NEXTLABS®

servicenow

Application Enforcer for ServiceNow

Enforce ABAC & Externalize Authorization

OVERVIEW

ServiceNow is a SaaS vendor that focuses on the IT Services Management, IT Operations Management, and IT Business Management segments. However, ServiceNow also has offerings for software asset management, performance analytics, security operations, HR service delivery, customer service management, and GRC (Governance, Risk, and Compliance) – benefiting stakeholders enterprise-wide.

ServiceNow's core mission is to help companies work smarter and faster by automating many of the processes that employees need to do their jobs and be productive. In order to achieve this, organizations must first overcome several challenges, such as gaining control over their IT management processes, consolidating legacy applications, and aligning IT to strategic business objectives.

Yet, while conquering these challenges, organizations must still be mindful of protecting their most valuable asset: their data. As businesses move forward on their process automation projects, they also have to consider the impact of a more distributed workforce, the proliferation of mobile and cloud technologies, mergers and acquisitions (M&A) activities, or perhaps new regulatory requirements. All of these underscore the need for a dynamic approach to data security that allows sufficient flexibility for businesses to achieve their objectives while also safeguarding valuable data.

THE SOLUTION

NextLabs Application Enforcer for ServiceNow provides granular access control and data governance for ServiceNow applications. Through NextLabs' patented Dynamic Authorization platform, organizations can leverage attribute-based access control and centralized policy management to improve their security and compliance posture for ServiceNow.

THE RESULTS

Application Enforcer for ServiceNow is a scalable data security solution that protects your ServiceNow 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 ServiceNow applications. Application Enforcer for ServiceNow's policies control access to business functions and sensitive customer data based on attributes such as records' field values, user roles, and metadata stored in ServiceNow
- **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. Application Enforcer for ServiceNow 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 ServiceNow instances or manage individual authorization or user groups.
- **Improve business agility -** Works natively with ServiceNow 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.

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. Application Enforcer for ServiceNow 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. For instance, with Application Enforcer for ServiceNow, you can set up policies to ensure that Access Control List (ACL) rules cannot be overwritten or that the record owner always has the right to access records owned by him or her.

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' cloudbased 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 ServiceNow applications.

Dynamic Runtime Policy Enforcement

Application Enforcer for ServiceNow'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; when accounts, incidents, or events are modified; or as other conditions and attributes change.

Granular Data Filtering

Application Enforcer for ServiceNow ensures that users can only view requests, incidents, or other data 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 incident severity, type of issue, etc. For example, you can filter data in charts and reports to quickly identify and troubleshoot the root cause of a given service issue.

Safeguarding of Business Transactions

Users can be given the permission to view a set of accounts and other entities while being authorized to edit, create, and delete a subset of these records. For instance, a finance manager may be given permission to view detailed cost information on all IT projects in North America but only allowed to create and edit information for security-related IT projects in California and Oregon.

Enforcement of Role Segregation

Application Enforcer for ServiceNow enables the creation and enforcement of role segregation policies across all ServiceNow applications. For instance, a company has two types of IT service management users: IT professionals and business process owners. The former should be able to view and work on all incidents; however, the latter should only be permitted to view incidents related to their business area and not be allowed to work on technical incidents.

Centralized Audit and Monitoring

Application Enforcer for ServiceNow tracks and stores user activities and data access across all ServiceNow and non-ServiceNow 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.

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.