NEXTLABS

Entitlement Management

DATASHEET

Entitlement Management for Microsoft Dynamics 365

Enterprise applications contain sensitive information that needs to be protected but remain accessible. CRM applications contain some of the most sensitive information in a company. However, organizations need to consider a variety of factors before granting permission to view highly sensitive information – customer status, revenue, support issues - but this level of scrutiny cannot jeopardize the pace of business or the ability to access 24/7. NextLabs Entitlement Management seamlessly provides and additional layer of protection with fine-grained access control, to protect critical data.

KEY FEATURES

Attribute Based Access Control (ABAC)

ABAC enables fine-grained access controls which are granted dynamically based on characteristics, or attributes, about the user, data and environment. Authorization policies, defined as human readable business rules, determine which data a user can view and which business transactions they can perform in Dynamics 365. Decisions are made using a variety of attributes, including the user, account, lead, opportunity, and environment. A simple policy may state that account executives can view and edit accounts, leads, and opportunities that belong to the industry, region, and size of company for which the user is responsible.

Dynamic Runtime Policy Enforcement

Authorization policies are evaluated based on the attributes and dynamically enforced at runtime. This means that administrators no longer need to maintain and keep track of role, permission, and data ownership assignments as users move between departments, territories, locations; when accounts, campaigns, or support cases are modified; or as other conditions and attributes change. Attributes can be retrieved at runtime from a variety of sources, including but not limited to Dynamics 365, HR and Identity Management systems, Azure AD, LDAP servers, APIs and web services.

Row Level Data Filtering

Users can only view accounts, opportunities, leads, contacts, support cases, or other entities for which they have been authorized. Access can be determined based on the location, department, position, project assignment or any other attribute of the user, which can then be compared against the attributes of each business object and record such as the region, revenue, support case severity, sensitivity, or any other information about the record.

Policy Enforcement Across Related Entities

Authorization policies can also be inherited and enforced across related entities or business objects. For example, an account executive can only access opportunities and leads for the accounts that they have been authorized to view.

Field Level Data Redaction & Masking

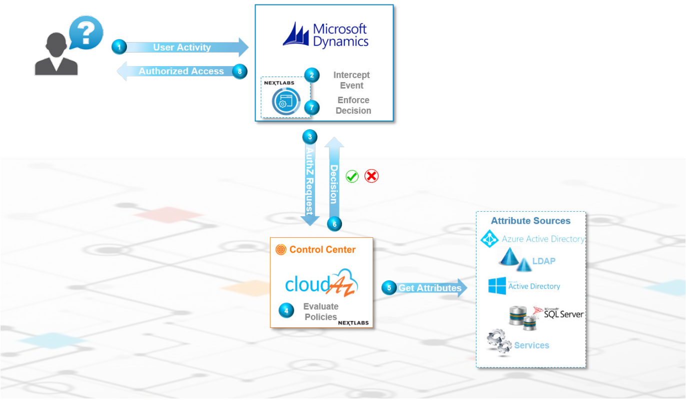
Authorization policies can be defined to redact and mask sensitive fields on a row by row level. For example, an account executive can only see the social security number and date of birth for contacts that they created. Authorization policies can also be inherited and enforced across related entities or business objects. For example, an account executive can only access opportunities and leads for the accounts that they have been authorized to view.

Preventative Runtime SoD Enforcement

NextLabs removes the risk of fraud by enforcing segregation of duties to prevent compliance violations and conflicts of interest. This is accomplished by the dynamic evaluation of policies and attributes at time of request.

Secure Business Transactions

With NextLabs, users can be given permission to view a set of accounts and other entities, but only authorized to edit, create, and delete a subset of these records. An account executive may be given the permission to view all accounts in North America, while only allowed to create, edit, and delete accounts that belong to the west coast region and financial services industry.



Centralized Policy Management

NextLabs allows you to centrally manage and review authorization policies across your applications and services. For example, a policy that determines what accounts a user can view in Dynamics 365 can also control that the user can only access documents in SharePoint related to those accounts.

Centralized Audit & Monitoring

The solution tracks and stores user activity and data access across Dynamics 365 and other applications and services in a central audit server. Insight into user behavior and access patterns is provided through dashboards, reports and automated monitoring facilities.

SaaS, Private Cloud, and On-Premise Deployments

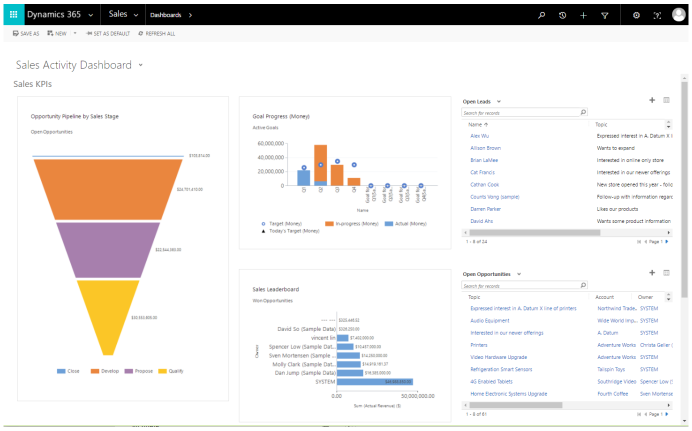
NextLabs is available for SaaS and on-premise deployments of Dynamics 365.

KEY BENEFITS

NextLabs advanced security solution for Dynamics 365 provides you with the foundation to protect all your Microsoft cloud and on premise enterprise applications and can scale as your enterprise grows. The benefits of more advanced access control in Dynamics 365 CRM include:

- **Secure Access** to the most sensitive customer information by leveraging more detailed information about who is accessing what data and when.
- **Increased Business Agility** by minimizing manual changes and eliminating code changes to adapt to changes in user status or the business environment.
- **Automated Security Controls** to simplify data access governance, ensure enforcement, eliminate mistakes, and reduce administration.
- **Comprehensive Visibility and Reporting** into events and data access for audit, oversight, and troubleshooting. Identify anomalies before they become major breaches.

NextLabs Entitlement Manager for Microsoft Dynamics 365 CRM is a data-centric security solution that seamlessly integrates with Dynamics to provide a more granular level of information governance to safeguard your most sensitive customer information. NextLabs provides an attribute-based policy platform to automate security controls in the application to ensure only authorized users have access to sensitive data. The platform extends the base level security controls in Dynamics to create a more robust and consistent mechanism to keep your data safe.



Open Leads

Name ↑	Topic
Alex Wu	Expressed interest in A. Datum X li
Allison Brown	Wants to expand
Brian LaMee	Interested in online only store
Cat Francis	Interested in our newer offerings
Cathan Cook	New store opened this year - follo
Counts Vong (sample)	Follow-up with information regarc
Darren Parker	Likes our products
David Ahs	Wants some product information

Open Opportunities

Topic	Account	Owner
Expressed interest in A. Datum X line of printers	Northwind Trade...	SYSTEM
Audio Equipment	Wide World Imp...	SYSTEM
Interested in our newer offerings	A. Datum	SYSTEM
Printers	Adventure Works	Christa Geller (
Video Hardware Upgrade	Adventure Works	SYSTEM
Refrigeration Smart Sensors	Tailspin Toys	SYSTEM
4G Enabled Tablets	Southridge Video	Spencer Low (S
Home Electronic Systems Upgrade	Fourth Coffee	Sven Mortense

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

© 2007-2017 NEXTLABS INC. ALL RIGHTS RESERVED