NEXTLABS

SOLUTION BRIEF

Design & Manufacturing

Information Risk Management Solutions to Prevent Intellectual Property Loss, Mitigate Conflict of Interest Activity, and Control & Audit Information Flow to Comply with Export Regulations

SOLUTION HIGHLIGHTS

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

INFORMATION RISK MANAGEMENT CHALLENGES

High tech electronics firms, aerospace & defense, and similar industrial manufacturers rely upon CAD/CAM tools, sourcing, supply chain management, and product lifecycle management systems. With communication and collaborative workflow extending across a global supply chain during product lifecycles, companies must stay flexible and efficient, while safeguarding data. But when intellectual property (IP), restricted information (ERI), and confidential data is exported, accessed, or shared by users outside the company and across supply chains, the risks of data loss, conflicts of interest, and export violations increase—along with regulatory penalties, client lawsuits, and damaged business reputation. Risks are only compounded across a geographically dispersed supply chain and a mobile workforce. Today, companies struggle to protect data within this environment, while still trying to stay agile with business needs.

Automating and maintaining effective, top-down policies that can maintain data confidentiality across multiple vectors of risk, such as internal disclosure, conflict of interest, FTP, e-mail, Web, and removable media, is a daunting task. Current solutions fail to provide comprehensive coverage or understand complex business relationships when attempting to protect the disclosure of sensitive data.

THE SOLUTION

The Solution for design and manufacturing companies centrally manages and controls risks associated with intellectual property, client data, and confidential data loss and inappropriate disclosure. Companies can now stop leakage of IP and confidential data across global supply chains and during product lifecycles; comply with export regulations; avoid conflicts of interest across project teams and organizations; and prevent data loss at endpoints, both inside and outside the enterprise. The Solution helps to safeguard sensitive data and confidential client data, mitigate data loss at endpoints, ensure compliance with export controls when dealing with global suppliers, and restrict the access and disclosure of controlled information to authorized users.

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

The Solution is designed to address requirements that deal with the disclosure and protection of IP, ERI, and confidential data. It integrates with, and leverages, existing infrastructure to apply identity-driven policies across users and resources. Identity-driven policies understand user context and environment variables to enforce appropriate policies that prevent data loss and inappropriate disclosure.

The Solution addresses risk management requirements by enabling design and manufacturing companies to:

- Define authorized users
- Identify controlled technical data and intellectual property
- Control data access, use, and disclosure according to defined business policies
- Align controls with defined business policies, regulatory rules and contractual obligations such as export control, approved licenses, and NDAs, and
- Provide a full audit trail of data flow history and user activity to satisfy internal and regulatory compliance requirement

KEY APPLICATIONS

The Solution includes three (3) key applications to address information compliance and protection problems, and workflow scenarios, that are specific to design and manufacturing firms.

Intellectual Property Protection

It is essential to protect intellectual property across global supply chains and during product lifecycles to reduce risk of data loss, and enable safe and compliant communication and collaboration between project teams. The application enforces nondisclosure internally between teams to avoid conflicts of interest and IP misuse. Appropriate handling procedures are automated to improve compliance, avoid loss, and inappropriate disclosure. Most importantly, confidentiality is protected across extended enterprises to support partner collaboration. Data loss across endpoints and communication channels is prevented, with complete auditing and reporting during the product lifecycle and supply chain collaboration to ease audit and compliance.

Data Loss Prevention

Information on desktops or mobile devices is easily leaked when copied to removable media, uploaded or copied to unsafe areas such as unsecured FTP, or misdirected via e-mail or IM to wrong recipients. It is important to protect ERI, IP, and confidential client data from inappropriate access and disclosure, even when users are off the network or disconnected—while educating them of policies, and automating document workflow and remediation procedures to eliminate user errors and simplify information use.

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.

SOLUTION DEPLOYMENT

NextLabs utilizes a combination of GRC and security expertise, industry best practices, and proven services and implementation methodology to deliver a solution built on its leading information risk management software. 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 a XACML-based 4GL 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 audit, and compliance analysis.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based 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, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.

NEXTLABS