# Ensuring Secure Innovation and Compliance in U.S. Manufacturing

## With Forcepoint's Unified Data Security Platform

Forcepoint

Brochure

In U.S. manufacturing sectors, including defense contracting, automotive, and semiconductor production, protecting sensitive data is not just good practice, it's a contractual and legal mandate. Intellectual Property (IP) such as CAD design files, chip schematics and technical data often falls under strict regulations including ITAR, EAR, and DFARS, as well as frameworks like CMMC (built on NIST 800-171)

Compliance officers and CISOs face mounting pressure to safeguard this data against nation-state espionage and insider threats while proving compliance with these Governance, Risk and Compliance (GRC) mandates. In fact, the U.S. Department of Defense reported over 12,000 cyber incidents since 2015, with a sharp rise in attacks on the defense industrial base in recent years. Meeting regulatory requirements and preventing breaches requires comprehensive visibility and control over sensitive information.

## Challenges and Compliance Mandates in Manufacturing

**Forcepoint Data Security Cloud** offers a unified approach to address these challenges. By combining **Data Security Posture Management (DSPM)**, **Data Detection and Response (DDR)**, **Data Loss Prevention (DLP)** and **Cloud Access Security Broker (CASB)** the platform allows manufacturing organizations to **discover, monitor and protect** sensitive data through its entire lifecycle. This all-in-one solution helps companies comply with export control laws, cybersecurity standards, and enforce IP protection policies while enabling secure innovation on a global scale.

**Manufacturing and defense companies operate under a web of industry-specific and national regulations designed to protect sensitive data and national security. Key mandates include:**

## ITAR and EAR (Exports Controls)

Regulate the handling and export of military and dual-use technical data. For example, ITAR covers defense-related technical information (encryption, space, military and nuclear technology, source code, etc.) Under ITAR regulations, designs for weapons systems or aerospace components must not be shared with unauthorized individuals or foreign nations.

Organizations must prevent unapproved export or disclosure of such data, with severe penalties for violations.

## CMMC and NIST 800-171

The Cybersecurity Maturity Model Certification (required for DoD contractors) builds on NIST 800-171 controls to protect Controlled Unclassified Information (CUI).

Companies must implement strict access controls, continuous monitoring and incident reporting to safeguard sensitive defense data. Evolving CMMC requirements and supply chain security challenges make achieving and maintaining compliance complex.

## Intellectual Property (IP) Protection and Insider Risk

Beyond formal regulations, manufacturers uphold internal IP protection policies to guard trade secrets (designs, formulas and software source code). Insider threat and industrial espionage controls are critical, as insiders or advanced persistent threats may target proprietary designs or production data.

High-profile breaches in the sector underscore the need for monitoring user activity and preventing data exfiltration.

## ISO 27001

The global standard for information security management. Manufacturing firms pursue ISO 27001 to systematically manage risk and data protection, and require audit trails, data classification and other risk mitigation techniques.


## DFARS 252.204-7012

A DoD federal acquisition regulation that mandates adherence to NIST 800-171 and reporting of cyber incidents. Non-compliance can mean lost contracts.

A recent NSA warning noted increasing cyber espionage attempts against defense contractors, putting manufacturers' sensitive design data at risk. This highlights why an end-to-end data protection strategy is essential.

## Key GRC Challenges

These mandates demand robust data governance, knowing what sensitive data you have, where it resides, who accesses it, and how it's used. CISOs often struggle with fragmented tools (separate DLP, cloud security, etc.) that result in siloed visibility and inconsistent policies. Without integration, tracking data flow for a CAD drawing through network shares, emails, and cloud apps can be painstaking. Audits for ISO 27001 or customer-required attestations turn into fire drills to compile evidence from multiple systems.

The lack of a unified view also creates gaps that sophisticated insiders or attackers can exploit. To confidently meet ITAR/EAR export controls or pass a CMMC audit, organizations need an integrated platform that covers discovery, monitoring, and enforcement of data security policies enterprise-wide.

## Addressing Data Security Challenges with Forcepoint Data Security Cloud

Forcepoint addresses these challenges with a unified data-first security platform that consolidates critical capabilities under one roof. Instead of managing separate point solutions, security teams get a single integrated system that streamlines compliance and protection.

Forcepoint's integrated data security workflow uses DSPM to discover, classify, and remediate data risk, DDR to monitor data usage and triggers alerts to potential data breaches, and DLP and CASB to enforce policies on endpoints, network, web and cloud apps. All this functionality is governed through unified management.

**At the core of this platform are four key components working in concert:**

### DSPM

**Discovery and classification** of data across cloud and on-premises repositories with AI-driven accuracy. DSPM gives a centralized view of where sensitive data resides across the enterprise. Using Forcepoint's AI analytics, DSPM can automatically find CAD files, technical drawings, engineering documents and other IP, and classify them (e.g. as ITAR-controlled, CUI, or trade secret). This proactive discovery builds a strong foundation for governance. It then can remediate data risks that have been discovered, securing the data posture from potential data breaches and non-compliance with privacy regulations. It also streamlines compliance reporting, as DSPM can generate audit-ready reports showing data inventory and policy status for regulations, speeding up the audit process.

### DDR

**Continuous monitoring and risk detection** for data. Available as an add-on to DSPM, Forcepoint DDR continuously watches data repositories and user actions to spot potential breaches dynamically. It fills the visibility gap left by periodic scans. Instead of discovering an incident weeks or months later, DDR raises alerts as suspicious activity happens. DDR provides extensive visibility across cloud locations and endpoints, helping organizations identify and stop data exfiltration attempts as they occur. Importantly, DDR includes data lineage tracking, which offers forensic-level detail of a file's lifecycle.

### DLP

**Policy enforcement and protection** of data across endpoints, networks, web and cloud applications. Forcepoint is recognized as an industry leader in DLP, and its solution enables organizations to prevent data loss anywhere users interact with data. Through a unified policy engine, Forcepoint DLP can block or quarantine sensitive files when a violation is detected, whether someone attempts to email out a controlled document, upload it to a cloud app, or copy it to removable media. The platform contains a vast library of over 1,700 policies, classifiers and templates to simplify deployment and DLP management that cover global regulations and industry standards across over 160 regions.

### CASB

**Cloud application visibility and control**. Modern manufacturers rely on cloud services (from Office 365 and AWS to niche engineering SaaS apps) and CASB extends data protection to these cloud environments. Forcepoint CASB (part of the Forcepoint Data Security Cloud platform) provides deep visibility into sensitive data residing within the corporate-sanctioned SaaS apps and enforces security policies to protect the data. Crucially, Forcepoint CASB has built-in DLP enforcement and an extensive policy library. The DLP policies and incident alerts can also be managed from a single interface across endpoint, CASB, SWG and email DLP.

## Use Cases: Protecting IP and Ensuring Compliance in Action

### Protecting CAD Designs and Controlling Technical Data

An aerospace contractor stores proprietary CAD drawings of a defense project. These files are subject to ITAR controls, meaning they cannot be shared with foreign nationals or exported without authorization.

Using DSPM, the contractor discovers and labels all CAD files containing ITAR-controlled technical data across on-premises servers and cloud storage. When an engineer attempts to upload a labeled CAD design to a personal cloud storage service (OneDrive, Google Drive, etc.), Forcepoint CASB with DLP detects the sensitive content and blocks the upload, preventing an ITAR violation in real time.

### Preventing Insider Theft of Intellectual Property

A semiconductor manufacturer's IP is a prime target for insider espionage. When a malicious insider tries to slowly exfiltrate proprietary design documents, analytics in DLP and DDR establish a baseline for normal user behavior and detect the anomaly.

Cumulative analysis for "drip DLP" recognizes that a series of small data transfers constitute a larger exfiltration attempt. Through data lineage, security can trace exactly which files were touched, providing forensic evidence to act upon.

### Streamlining Audits and Reporting

With Forcepoint, reporting is centralized. The CISO can generate compliance reports that show all sensitive data locations, the policies applied, and a summary of incidents prevented.

Because the platform has unified management and reporting, these reports cover endpoint, network, email, and cloud activity in one view. This not only simplifies passing an ISO 27001 certification audit but also reduces the compliance burden on staff.

For CISOs and compliance officers in U.S. defense, automotive and semiconductor firms, Forcepoint offers **the most complete data security platform** to meet today's stringent GRC mandates. By unifying data discovery, monitoring and protection, Forcepoint eliminates security gaps that can occur when using siloed tools. The platform's discover, classify, prioritize, remediate and protect workflow maps perfectly to compliance requirements, from identifying regulated data, to keeping watch over its usage (with full audit trails), to enforcing policies that prevent data leaks or unauthorized exports.

In summary, Forcepoint Data Security Cloud provides U.S. manufacturers and defense contractors with unparalleled visibility and control over sensitive data across endpoints, networks, web and cloud. It delivers continuous risk reduction through AI-powered monitoring and adapts enforcement to wherever your data goes. By choosing this unified solution, organizations ensure that every byte of critical data is accounted for and guarded in accordance with regulatory requirements. This means less worry about passing the next audit or a potential insider breach, and more focus on advancing your core mission. Secure innovation at global scale becomes a reality, backed by a platform designed to meet the exacting compliance standards of the manufacturing and defense sectors.

**Get a Free Data Risk Assessment**

Forcepoint

**forcepoint.com/contact**

## About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.


[FP-Brochure-Ensuring Secure Innovation and Compliance in U.S. Manufacturing-EN] 16Apr2025