NextLabs Releases Salesforce and Snowflake Enforcers for Data Masking, Segregation, and Policy-Based Access Control

NextLabs extends Zero Trust data security to leading enterprise cloud platforms with centralized, attribute-based authorization and real-time data protection



NextLabs Announces the Release of Enforcers for Salesforce and Snowflake to Protect Sensitive Data with Dynamic Data Masking, Logical Data Segregation, and Policy-Based Access Control

SAN MATEO, CA, UNITED STATES, September 29, 2026 / EINPresswire.com/ -- NextLabs, a leader in Zero Trust data security and dynamic authorization solutions, today announced the availability of NextLabs Enforcer for Salesforce and NextLabs Enforcer for Snowflake, extending fine-grained, policy-driven data security to two widely used enterprise cloud platforms. This expands NextLabs existing support for enterprise applications and cloud data platforms such as ServiceNow, Microsoft 365, Dynamics 365, Databricks, AWS S3, and Azure Storage.

Salesforce and Snowflake have become critical repositories for sensitive customer, financial, operational, and business information. As organizations increasingly rely on these platforms to support business operations, analytics, and collaboration, security teams require more granular controls than traditional roles, permissions, and static authorization mechanisms can provide.

NextLabs Enforcer for Salesforce and Enforcer for Snowflake extend Zero Trust principles to these environments by externalizing authorization and evaluating access requests dynamically based on identity, data, organizational, environmental, and business attributes. The solutions enable organizations to control not only whether users can access data, but also which records they have access to, which sensitive fields they can view, and which individuals are explicitly authorized to update protected information.

“Organizations are moving more critical business data into cloud applications and data

platforms, but traditional authorization models can make it difficult to enforce consistent, fine-grained policies as business conditions change," said Keng Lim, CEO of NextLabs. "Enforcer for Salesforce and Enforcer for Snowflake extend our Zero Trust data-centric security approach across on-premises, cloud, and hybrid environments, enabling organizations to centrally manage authorization policies and dynamically protect sensitive information without extensive application customization."

NextLabs Enforcer for Salesforce
NextLabs Enforcer for Salesforce extends Salesforce with dynamic, policy-driven authorization based on Attribute-Based Access Control (ABAC), centralized policy management, dynamic record filtering, runtime data masking, and policy-driven information sharing.

The solution evaluates authorization requests in real time using attributes describing the user, requested data, business transaction, environment, device, location, data classification, and organizational context. This enables organizations to dynamically determine which Salesforce records users can access and which sensitive fields should be masked.

NextLabs Enforcer for Snowflake
NextLabs Enforcer for Snowflake provides fine-grained data access control, dynamic data filtering, dynamic data masking, and policy-driven information governance for Snowflake. The solution places a Policy Enforcement Point between Snowflake clients and the Snowflake service and evaluates access requests using user, resource, SQL, and business context.

Enforcer for Snowflake enables organizations to apply Zero Trust principles to Snowflake data by dynamically evaluating access requests and enforcing centralized ABAC policies across supported Snowflake interfaces.

Key capabilities of NextLabs Enforcers for Salesforce and Snowflake include:

- Real-Time Attribute-Based Access Control (ABAC) evaluates access and authorization requests using attributes such as resource, user, organizational unit, job function, geography, project membership, data classification, customer ownership, and other business context.
- Dynamic Data Filtering limits query results to only the records users are authorized to access, based on identity, organizational attributes, geography, business unit, project membership, data classification, and other policy attributes.
- Dynamic Data Masking conceals sensitive fields while allowing users to work with authorized datasets. Supported information types include PII, customer identifiers, financial information, employee information, pricing information, and confidential business information.
- Centralized Policy Management using NextLabs CloudAz enables consistent authorization policies across Salesforce, Snowflake and other enterprise applications, cloud services, databases, and data repositories.
- Policy Enforcement Across Interfaces, including Web Console, CLI, and REST API.
- Fine-Grained Business Transaction Authorization can distinguish between viewing, creating,

updating, deleting, approving, and administrative actions.
- Allowed User List Obligations to restrict access to highly sensitive datasets or designated operations to specifically identified users or groups.
- Segregation of Duties Enforcement applies policy-based separation of responsibilities to sensitive data and operations.
- Centralized Audit and Monitoring providing visibility into access requests, resources, policies evaluated, and authorization outcomes to support security investigations, compliance reporting, and ongoing policy monitoring.

By externalizing authorization from Salesforce and Snowflake and applying dynamic policies at the point of access, NextLabs enables organizations to implement least-privilege access, reduce data exposure, simplify security administration, and adapt data protection policies as users, organizational responsibilities, business requirements, and regulatory requirements change.

Together, Enforcer for Salesforce and Enforcer for Snowflake expand NextLabs' data-centric security approach across enterprise applications and cloud data platforms, helping organizations consistently apply Zero Trust authorization and data protection policies across diverse business environments.

Tony Berning
NextLabs
+1 650-577-9101
email us here
Visit us on social media:
LinkedIn
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/945277930

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.