NEXTLABS®

PRODUCT BROCHURE

Rights Management

Ready to Make the Shift?

Across industries, information sharing practices are shifting dramatically. Less complex requirements to secure data on managed devices and applications residing inside the corporate network are evolving into more complex requirements to share data securely across the extended enterprise. Information consumers are requiring access to data anytime, anywhere, and on any device.

The challenge: How can organizations share data the way today's business models demand, while still protecting trade secrets and valuable intellectual property against loss, leak, and noncompliance?

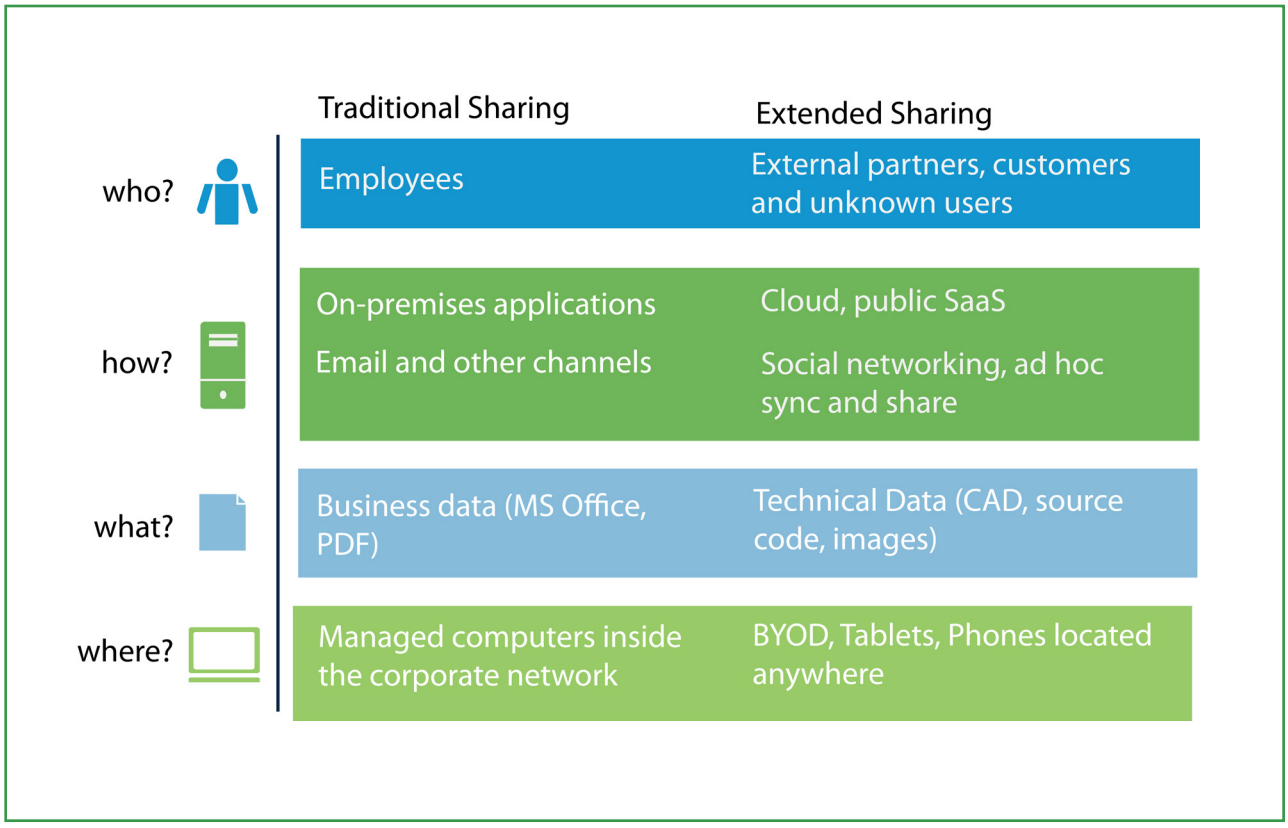
CONTROLS ACROSS THE EXTENDED ENTERPRISE

NextLabs Rights Management is designed to protect data across today's extended enterprise. Data can be protected in any file type and can be accessed from any device. And, users can now view protected files from a web browser - no need to install client software. The result is flexible, secure collaboration ecosystems that easily handle use cases that elude traditional IT solutions.

Rights Management components are easily configurable to adapt to dynamic business process and ad hoc data sharing use cases, while allowing organizations to maintain centralized control of data sharing policies and stringent auditing and reporting.

Organizations can easily set up ecosystems to accommodate complicated sharing requirements, such as:

- Securing collaboration with external suppliers, partners, and on-the-move employees outside the network
- Protecting data shared in public cloud and SaaS applications, and ad hoc sync and share use cases
- Evaluating data access requests coming from unmanaged mobile devices and unknown users
- Sharing valuable technical and business data typically stored in Line of Business (LOB) applications (PLM, ERP, SCM, ECM, and so on) including CAD files and rich media
- Supporting rich edit permissions in native applications for data creators and owners, as well as file-type agnostic, view-only protection for other users
- Comprehensive visibility into data access and usage events, even during external sharing



HOW IT WORKS

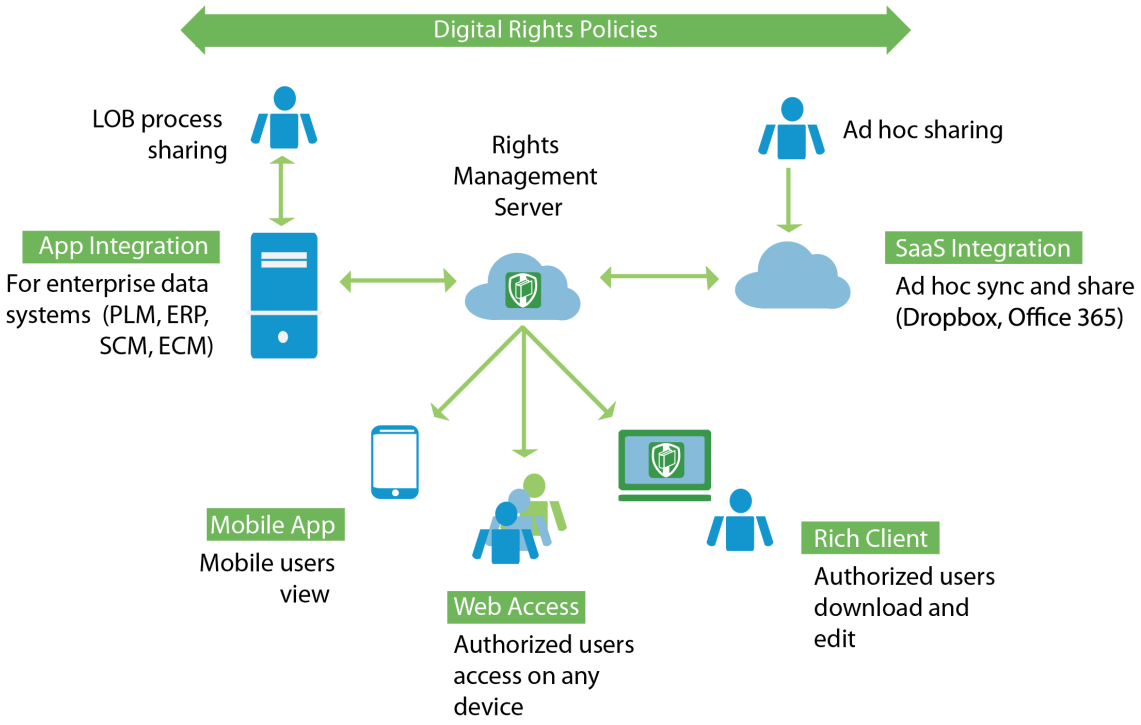
NextLabs Rights Management consists of integrated components deployed according to a company's business requirements.

Digital Rights Policies

Data protection requirements are expressed as attribute-based policies, which are centrally managed and deployed across systems. Wherever possible, data and user attributes are leveraged from existing security infrastructure, including identity attributes that are procured from external sources for extended enterprise use cases. Then, Digital Rights Policies automate data classification and protection, with support for both mandatory and discretionary use cases.

Application Integration

Integration with enterprise data systems (PLM, ERP, SCM, ECM) and SaaS applications (Dropbox, Box, Google Drive, OneDrive) allows data classification and protection to be seamlessly integrated into existing workflows. This applies for both highly regulated line of business (LOB) and process-oriented sharing, as well as for ad hoc "on the fly" sync and share.



Secure Access Anytime, Anywhere

Once protected, files can be stored anywhere securely—on endpoints where data creators work in native applications, in content repositories located in enterprise applications or in the cloud or SaaS applications. Organizations can utilize three different types of clients for secure access, usage, and monitoring, regardless of how files are consumed and the type of user:

- Rich Client endpoints (even when disconnected from the corporate network), where users require rich interaction with data (download and edit content in native applications)
- On-demand Web Access that supplies instant access anywhere, on any device
- Mobile App for an authentic mobile browsing and viewing experience

This flexible architecture supports extended sharing use cases easily, while centrally monitoring all access and usage events.

ATTRIBUTE-BASED DIGITAL RIGHTS POLICIES

Digital Rights Policies are digital renditions of your organization's compliance, legal, and security policies. These policies apply classification, access control, automated protection (encryption) and other controls, with central management of a single set of policies that can be deployed cross-system.

Policies are defined using Attribute-Based Access Control, which enables highly granular access, usage, and handling controls to capture the complexity of business requirements. Policies can be defined at the data and data attribute level—allowing you to create highly precise controls that can target classes of data cross-system, by file attribute, content, file type, user attribute, and more.

INTEGRATION WITH ENTERPRISE & CLOUD APPLICATIONS

NextLabs Rights Management is integrated into core Line of Business (LOB) and enterprise content sharing applications. The result is that data can be protected (tagged and encrypted) on upload, or in batch processes for data-at-rest—before data is even shared.

Content repositories are easily integrated with Rights Management Server for on-demand viewing in NextLabs Web Access Client. Data shared using ad hoc sync and share and SaaS applications can also be protected.

Unlike other products, which only support a handful of file formats and applications, Rights Management is built to support any file format and application, allowing customers to protect not only Office and Adobe files, but also engineering data in CAD, source code, and 3D file formats.

FLEXIBLE CLIENT OPTIONS

Because Rights Management is component-based, you can position clients where they are needed based on your data sharing and protection requirements: rich collaboration or on-demand.

Rich Collaboration Client

For users who require rich collaboration, NextLabs Rights Management Client provides secure access and editing of protected files within native applications.

Rights Management Client works completely offline, making it well-suited for mobile users in the field that need offline access to data.

On-Demand Web Access Client

An on-demand Web Access client provides secure viewing of protected documents from any device via any HTML5 web browser - without installing any client software.

Available either on-premises or in the cloud, the Web Access client supports hundreds of file types, including comprehensive CAD coverage, and is well-suited for cases where product data needs to be shared with external users who are unable to install client-side software or where users prefer to view the shared documents from mobile devices.

Mobile App Client

For users that want authentic mobile browsing and access, Rights Management includes an iOS App client, which provides secure access anywhere.

IDENTITY MANAGEMENT FOR EXTENDED ENTERPRISE SUPPORT

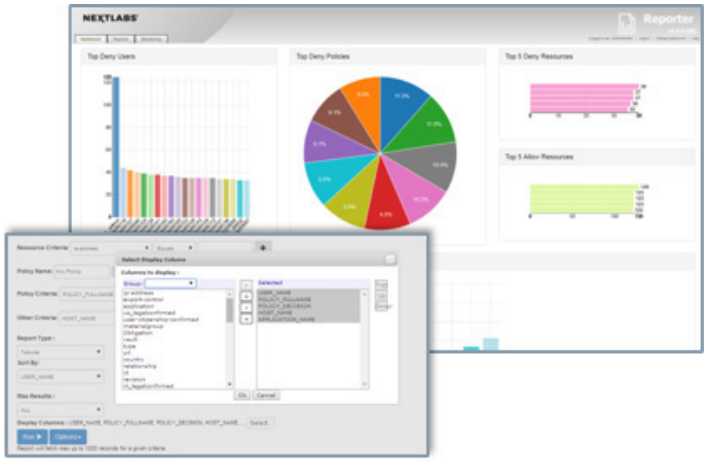
One of the challenges in extended enterprise data sharing is identity management. In global supply chain and collaborative engineering projects, for example, you often need to share information with business partners while maintaining control over what their users can do with the data after it leaves your enterprise network. NextLabs Enterprise Digital Rights Management (EDRM) supports two methods of addressing this requirement.

Users can be managed locally in an identity management system connected to NextLabs EDRM if they are known ahead of time or required to register to gain access to your data. In this mode, users authenticate directly to the EDRM system and the underlying identity system before being able to access authorized content. With a lot of external users, this may present some challenges as a process needs to be put in place to keep track of the changes in user status which can affect access rights.

To address this, the solution also provides support for federated identity. In this case, identities of external users are managed and authenticated by the business partner's identity management system and do not need to be known ahead of time by the organization deploying EDRM. With federated identity, each business partner will maintain their own user identity, attributes related to the user, and changes in user status. Identity and attributes of a user can, as part of the authentication process, dynamically be made available to NextLabs EDRM to determine access at that point in time.

CENTRAL ACTIVITY AUDIT AND REPORTING

Information control and activity audit data is collected centrally for comprehensive visibility and activity analytics, whether access and usage events occur inside or outside the network.



DEPLOYMENT OPTIONS

NextLabs Rights Management is available on-premises or in the cloud. Both can work together to enable secure collaboration between partners, vendors, customers, and multi-tier supply chains.

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, bmp, etc.), CAD (AutoCAD, SolidWorks, ProE, CATIA V5/V6, Parasolid, NX, Solid Edge, Siemens JT), SAP Visual Enterprise (Web Viewer only), Common CAD formats (igs, iges, stp, stl, step, etc.)
Supported Controls	View (Access Control), Edit (Requires RMX), Print, Re-share, Save As (Make a Local Copy), Extract (Make a Decrypted Copy), Watermark (User-defined Control), Expiration (User-defined Control)
Server Platforms	Docker CE, RHEL, CentOS
Client Platforms	Web, iOS, Windows
Supported Identity Providers	Active Directory (AD), Okta, Active Directory Federation Services (ADFS), OneLogin, PingOne
Supported Cloud and SaaS Apps	Google Drive, OneDrive, SharePoint Online, SharePoint On-Premises, Box, Dropbox
RMX for CAD and Authoring Tools	Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Siemens NX, PTC Creo
RMX for Enterprise Applications	Siemens Teamcenter, Microsoft SharePoint, SAP ERP

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®