

Q3 2023 Partner Update

Bringing you latest highlights & news



Latest Announcements

A Zero Trust Data-Centric Approach
to CMMC 2.0 and CUI

Data-Centric Security for
CMMC and CUI Videos



Learn how Petrobras with the support of Deloitte and NextLabs resources, worked in tight collaboration to implement the primary deliverable of Nextlabs SAP DAM within four months to quickly deploy and meet the data governance-initiatives set forth. With this zero-trust data-centric approach using SAP DAM, Petrobras is now able to ensure fine-grained access control for applications that create, store, or modify personal data, while also ensuring compliance and maintaining agility.

[Watch More](#)

PRESS RELEASE

NextLabs® Announces Successful Go-Live With Solvay to Strengthen Access Management and Data Security

NextLabs' Zero Trust Data Security suite is chosen to enhance compliance and protect export controlled and EH&S data in global SAP S/4HANA and SAP ECC instance

San Mateo, Calif. – September 11, 2023 – NextLabs announced the successful go-live of its Zero Trust Data Security suite with Solvay, one of the largest multinational chemical manufacturers in the world. NextLabs' solution safeguards sensitive data including EH&S and export-controlled technical data, maintains regulatory compliance, and strengthens cybersecurity. This is achieved through a comprehensive data-centric security solution based on zero trust principles that automates data compliance and prevents data breaches.

[Read More](#)



San Mateo, Calif. – July 19, 2023 – NextLabs announces the successful go-live of its Zero Trust Data Security Suite with Fiserv, a global leader in financial services technology. NextLabs' solution will allow Fiserv to safeguard the confidentiality and integrity of its customer and financial data through a comprehensive data-centric security framework. The solution enables dynamic data-level security controls such as encryption, decryption, masking, and filtering, to strengthen Fiserv's cybersecurity for its digital transformation initiative.

[Read More](#)



NextLabs recently expanded PLM and CAD integration besides extended many of its SkyDRM capabilities to improve functionality and user experience for file protection, project collaboration, offline and Desktop capabilities, automatic and rule-based batch protection of files, and Microsoft Exchange, SharePoint, and Office 365 integration.

[Read More](#)



A Zero Trust Data-Centric Approach to CMMC 2.0 and CUI

The Cybersecurity Maturity Model Certification (CMMC) program aims to ensure the cybersecurity of organizations working with the United States Department of Defense (DoD) and making up the United States Defense Industrial Base (DIB). A Zero Trust data-centric approach can help organizations comply with the latest version of the requirements, CMMC 2.0, and protect their Controlled Unclassified Information (CUI). The Zero Trust approach shifts the focus of cybersecurity from traditional perimeter-based security to a data-centric model that aligns seamlessly with the goals of CMMC.

Whether an organization needs to be certified as Level 1 (Foundational), Level 2 (Advanced), or Level 3 (Expert), a Zero Trust security approach starts with the assumption that threats can exist both within and outside an organization's network. In the context of CMMC and CUI, this means that access to sensitive information, such as CUI, is not automatically granted to users, regardless of location, even from within trusted networks. By implementing a Zero Trust data-centric approach, organizations can significantly enhance their ability to protect CUI.

In the Zero Trust framework, specifically as defined by the controls in NIST SP 800-171, data is considered the core asset that needs protection. This aligns with CMMC's emphasis on safeguarding sensitive information. By implementing strong data encryption, access controls, and user authentication mechanisms, a Zero Trust approach ensures that only authorized individuals can access CUI. Additionally, it employs continuous monitoring and behavioral analysis to detect anomalies and potential breaches promptly.

Latest Announcements

A Zero Trust Data-Centric Approach to CMMC 2.0 and CUI

Data-Centric Security for CMMC and CUI Videos

Zero Trust's focus on least privilege access is particularly relevant to CMMC. Users and systems are granted only the necessary level of access to perform their functions, minimizing the attack surface for potential adversaries seeking to exploit vulnerabilities. This concept aligns well with CMMC's requirements to restrict access to CUI to only those who require it for their roles.

Furthermore, the integration of Zero Trust principles bolsters compliance efforts for CMMC certification. As CMMC aims to standardize cybersecurity practices across the DIB sector, a Zero Trust approach provides a comprehensive framework that can be tailored to the specific requirements of different CMMC maturity levels.

By treating data as the focal point of security measures and maintaining a posture of continuous verification and monitoring, organizations can effectively safeguard CUI and other sensitive information. This not only strengthens cybersecurity but also contributes to meeting the stringent requirements of CMMC certification and maintaining the integrity and confidentiality of sensitive data



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 CMMC and CUI Videos



Understanding CMMC:
Cybersecurity Requirement for
Defense Contractors



Protect Assemblies and 3D Models
with Digital Rights Management
(DRM) for CMMC Compliance



Demystifying CUI: Protecting
Controlled Unclassified Information

Follow Us



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

© 2023 NextLabs Inc. All Rights Reserved

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>.

