Forcepoint

Customer Story

Global Aviation Leader Achieves CMMC Compliance with Forcepoint DSPM

A leading aerospace manufacturer faced stringent cybersecurity requirements due to its work with the U.S. Department of War (DOW). The Cybersecurity Maturity Model Certification (CMMC) framework mandates that defense contractors implement robust controls to safeguard sensitive data.

Because of this, data leaders need a strategic approach to CMMC compliance that protects critical intellectual property and streamlines oversight for audit readiness.

Data Security Challenges in Meeting CMMC Requirements

The manufacturer must secure a wide array of information ranging from flight telemetry and proprietary engineering designs to supplier data, manufacturing instructions and maintenance logs against sophisticated threats and insider risks.

Government security standards like NIST SP 800-171 and CMMC Level 2/3 require comprehensive data protection measures, which cannot be met with siloed or piecemeal solutions.

Its challenges included:

- **Evolving Regulatory Demands:** CMMC mandates stringent controls for DOW contractors. Staying compliant with standards like NIST SP 800- 171 and CMMC Level 2/3 requires continuous adaptation.
- **Diverse Critical Data Types:** The company handles a wide array of sensitive information, from flight telemetry and engineering designs to supplier data and maintenance logs, all requiring robust protection.
- **Sophisticated Threat Environment:** Nation-state attackers frequently target the defense supply chain, exploiting vulnerabilities and misconfigurations, posing a constant threat to critical data.

Customer Profile:

- A leading U.S. based private jet manufacturer supporting defense programs aimed to protect sensitive engineering, operational, and supplier data.

Industry:

- Aviation

HQ Country:

- United States

Product(s):

- **Forcepoint DSPM**
- **Forcepoint DDR**

Evolving Compliance Demands for CMMC

CMMC 2.0 (Level 2 "Advanced" and Level 3 "Expert") mandates rigorous NIST standards, requiring regulated organizations to implement 110+ security controls for the effective protection of Controlled Unclassified Information (CUI). This includes strict access controls, continuous monitoring, and robust audit trails for sensitive defense-related data.

This company handles highly sensitive data that would be devastating in the wrong hands or if improperly exposed. Examples of key categories of data include:

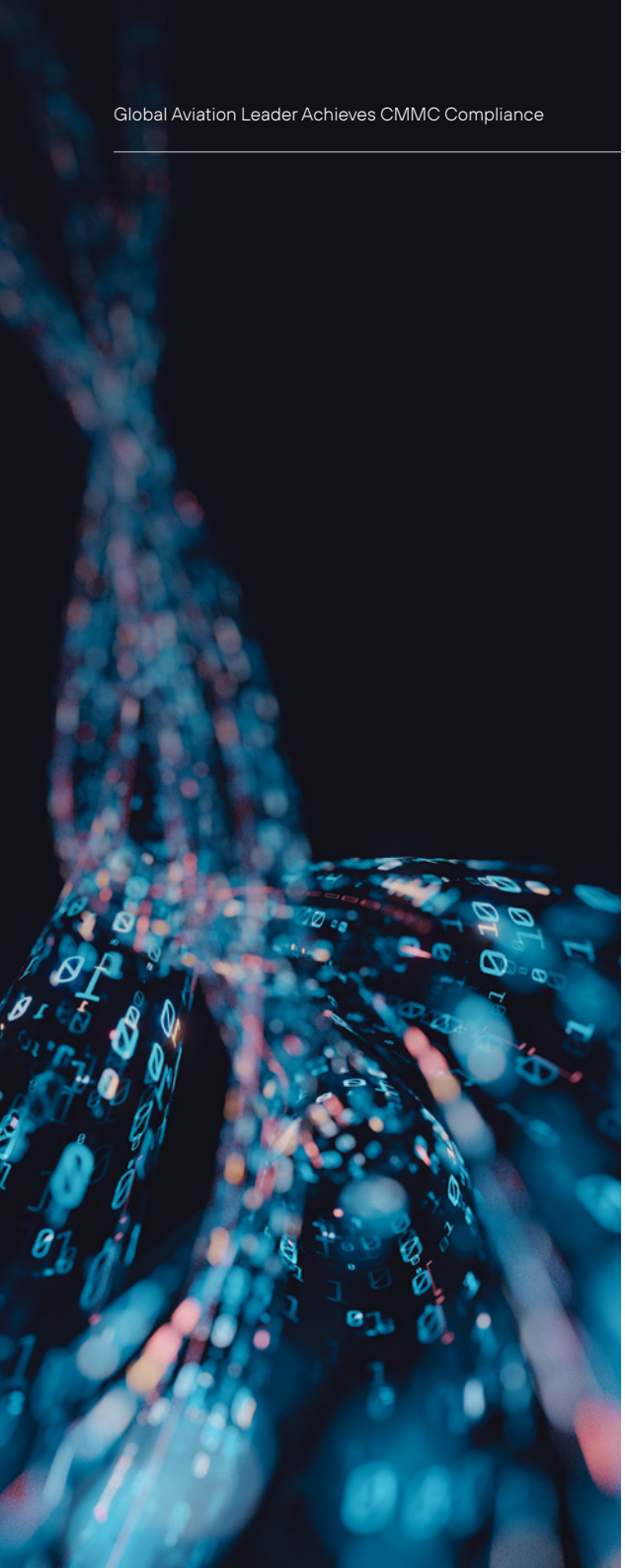
- **Flight Telemetry Data:** Real-time and recorded data from test flights and operations, which can reveal aircraft performance characteristics and mission details.
- **Proprietary Engineering Designs:** Detailed blueprints, CAD models, and specifications of the company's jets constitute core intellectual property.
- **Supplier and Subcontractor Information:** Data shared with or received from suppliers (e.g. component designs, integration documents, procurement details) often extends outside the companies direct network.
- **Manufacturing Instructions and Process Data:** Step-by-step instructions, CNC machine code and assembly procedures used in production are trade secrets. Exposure could enable counterfeit part production or sabotage.
- **Maintenance Logs and Performance Data:** Detailed maintenance records and telemetry from aircraft in service (including any military operated jets) can indicate operational readiness or vulnerabilities.

Protecting these diverse data types poses significant challenges. Sensitive files reside across on-premises servers, cloud storage, engineering PLM systems, employee devices and collaboration platforms. Shadow IT and over-permissive access can lead to blind spots where CUI is stored without proper controls.

The company's security team needs to know exactly where sensitive data lives, who can access it and how it's being used at all times – a daunting task if done manually.

Beyond compliance, the organization faced an active threat environment. Sophisticated adversaries specifically target defense contractors for espionage. Attackers may exploit supply chain vulnerabilities, compromising weaker partners to gain a foothold. Additionally, insider threats are a significant concern, as knowledgeable employees or contractors can deliberately exfiltrate or unintentionally leak proprietary data.

The CIO and CISO confronted a dual challenge: protect a vast, distributed data estate against advanced threats and human error, while proving compliance with CMMC and other regulations. This required moving beyond point solutions to a unified and adaptive data security strategy.



CMMC Compliance with AI-Native Data Security Posture Management (DSPM) and Data Detection and Response (DDR)

To address these challenges, the company partnered with Forcepoint for DSPM and DDR.

Backed by Forcepoint's AI Mesh technology, this unified approach offers comprehensive visibility into CUI data, remediation capabilities and real-time threat detection, all aligned with CMMC requirements. Forcepoint's comprehensive Data Security Everywhere approach is an ideal solution for strict government frameworks, enabling defense contractors to "know their data, secure it everywhere, and rapidly respond to risk, all from a single integrated solution".

Forcepoint DSPM provides the foundation of data protection strategy. DSPM continuously discovers and classifies sensitive data across all of the organization's repositories, from on-premises file servers and databases to cloud storage and SaaS applications.

The security team gains a current map of sensitive data; where it resides, who uses it and what protections are in place. This level of visibility is crucial for identifying pockets of CUI (e.g. design documents or telemetry datasets saved in unapproved locations) that were previously unknown.

Forcepoint DSPM uses proprietary AI Mesh technology to achieve highly accurate classification at scale. The AI Mesh is a network of advanced AI models (including small language models (SLMs) and deep neural networks) that can intelligently determine a file's sensitivity and criticality based on context. This allows Forcepoint DSPM to recognize unique data patterns, from CAD drawings of aircraft parts to specialized maintenance codes, with lightning-fast speed and bull's-eye accuracy.

Critically, DSPM doesn't just locate data; it also evaluates its security posture. The platform highlights where sensitive data is stored that might put it at risk. For example, DSPM can flag if a folder containing jet design specs is open to all engineers when it should be restricted, or if flight telemetry files are found in a cloud drive that isn't approved for CUI.

Continuous Monitoring and Threat Response (DDR)

Forcepoint DDR adds a dynamic defense layer, monitoring activity and detecting threats in real time before risks can escalate. Forcepoint DDR provides continuous monitoring of data activity across file storage and cloud services, instantly alerting on suspicious behavior or policy violations.

For the jet manufacturer, this means every access, download, share or modification of sensitive files is being evaluated against normal patterns and security policies. For example, if an engineer typically accesses a few design documents per day but suddenly bulk downloads an entire repository of aircraft schematics at 2 AM, DDR will flag this unusual behavior immediately.

Another powerful feature of DDR is data lineage tracking. Forcepoint DDR maintains a forensic trail of where files travel and how they change over time.

In practice, this means if a maintenance log or design document is copied from a secure server to a USB drive or uploaded to a cloud app, DDR records that sequence. This lineage visibility is invaluable for investigations and compliance reporting.

Strategic Benefits for Leadership

Implementing Forcepoint DSPM and DDR yielded significant benefits, strengthening its business case for adoption. Key advantages include:

- → **Audit Readiness and Compliance Confidence:** By mapping data to compliance controls and generating audit-friendly reports, Forcepoint simplified their path to passing CMMC audits and other inspections. Security and Risk Officers can demonstrate adherence to CMMC Level 2/3 requirements with up-to-date evidence at any time.
- → **Protection of Intellectual Property and Trade Secrets**: With DSPM and DDR in place, the most valuable data is shielded by multiple layers of defense. Safeguarding IP means the organization maintains its competitive edge and prevents potential loss of future defense contracts that could occur if critical technology leaked to adversaries.
- → **Operational Efficiency and Cost Reduction:** Automation of data discovery, classification and incident response tasks reduces the manual workload on their security and IT teams. Fewer incidents and faster detection also means lower costs related to breaches. Additionally, consolidating capabilities (DSPM, DDR, and potentially other solutions such as DLP or CASB) into a single integrated platform can eliminate the need for multiple point products, simplifying the security architecture and potentially reducing licensing and maintenance expenses.