NEXTLABS®

SkyDRM

Protect Data at Rest, Shared File, and Payload

OVERVIEW

For companies operating in today's global and competitive environment, sharing valuable information is an absolute necessity. However, there is a direct correlation between sharing and risk – the more sharing you do, the more risks you take on. Mitigating these risks requires rethinking how you control and secure your data as it moves outside the corporate network, is shared with external partners and collaborators, or is downloaded to unmanaged or mobile devices.

THE SOLUTION

NextLabs SkyDRM enables secure collaboration for sensitive documents flowing through internal and external business processes by automating access and usage controls across enterprise applications, cloud applications, and endpoints.

KEY FEATURES

Dynamic Authorization

SkyDRM utilizes dynamic authorization to determine access rights to documents in real-time. It leverages data classification and user and environment attributes such as group, department, device type, IP address, etc., to make those determinations.

Automated Rights Protection

SkyDRM uses encryption, identity, and authorization policies to secure your files. You can apply digital rights to the files being shared and control what usage permissions, such as View, Edit, Print, ReShare, Save As, and Extract, you want to grant to the intended recipients. Protection stays with the files regardless of where those files are located - inside or outside your network, on file servers, or in the cloud. With SkyDRM, you control your files, even when those files are shared with other people.

Seamless Collaboration

SkyDRM enables teams to collaborate without having to worry about leakage of intellectual property and trade secrets, essentially providing a forum for sharing critical documents securely. It allows teams to create virtual project data rooms to store and share important documents securely. Any document uploaded to SkyDRM is automatically protected with digital rights and tracking by default.

Secure Viewing in Browser

In SkyDRM, a user is able to view protected data via any HTML5-compatible browser. Supported file types include Microsoft Office documents, PDF, JPG, PNG, and a variety of CAD formats, such as JT, PRT, CATIA, and VDS, etc. The viewer provides a multitude of interactive visualization capabilities like Zoom In, Zoom Out, and Rotate.

Document Access and Usage Controls

You can apply rights protection policies in real-time to control access and usage across all applications and file types. Controls are based on context, content, and identity attributes, originating from both internal and external sources, and can be defined at both the enterprise and project levels. Usage controls within an application require a Rights Management Extension (RMX) plugin for that application.

Federated Identities

SkyDRM supports federated identities (e.g., SAML, OpenID), where each business partner maintains their own user identity, user attributes, and changes in user status. The identity and attributes of a user can, as part of the authentication process, dynamically be made available to SkyDRM to determine access at that point in time.

Flexible Policy Creation

Policies can be "user-defined" or "company-defined." With a "user-defined" (or ad hoc) policy, you can share a file or document with anyone by entering their email address and assigning them specific controls, whereas "company-defined" (or central) policies apply to all files and are based on document metadata and user attributes.

SkyDRM Rights Management Server

SkyDRM Rights Management Server provides end-to-end protection of your sensitive data with authorization, rights protection, rights enforcement, and document activity monitoring.

Application Integration

SkyDRM integrates with your line of business applications (PLM, ERP, SCM, ECM) to automate rights (classification and encryption) of sensitive data stored in those applications. This allows seamless integration with your business processes and ensures data is protected right at the source.

Enterprise Applications

SkyDRM supports the following enterprise applications:

- Siemens Teamcenter and PTC Windchill
- SharePoint and SharePoint Online
- SAP ERP
- Bentley ProjectWise
- Microsoft Exchange
- iManage

Desktop Applications

SkyDRM supports the following desktop applications on Windows.

Productivity

- Microsoft Office
- Adobe Acrobat Reader
- Adobe Acrobat Pro

3D Modeling

- Autodesk 3ds Max
- Autodesk Maya
- Autodesk Navisworks Freedom
- Bentley View
- Bricsys BricsCAD
- PTC Creo View MCAD/Lite/Express
- Rhinoceros 3D Rhino
- SAP 3D VE Viewer
- Siemens JT2Go
- Trimble SketchUp
- Trimble Layout
- Siemens NX
- Siemens Solid Edge
- Dassault SolidWorks
- PTC Creo
- Autodesk AutoCAD
- Autodesk Inventor

Building Information Modeling (BIM)

- Bentley MicroStation
- Autodesk Revit

Electronic CAD

- Altium ECAD/Designer
- PTC Creo View ECAD

Electrical CAD

- EPLAN Electric
- Zuken E3.Series

CAM

- Autodesk Netfabb
- Materialise Magics

Simulation

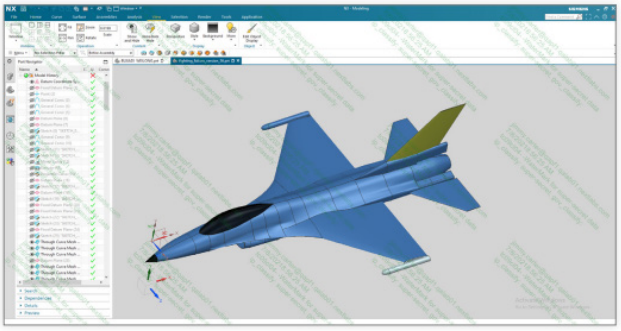
- Siemens SimCenter Star-CCM+

Graphic Design, Photo and Video

- Adobe After Effect
- Adobe Illustrator
- Adobe In Design
- Adobe Photoshop

Molecular Modeling

- ChemDoodle 2D
- ChemDoodle 3D



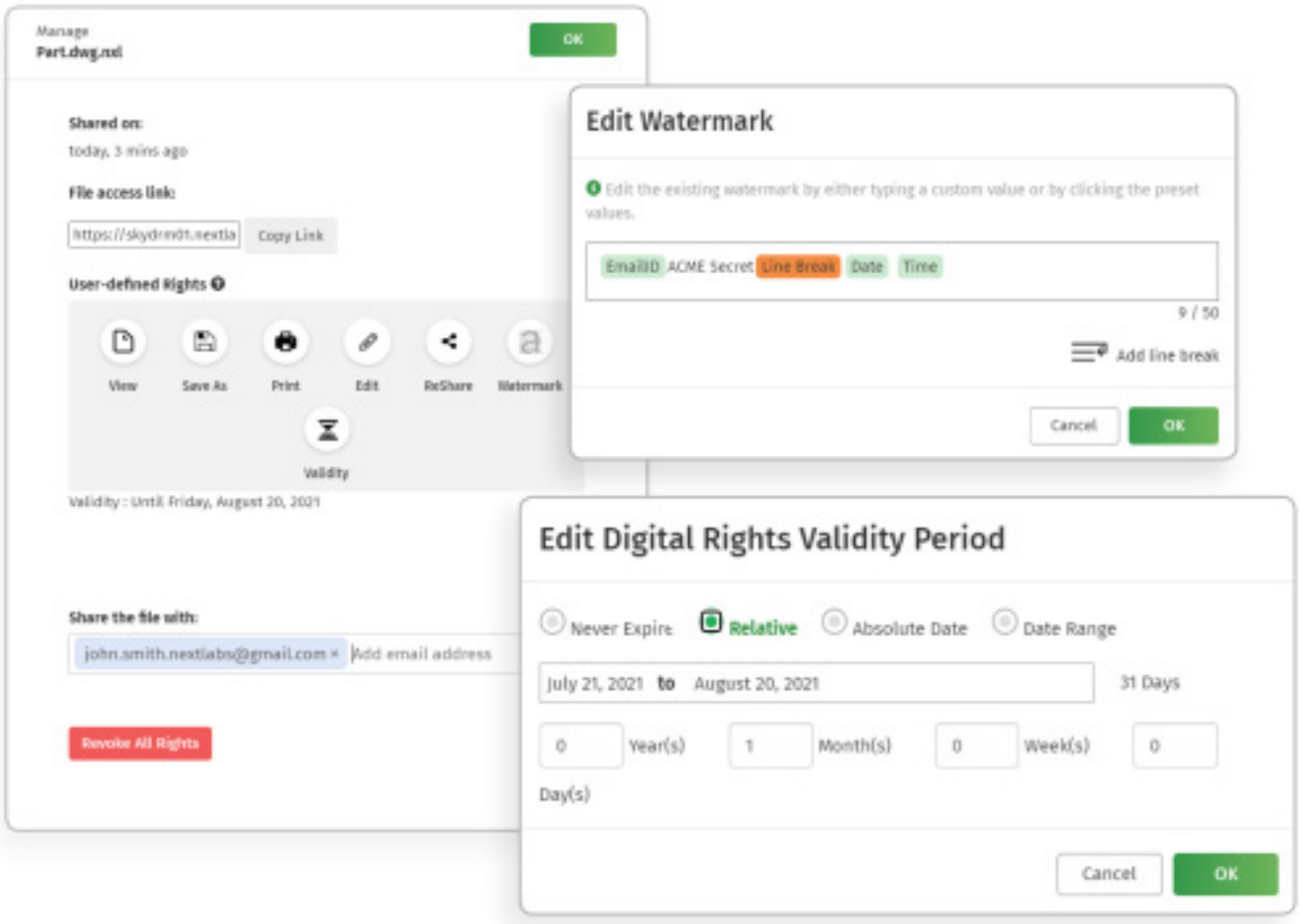
Cloud and SaaS Application Integration

SkyDRM integrates with SaaS applications such as SharePoint Online, OneDrive, Google Drive, and Dropbox to protect sensitive documents stored in the cloud. Users can automate rights protection, view protected documents and share protected documents easily and securely within SaaS applications.

SkyDRM Rights Management Clients

Rights Management Client provides attribute-based security to control access and usage of documents on endpoint devices.

- SkyDRM Desktop for Windows—document owners and collaborators protect sensitive documents at creation, view and edit protected documents using native applications, share data securely, even offline, and provide the sanctuary folder functionality. A sanctuary folder is a special SkyDRM folder in the Windows file system, where only the trusted application can access the files inside. When an unprotected file is copied or moved outside of the folder, the file will be protected automatically. Additionally, a 3rd party application can be configured as a trusted application where the trusted application is automatically integrated with the SkyDRM policy engine and can handle NXL protected files directly.
- SkyDRM Web App—easy protecting and sharing with internal and external users. Users can share and access their documents stored in enterprise content repositories or cloud applications securely using SkyDRM on any device anywhere.
- SkyDRM App for iOS, Android, and MacOS —native mobile protecting documents, browsing, viewing and sharing experiences for protected documents.



SkyDRM Rights Management SDK

You can integrate rights protection into any application through the use of SkyDRM Client SDK for Windows and Mobile (iOS and Android) and SkyDRM Server SDK. By doing so, you can reap the same benefits as those provided by the SkyDRM Rights Management Extensions above.

SkyDRM Rights Protection Tool

SkyDRM Rights Protection Tool (RPT) provides bulk protection of files automatically based on schedule using centrally defined rules.

SUPPORT INFORMATION	
Supported File Types in Viewer	Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Microsoft Visio (Web Viewer only), Adobe PDF, Source code (java, cpp, xml, html, etc.), Picture file (jpg, png, tif, tiff, bmp, etc.), Text file (txt, log), CAD (AutoCAD, Inventor, TrueView, SolidWorks, ProE, CATIA V5/V6, Parasolid, NX, Solid Edge, Creo, Siemens JT), SAP Visual Enterprise (Web Viewer only), Common CAD formats (igs, iges, stp, stl, step, etc.)
Supported Controls	View, Edit, Print, Re-share, Save As, Extract, Watermark, Expiration, Number of Uses
Server Platforms	Docker CE, RHEL, , Windows, Kubernetes, OpenShift
Client Platforms	Web, iOS, Windows, macOS, Android
Supported Identity Providers	Active Directory (AD), Okta, Active Directory Federation Services (ADFS), OneLogin, PingOne, Google, Facebook

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.