

## Rights Protection Tool

Protect Data at Rest, Shared File, and Payload



### OVERVIEW

Companies are increasingly challenged with how to secure large volumes of data. Companies have terabytes of data in archive that need to be managed, classified, and controlled. As more data is collected and shared, it has become increasingly difficult to ensure data is available to the right person at the right time. To meet the needs for access to data from anywhere, anytime, and any device, while remaining compliant with corporate information security policies and regulatory mandates, companies must classify and encrypt their data. Accurate classification and protection is fundamental to ensure adequate protection of the sensitive data and to ensure it stays secure on the move. Access and usage policies can then be defined based on different classification of data.

### THE SOLUTION

Rights Protection Tool, an add-on to NextLabs' Digital Rights Management solution, provides policy-driven Automated Encryption of Enterprise Data. It works with most common repositories to automatically classify and protect enterprise data in bulk.

Key solution capabilities include:

- **Policy-driven batch rights protection**  
Bulk Classify and protect data in multiple repositories and folders based on complex rules using keywords & metadata in English like sentences.
- **Scheduling rules to run automatically**  
Rules can be executed on demand or can be configured to be executed daily, weekly or monthly.
- **Centralized management and reporting**  
Centrally manage rules and audit reports to understand how data is distributed and stored.
- **Support for wide variety of repositories**  
Supports Windows file systems and a variety of cloud repositories.

### THE RESULTS

Effective data classification and rights management is the cornerstone of good data protection policies. With the NextLabs solution for Automated Encryption of Enterprise Data, customers can enjoy the following benefits:

- Enhance compliance with regulatory mandates, such as data privacy and export control laws, by automatically encrypting data.
- Improve protection of sensitive data through-out its lifecycle wherever it resides and travels.
- Eliminate manual classification and encryption errors, by setting up automatic scheduled or on demand rule executions.

## KEY FEATURES

### Policy-driven bulk rights protection

Write rules to bulk classify and protect different repositories and folders.

### Scheduling rules to run automatically

By scheduling rules to run periodically, ensure that any new data created remains protected and secure.

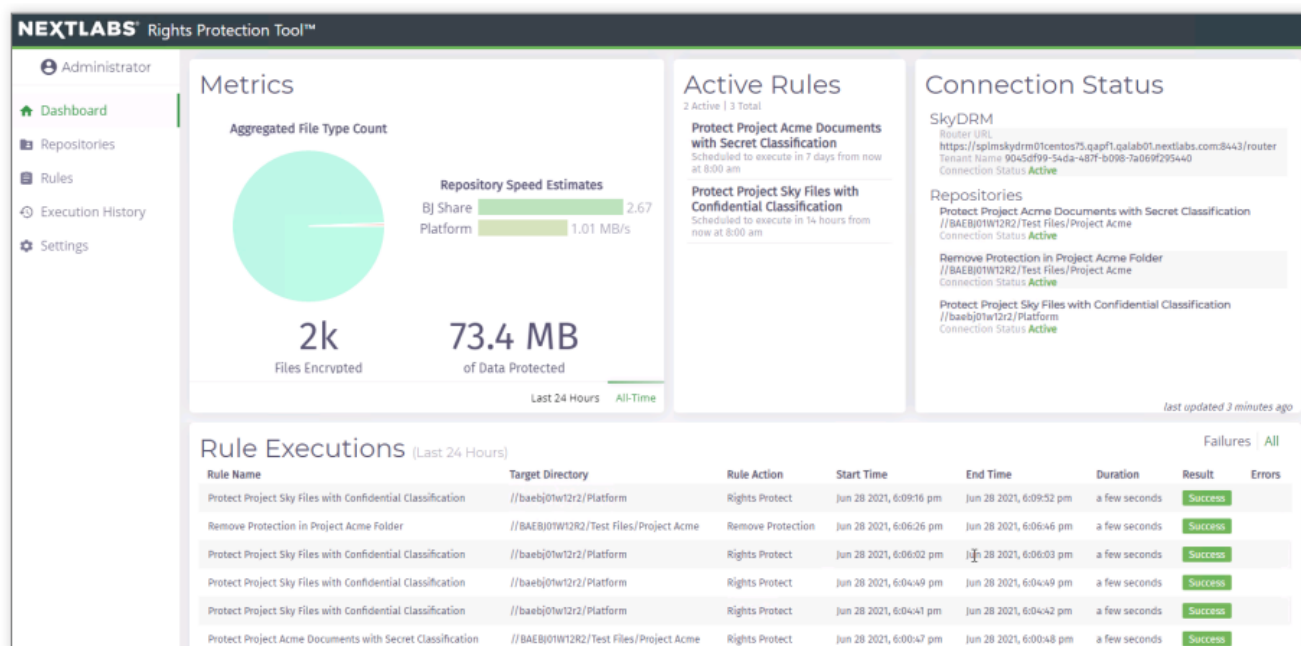
### Centralized Management, reporting & notification

Provide reports based on policy-driven scan results to understand the rule execution and distribution of file types across your storage infrastructure.

### Support for wide variety of repositories

Apply similar rules to data stored in different repositories thus protecting sensitive data wherever it is stored or shared from.

| FEATURE           | SUPPORT   |
|-------------------|---|
| File Repositories | Windows File Server, Microsoft SharePoint On-premise, SharePoint Online, OneDrive for Business, Azure File Storage and CIFS-based file repositories |
| File Formats      | Word, Excel, PowerPoint, PDF, AutoCAD, ZIPs, MSGs, Visio, NXL and hundreds more   |



## 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>.