Solution Brief

Aerospace & Defense

Information Compliance & Protection Solutions that Control and Audit Information Flow to Comply with Export Regulations, and Protect Sensitive Data from Conflicts of Interest and Loss

FINANCIAL SERVICES AND APPLICATIONS

Export Control for Technical Data
Control and audit information flow to comply with export regulations

Intellectual Property Protection
Prevent data loss during PLM and prevent conflicts of interest between projects

Data Loss Prevention
Stop leakage and improper data mobility, inside and outside the enterprise

INFORMATION COMPLIANCE & PROTECTION CHALLENGES

Today's aerospace and defense industry is under intense pressure to comply with regulatory controls, and protect sensitive data against conflicts of interest and leakage, within a complex networked environment. A geographically dispersed supply chain, resource overlap between government and commercial projects, multiple client projects, and a mobile workforce combine to create risks when collaboration and disclosure occur. Companies struggle to avoid severe penalties and loss of business integrity within this environment, while also trying to stay agile to business needs.

Automating and maintaining effective, top-down policies that can effectively drive information controls universally across this environment is a daunting task. Current solutions fail to provide complete coverage or support business complexity. As a result, companies simply resign to paying regulatory fines when information is compromised, suffer brand damage and client lawsuits, while accepting consequences as inevitable.

THE SOLUTION

A&D companies can now comply with regulations for export restricted information (ERI), prevent IP leakage during product lifecycle management (PLM), prevent internal conflicts of interest, and prevent data loss. Solutions help to safeguard information within the enterprise, ensure compliance with export regulations when dealing with global suppliers, and restrict access to controlled information to authorized users.

IDENTITY-DRIVEN POLICY TO ENFORCE DATA CONFIDENTIALITY AND DATA PROTECTION CONTROLS

Solutions are designed to address requirements that deal with the handling and protection of technical data and intellectual property. Solutions integrate with, and leverage, existing infrastructure to apply identity-driven policies across users and resources. Fine-grain policies understand business context for appropriate information use to enforce appropriate controls.

The solution addresses information risk management requirements by enabling A&D companies to:

- Define authorized users
- Identify controlled technical data and intellectual property
- Control data access, use, and disclosure according to defined business policies

- Control technical data and intellectual property corresponding with approved licenses and defined business policies

- Provide a full audit trail detailing sensitive data flow history to satisfy internal and regulatory compliance requirements.

KEY APPLICATIONS

Applications are designed to address information risk problems and workflow scenarios that are specific to Aerospace & Defense firms. These applications include:

Export Control for Technical Data

Technical data disclosure is tracked and audited to comply with authorized use and export licenses, while denying improper party access, as information is accessed and handled across borders, extended enterprises, and the global supply chain. In addition, users are educated of safe handling policies, remediation procedures are automated to enable compliance, and inappropriate disclosure is prevented.

Intellectual Property Protection

The Solution supports PLM applications and systems, including CAD/CAM/EDA and PDM, to protect data during project team collaboration. The Solution enforces identity-driven policies that ensure appropriate data access, handling, and disclosure based on projects, user roles, data types, and business conditions. Information handling is monitored, and proper handling and disclosure is enforced, when data is used inside or outside of PLM. The Solution protects data privacy between projects to prevent conflicts of interest and avoid data loss.

Data Loss Prevention

Information handled on desktops and mobile devices is easily leaked when copied to removable media, uploaded or copied to unsafe areas such as unsecured FTP, or distributed inappropriately via e-mail or IM. The Solution protects sensitive data and applications from inappropriate access and use, even when users are off the network or disconnected, while educating them of policies, and automating procedures to remove indiscretion when using sensitive data.

SOLUTION DEPLOYMENT

NextLabs follows a proven method by utilizing a combination of expert product knowledge and a services best practices methodology. NextLabs will deploy solutions and assist clients with identifying their controlled documents, as well as defining access control policies. The deployment process includes:

Step 1: Monitor, record, and analyze information handling activities to discover and identify the risks of data loss.

Step 2: Author, manage, and deploy policies using XACML-based 4 GL policy language(ACPL) to achieve information compliance and data protection controls across applications and communication channels.

Step 3: Apply controls to educate users about policies and procedures; automate workflow and remediation to improve data handling; or block activities or alert policy stakeholders.

Step 4: Measure the effectiveness of information compliance and protection controls with reporting, continuous analysis.

NEXTLABS® | Zero Trust Data-Centric Security

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit: **http://www.nextlabs.com**.