files traveled and log failed access attempts (i.e. by unauthorized personnel) with Purview Audit.
- **Label CAD files by sensitivity.** HaloCAD enforced file security depending on the chosen MPIP sensitivity label, including read-only privileges, password-controlled access and admin-only use, which enabled the Aerospace Contractor to control who accessed CAD files that were considered CUI beyond its IT perimeter.

The Results

With HaloCAD, the Aerospace Contractor was able to protect its CAD files that were CUI, track where its CUI lived and retain operational efficiency.

In particular, HaloCAD enabled the Aerospace Contractor to:

- **Secure all CAD files that were CUI.** Applying MPIP labels to CAD files ensured the client's CUI was protected to the highest standards and controlled in line with CMMC 2.0 requirements. For example, with HaloCAD's lifelong sensitivity labels, the Aerospace Contractor could prove that former employers, non-US entities and non-US citizens based in their North American divisions teams didn't have access to the CUI-CAD files (required by CMMC 2.0).
- **Prove location and access control of CUI.** Combined with MPIP, HaloCAD provided a log of where the Aerospace Contractor's CUI-CAD traveled and who had access to the files.
- **Balance security with productivity.** With HaloCAD, the Aerospace Contractor was able to restrict file access where required, but also enable its engineers to use the same set of tools and familiar processes as before to ensure a seamless secure workflow that was both operationally efficient and CMMC compliant.

As a result, the Aerospace Contractor was able to simplify and speed up its CMMC compliance and ensure it's in a great position to be compliant before the Q1 2025 deadline.

Summary

Secude's HaloCAD for CAD security enabled the Aerospace Contractor to:

- Secure CAD files that are CUI in accordance with CMMC 2.0 requirements.
- Track and control access to CAD files that are CUI both inside and outside its IT perimeter.
- Simplify and speed up its CMMC compliance.

For more information about Secude: www.secude.com

Phone: USA/Canada: +1 800-900-9633 | India: +91 44 4777 9704 | Switzerland: + 41 41 510 70 70
Email: USA/Canada: AmericasSales@secude.com | EMEA: EMEASales@secude.com