NEXTLABS®

Data Access Enforcer for Atlassian JIRA

Control Global Data Access from Anywhere

OVERVIEW

As companies adopt agile methodologies and scale their operations, Atlassian JIRA has become a critical tool for project management and workflow automation. It allows teams to efficiently track, prioritize, and manage development tasks, making it indispensable for organizations in fast-paced industries. However, JIRA's central role in handling sensitive project information, such as customer data, internal documentation, and intellectual property, has made data security a growing concern. The vast amount of data stored within JIRA, combined with its integration into other systems and CI/CD pipelines, exposes companies to potential security risks, such as unauthorized access, data breaches, or insider threats.

Protecting data within JIRA requires more than simple access restrictions. As teams collaborate across departments and regions, the need for robust security controls, such as attribute-based access controls (ABAC), encryption, and dynamic authorization, becomes essential. Additionally, JIRA's integrations with various development and communication tools can increase the risk of vulnerabilities if not properly secured. Since JIRA is often deployed in conjunction with other Atlassian products, like Confluence, Bamboo, and BitBucket, policies must be consistently enforced across all products. Companies must ensure that they have stringent data protection protocols in place, safeguarding both internal and customer information. By embedding data security into their JIRA environments, organizations can mitigate the risk of data breaches, maintain compliance with industry regulations, and foster trust with their stakeholders in an increasingly connected world.

THE SOLUTION

NextLabs Data Access Enforcer for Atlassian JIRA provides dynamic data-level security controls and fine-grained data access governance for data in JIRA and other Atlassian products like Confluence, BitBucket, and Bamboo. This complements the protection provided by JIRA's built-in access controls. Through NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based policy and centralized policy management to improve their security and compliance posture for JIRA. DAE for Atlassian JIRA enforces policies based on the user's identity, enforces data-level security controls such as field level data masking and record level data segregation, and monitors data access activity, all within the data access layer of Atlassian JIRA.

DAE for Atlassian JIRA prevents unauthorized access to data in JIRA through fine-grained data-level security controls, protecting data and addressing compliance requirements. DAE for Atlassian JIRA enables organizations to secure data stored within the JIRA platform with a seamless integration deployed with zero code and no disruption to existing Atlassian JIRA systems.

THE BENEFITS

DAE for Atlassian JIRA provides the following benefits:

- Externalize authorization management to simplify and reduce the time spent on administering access control policies
- React more rapidly to changes in business requirements, market conditions, or regulatory environment with policy changes that can be made without code changes or application downtime
- Lower your total cost of ownership by leveraging your existing investment in the NextLabs platform
- Reduce the cost of compliance through more efficient and cost-effective monitoring and auditing of your data

Key Features

Feature	Detail
Real-time enforcement of attribute-based access policies	Access to data based on policies that examine attributes of the data being accessed, the context of the request, and user identity. DAE dynamically applies the relevant policies, factoring in changes in the attributes of data or the user to enforce fine-grained entitlement and security controls to data regardless of where or how the data is being accessed. Rules are validated in real-time when a user attempts to access data, only then granting access.
Field-Level Data Masking	DAE ensures that users can only view the fields on the record to which they have been granted access, dynamically masking the value of the field for which users are not authorized. It uses policy-driven approach to mask the data in the unauthorized fields based on attributes at the time of data access. These centrally managed policies define masking patterns and rules to determine who, what, when, where, and why to mask field(s) in real-time.
Format Preserving Encryption (FPE) Data Masking	Data can be masked at rest or in motion such that the masked data preserves the length and format of the original data, making the masking non-obvious to unauthorized users and maintaining application dependencies. Masking can be reversed to allow authorized users to view the original data. DAE for Atlassian JIRA includes a built-in FPE library or can integrate with 3rd party encryption tools. DAE's Bulk Obfuscation Tool (BOT) makes applying FPE masking at rest consistent and straightforward across all affected tables and fields pre- and post-implementation of DAE.
Record-level Data Segregation and Filtering	DAE ensures that users and entities can only view records or data they are authorized to access and that sensitive records are excluded. 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 sensitivity level, type of transaction, etc. For example, development or support tickets within JIRA may contain sensitive data that should only be accessed by a restricted group of users. Those repositories can then be excluded when other users or entities attempt to access them.
Centrally Managed Policies	Authorization policies can be centrally managed and reviewed across all an organization's applications, substantially reducing administration costs.
Centralized Logging, Monitoring, and Auditing	DAE tracks and stores user activities and data access across all 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.
Out of the Box Integration	DAE for Atlassian JIRA integrates with Atlassian JIRA systems through an application extension with no custom code required. Data models incorporate Atlassian JIRA's object structure for seamless integration.

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust 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, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.