NEXTLABS®

DATASHEET

Entitlement Management

Entitlement Manager for Slack

THE SITUATION

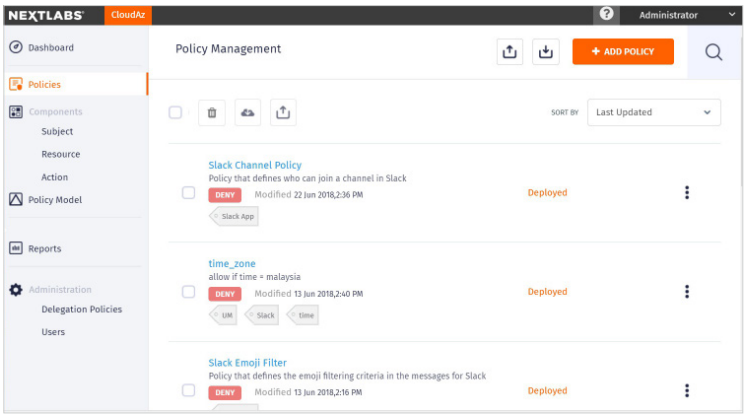
Slack is a cloud-based application that allows team members to collaborate on projects in real-time and to share documents, images, videos, and other data. It is available as a standalone app for desktops, mobile devices (Android, iOS, and Windows), and via web browsers. Slack provides public and private channels whereby users can sign up either on their own or by invitation.

However, this model becomes too cumbersome and difficult to manage for organizations with large numbers of users. Because a channel is often created so teams can collaborate on a common project, security policies need to be created to control which users are allowed to participate, thereby minimizing the risk of sensitive data leakage.

OVERVIEW

CloudAz is the industry-leading cloud authorization service that provides dynamic authorization and attribute-based access control (ABAC) for managing access to enterprise resources. With Entitlement Manager for Slack (EM for Slack), organizations can integrate CloudAz into their existing Slack instance, enforcing CloudAz policies to secure Slack channels.

EM for Slack enables support for controlling access to channels based on attributes. For instance, you can have a policy such that only users that belong to certain departments are allowed to join a given channel. Additionally, organizations can leverage additional custom attributes of CloudAz to enforce access rules with associated security and data governance policies.



Setting policies for Slack

KEY FEATURES

Attribute-Based Access Control (ABAC)

ABAC solutions control access to data, business transactions, and batch processes based on policies that examine attributes of the data being accessed, the context of the request, and the user's identity. EM for Slack takes into account any changes in the attributes of the data or the user and dynamically applies the relevant policies to enforce fine-grained access controls across a wide range of business functions.

This flexibility greatly streamlines change management processes by reducing the need to develop customized code to modify existing roles every time they must be updated, i.e., to account for changes in a user's business function, organizational assignment, location, etc.

Centralized Policy Management

Authorization policies stored in CloudAz, NextLabs' cloud-based centralized policy server, can be managed directly by data or compliance owners with simple natural language statements (i.e., no need for any coding expertise). CloudAz allows you to centrally manage and review authorization policies across all your applications and services, not just for Slack applications. For instance, the same policy can enforce which specific channels a user can access in a Slack workspace and also which records in Salesforce Service Cloud that are related to those events.

Dynamic Runtime Policy Enforcement

EM for Slack's policy engine performs evaluations dynamically using the real-time value of the attributes specified in the policies to determine if a user is authorized to access the data at runtime or perform the business transaction in question. This eliminates the need for administrators to maintain and keep track of roles, permissions, and data ownership assignments as users move between departments, territories, or locations, or as other conditions and attributes change.

Granular Channel Filtering

EM for Slack ensures that users can only view messages they have been granted access to. Authorization can be determined based on the industry, location, department, position, project assignment, or any other attribute of the user, which can then be compared against other attributes of an entity or record such as data type, project name, etc.

Safeguarding of Business Communications

Users can be given permission to access a set of channels that are relevant to their job functions. For instance, an engineering manager may be given permission to view the company's product and quality assurance channels, but a product tester can only access the quality assurance channel.

Enforcement of Role Segregation

EM for Slack enables the creation and enforcement of role segregation policies across all Slack channels in real-time. For instance, a company allows Engineering and Support to view support-related channels. However, corporate policy dictates that Engineering has view-only rights to the messages and only Support personnel can create the messages.

Centralized Audit and Monitoring

EM for Slack tracks and stores user activities and data access across all Slack and non-Slack applications in a central audit server, simplifying compliance management.

Analytics for user behavior and access patterns are provided via dashboards, reports, and automated monitoring facilities.

KEY BENEFITS

EM for Slack is a scalable data security solution that protects your Slack data in real-time. Benefits include the following:

- **Protect sensitive data**
  Leverage a transaction- and data-level access management system to secure access and protect data across all Slack channels. The add-on's policies control access to business functions and sensitive customer data based on attributes such as data classification, environmental information, user roles and metadata, location, and client system.

- **Ensure compliance**
  Create information barriers to segregate regulated data or between confidential projects to avoid data spills or contamination. Manage, educate, enforce, and audit access policies to sensitive corporate data to ensure compliance with regulations such as GDPR, SOX, and HIPAA.

- **Streamline compliance**
  Automate the process of auditing authorization and data access to demonstrate compliance to auditors, regulators, and customers. The add-on for Slack provides comprehensive visibility about who is accessing what data and when, identifies anomalies before they become major breaches, and monitors and tracks events for audit, oversight, and investigation.

- **Reduce security and compliance management costs**
  Eliminate the need to implement and maintain costly customizations to meet security, compliance, and governance requirements. Attribute-driven dynamic authorization eliminates the need to maintain multiple Slack instances or manage individual authorization or user groups.

- **Improve business agility**
  The add-on works natively with Slack and manages authorization logic through an externalized, standards-based policy framework. As a result, this slashes application development time and automates change management processes, thereby enhancing business agility.

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

NEXTLABS®