NEXTLABS®

SkyDRM for Solid Edge

Protect Data at Rest, Shared File, and Payload

OVERVIEW

Solid Edge is a comprehensive 3D CAD (Computer-Aided Design) software developed by Siemens Digital Industries Software. It is designed to support various aspects of the product development process, from initial design to manufacturing. Solid Edge is known for its ease of use and flexibility, making it a popular choice among engineers and designers in various

Even though sharing design documents with external partners provides these business advantages, it can also introduce potential security risks, including the following:

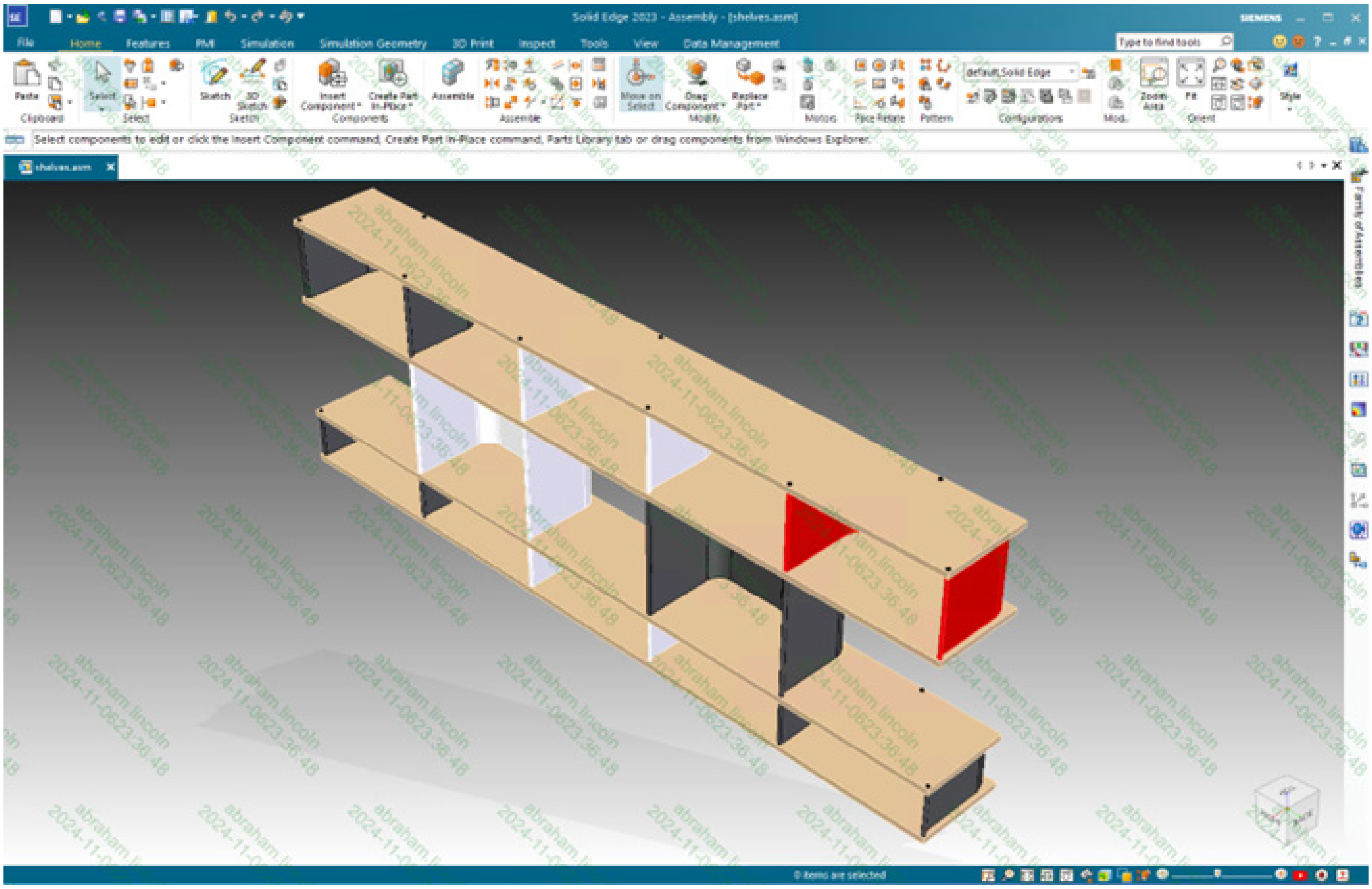
- **Data Breaches**: If an external partner's security measures are inadequate, sensitive design information can be exposed to unauthorized parties
- **Intellectual Property Theft**: Proprietary designs can be stolen or misused by partners or third parties
- **Compliance Violations**: Sharing sensitive information without proper safeguards can lead to violations of data protection regulations, resulting in legal and financial penalties
- **Supply Chain Attacks**: Cyber attackers can target external partners to gain access to design documents, exploiting vulnerabilities in their systems

THE SOLUTION

To mitigate these risks, it is crucial to implement strong measures such as:

- **Data Encryption**: To protect data both in transit when it is shared and at rest.
- **Access and Usage Controls**: Implement the principle of least privileged access, limiting access to sensitive documents to only users who need them.
- **Regular Audits**: Conduct regular security audits of partners to ensure compliance with security standards.

NextLabs' SkyDRM is Enterprise Digital Rights Management (E-DRM) designed to protect data in use, in transit, at rest and when shared across extended enterprises with audit capabilities. With SkyDRM, any file type can be protected and accessed from any device to ensure secure collaboration with access and usage controls. SkyDRM integrates seamlessly with Solid Edge through a Rights Management Extension (RMX) to allow authorized users to open, view, import, and even modify the protected files natively within Solid Edge, providing persistent data protection for secure collaboration with internal users and external partners.



Solid Edge 2023 - Assembly - [shelves.asm]

Select components to edit or click the Insert Component command, Create Part In-Place command, Parts Library tab or drag components from Windows Explorer.

KEY FEATURES

KEY FEATURES	
Access Control	Allow authorized users to open the protected file within Solid Edge
Usage Control	Enforce permissions granted on the protected file to control the commands (view / edit / import / print / screen capture / copy content) a user can execute within Solid Edge
Persistent Protection	Protect a new file automatically if it is generated (save) from a protected file within Solid Edge, transferring the source file's metadata to the target file
Dynamic Watermark	Show a secure overlay containing dynamic watermark text preconfigured in the policy when opening a protected file in Solid Edge
Anti-Screen Capture	Design screen cannot be captured by screenshot tool or shared by video communication software without proper rights
Centralized Visibility	Centralized monitoring and reporting on data use for full visibility

KEY COMPONENTS

KEY COMPONENTS	
SkyDRM Rights Management Server (RMS)	SkyDRM Rights Management Server provides end-to-end protection of sensitive data with authorization, rights protection, rights enforcement, and document activity monitoring
SkyDRM Rights Management Desktop (RMD)	Document owners and collaborators can use SkyDRM Desktop for Windows to protect sensitive documents at creation, view and edit protected documents using native applications, share data securely, even offline, and provide the sanctuary folder functionality
SkyDRM RMX for AutoCAD	SkyDRM RMX for Solid Edge allows authorized users to open, view, and modify the protected files using Solid Edge software natively

BENEFITS

BENEFITS	
Secure Information Sharing	Enable product data to be securely shared between design partners, suppliers, foreign employees, joint ventures, and customers worldwide by providing policy-driven protection and an end-to-end audit trail
Improved Compliance	Improve compliance and governance programs by automating information controls for sensitive product data with a comprehensive audit trail
Complete Data Protection	Protect sensitive product data by controlling access and usage as data moves across PLM, CAD, and Visualization systems. Protect data regardless of where it is – in a public Cloud, in SaaS applications, or on the move
Rapid Deployment and Adoption	Deep integration and zero-code client installation allows for rapid deployment among the extended partner networks

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.