



WHAT WE DO

PROTECT CRITICAL ASSETS - YOUR DATA AND APPLICATIONS

NextLabs provides industry-leading security solutions to protect business-critical data and applications. Our data-centric security platform helps you identify and protect critical data, and monitor and control access to that data to prevent security violations caused by information sharing, external breaches and internal misuse.

The proliferation of unsecured data sources containing sensitive information has dramatically increased exposure to data breaches and corporate fraud. Traditionally, organizations have focused on securing the network perimeter to protect sensitive systems and information, but that approach is demonstrably inadequate. Perimeter defenses are porous – they leave sensitive data and applications vulnerable. Furthermore, they do not protect against insider misuse.

Effective protection strategies must incorporate data-centric security as an integral part of an overall security architecture. Data-centric security provides additional controls around the data itself to ensure protection irrespective of device, location, or application.

OUR TECHNOLOGY

Attribute-Based Policy Platform With Dynamic Authorization Technology

At the core of the NextLabs data-centric security suite is our dynamic authorization technology and attribute-based policy platform. The dynamic authorization technology allows organizations to grant authorization in real-time based on information about the user, the action they want to execute, and the resource they want to access. NextLabs Dynamic Authorization defines and automates the enforcement of data security controls, in the form of policies, across all applications, data repositories, and unstructured data. It enables organizations to leverage contextual factors, at the time of request, that influence whether users should be granted permission to access sensitive information and apply them consistently across the organization. These factors, or attributes, may include group, project, classification, device, and network, as well as any other relevant variables.

The attribute-based policy platform provides centralized management of compliance and security controls across all data repositories and applications for enforcement of business and security policies. It enables organizations to automate controls to prevent regulatory and corporate violations, monitor information access and usage, and streamline the audit process.

With a policy-driven model, data security policies can be applied to an application or document to define who can access what data and what actions they are authorized to execute. This model allows you to simplify the access control process, minimizing the number of individual policies needed, and eliminates the need to create roles to address every possible situation. Policies are centrally enforced and can be created or amended easily.

A key component of any robust security strategy is protecting data whether it resides in an application or is being shared – internally or externally. NextLabs incorporates Entitlement Management and Rights Management technology into a unified platform to extend protection to business documents, technical data, and other sensitive corporate information - wherever it resides - at rest, in use, or on the move. Data can be on mobile devices, file servers, content management systems, in the cloud, or shared with business partners.

NextLabs data-centric security solutions, powered by its attribute-based policy platform with Dynamic Authorization technology, provides data protection throughout all stages of the data lifecycle, as well as everywhere data resides, to help organizations prevent breaches and internal misuse. The company currently holds over 50 patents for the policy-based authorization platform to automate the enforcement of security policies to protect data and make information sharing more secure.



Identify & Protect



Monitor & Control



Prevent & Comply

OUR PRODUCTS

Platform - Control Center

Control Center provides the foundation for the NextLabs suite of data-centric security products. The platform allows organizations to enforce, scale, and automate security controls across applications and data repositories so they are consistent and closely aligned to business policies. These automated data access controls are used to enhance the level of security around data and application access, data use, and data sharing across server, client, and cloud applications. Control Center integrates with existing identity management solutions, incorporates data classification, and enforces security controls or policies to eliminate inconsistencies in security policies and to streamline controls. It also provides comprehensive logging, auditing, and reporting capabilities to track all data usage and streamline compliance requirements.

Application Security - NextLabs Entitlement Management

The Entitlement Manager allows organizations to control who has access to what data and what they can do with the data within the application. The solution integrates our attribute-based policy platform with leading enterprise and cloud applications to enhance access control and data security. NextLabs provides out-of-the-box integrations with key applications, including ERP, CRM, PLM, HCM, and SCM, to accelerate time to market and a smooth transition. You can also easily integrate Entitlement Management with your homegrown applications using the Software Developer Kit (SDK).

The solution also leverages Externalized Authorization Management, which centralizes policy management, decoupling it from the application. This enables your organization to make changes to your security policies easily, without making changes to the application directly.

Data Protection - NextLabs Rights Management

Enterprise Digital Rights Management (EDRM) protects sensitive information from unauthorized access when being shared inside and outside the enterprise. Our next-generation Rights Management solution protects any type of file to safeguard all information sharing with suppliers, partners, and the mobile workforce. Documents are protected with a security envelope (encryption) and can then be accessed only by authorized viewers who have specific rights to view, share, copy, and edit. Documents are protected regardless of where they reside - in SaaS applications, document management systems, or file servers. NextLabs EDRM is unique in that it protects any file type, can be accessed from any device, and users do not need to install software to access protected documents. A browser-based model allows for secure access from any device - making adoption simple and highly scalable. Comprehensive tracking of all data usage ensures adequate policies are in place.

NextLabs solutions are pre-integrated with key cloud and enterprise applications such as OneDrive, Dropbox, Box, SAP ERP, Microsoft SharePoint, and Siemens Teamcenter, among others.

OUR SOLUTIONS

SECURE INFORMATION SHARING

- Regulatory Compliance - discover compliance risks, prevent violations, automate procedures, and audit data usage
- Secure Partner Collaboration - protect data in PLM and SCM applications when it is shared with partners and suppliers
- Intellectual Property Protection - keep IP confidential, prevent theft of trade secrets, and protect product information throughout its lifecycle
- Audit and Compliance - monitor information usage, provide analysis and reports, facilitate preparation for audits, and detect anomalies

INDUSTRY

- Aerospace and Defense
- High Tech
- Manufacturing
- Financial Services
- Government
- Chemicals
- Life Sciences, Pharma
- Energy

TECHNOLOGY

- Externalized Authorization Management - decouple authorization from applications to centralize and streamline access management
- Data Classification - automate classification of sensitive data at enterprise scale

Organizations use NextLabs to help achieve business objectives without compromising their most sensitive information. Companies are able to expand globally, consolidate systems, and safely collaborate with their extended enterprise with minimal risk of data breach. The bottom line is enhanced business agility, reduced costs, and greater efficiency. Benefits include:

Increased Security

- Prevent internal or external unauthorized users from gaining access to applications and data and executing fraudulent business transactions
- Gain central visibility, control, and reporting about information access and usage and the ability to detect anomalies

Increased Automation & Operational Efficiency

- Simplify and automate policy creation and implementation; eliminate lengthy manual approvals
- Change policy decisions in real-time with automated workflow to ensure short implementation

Agility & Faster Time to Market

- Easy to integrate with existing applications; no need to make changes to applications to change policies
- Makes the collaboration process more flexible and seamless – facilitates coordination with extended enterprise

Increased Compliance

- Automated policy enforcement and compliance reporting ensures regulatory compliance
- Centralized reporting and audit highlights deficiencies quickly

OUR DIFFERENTIATORS

NextLabs automates protection throughout the information lifecycle, including classification, access control, rights protection, and activity monitoring.

- Patented attribute-based policy platform powered by the Dynamic Authorization engine is the most scalable authorization platform for data-centric security
- Only security solution that protects both data and applications
- Only attribute-based policy solution that is integrated with SAP, Siemens, Microsoft, and other key applications

- Out-of-the-box application and business process integration with key applications on-premises and in the cloud
- Technology leader with over 50 patents issued and more pending
- Technology and platform based on industry standards adopted by NIST and Oasis
- Only application- and file-type-agnostic EDRM solution with browser-based access

STRATEGIC ALLIANCES

NextLabs has strong partnerships with SAP, Microsoft, and Siemens for joint development, sales, and marketing.



NextLabs partners with SAP to provide advanced data-centric security solutions for the SAP ecosystem. NextLabs data-centric security suite consists of Entitlement Manager for SAP, Integrated EDRM for SAP, and Technical Data Export Compliance for SAP. SAP resells the suite globally under the following brands: SAP Dynamic Authorization Management by NextLabs, SAP Technical Data Export Compliance by NextLabs, and SAP Enterprise Digital Rights Management by NextLabs.



NextLabs partners with Microsoft to provide data-centric security solutions to help Microsoft customers protect intellectual property, enable secure collaboration, and enhance audit and compliance. The solution is integrated with SharePoint, Outlook, Exchange, Windows File Server, Windows desktop, and Office 365. NextLabs data-centric security suite for Microsoft consists of Entitlement Manager for SharePoint and Windows File Server, Email Protection for Outlook and Exchange, Data Protection for Office 365, and Desktop Data Protection for Windows.



NextLabs partners with Siemens PLM to provide an end-to-end solution to protect sensitive PLM data throughout the Teamcenter ecosystem. NextLabs Integrated Enterprise Digital Rights Management (EDRM) provides out-of-the-box integration with Teamcenter, CAD tools, and JT2Go to enhance secure information sharing within and outside of Teamcenter. EDRM for Teamcenter is jointly promoted as the solution to protect IP as data is shared with partners, suppliers, contractors, and employees globally.

NextLabs also partners with leading Systems Integrators such as SAP, Siemens, Microsoft, IBM, Infosys, KPMG, Deloitte, and HCL Axon to bring to market data-centric security solutions using industry best practices to meet customers' security, risk, and compliance requirements.

GLOBAL CUSTOMERS

NextLabs customers include some of the largest companies in the Fortune 1000 and organizations with the most stringent and complex data security requirements.



DON'T LEAVE YOUR DATA AND APPLICATIONS VULNERABLE

Data, whether in the application or on the move, is protected throughout the information lifecycle - from initial creation to archiving - in an automated and seamless manner. To find out how you can prevent data breaches and fraud in your organization with NextLabs, please contact info@nextlabs.com.