

Rethinking Secure Information Sharing in Aerospace

A rocket is shown launching vertically from the bottom center of the frame. A large, bright white plume of smoke and fire trails behind it, extending upwards. The background is a deep blue space filled with numerous small white stars. At the very bottom, there is a layer of white, fluffy clouds.

eSHARE

Introduction

In Aerospace and Defense, secure information sharing isn't optional—it's mission-critical. Whether working with government agencies, suppliers, or internal teams, organizations must exchange sensitive data daily ranging from intellectual property to country specific compliance requirements (e.g. Controlled Unclassified Information (CUI) in the United States).

Strict Aerospace and Defense regulatory frameworks demand full compliance, while the risk of data leaks or unauthorized access can jeopardize national security and innovation. At the same time, speed and collaboration remain essential for project delivery, R&D, and operational efficiency.

The Need for Change: Stop Hoping, Start Handling

In Aerospace & Defense, data sensitivity is non-negotiable. But the way this data is shared hasn't kept up. Traditional methods, encrypting a file, sending it, and hoping it's handled correctly, are risky and inefficient. Once data leaves your hands, visibility and control are gone.

A new approach is needed: one that enables collaboration without compromising security while enabling organizations to keep a handle on their data.

The Problem with the Old Way

Encryption + File Transfer = No Visibility. No Control.

The old method of sharing sensitive information in Aerospace and Defense often involves encrypting a file, sending it to the recipient, and hoping it's properly managed. While encryption adds a layer of security, it doesn't solve the core issues of visibility and control, and most importantly, it limits collaboration.

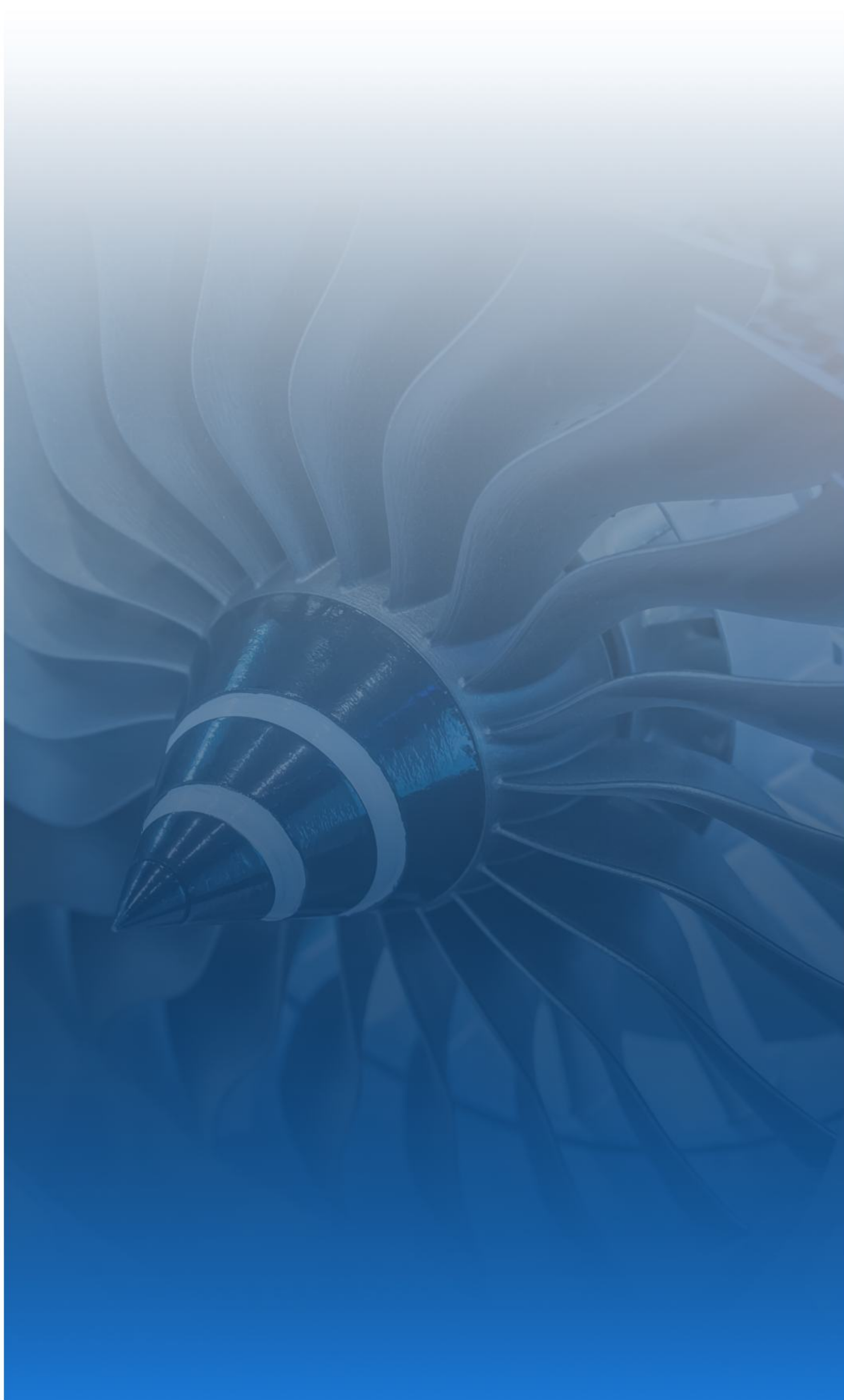
Once a file is sent, the sender loses visibility over its usage. Does the recipient manage it securely? Is it being shared with others in a way that violates compliance or governance policies? These questions often remain unanswered, increasing risk.

Governance Roadblocks & Compliance Gaps

The critical path to secure collaboration across the Aerospace and Defense ecosystem—spanning suppliers and customers—is strict governance, often driven by compliance requirements. With few alternatives, many organizations end up blocking link-based external sharing altogether, making it difficult to collaborate effectively with external partners—or even across internal teams.

This lack of flexibility prevents teams from working in a way that is both secure and efficient.

Outdated governance models prevent collaboration from happening smoothly. The result? Increased friction, lower productivity, and a higher likelihood of compliance risks.



The Modern Way: Share Information, Not Files

Apply Zero Trust to Link-Based Sharing

The traditional method of trusting the user or device is no longer sufficient. With a Zero Trust security model, trust is never assumed. Every time a link is accessed it is verified based on a set of security policies that consider the context of both the data and the user.

By applying Zero Trust principles, eSHARE ensures that only authorized users can access sensitive information, and only under the right conditions. This creates a much stronger, more reliable security posture.

Data-Centric Security

Unlike traditional security models that focus on securing the storage location, eSHARE uses a data-centric security approach. This means access to the data (through links) is continuously evaluated, no matter where it travels or where it's stored.

With data-centric security, access to data is defined by contextual signals (e.g labels, department, citizenship, export license status) from both the file as well as collaborators, ensuring that it is only accessible by those who are authorized to view it. This approach eliminates the risks of unauthorized access, even when collaborating with external partners, customers and suppliers.

A Single Source of Truth

Another key aspect of modern information sharing is moving away from desktop-based storage to embracing collaboration in secure cloud environments (Microsoft 365). In this model, there is an opportunity to shift from the mindset of sharing files to sharing links that maintain a single source of truth.

In return, organizations share sensitive information, and the data never leaves their Microsoft 365 tenant. This reduces the chances of data leaks or loss, ensuring that all parties involved can collaborate while keeping the data safe.

“

With eSHARE, you stay in control even after sharing.

”



Enabling Secure Collaboration: How It Works



Leverage Advanced Signals & Tracking

eSHARE offers powerful tracking capabilities. You can monitor and understand exactly who is accessing your data, how they're interacting with it, and even when it's being shared. This transparency gives you the insights needed to ensure data is being handled properly.



Zero Trust Enforcement

Security policies are dynamically enforced with Zero Trust principles, meaning every action taken with the data is scrutinized based on the user's identity and the context of the data. Whether internal or external collaborators are involved, you can be confident that data access is always verified and secure.



Maintain Control

With eSHARE, your organization retains complete control over your data at every stage. Sensitive information remains within a secure, compliant environment, and you can monitor who is accessing it, when, and for what purpose.



Use Familiar Platforms

One of the biggest hurdles to adopting new security measures is the disruption to existing workflows. eSHARE integrates seamlessly with the platforms your teams already use, such as Microsoft 365. There's no need for extensive training or drastic changes—security is added on top of the tools that are already part of your daily workflow.

eSHARE in Action: An Aerospace Leader Achieves Secure Collaboration & CMMC Compliance

A leading aerospace manufacturer, trusted by the Department of Defense, needed a secure way to collaborate on sensitive program data—without compromising compliance. With eSHARE, they enabled secure external sharing, met strict CMMC requirements, and maintained full control over Controlled Unclassified Information (CUI).



Download the full case study

See how eSHARE supports secure, compliant collaboration in Aerospace & Defense.

Modern Secure Sharing Starts with eSHARE

With eSHARE, you maintain control, enforce Zero Trust policies, and keep data protected—wherever it goes.

About eSHARE

Get in touch to find out how eSHARE can enhance your security framework and redefine the way you collaborate.

LinkedIn

info@eshare.com

www.eshare.com

