NEXTLABS®
Zero Trust Data Centric Security

Utilizing NextLabs Data Segregation to Control Data Access in M&A, JVs, and Divestitures | Case Study: Mitigating Unauthorized Disclosure and Safeguarding Data in Joint Ventures | Webinar | M&A, JVs, and Divestitures Use Cases

Q4 2023 Partner Update

Utilizing NextLabs Data Segregation to Control Data Access in M&A, JVs, and Divestitures

NEXTLABS®
Zero Trust Data Centric Security

Utilizing NextLabs Data Segregation to Control Data Access in M&A, JVs, and Divestitures | Case Study: Mitigating Unauthorized Disclosure and Safeguarding Data in Joint Ventures | Webinar | M&A, JVs, and Divestitures Use Cases

When organizations are going through structural changes it is important that access to data reflects the changes in organizational structure and there is no unauthorized access to sensitive data.

Safeguarding Data in Joint Ventures, Mergers & Acquisitions, Divestitures, and Sanctions

NextLabs' zero-trust data-centric security platform, CloudAz, with its unified policy engine is used by customers to address the challenges posed by mergers, acquisitions, joint ventures, or divestitures. A key component of the NextLabs solution is advanced data segregation driven by attribute-based data security policies. This functionality allows organizations to protect critical data and reduce the risk of unauthorized access while supporting the key requirements of M&A, JVs, and divestitures, i.e. data integration, collaboration, and asset separation.

One of the primary challenges during mergers and acquisitions is the secure integration of disparate data systems. NextLabs' approach emphasizes data-centric security, ensuring that the focus extends beyond network boundaries to safeguard the data itself. The incorporation of advanced data segregation techniques allows organizations to categorize and compartmentalize data based on sensitivity and criticality. This ensures that during the consolidation of databases, sensitive information is meticulously controlled, reducing the risk of data breaches or unauthorized access.

Read More

In the context of joint ventures, where secure collaboration is paramount, NextLabs' zero-trust model with data segregation capabilities facilitates granular control over data access. By categorizing data and applying fine-grained access controls, organizations can enable seamless collaboration while preserving the confidentiality of sensitive information. This is particularly crucial in joint ventures where trust boundaries extend across organizational lines, necessitating a robust security framework that adapts to dynamic collaboration requirements.

For companies undertaking divestitures, NextLabs' approach aids in the secure separation of assets. The advanced data segregation features allow organizations to clearly define and isolate data associated with divested assets. This ensures that sensitive information is neither inadvertently retained nor exposed during the divestiture process, safeguarding both the interests of the divesting entity and the privacy of the divested assets.

NextLabs' zero-trust data-centric approach, enriched by cutting-edge data segregation capabilities, thus provides a comprehensive and tailored solution for companies navigating the intricate landscape of mergers, acquisitions, joint ventures, or divestitures. By prioritizing data security, implementing fine-grained access controls, and adapting to the specific demands of each transformative event, organizations can confidently manage risks, protect critical assets, and ensure the integrity of their information throughout the complex business transitions.

Data Segregation enforced by ABAC policies is available in all of NextLabs' products lines, including:

CloudAz
Zero Trust Policy Platform

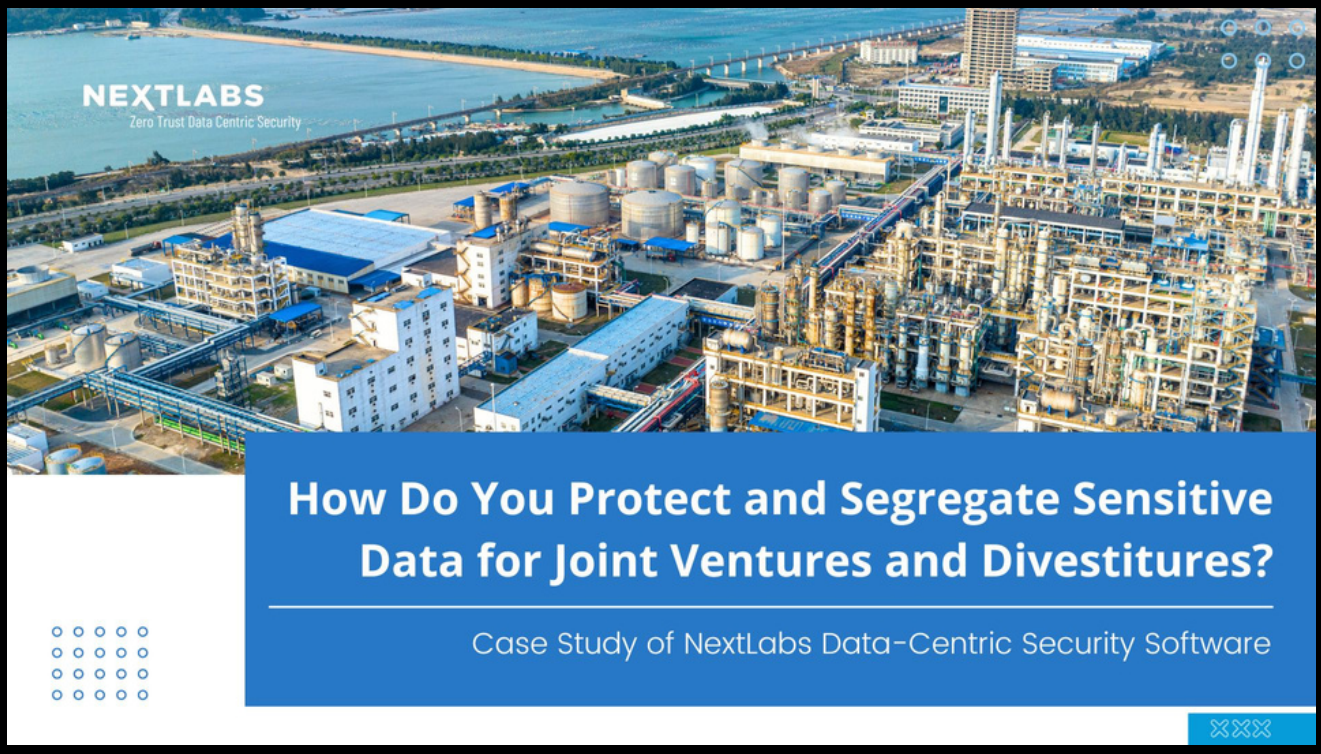
SkyDRM
Digital Rights Management

Application Enforcer
Entitlement Management

Data Access Enforcer
Data Access Security

NEXTLABS®
Zero Trust Data Centric Security

Case Study: Mitigating Unauthorized Disclosure & Safeguarding Data in JVs



Asset and resource sharing is a common concern among companies involved in joint ventures as each company wants to share specific assets designated to the joint venture only to those who has the need to know, while not accidentally giving access to trade secrets or other proprietary information that is not part of the joint venture.

Explore how NextLabs' Dynamic Authorization Policy Management System and Data Access Enforcer (DAE) empowered a leading global chemical company. Facilitating the implementation of attribute-based security, they dynamically enforced need-to-know policies to safeguard data at runtime across key business processes in SAP ERP and SAP Business Warehouse.

Read More

Webinar

Joint ventures are becoming more and more of a common strategy to contribute assets to each other's benefit. However, this collaboration can leave many sides of both companies vulnerable to accidental data breaches. Each organization needs to share only the specific assets designated for the joint venture, while not accidentally giving access to assets that need to remain private. Employees assigned to the joint venture may also still have responsibilities to their company outside of the joint venture and require access to assets for both.

Watch how our webinar covers essential topics such as ensuring secure collaboration with partners, seamlessly segregating data without disrupting workflow, and implementing effective tracking mechanisms to monitor data access and edits.

Watch Now

NEXTLABS®
Zero Trust Data Centric Security

M&A, JV, and Divestiture Use Cases

Using Dynamic Data Segregation and Masking to Protect Data in Joint Ventures, M&A, and Divestitures

Learn how attribute-based security can be used to protect data in Joint Ventures, Mergers & Acquisitions, and Divestitures with dynamic data segregation and dynamic data masking.

Watch Now

Smart Classifier: Bulk Classification & Data Segregation

Discover how to automatically classify, organize, and protect documents in repositories at a large scale while using NextLabs' Smart Classifier.

Watch Now

Dynamic Data Segregation and Filtering Tutorial

Explore how to filter and segregate data using NextLabs' Data Access Enforcer (DAE), a solution that strengthens data access security within SAP.

Watch Now

Dynamically Segregate Record Level Data in SAP

Find out how to dynamically segregate record-level data across databases and apps. With DAE for SAP, users view only granted records. Unauthorized records are filtered at the data access level, unavailable in the app layer.

Watch Now

NEXTLABS®
Zero Trust Data Centric Security

Utilizing NextLabs Data Segregation to Control Data Access in M&A, JVs, and Divestitures | Case Study: Mitigating Unauthorized Disclosure and Safeguarding Data in Joint Ventures | Webinar | M&A, JVs, and Divestitures Use Cases

On-Demand Video Catalog

Our on-demand video catalog provides a variety of information about NextLabs' solutions and technology. The catalog includes regularly uploaded webinars, demos, and informational introductory videos featured through the NextLabs' YouTube channel.

Enable automatic protection of ProjectWise files- SkyDRM Rights Management eXtension for ProjectWise

Protecting Intellectual Property and Trade Secrets with a Data-Centric Security Model

Anonymize SAP HANA Data using ABAC and FPE in Data Access Enforcer (DAE) for SAP

NEXTLABS®
Zero Trust Data Centric Security

Follow Us

https://www.nextlabs.com/contact-us

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