NEXTLABS®
Zero Trust Data Centric Security

Latest Announcements   Applying Data-Centric Security to Big Data   Expert Series

Q2 2023 Partner Update

Bringing you latest highlights & news

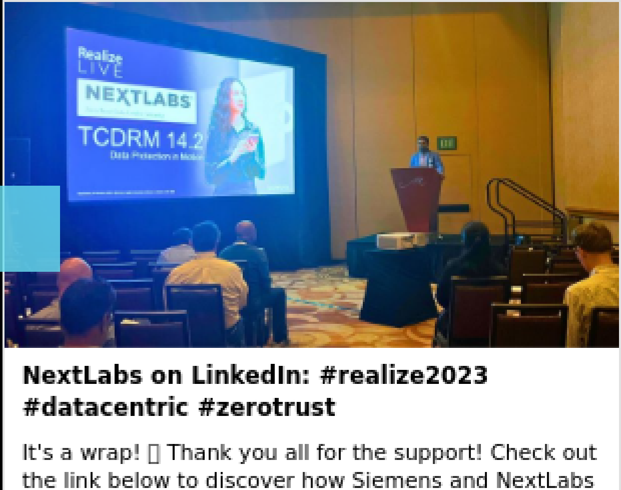
NEXTLABS
Zero Trust Data Centric Security

SIEMENS REALIZE LIVE

Las Vegas, Nevada

Las Vegas, June 15 2023 - NextLabs spoke at Siemens' Realize LIVE Americas Tech Talk/Product Breakout. Featuring how to protect product data and other critical data at rest and on the move, enabling seamless and secure collaboration regardless of where the data is shared.

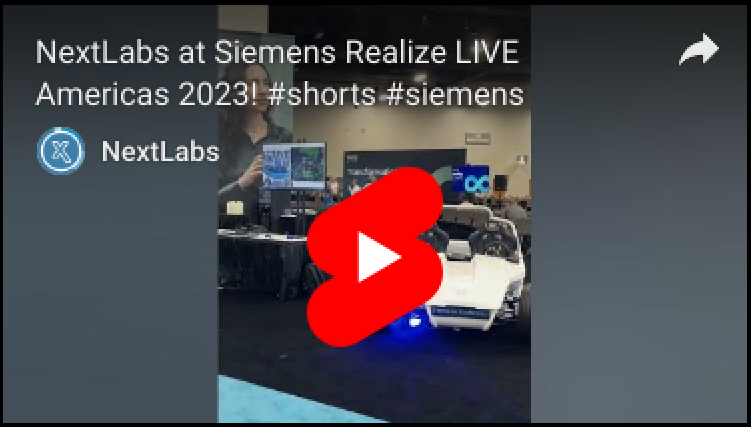
LinkedIn



NextLabs on LinkedIn: #realize2023 #datacentric #zerotrust

It's a wrap! ▯ Thank you all for the support! Check out the link below to discover how Siemens and NextLabs

NEXTLABS Zero Trust Data-Centric Security
Teamcenter Digital Rights Management
Extend Teamcenter security to safeguard data file for sharing
NEXTLABS Zero Trust Data-Centric Security



NextLabs at Siemens Realize LIVE Americas 2023! #shorts #siemens

NextLabs

Youtube Short

NEXTLABS®
Zero Trust Data Centric Security

Latest Announcements | Applying Data-Centric Security to Big Data | Expert Series

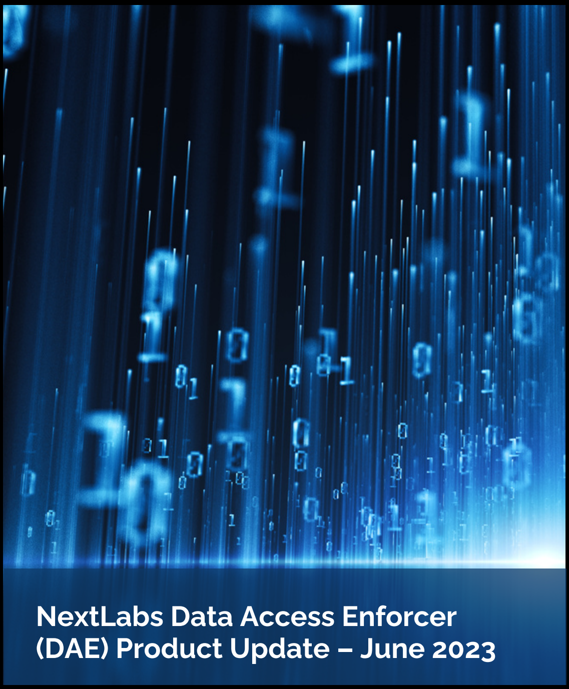
Whitepaper: The Next Frontier of SASE

The Next Frontier of SASE

In this white paper, the next frontier of SASE is discussed, along with the importance of securing access to protect data and applications in addition to networks and devices.

Secure Access Service Edge (SASE) is a model introduced by Gartner in 2019 to combine network and security capabilities as a service, based on the identity of device or entity, and real-time context. The model works to streamline network access and improve the adherence to security and compliance policies. In today's increasingly digital world, it is imperative for organizations to realize that what matters most in the network environment is its data. Especially with ever-changing security dynamics, it is important to properly secure data access; protecting the organization's data in its multi-cloud environments from unauthorized access, usage, changes, or theft.

Read More

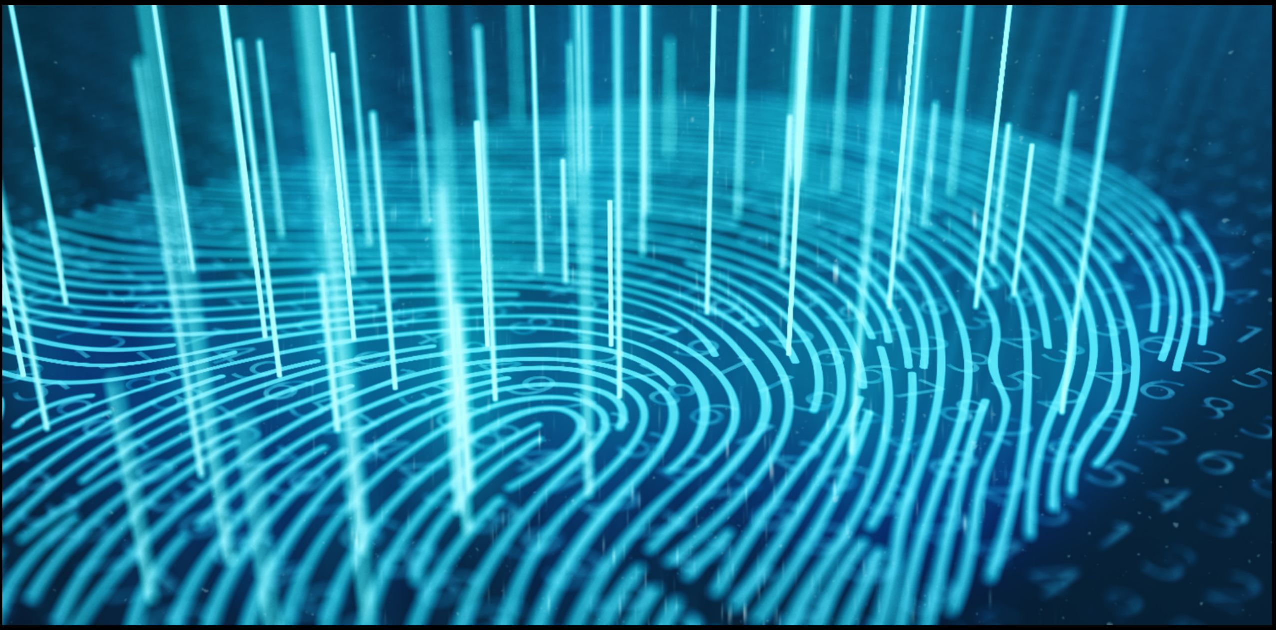

NextLabs Data Access Enforcer (DAE) Product Update – June 2023

NextLabs Data Access Enforcer (DAE) Product Update – June 2023

NextLabs announced its expansion of integration and certification of its DAE product line for use with many more enterprise software products, allowing customers to quickly and easily deploy DAE with those products.

This extends DAE's plug and play capabilities that allow customers to deploy DAE with zero code required for deployment or maintenance.

Read More



Applying Data-Centric Security to Big Data

Big Data refers to vast amounts of sensitive and valuable information that organizations collect and analyze. Different types of data, both unstructured and structured, are often used together by enterprises as part of their data mining efforts. This data often contains personally identifiable information, trade secrets, financial data, or intellectual property, making it a prime target for cybercriminals. Because of the heterogeneity of the data being used, and the different controls that must be applied to different subset of the data, it is important to define and apply data security policies on as granular of a level as possible. By adopting Data-Centric Security, organizations can ensure that appropriate controls are in place to protect this valuable information from unauthorized access, alteration, or misuse.

Big Data environments are typically complex, with data being stored and processed across multiple platforms, systems, and networks. Data from many different sources is often consolidated into large data stores, such as data warehouses or data lakes, which increases the importance of handling access to that data appropriately. Data-Centric Security provides a unified and holistic approach to securing this data, regardless of where it originated or where it is stored, or the technologies used. It focuses on protecting the data itself rather than solely relying on perimeter defenses, which may be insufficient against advanced cyber threats. A data-centric approach that incorporates the principle of least-privileged access can also allow sensitive data to be used in data models that would not be possible if access was not as tightly controlled.

For organizations relying on Big Data, security breaches can have severe consequences, including financial loss, reputational damage, legal and regulatory penalties, and loss of customer trust. An inability to appropriately handle different types of data may also restrict an organization's access to more sensitive data, which could limit the value they can extract from large data sets. Implementing Data-Centric Security principles enables organizations to dynamically identify and classify sensitive data, apply encryption and access controls, monitor data usage, and detect anomalies or unauthorized activities promptly. All of this can be done at the granular level required when handling the many types of data that are incorporated into Big Data models.

Zero Trust Data-Centric Security is the core technology powering all of NextLabs' products lines, including:

CloudAz

Zero Trust Policy Platform ›

SkyDRM

Digital Rights Management ›

Application Enforcer

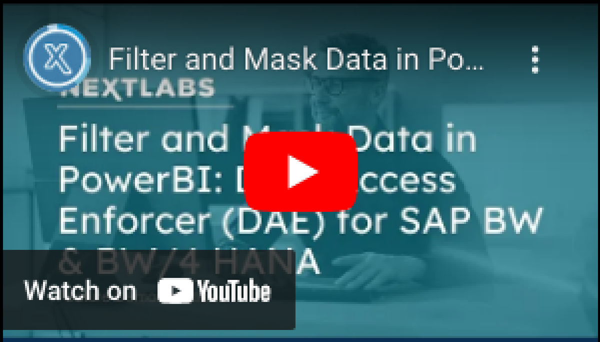
Entitlement Management ›

Data Access Enforcer

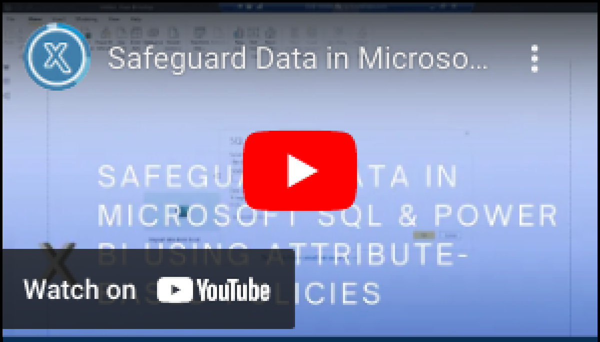
Data Access Security ›

Data-Centric Security for Big Data Videos

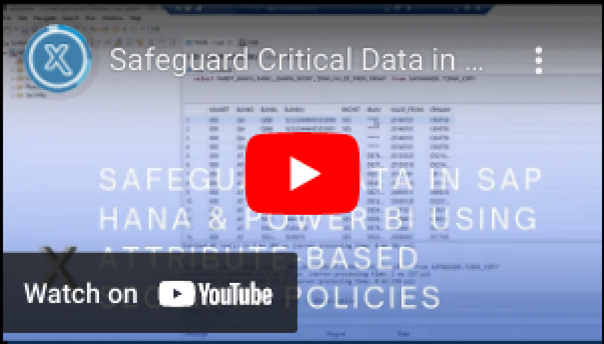
How to Safeguard Data in Oracle DBMS using Dynamically Enforced Attribute-Based Policies


Filter and Mask Data in Po...
NEXTLABS
Filter and Mask Data in PowerBI: Data Access Enforcer (DAE) for SAP BW & BW/4 HANA
Watch on YouTube

Filter and Mask Data in PowerBI: DAE for SAP BW & BW/4HANA


Safeguard Data in Microso...
SAFEGUARD DATA IN MICROSOFT SQL & POWER BI USING ATTRIBUTE-BASED POLICIES
Watch on YouTube

Safeguard Data in Microsoft SQL and Power BI using Dynamically Enforced Attribute-Based Policies


Safeguard Critical Data in ...
SAFEGUARD DATA IN SAP HANA & POWER BI USING ATTRIBUTE-BASED POLICIES
Watch on YouTube

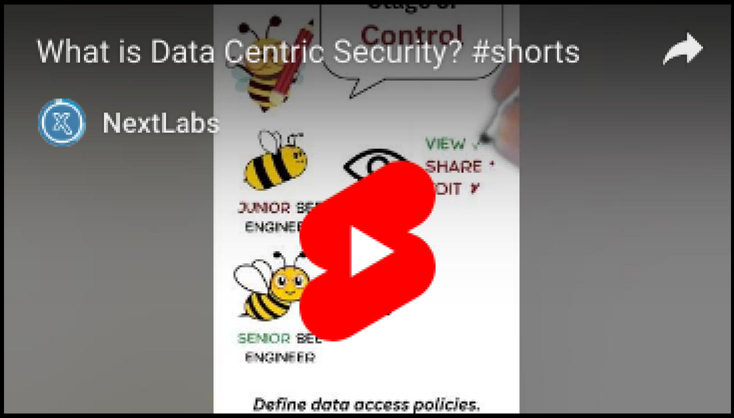
Safeguard Critical Data in SAP HANA & Power BI using Attribute Based Security Policies

NextLabs Data Access Security for BigQuery Overview

Data-Centric Security Videos

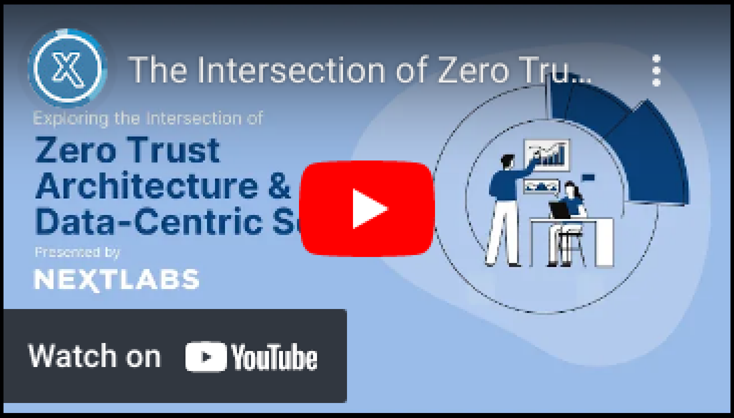
What is Data-Centric Security?

Watch More


What is Data Centric Security? #shorts
NextLabs
Control
VIEW
SHARE
DIT
JUNIOR BE
ENGINE
SENIOR BEE
ENGINEER
Define data access policies.

The Intersection of Zero Trust Architecture (ZTA) and Data-Centric Security

Watch More



Data-Centric Security Playlist on the NextLabs YouTube channel

Watch More

Moving from a Network-Cent...
NEXTLABS
Moving from a N entric to
Data-Centric Sec ategy
Business Solution Webinar
Watch on YouTube

Latest Expert Series Videos

Challenges in Implementing a ZTA with Michal Davidson

In the ninth episode of the NextLabs Cybersecurity Expert Series, Michal Davidson shares her insights on the challenges faced when implementing a Zero-Trust architecture. Michal also covers the difficulties in adapting a ZTA to a multi-cloud environment, as well as where vulnerabilities are commonly identified in a security review process.

Watch More

Challenges in Implementin...
Expert Q&A
Cybersecurity Series
Episode 9: Challenges in Implementing a Zero-Trus Architecture
Watch on YouTube

Securing Microservices to Prevent Cybersecurity Attacks

In the tenth episode of the NextLabs Cybersecurity Expert Series, Alexandru Ghinea shares his insights on securing microservices to prevent cybersecurity attacks. He covers what a microservices architecture looks like, what threats this architecture may pose, and how to implement a data-centric security approach with this architecture.

Watch More

Securing Microservices to ...
Expert Q&A
Cybersecurity Series
Episode 10: Securing Microservices to Prevent Cybersecurity Attacks
Watch on YouTube

Using Dynamic Authorization & Zero Trust in Controlled Environments

In the 11th episode of the NextLabs Cybersecurity Expert Series, Giles Dalton shares his insights on using dynamic authorization and zero trust in controlled environments. He covers the limitations and risks of traditional techniques for protecting controlled data, what the conjunction of dynamic authorizations and zero trust bring, and more.

Watch More

Using Dynamic Authorizati...
Expert Q&A
Cybersecurity Series
Episode 11: Using Dynamic Authorization and Zero Tr in Controlled Environments

Limitations of Traditional Authorizations in the SAP Space

In the twelfth episode of the NextLabs Cybersecurity Expert Series, Janne Nurmi dives into the limitations of traditional authorizations in the SAP space. He covers how ABAC can solve this issue, whether ABAC will replace RBAC, the Zero-Trust Principle for SAP, and more.

Watch More

Limitations of Traditional A...
Expert Q&A
Cybersecurity Series
Episode 12: Limitations of traditional authorizations the SAP space

NEXTLABS®
Zero Trust Data Centric Security

Follow Us

in 🐦 ▶

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.