NEXTLABS®

White Paper

Secure Collaboration for PLM

OVERVIEW

R&D, design, and engineering organizations consistently describe the control of sensitive product data as a critical priority for their I.T. (Information Technology) departments. Additionally, organizations find themselves grappling with the increasing complexity of multiple, overlapping dimensions of information risk that expand beyond the subject matter expertise and solution design of their I.T. departments.

This white paper examines two major sources of information risk:
1) risk embedded in collaboration models related to core business initiatives and 2) risk inherent in the expanding functionality of PLM applications.

If organizations want to reap the benefits of new collaboration models and PLM technologies, they must first devise new methods to address new business risks and data vulnerabilities. This white paper describes prevalent risks and vulnerabilities and describes a platform-based solution to enable secure collaboration across PLM business processes and applications.

COLLABORATION AND BUSINESS RISK

Significant sources of risk are inherently embedded within core business initiatives that involve extending or expanding collaboration models. The following sections outline four business initiatives that produce significant business risk if information control requirements are not met.

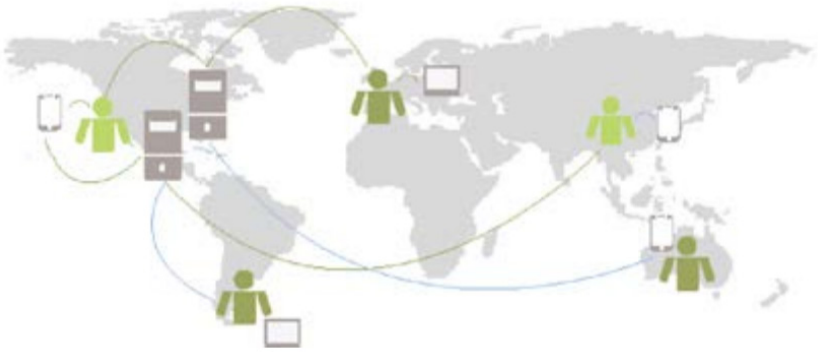
Globalization and Growth

Product growth and proliferation mean data growth and proliferation. Typically, rapid product growth and proliferation is achieved through the re-purposing of legacy projects through the introduction of product variants and/or designing modular, reusable components across product versions.

This process can become stymied if I.T. must go through cumbersome processes to instrument proper data controls for each new variant and component. The more cumbersome and complex the process, the more product data becomes vulnerable to improper access and leakage without appropriate controls that are dynamic, flexible, and can scale for growth and diversification of data.

No matter how agile a process, it runs the risk of congesting the network when I.T. manually enforces information controls. Where possible, core controls should be inherited from legacy product lines or components so controls can be applied automatically. Then, product-specific controls can be applied, if necessary, to complement baseline controls.

New Requirement: Update controls to keep pace with growing and proliferating products and data



Reducing the Risk: It is advised to mitigate business risk in design cycles by introducing automated controls that scale in parallel to data growth to prevent unauthorized access, improper handling, and leakage.

Multi-tier Product Design Collaboration

The key data challenge with multi-tier design collaboration is added complexity in process. Large designs are usually implemented as assemblies of multiple components and subcomponents, with different components being farmed out to different design teams (both externally and internally). This can mean critical Intellectual Property (IP) is distributed across systems and beyond an organization's control.

Controlling product data in a multi-tier collaboration model requires the capability to track files that are associated with specific components, and the ability to identify which components should be accessible by specified product teams. Document-level controls, as well as visibility into how documents are being accessed, used, and distributed need to be transparent to product teams.

Multi-tier, cross-team, and cross-organization collaboration put product data outside controlled environments where it is vulnerable to unauthorized access and use.

New Requirement: Controls need to protect IP in more complex design models and on systems outside the organization's IT infrastructure

Business Risk: Lack of visibility and controls for how contractors and subcontractors are sharing product data.

Cross-Team and Cross-Organizational Sharing

Cross-team and cross-organizational sharing is a common business requirement. However, similar to multi-tier design collaboration, this kind of sharing often puts product data outside systems where information controls are in place.

This challenge can apply both internally and externally. For example, design data may need to be shared with external partners, on hosts outside the corporate network where there are no data controls in place. Product data may also need to be shared with teams within the organization, where controls similarly do not exist (for example, teams such as sales, services, or support that access data on mobile devices).

New Requirement: Data must be shared cross teams and organizations

Business Risk: Lack of visibility and controls for product data outside traditional locations, applications, and systems; organizations are forced to "silo" product data

Compliance

Maintaining compliance with regulations is a daunting task in itself. Regulations can include internal corporate policies, industry or government regulations (for example, for export control: ITAR, EAR, UKMOD), and/or contractual agreements (NDA, PIA). Each form of data sharing mentioned can make complying with regulations difficult.

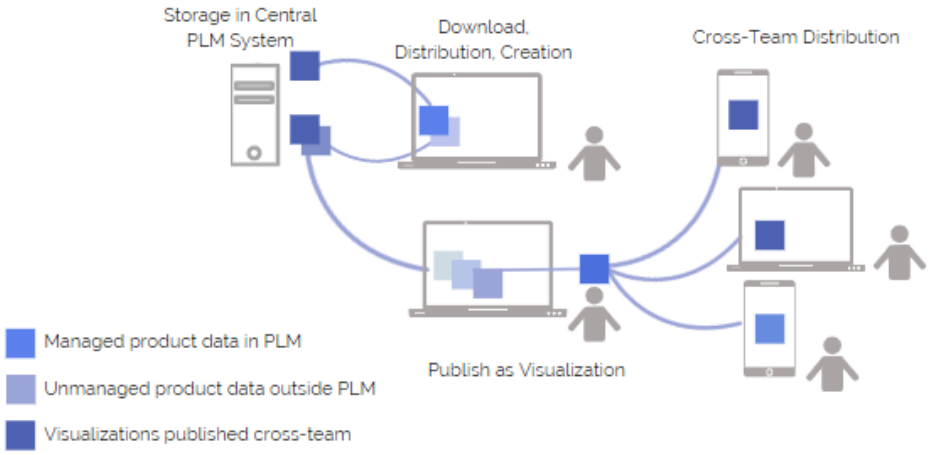
New Requirements: Maintain compliance with regulations even as data sharing becomes broader and more complex

Business Risk: Non-compliance with regulations can result in infractions, fees, and damage to corporate ethos

COLLABORATION AND DATA VULNERABILITIES

For each of these areas of business risk, specific data vulnerabilities may apply, depending on whether and how an organization takes advantage of PLM application features.

As PLM applications evolve into more complex ecosystems, design engineering teams are empowered to collaborate in new ways. However, as collaboration becomes more fluid, and process more agile, new technical capabilities in PLM can expose an organization to more risk. This section articulates new data vulnerabilities that are emerging as PLM technologies grow more complex.



(Un)Managed Data

As PLM applications evolve into more complex ecosystems, collaboration is more fluid, process more agile, and your organization more exposed to information risk.

PLM applications are evolving in ways that blur the distinctions between managed data (on the server, housed within a central application) and unmanaged data (on the client, outside a central application). For example, PLM applications that support tight integration with client design applications that “import into session” capabilities in which designers can create new designs “on the fly” by leveraging legacy components are already reflecting the same resource storage architecture challenges as cloud and SaaS paradigms.

A benefit of PLM and design integration is that engineers can easily re-purpose existing components. However, this benefit of re-purposing - an agile product design methodology - cannot be exploited without agile controls in place that can dynamically determine how newly produced designs should be stored, accessed, used, and distributed.

Business Risk: Accelerated design process can results in rapidly re-purposed design data with data vulnerabilities.

Data Vulnerabilities:

- Product designs in PLM applications lack controls or have improper controls
- Inadequately controlled components result in inadequately controlled assemblies
- Lack of controls in PLM encourage product designs to be downloaded by unauthorized users that can leak or mishandle data
- Lack of visibility into new assemblies being created in design applications
- Automated and dynamic controls mitigate the risk of repurposed design data.

Visualizations

Product data managed in PLM is increasingly exported outside the engineering function in the form of visualizations, typically in 2- or 3-D videos of large assemblies that contain many components. Visualizations are intended for cross-team sharing (with manufacturing, support and services, field sales) and increasingly, are enabled for consumption on mobile devices.

Clearly, exporting cross-functional design knowledge drives products to market at faster rates of production. However, cross functional design knowledge distributed to large sets of users requires automated information risk controls to be applied

New Risk: Product data distributed more broadly across teams in visualization format increases data vulnerabilities.

Data Vulnerabilities:

- Product visualizations that lack or have improper controls
- Product visualizations, as part of larger assemblies are leak sensitive due to lack of appropriate controls established for all the individual components in an assembly
- Lack of controls for broader set of users and devices across organizations where visualizations are distributed
- Lack of visibility into how visualizations are being accessed and distributed

Data-on-the-Move

Managed data within PLM may already have adequate controls. However, with the rise in globalization, controls within PLM must be complemented with controls outside. Product data can be downloaded by authorized users, product designs can be created, imported, and modified in design applications, and visualizations are intended for broader distribution. Securing data-on-the-move can introduce new challenges, such as the overhead of managing and coordinating multiple sets of controls.

In the context of design organizations, data on the move is often data in transformation. When data is exported into different formats for sharing, it might require different controls depending on the format and how the file will be distributed and consumed.

Exporting product design knowledge cross-function can be a boon for business. However, controls will also need to be applied for a drastically larger set of users and devices.

For example, perhaps a given visualization does not include enough detail that an organization is concerned about broad distribution. In this case, the same controls that apply to CAD files and PDFs on endpoints and structured and unstructured data in PLM do not need to apply to visualizations. Or the reverse may be true: for highly sensitive information, any data, in any format, may require the same controls.

The point is that organizations will have to think through these scenarios as they work to design and enforce proper data- and format-centric controls.

New Challenge: product data, designs, and visualizations are increasingly on-the-move between systems, groups, users, organizations

Data vulnerabilities:

- Lack of integrated classification to track PLM data, design, and visualizations consistently as they move in and out of the PLM application
- Lack of controls that can be both data-specific (meaning, appropriate for the components included in the assembly) and format-specific (meaning relevant to the degree of detail in the format as product and design data is packaged for different audiences)
- Lack of visibility into access and usage of data-on-the-move across applications, systems, and devices

In the context of product design, data-on-the-move is often data-in-transformation. When data is exported into different formats for sharing, it might require different controls.

COMMON DATA VULNERABILITIES IN DESIGN COLLABORATION

The following table organizes vulnerabilities discussed in this white paper by different stages of an information life-cycle.

Information Life-cycle	Vulnerability
Storage	Product designs stored in PLM applications lack controls or have improper controls
Classification	Lack of integrated classification to track PLM data, design, and visualizations consistently as they move in and out of the central PLM application
	Lack of inheritance logic so new product variants and components automatically inherit baseline controls
	Lack of inheritance logic so assemblies can inherit the classification of components
Access and Usage	Due to lack of controls in PLM, product designs are downloaded by unauthorized users who leak or handle data inappropriately
	Inadequately controlled components result in inadequately controlled assemblies
	Product designs and visualizations lack controls or have improper controls for all the components included in the assembly
	Lack of controls that are both data-specific (meaning, appropriate for the components included in the assembly) and format-specific (meaning relevant to the degree of detail in the format, as product and design data is packaged for different audiences)
Visibility	Lack of visibility into new assemblies being created and re-purposed in design applications
	Lack of visibility into how partners and other external parties are accessing, using, and distributing product data and designs
	Lack of visibility into access and usage of data-on-the-move across applications, systems, and devices

SECURING THE PLM ECOSYSTEM

Secure Product Design

Secure Product Design means enforcing controls on managed and unmanaged data in the form of design files, no matter where they are being created, downloaded, edited, or distributed:

- Automate Data Classification and Rights Protection for product designs as they are created or edited in a design application. Products designs may be categorized as managed or unmanaged data depending on the tightness of the integration between PLM and design applications
- Provide document-level Access Controls across Identity domains for unmanaged designs, especially when design files are shared cross-team
- Provide Activity Monitoring to log all user interaction with unmananged product designs and route information to the platform

Secure Product Visualization

In a platform-based approach, Secure Product Visualization means enforcing document-level protections on managed and unmanaged data in the form of visualization files, no matter where they are created, stored, accessed, or distributed NextLabs Solutions:

- Automate Data Classification and Rights Protection for unmanaged product visualizations as they are created or edited in a visualization application
- Provide document-level Access Controls across Identity domains for visualizations, especially when visualizations are shared cross-team
- Provide Activity Monitoring to log all user interaction with managed and unmanaged visualizations and route information to the platform

A platform-based approach enables persistent document-level protections for Product Designs and Visualizations no matter where they are created, stored, accessed, or distributed.

Integrated Coverage for Data-on-the-Move

The platform-based approach enables organizations to deploy integrated controls that protect and secure sensitive product data no matter where it resides in the PLM ecosystem and the current stage of the information life-cycle.

Reducing the Risk

An often-mentioned solution for secure collaboration across the PLM design ecosystem is the design and instrumentation of disparate controls for different kinds of data.

Instead, this white paper recommends a platform-based approach that can leverage the same set of classifications and integrated controls and enforce them consistently across the PLM ecosystem. As data-on-the-move evolves across different systems, devices, applications, and file formats, implementing a platform-based approach would severely excise data vulnerabilities in design organizations.

Secure Collaboration Platform

NextLabs provides solutions that enable organizations to secure managed and unmanaged data across the PLM ecosystem:

- Security Control Automation to enforce controls automatically activated at the access, creation, storage, or communication of an event
- Standardized attribute-based Information Control Policy Model that can be applied across environments, systems, and applications.
    - Data Classification
    - Data Segregation
    - Access Control
    - Rights Protection
    - Communication Control - Activity Monitoring

The benefit of implementing a platform-based approach is the ability to provide controls that are based on attributes of data. When controls are attribute-based digital policies, they can be applied consistently across a business process. This is because attributes of product data can determine how the data should be uniformly controlled across project teams, product lines, etc.

A platform-based approach also provides data-centric activity monitoring for auditing and analytics to maintain visibility, no matter where product data resides.

Secure Product Data

In a platform-based approach, securing product data means enforcing attribute based controls on managed data in PLM as well as applying controls that persist when data becomes unmanaged outside of PLM NextLabs solutions:

- Automatically apply Data Classification to Product Data as managed data is created or unmanaged data is uploaded into PLM
- Data Segregation controls ensure managed data is stored in proper locations on the PLM server
- Access Controls govern how managed Product Data is accessed and downloaded
- Provide integrated Rights Protection to automatically apply protection to managed documents in PLM, so document-level controls persist when data leaves the PLM application (i.e., downloaded by an authorized user)
- Apply Activity Monitoring to log all PLM events for managed data and route information to the platform for reporting

When controls are implemented as attribute-based digital policies, they can be applied uniformly across multiple business processes.

System	Life-cycle Stage	Necessary Controls
Central PLM Application	Create managed data in PLM	Segregation Controls Data Classification Controls (inheritance from existing product data, if applicable) Rights Protection
	Upload unmanaged data into PLM	
	Access or download managed data in PLM	Access Controls Persistence of Classification and Rights Protection
	Across the life-cycle	Activity Monitoring Controls
Design Application	Create or edit designs (managed or unmanaged, depending on integration)	Data Classification Controls (inheritance from existing designs, if applicable) Rights Protection
	Distribute designs	Access Controls Persistence of Data Classification and Rights Protection
	Across the life-cycle	**Activity Monitoring Controls**
Visualizations	Create visualizations (managed or unmanaged, depending on integration)	Data Classification Controls (inheritance from components, if applicable) Rights Protection
	Distribute visualizations	Access Controls Persistence of Classification and Rights Protection
	Across the life-cycle	Activity Monitoring Controls

SUPPORTED PLM ECOSYSTEMS

The following table lists PLM Ecosystem vendors and applications for which NextLabs currently offers platform-based Information Risk Management solutions.

Vendor	Applications
Siemens AG	Teamcenter, NX, Solid Edge, Life-cycle Visualization
Dassault Systemes	ENOVIA, CATIA, SOLIDWORKS
PTC®	Windchill, Creo
SAP®	SAP PLM, Visual Enterprise
AUTODESK®	AutoCAD

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.