Teamcenter Digital Rights Management

Extending Teamcenter PLM security throughout the data file lifecycle

Benefits

- Protect sensitive intellectual property from data leakage or theft
- Automatically extend PLM security to product data files downloaded from Teamcenter
- Enable secure collaboration with supply chain partners
- Eliminate manual security procedures that impede product collaboration
- Control the access and use of product data shared with employees, partners and suppliers
- Comply with applicable regulatory requirements

Summary

Product design is a company's most valuable secret, and it often needs to be shared internally with a global workforce and externally with engineering and manufacturing partners and suppliers. Unfortunately, intellectual property (IP) theft is on the rise and impacts a company's business, compliance readiness and competitiveness. A survey of leading executives indicates that mishandling product data by insiders, suppliers and partners is the leading cause of IP breaches.

Teamcenter® Digital Rights Management (DRM) is an integrated solution that is used to automatically encrypt files before they can be shared with employees, suppliers and partners. The encrypted wrapper includes security labels from Teamcenter® software that are used to determine the rights of users to access the data. Authorized users can open, view and even modify the protected files using the native applications, including NX™ software, JT2Go and Solid Edge® software. Data owners get full visibility into how their data is being shared, accessed and used.

Teamcenter DRM enables users to protect IP from data leakage or theft, automatically extend product lifecycle management (PLM) security to product data files downloaded from Teamcenter, facilitate secure collaboration with supply chain partners, get rid of manual security procedures that hamper collaboration, control the access and use of product data shared with employees, partners and suppliers and comply with applicable regulatory requirements.

Features

- Automated rights protection, including encrypting and tagging files managed in Teamcenter
- User, workflow-initiated and batch-mode protection
- Protection at the item-revision or data-set level
- Integration with Siemens' rich application client (RAC) and Active Workspace client (AWC) for protection and access to protected files
- Access to, and usage control of files, such as limiting access, printing, copying, or screen capture, and enforcing time-based rights
- Support for native file formats such as 2D and 3D CAD, source code, Microsoft Office, PDF, NX and the JT™ data format

NEXTLABS®

www.siemens.com/teamcenter
www.nextlabs.com/products/siemens/

Teamcenter Digital Rights Management

Features *continued*

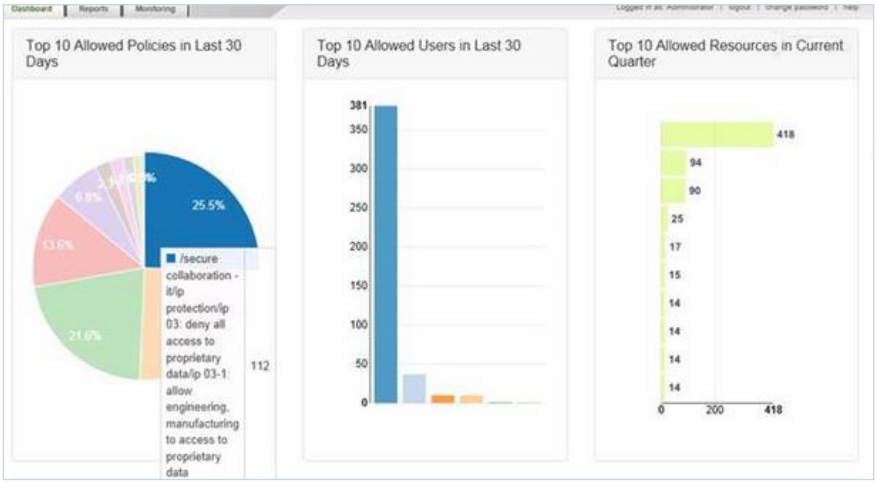
- Integration with Microsoft Office appli-cations and Adobe Reader for usage controls
- Secure viewing from any device with an HTML 5 browser
- Integration with various cloud reposi-tories for external sharing
- Monitoring and reporting on data use to get full visibility into IP data sharing
- Protect data based on Teamcenter ADA model and User attributes
- Automatic metadata synchronization and protection during check-in
- Protect compound files and dependencies
- Support Multi-CAD and working with protected CAD files in native application

Solution components

Teamcenter DRM is comprised of multiple integrated components selected and deployed according to a company's specific requirements. The complete solution allows companies to securely share product data both internally with global employees and externally with collaborative partners and suppliers. The components include:

Rights Manager for Teamcenter

Rights Manager for Teamcenter automatically protects sensitive files according to Teamcenter data classification and security. It integrates Teamcenter and the NextLabs Rights Management Server to protect (tag and encrypt) files either at rest or before data is shared. It includes integrations with various Teamcenter applications and components, such as, RAC, AWC, NX, dispatcher and the file management system (FMS).



Audit and reporting.

NextLabs Rights Management server

NextLabs Rights Management server provides two functions. First, it provides rights protection service for applications, and secondly it enables the secure view-ing of protected documents from any device via an HTML 5 web browser. Available either on-premises or in the cloud, secure viewing is well-suited for use cases in which product data needs to be shared with external users who are unable to install client side software, or when users prefer to view the shared documents from mobile devices.

The NextLabs Rights Management server allows you to use various document reposi-tories, such as SharePoint, OneDrive and Google Drive for sharing files with external users. It uses both Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML) to authenticate external users and user attributes.

NextLabs Rights Management server

Feature	Support
Supported file formats in secure viewer	Hundreds of supported file formats, including Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Adobe PDF, source code (Java, C++, XML, HTML, etc.) and 2D and 3D CAD formats.
Controls in secure viewer	Time-based (policy-driven) Access control (viewing only) Print control Dynamic watermarks
Repositories for external sharing	SharePoint, SharePoint Online, OneDrive, Google Drive, Dropbox and box
Identity provider integrations	LDAP, SAML, Okta

NextLabs Rights Management client
The NextLabs Rights Management client provides secure access, viewing and editing of protected files using native applications.

Unlike other rights management products, which only support a handful of file formats and applications, the NextLabs product is built to support any file format and application, allowing customers to protect engineering data in computer-aided design (CAD), source code and 3D file formats.

For Siemens customers, native support for NX and JT file formats is available, making it well-suited for collaborative engineering use cases. The NextLabs Rights Management client also works offline, making it ideal for mobile users in the field that need offline access to product data.

NextLabs Rights Management client

Feature	Support
Supported File Formats	Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Adobe PDF, Source code (Java, C++, XML, HTML, etc.) CAD (AutoCAD, SolidWorks, PTC Creo, CATIA, NX) Siemens (NX, JT), MicroStation Binary files (EXE, BIN)
Supported CAD tool	NX, AutoCAD, SolidWorks, PTC Creo, Dassault CATIA, Bentley MicroStation, CNC and CAM tools
Controls	Access control (viewing only) Usage control (print, save as, copy/paste, screen capture) Time-based (policy driven)* Dynamic watermarks
Client platforms	Windows 7 and 10 Microsoft Office 2013, 2016, 2019 Adobe Reader XI, DC, 2017, 2020
Offline Support	Yes

Log Details Report

Event Details:

Policy:	/secure collaboration - pr/pr-01 01: deny all access to pr-01 documents	Enforcement:	Deny
User:	adam.ivan@labs01.nextlabs.com	Action:	Open
From Resource:	file:///c:/demo/pr-01/pr-01 budget template.xls.nxl		
To Resource:			
Host:	labs-cl04.labs01.nextlabs.com	Host IP:	192.168.187.83
Application:	nxlfilehandler.exe	Event Level:	Event Level 3

Custom Attributes:

jurisdiction	Not Applicable
exportlicense	
project	PR-01
First Name	adam
User Principal Name	adam.ivan@labs01.nextlabs.com
Last Name	ivan
is checked out to local	
scopeid	
content type id	
edit menu table end	
release	
ip-classification	
_author	
unique id	
ip-owner	
vti_cachedcustomprops	
vti_cachedtitle	
description0	
slides	
Citizenship	us
UNIX User ID	
Full Name	adam ivan
Location	in
Company	acme

Centralized management reporting
Teamcenter DRM is built on NextLabs Control Center, an industry leading information control policy platform for central management, control and activity analytics. You can now have one set of policies for all Teamcenter data with centralized visibility to quickly highlight unusual access patterns or behavior – preventing breaches, misuse and violations.

Secure collaboration using Teamcenter DRM

Global engineering collaboration
Global PLM systems enable streamlined collaboration and processes across divisions and geographies, but make it challenging to control data for need-to-know projects, new product introductions (NPIs) and regulatory export requirements. Companies must achieve a delicate balance between sharing and securing data.

Information risks involved:
- Violation of global regulatory export requirements for controlled technical data
- Misuse of NPI engineering data shared outside team members

Specific challenges include:
- Control access to data based on classification, user project assignments and location
- Ensure data is up-to-date
- Prevent skirting of access controls by sharing via unauthorized channels (for example, email, file server)

Field service representatives
Field service representatives need access to technical product manuals and service instructions on various devices. Aftermarket services has become a critical business for many manufacturing companies. The risk of IP theft by insiders and competitors is a direct threat to services revenue.

Information risks involved:
- Company IP and customer confidential data loss due to lost or stolen devices
- Insider threat of remote employees stealing know-how and service customers