

NextLabs Enterprise Digital Rights Management (EDRM) for Microsoft SharePoint

THE SITUATION

Microsoft SharePoint has long been a tool to enable fast and easy collaboration--both internally and externally. However, today's business models increasingly require sensitive and restricted data to be shared with a global workforce, customers, and external partner organizations, often accessing information on unmanaged or devices and devices. How can companies continue to leverage the benefits of using Microsoft SharePoint for agile collaboration, but also secure data-on-the-move across today's extended enterprise?



THE SOLUTION

NextLabs Enterprise Digital Rights Management (EDRM) for Microsoft SharePoint integrates with SharePoint to automatically wrap valuable files with encryption before they are downloaded and shared. The encrypted wrapper includes security labels from SharePoint 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 native applications. Data owners get full visibility into how their data is being shared, accessed, and used. The EDRM solution provides the following key capabilities:

- **Automated Rights Protection** encrypts and tags valuable files managed in SharePoint
- **Access and Usage Control** over rights protected files enables access, printing, copying, and screen capture
- **File-Type Agnostic, First-time Offline Access** so users can download and view files in native applications with no interruption of normal process
- **Secure Viewing from Any Device** with an HTML5 browser
- **Zero Client Install** enables easy access without needing to install any client software
- **Monitoring and Reporting** for full audit visibility across the extended enterprise

THE RESULTS

Using EDRM for Microsoft SharePoint, companies are able to:

- Automatically extend SharePoint security to product data in downloaded files
- Control the access and usage of product data shared with internal employees and external users
- Eliminate manual security procedures that impede collaboration
- Achieve comprehensive visibility into events and data for audit, oversight, and troubleshooting

SOLUTION COMPONENTS

The EDRM solution is comprised of multiple integrated components selected and deployed according to the company's use case. The complete solution allows companies to securely share product data both internally with global employees and externally with collaborative partners and suppliers.

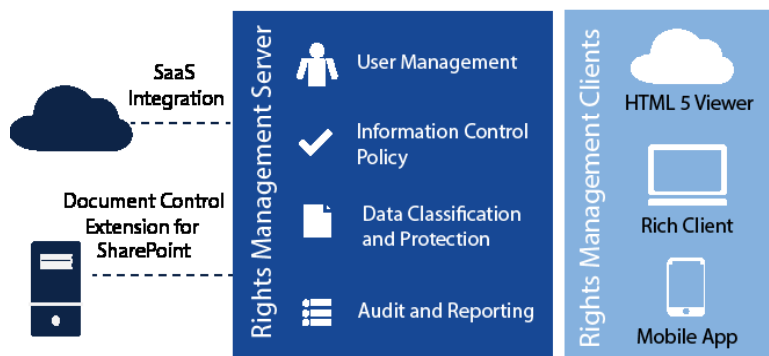
Document Control Extension for Microsoft SharePoint

The Document Control Extension for Microsoft SharePoint automatically protects sensitive files according to SharePoint data classification and security. The Document Control Extension integrates SharePoint and the NextLabs Rights Management Server to protect (tag and encrypt) files either at-rest or before data is shared.

NextLabs Rights Management Server

The NextLabs Rights Management Server provides two functions. First, it applies rights protection to ensure only authorized people get access, and second, it provides secure viewing of protected documents from any device via any HTML5 web browser. Available either on-premise or in the cloud, Secure Viewing is well-suited for use 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.

| Feature | Support |
|------------------------|--|
| Supported File Formats | 100s of supported file formats including Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Adobe PDF, Source code (java, cpp, xml, html, etc.), and CAD formats |
| Controls | Encryption, Data Tagging, Access Control (Viewing only), Print Control, Copy/Paste Control, Dynamic Watermarks, Activity Logging |
| Supported Clients | HTML 5 Browsers (Internet Explorer, Safari, Chrome, Firefox) on OS X, Windows, iOS, and Android |



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 that only support a handful of file formats and applications, the NextLabs product is built to support any file format and any application.

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

| Feature | Support |
|------------------------|--|
| Supported File Formats | Microsoft Word, Microsoft PowerPoint, Microsoft Excel, Adobe PDF, Source code (java, cpp, xml, html, etc.), CAD (AutoCAD, Solidworks, ProE, Catia, NX), Siemens (NX, JT), SAP Visual Enterprise (VE) |
| Controls | Access Control (Viewing and Editing), Print Control, Copy/Paste Control, Dynamic Watermarks, Screen Capture Control, Activity Logging |
| Client Platforms | Windows 7, Windows 10 Microsoft Office 2013, 2010, 2007 Adobe Reader X, XI |
| Offline Support | First-time offline access to documents (no need for server login) Offline access lease |

Centralized Management and Reporting

EDRM is built on the NextLabs Control Center, the industry leading information control policy platform for central management, control and activity analytics.

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

© 2007-2016 NEXTLABS INC. ALL RIGHTS RESERVED