

NextLabs Announces Data-Centric Security for AWS S3 with Fine-Grained ABAC and Dynamic Data Masking

NextLabs Announces Data-Centric Security for AWS S3 with Fine-Grained ABAC and Dynamic Data Masking

SAN MATEO, CA, UNITED STATES, July 14, 2026 /EINPresswire.com/ -- NextLabs, a leader in Zero Trust data security and dynamic authorization solutions, today announced the availability of NextLabs Data-Centric Security for AWS S3 (DCS for AWS S3), a solution that enables organizations to secure both application and user access to Amazon S3 using centralized Attribute-Based Access Control (ABAC) policies.



PRESS RELEASE

NextLabs Announces Data-Centric Security for AWS S3 to Secure Access and Protect Data with Fine-Grained Attribute-Based Authorization and Dynamic Data Masking

Zero Trust protection for AWS S3 through dynamic ABAC policies, centralized authorization, and real-time data access governance

NextLabs Announces Data-Centric Security for AWS S3 to Secure Access and Protect Data with Fine-Grained Attribute-Based Authorization and Dynamic Data Masking

AWS S3 has become the foundation for storing business-critical information used by enterprise applications, analytics platforms, AI services, and data lakes. Organizations require more granular, policy-driven authorization to determine exactly which applications, users, and business processes should be permitted to access specific data under specific conditions.

NextLabs Data-Centric Security for AWS S3 extends Zero Trust principles directly to AWS S3 by evaluating every data access request against centrally managed ABAC policies. Built on the company's patented Dynamic Authorization policy engine and Zero Trust policy platform, the solution enables organizations to make real-time authorization decisions based on attributes of the application, user, environment, requested resource, and business context—without requiring application code changes. Policies can be enforced at the tenet, bucket, directory, query, or object level for all bucket types.

"As more applications rely on AWS S3 to store their data it is more important to safeguard data privacy and confidentiality," said Keng Lim, CEO of NextLabs. "Data-Centric Security for AWS S3 enables organizations to externalize authorization from their applications and centrally manage

fine-grained ABAC policies that secure access to every bucket, folder, object, and table while supporting Zero Trust security initiatives."

NextLabs externalizes authorization logic from applications, allowing organizations to centrally administer security policies that can be updated immediately without application downtime or software modifications. Every request is evaluated dynamically using ABAC policies that consider user identity, application identity, resource attributes, environmental conditions, and the context of the request before access is granted.

Key capabilities of NextLabs Data-Centric Security for AWS S3 include:

- Real-Time Attribute-Based Access Control (ABAC) Policy Engine evaluates every request using application, user, resource, and environmental attributes.
- Enforcement of ABAC Policies at the Tenant, Bucket, Folder, and Object levels, providing fine-grained authorization across all Amazon S3 bucket types.
- Bucket, Folder, and Object-Level Filtering ensures applications and users only see the data they are authorized to access.
- Table Bucket Security with row-level and column-level authorization for Amazon S3 Table Buckets used in analytics workloads.
- Dynamic Field-Level Data Masking for Table Buckets that protects sensitive information in real time using centrally managed masking policies.
- Record-Level Data Segregation and Filtering for Table Buckets based on user, application, data, and business attributes.
- Granular Enforcement of Amazon S3 Operations, including authorization for create, insert, update, and delete operations.
- Centralized Policy Management that enables consistent authorization across applications while simplifying policy administration.
- Comprehensive Monitoring and Auditing that captures application and user access activity for compliance reporting, security analytics, and operational visibility.
- Support any applications using Amazon S3 Out-of-the-Box, allowing organizations to apply NextLabs Data Security Policies without custom application development.

By externalizing authorization and applying dynamic ABAC policies at every access request, NextLabs enables organizations to implement least-privilege access, protect data, improve regulatory compliance, and accelerate cloud adoption without sacrificing security. The solution protects sensitive business information while enabling secure collaboration across employees, partners, suppliers, contractors, and cloud-native applications.

Tony Berning

NextLabs

+1 650-577-9101

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/925799338>

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.