

Enterprise Entitlements Management

Centrally audit and manage fine-grained authorization across all file servers, portals, and document management systems in the enterprise to reduce administrative and audit costs



Controlling access to applications and data is critical for enterprises to demonstrate and maintain compliance and assure information integrity. Today's companies face the critical challenge of managing not only access to data within databases or enterprise applications, but also fine-grained entitlements to application functions and unstructured data across hundreds of applications, file servers, desktops, portals, and document management systems.

THE SOLUTION

The Enterprise Entitlements Management Solution, based on Compliant Enterprise®, allows companies to centralize and standardize the management of entitlements across unstructured data repositories. The Solution immediately helps organizations reduce the cost of administration; simplify the audit of authorizations for compliance; and enable IT to react quickly to business changes, regulations, or legal inquiries.

SOLUTION HIGHLIGHTS

- **Lower Cost of Administration**
Centrally-managed, fine-grained entitlements to unstructured data & applications
- **Comprehensive Coverage**
Includes applications and data on file servers, desktops, portals, and document management systems
- **Simplifies Compliance Audit**
Lowers the cost of authorization and activity audit, incident investigation, or legal discovery
- **Out-of-the-Box Deployment**
Includes pre-built connectors to commercial applications and systems for immediate deployment

USING THE SOLUTION, COMPANIES CAN:

Identify resources including data residing on file servers, desktops, and SharePoint sites, lists and document libraries

- Centrally audit the access rights or authorizations to these resources
- Centrally audit the actual user activity on these resources, and
- Centrally define and apply fine-grained role- or rule based entitlements to these resources.

The Solution includes out-of-the box connectors to common applications and systems, allowing quick deployment, without costly custom integration. Further integration into customer applications can be achieved using the Compliant Enterprise Software Development Kits (SDKs). Entitlements that Understand Business Context Managing entitlements is difficult when devices, data, and users are mobile, or if users, customers, partners, and supply chains are spread across multiple locations. The Solution allows entitlements to be described using context—such as identity, data type and activities, and business conditions—to align with business policy.

The Solution includes:

■ Authorization Audit

Analysis of who is authorized to access applications and data across systems. Centralized entitlements simplifies the process of auditing data and application authorization for governance or compliance audits.

■ Activity Audit

Analysis of authorized user activity on data and applications across systems. User activity, including access and usage of data, is collected and analyzed in a single activity journal. Reporting tools simplify incident investigation and legal discovery.

■ Risk Assessment

Analysis of information risk based on industry best practices, regulatory requirements, and analysis of access and activity data. This helps organizations identify the areas of greatest risk to prioritize and focus remediation projects.

■ Least Privilege Analysis

Analysis of authorization and activity data to identify over- or under- privileged resources. Helps organizations tighten security over critical functions or data.

■ Centralized Entitlements Management

Centralized management of e-grained, role- or rule-based authorization, based on policy. Eliminates the need to manage authorizations across multiple application and data silos.

Solution Deployment: How to Get Started Today

NextLabs implements the Solution by using expert product knowledge and a services best practices methodology. NextLabs can also assist clients with identifying their controlled data, as well as defining information control policies.

Step 1: Requirements Gathering

NextLabs works with you to understand your infrastructure, and security & policy requirements.

Step 2: Risk Assessment

We help you discover and identify current risks to help prioritize solution requirements with clear visibility into your environment.

Step 3: Policy Configuration

Entitlements are designed and electronically codified

Step 4: Install Connectors

Connectors are deployed across applications and systems, if applicable to requirements.

Step 5: Knowledge Transfer

Finally, NextLabs helps train your team to maintain the Solution.

ABOUT NEXTLABS COMPLIANT ENTERPRISE®

Compliant Enterprise is an extensible, XACML-based entitlement management system that allows enterprises to develop, administer, enforce, review, and audit the same fine-grained access policies and authorizations across heterogeneous applications. Easy-to-use, graphical policy tools and a high-level business policy language eliminate the need to translate business policy into code, allowing business users to directly manage entitlements. The software reduces the cost of custom rules development and policy administration, while streamlining audits.

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

© NEXTLABS INC. ALL RIGHTS RESERVED