SkyDRM

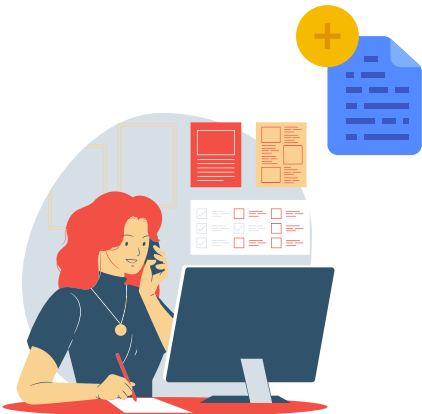Persistently protect files stored and shared anywhere

1

Collaboration: An Essential Need

In a rapidly evolving global economy, enterprises must embrace a **collaborative approach to data sharing** to operate worldwide and foster partnerships.

4

Navigating Extended Sharing

External collaboration exacerbates the **risk of IP leakage,** especially when operating within a global supply chain.

2

Need to Share vs. Need to Protect

This calls for the need to **balance between sharing information** and **safeguarding sensitive assets.**

3

Securing Shared Data

As more collaboration tools become widely available, organizations face the challenge of **protecting data once it is shared beyond the source**.
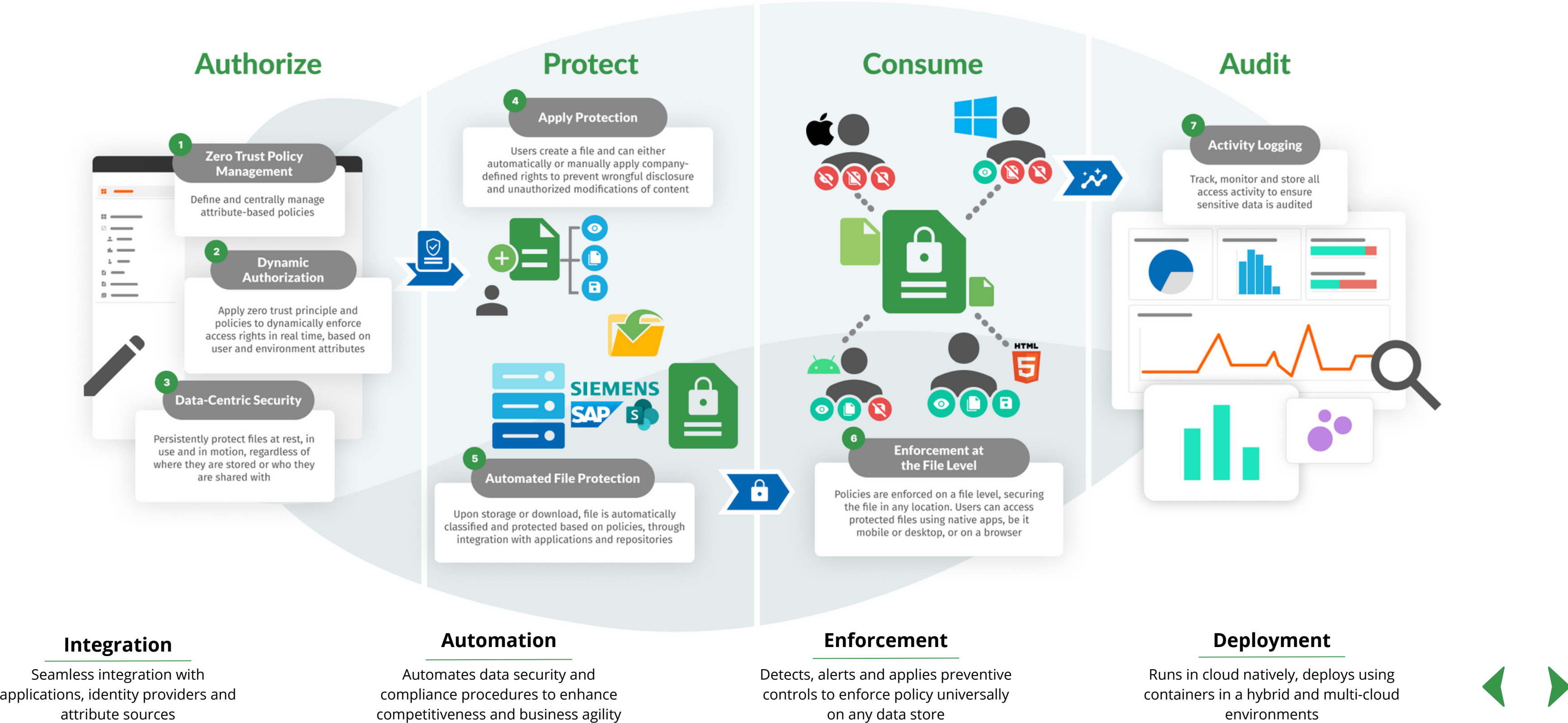
? How do organizations safeguard confidential information, such as trade secrets and IP, **from wrongful disclosure throughout its lifecycle** and **across the extended enterprise?**

Enterprise Digital Rights Management Solution that uses **zero trust principle** to automate persistent protection of sensitive information.
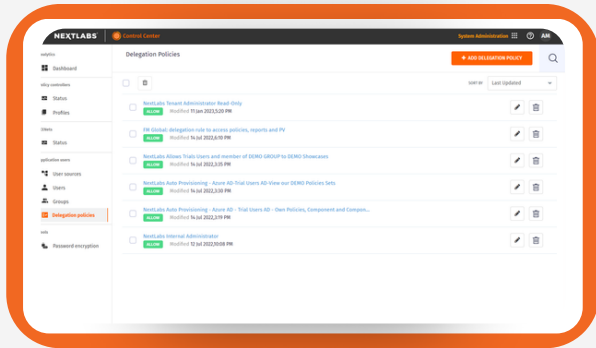
The solution persistently protects files across the information cycle using attribute-based policies. Attribute-based policies dynamically grant permissions for specific actions, such as viewing, editing, copying, forwarding, printing, and extracting content, based on the recipient's identity.
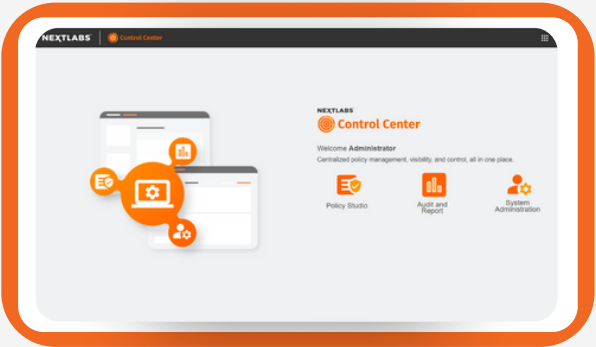

Authorize

1 Zero Trust Policy Management

Define and centrally manage attribute-based policies

2 Dynamic Authorization

Apply zero trust principle and policies to dynamically enforce access rights in real time, based on user and environment attributes

3 Data-Centric Security

Persistently protect files at rest, in use and in motion, regardless of where they are stored or who they are shared with

Protect

4 Apply Protection

Users create a file and can either automatically or manually apply company-defined rights to prevent wrongful disclosure and unauthorized modifications of content

SIEMENS
SAP

5 Automated File Protection

Upon storage or download, file is automatically classified and protected based on policies, through integration with applications and repositories

Consume

HTML 5

6 Enforcement at the File Level

Policies are enforced on a file level, securing the file in any location. Users can access protected files using native apps, be it mobile or desktop, or on a browser

Audit

7 Activity Logging

Track, monitor and store all access activity to ensure sensitive data is audited

---

Integration

Seamless integration with applications, identity providers and attribute sources

Automation

Automates data security and compliance procedures to enhance competitiveness and business agility

Enforcement

Detects, alerts and applies preventive controls to enforce policy universally on any data store

Deployment

Runs in cloud natively, deploys using containers in a hybrid and multi-cloud environments

SkyDRM provides persistent control of access and usage of digital information stored in file regardless of where it exists. It can safeguard and monitor your business-critical document such as intellectual property and product design, wherever it lives or travels – across devices, data centers, apps, cloud services, and on-premises.

Centrally Managed Policies

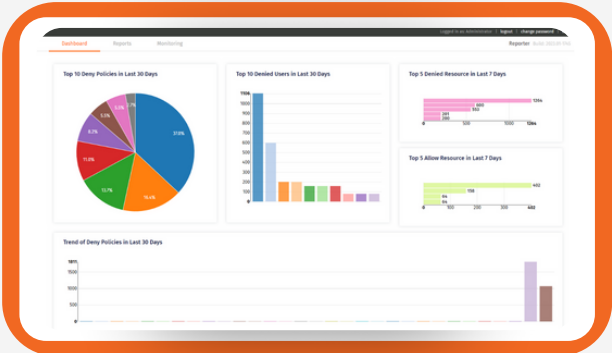Define single policies that can be consistently applied across the entire enterprise.

Dynamic Policy Evaluation

Apply Zero Trust principles to determine who can access what data, and **when** and **where** they can do so in real time
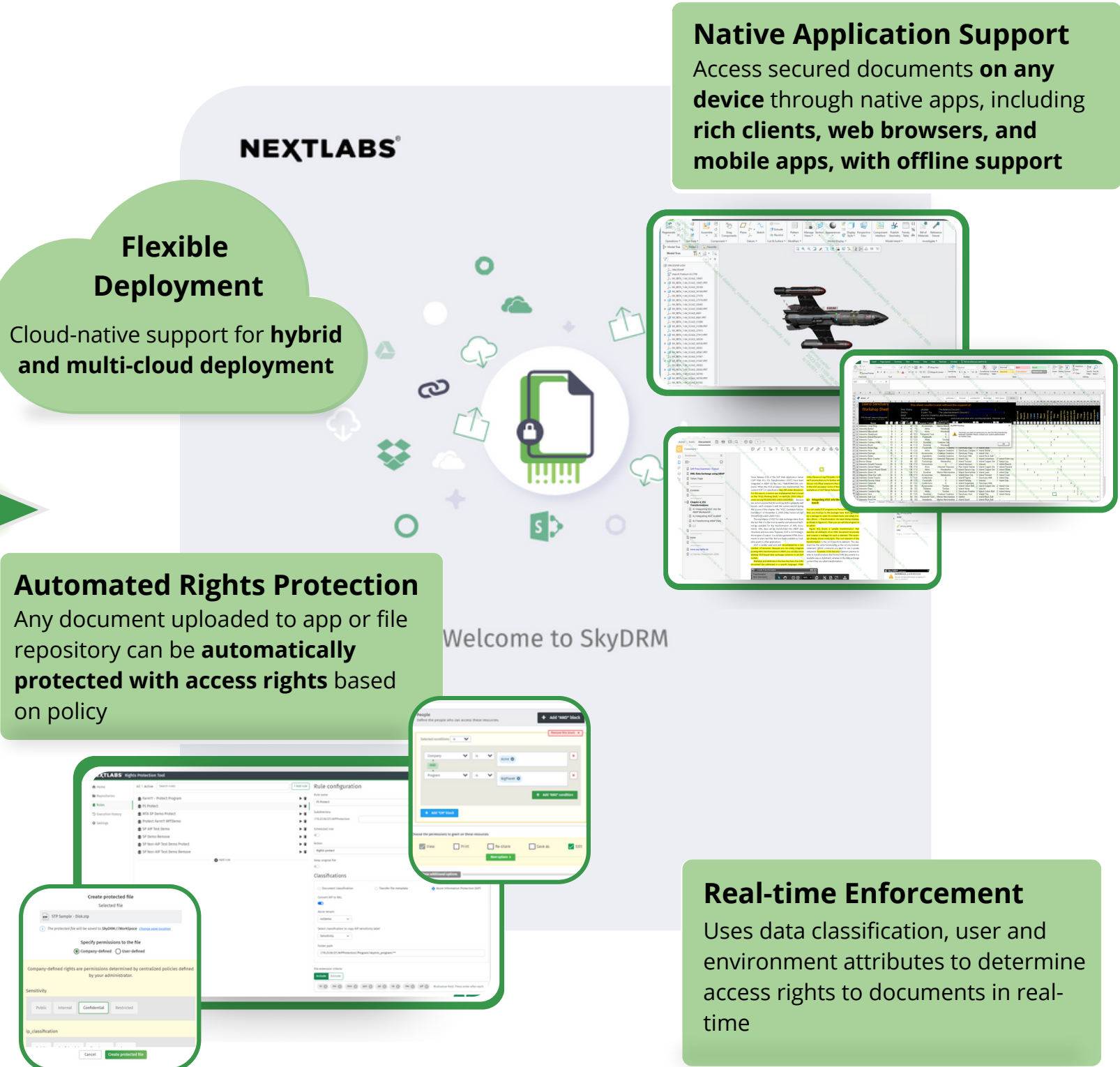
Centralized Monitoring & Auditing

Monitor, track, report, and alert on risky access activity to critical field(s) with the **central activity log**.

Native Application Support

Access secured documents **on any device** through native apps, including **rich clients, web browsers, and mobile apps, with offline support**

File Type Agnostic

Supports any file type, such as Microsoft Office, PDF, CAD, and rich media

Flexible Deployment

Cloud-native support for **hybrid and multi-cloud deployment**

Cross-enterprise Collaboration

Support for **federated identity** to enable frictionless collaboration across organizations

Automated Rights Protection

Any document uploaded to app or file repository can be **automatically protected with access rights** based on policy

Real-time Enforcement

Uses data classification, user and environment attributes to determine access rights to documents in real-time

NEXTLABS®

SkyDRM

Log in to your account

Email Address

Password

Log In

G Continue with Google

Continue with Facebook
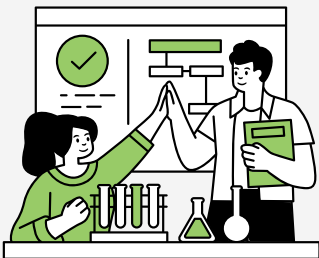
Sign in with Microsoft

Welcome to SkyDRM

SkyDRM Benefits:

Protect IP & Trade Secrets
Provide end-to-end protection across partner networks and prevent data breaches.

Accelerate Collaboration
Utilize fine-grained policies for flexible access, seamless integration preserves workflow without disruptions.

Improve Time-to-Market and Reduce Costs
Leverage global workforce and work with the supply chain more effectively without risking IP leakage.

Enhance Customer Satisfaction
Preserve business relationships by protecting customer and partner data, contracts, and preventing wrongful disclosure.

Ensure Compliance
Monitor and audit access by centrally tracking IP usage across the partner network, providing increased visibility for compliance.

SkyDRM product line provides support for the following systems:

Google Drive, OneDrive, SharePoint, Box, Dropbox

Bentley ProjectWise

SAP ERP

Autodesk AutoCAD

Microsoft Word, Microsoft PowerPoint, Microsoft Excel

Dassault Systems SolidWorks, Dassault CATIA

Siemens NX, Siemens Teamcenter

PTC Windchill, PTC Creo

Deployment Options

SaaS

Private Cloud

aws　Google Cloud
Azure　RED HAT OPENSHIFT Container Platform

On-Premise

NEXTLABS® | Zero Trust
Data-Centric Security

Follow us

www.nextlabs.com/contact-us

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.