NEXTLABS®

PRODUCT BROCHURE

Control Center 

# Why a Dynamic Authorization Management Platform?

A Dynamic Authorization Management Platform allows organizations to automate security controls across systems so they align more precisely with policy requirements.

Employees, partners, and contractors are required to handle sensitive corporate information consistent with legal, regulatory, and corporate policies. Enforcing these policies is generally manual and often ineffective, putting a company's information at risk.

**The challenge:** With global business requiring greater speed, agility and information sharing, how can IT improve information control and streamline security management at the same time?

## THE SOLUTION

Companies have traditionally implemented independent identity management, data authorization, and data security silos. These silos forced companies to use a jumble of manual IT and end-user procedures to meet compliance, legal, or corporate policy requirements.

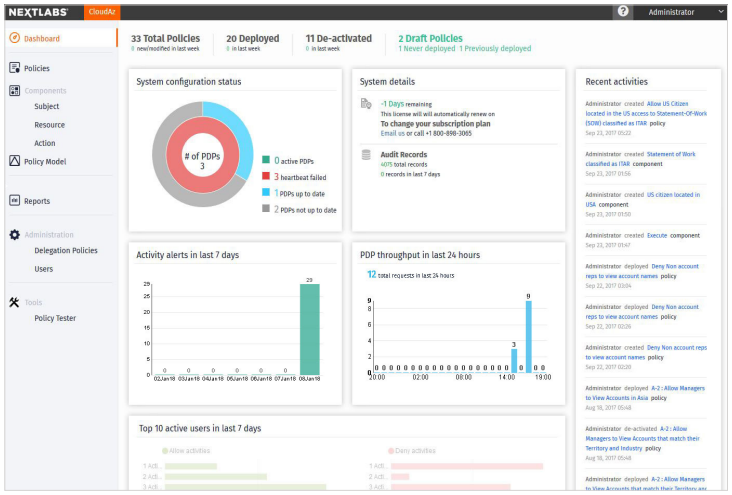
Using Control Center, companies can now coordinate across these silos to align security controls with policy requirements.

## THE RESULTS

- Streamlined compliance
- Application access control
- End-to-end information control
- Reduced security management costs

NextLabs Control Center is a dynamic authorization management platform that turns business policy into automated information controls for data access, use, and sharing across server, client, and cloud applications.

Control Center integrates identity management, data classification, and security controls into unified policies that work across systems and applications to eliminate security silos.




## CONTROL CENTER OVERVIEW

Using Control Center, enterprises can digitally manage policies to govern data classification, access, sharing, and use to automate security and compliance procedures to streamline business processes and improve information control at the same time.

Based on the eXtensible Access Control Markup Language (XACML) standard from Oasis, Control Center easily integrates with IT infrastructure and applications to increase the value of existing identity management, information management, and security management systems.

## POLICY MANAGEMENT FRAMEWORK

Control Center provides a flexible framework to create, manage, and automate compliance, governance, and data security policies. Examples include non-disclosure agreements (NDAs) and acceptable use policies.

### Policy Studio

Policy Studio provides graphical policy development and management that makes it easy for non-technical users to define, test, deploy, and review policies.

### Policy Component Model

Control Center is built on a flexible Policy Component Model that allows policy developers to define reusable components that can be leveraged by business users to translate regulatory and legal requirements into digital policies.

### Robust Policy Lifecycle Management

All policies and components are managed across their lifecycle-from draft to deployment to deactivation. Lifecycle management provides delegated administration, versioning, approval workflow, and full audit trails.

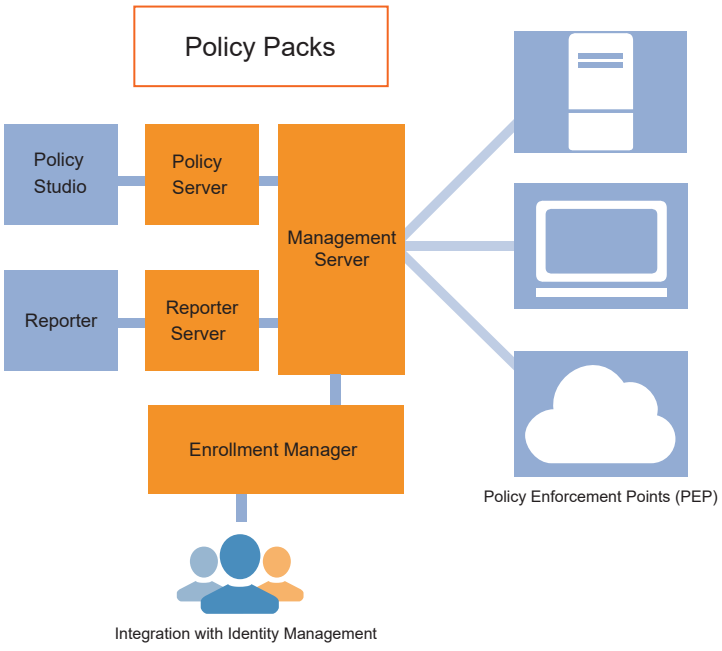
### Fast and Most Scalable Policy Evaluation

Authorization policies can be evaluated across platforms and applications by the Policy Controller, the industry's fastest and most scalable Policy Decision Point (PDP). Using a distributed architecture with patented Smart Deployment technology, the Policy Controller can make decisions in milliseconds with zero network round-trips, completely offline, in server, client, and cloud platforms.

## IDENTITY AND ATTRIBUTE INTEGRATIONS

**Control Center integrates with existing identity infrastructures, including common authentication and identity management systems. Identity attributes or claims can be leveraged in dynamic authorization policies, enabling very granular controls.**

**Using the Enrollment Manager, attributes can be enrolled with the Control Center integration dictionary from a variety of out-of-the box and custom sources, including identity infrastructure, SAML, AD Claims, SharePoint, HR management, and CRM applications.**




## SECURITY CONTROL AUTOMATION

Control Center supports a comprehensive set of policy enforcement points (PEPs), integrated with common information management and endpoint platforms, available from NextLabs and third-party vendors to automate security controls including:

- Dynamic Access Control including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)
- Rights Management including document access control, usage control, and visual markings
- Data Protection capabilities such as entitlement management, application access control, data segregation, segregation of duties, field-level security, and other data-centric security controls
- Communication Control including email, instant messaging, VoIP, and web meetings

## DATA CLASSIFICATION SERVICES

Classification is important for identifying data and applying appropriate control. Control Center includes data classification services to automate data classification tasks including data tagging and content analysis.

## SOFTWARE DEVELOPMENT KIT (SDK)

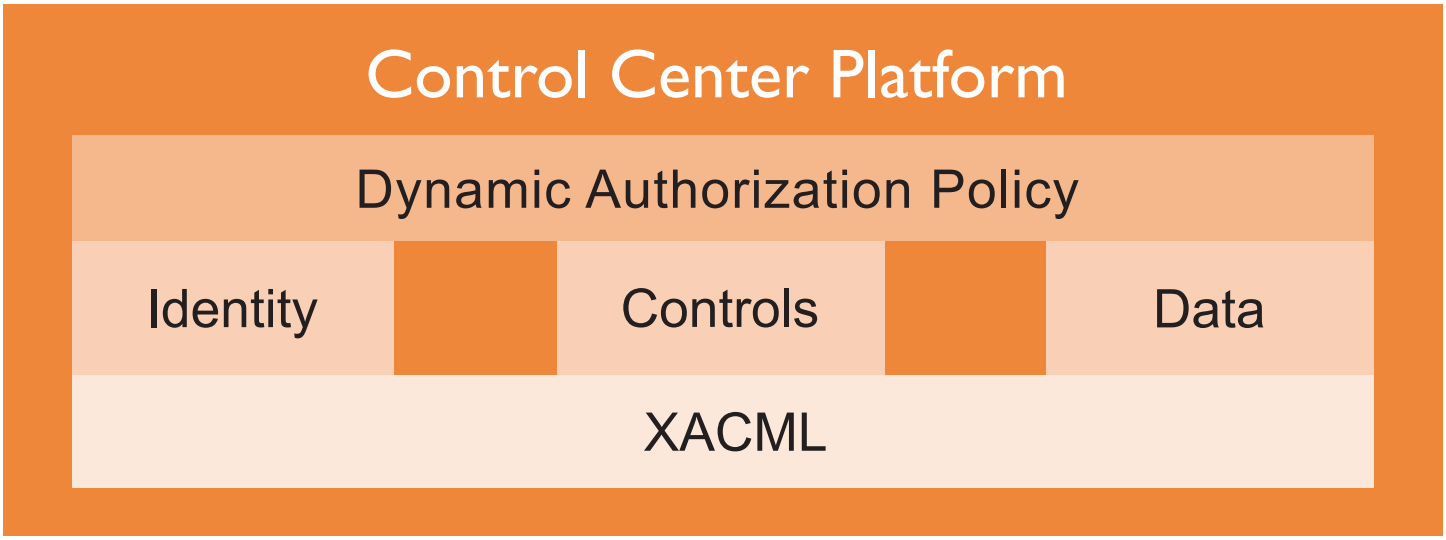
NextLabs' SDK enables the integration of your custom applications into the NextLabs platform. Through this SDK, organizations can enforce security, governance, and compliance policies for their custom applications, just as they can for their "off the shelf" applications, effectively making NextLabs a centralized policy enforcement platform.

## RISK ANALYTICS

Control Center Report Server aggregates information control and usage data, performs analyses, and provides audit reporting across enterprise applications, thereby enabling centralized visibility into information use and compliance risks.

## NEXTLABS INFORMATION RISK MANAGEMENT SUITE

NextLabs Entitlement Management and Rights Management products are built on the Control Center platform, providing companies with out-of-the-box enforcement for common enterprise applications, collaboration systems, and endpoint platforms.

## DEPLOYMENT OPTIONS

Control Center can be deployed either on-premises or in the cloud, ensuring that dynamic authorization can be enforced across all your applications and services, whether they're on-premises or in public, private, or hybrid clouds.

| Category | Feature(s) |
|---|---|
| Policy Lifecycle Management | Delegated Administration, Version History, Approval Workflow, Audit Trail, Deployment |
| Policy Authoring | Point-and-Click Graphical Editor, Policy Component Model |
| Pre-Built Information Controls | Dynamic Access Control |
| | Integrated Rights Management |
| | Communication Control |
| | Application Control |
| | Device Control |
| | Network Control |
| Policy Evaluation | Distributed Policy Controller, Dynamic Access Control Bridge |
| Data Classification Services | Document Tagging, Classification Analysis Services |
| Audit and Reporting | Information Control Audit, Information Control Activity Reporting |
| Pre-Built Identity Integration | Active Directory, AD Claims |
| | LDAP, SharePoint, SAP, Tivoli Identity Manager, Oracle Identity Manager, LDIF file, SAML |
| Platform Extensibility | Custom Information Control, Policy Enforcement Point SDK, Custom Obligation, Policy Language Extension, Identity Enrollment Adapter SDK, Activity Journal SDK |

## ABOUT NEXTLABS

NextLabs provides data-centric security software to protect business-critical data and applications. Our patented dynamic authorization technology and industry-leading attribute-based policy platform help enterprises identify and protect data, monitor and control access to sensitive data, and help prevent regulatory violations—whether on the cloud or on premise.

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.

For more information on NextLabs, please visit **http://www.nextlabs.com**

NEXTLABS®