Managing Global Data Access in the Cloud

Solution Highlights

Safeguard data across hybrid and multi-cloud environments with:

- A Zero Trust Policy Platform that addresses business and security needs with centrally managed, attribute-based policies.
- A Dynamic Authorization Policy Engine, which evaluates and authorizes least-privileged access based on attributes.
- Real-Time Enforcement, preventing unauthorized access of data via DRM, ABAC, data segregation, and data masking.
- Policy governance & orchestration, enabling streamlined policy lifecycle management., administration, and integrity.
- Continuous monitoring & centralized audit, ensuring full oversight of security policies and data access activities.

MODERNIZING WITH CLOUD TECHNOLOGIES

Fortune 1000 companies today are embarking on modernization initiatives more urgently than ever, racing to adopt new architectures and unify and consolidate their IT systems. Driven by the need for business scalability and infrastructure cost reduction, many are migrating high volumes of data from on-premises centers to private or public clouds. By doing so, they aim to facilitate collaboration across borders, streamline back-office operations, and optimize right-shoring.

However, the true benefits of the cloud can only be unlocked when its data is thoroughly secured. The cloud does not inherently secure the applications and data it hosts — according to Cloud Security Alliance, only 4% of organizations report that 100% of their sensitive data in the cloud is sufficiently secured. In other words, 96% of companies report insufficient security for at least some sensitive cloud data.

In this paper, we will explore how large-scale enterprises manage global data access in complex cloud environments to achieve security and compliance. We will address the challenges, requirements, and best practices for multi and hybrid cloud security. Additionally, we will delve into NextLabs' solutions and present a specific customer case study about ensuring data protection and regulatory compliance across multiple cloud environments.

DATA SECURITY CHALLENGES IN CLOUD ENVIRONMENTS

As organizations expand globally, they face complexities in safeguarding data transfer and collaboration across various locations, each with its own regulatory requirements. The fragmented nature of cloud applications with many on-prem systems often leads to inconsistent security policies and reduced control over data access and usage. As a result, many organizations struggle with visibility and monitoring of global data access activities across heterogeneous applications in hybrid cloud environments, making it difficult to quickly identify and address security incidents.

Privileged users, such as cloud service providers and offshore IT administrators, add another layer of complexity to cloud security. These users possess extensive access to critical systems and sensitive data, making them attractive targets for malicious actors. To mitigate these risks, it is crucial to monitor and secure their activities rigorously.

Multi and hybrid cloud environments pose further challenges with rapidly changing workloads, configurations, and access patterns, making it a challenge for organizations to ensure consistent data protection and regulatory compliance across these diverse settings.

According to a Radware report, 69% of organizations admitted to experiencing data breaches or exposures due to multi-cloud security configurations.

Workforce virtualization also means that the increasing number of devices, users, and bots, has led to an explosion in access and data volumes. This exponential growth in digital identities necessitates an automated approach to identity and access management, ensuring that only authorized individuals have access to the appropriate data.

DATA SECURITY REQUIREMENTS FOR THE CLOUD

Given the reduced visibility and growth in digital identities in the cloud, it is crucial to focus on securing data at its core. This requires a data-centric approach that safeguards data dynamically in real-time, both on-premises and across cloud platforms. Key to this approach is encrypting data at rest, in use and in transit, ensuring that even if unauthorized access occurs, the data remains unreadable and unusable.

To ensure the solution works across hybrid and multi- cloud environments, organizations must adopt a modern architecture that unifies data-centric security across these diverse settings. This unified approach must effectively operate across SaaS applications such as Salesforce, Workday, and ServiceNow, integrate with IaaS hosting ERP systems on private clouds, and support PaaS platforms for analytics and databases like those on Azure Cloud. Additionally, this strategy should extend to on-premises systems, including traditional data centers, legacy applications, and local file servers.

To operate effectively across a complex IT landscape, a solution must also seamlessly integrate with various enterprise systems including ERP, PLM, CRM, and BI applications. This facilitates improved collaboration, greater business agility by enabling rapid adaptation to changing market conditions, and more intelligent analytics through enhanced data insights.

WHAT DOES A DYNAMIC CLOUD SECURITY APPROACH LOOK LIKE?

Building on the need for a unified, data-centric security architecture across hybrid and multi-cloud environments, a dynamic security approach is essential to address the complexities of modern cloud operations. Organizations must implement security strategies that are versatile and responsive, capable of safeguarding data across SaaS, PaaS and IaaS layers.

- **Secure Data Anywhere and Everywhere**: To secure data across heterogeneous applications and diverse operational environments, organizations need controls that protect data irrespective of its enclave (database, app, file) and location, whether on-premises, in transit, or stored in various cloud platforms. This ensures comprehensive data protection and mitigates risks associated with data breaches and unauthorized access.
- **Zero Trust Architecture**: To fulfill the requirement for a modern architecture that unifies data-centric security, Zero Trust Architecture (ZTA) mandates verification from every user and device attempting to access the network. This ensures that no entity, whether inside or outside the organization's perimeter, is trusted by default. Instead, continuous verification and strict access controls are enforced, reducing the risk of breaches and unauthorized access.
- **Dynamic Authorization:** Dynamic authorization applies real-time analysis of user activity and data sensitivity, aligning with the principles of ZTA to make authorization decisions. By continuously assessing the context in which access requests are made, organizations can implement more granular and adaptive security controls, ensuring that only authorized users have access to sensitive data and resources.
- **Cloud-Native and Support Hybrid and Multi-Cloud**: The solution should operate efficiently in cloud environments, and compatible with hybrid and multi-cloud setups. This includes integrating solutions with both legacy systems and modern cloud applications, ensuring that security controls are uniformly applied across all environments.
- **Automate and Prevent**: An automate and prevent paradigm proactively enforce data security controls to prevent human error. Unlike the detect and respond model, which generates an overwhelming number of logs and necessitates extensive response efforts without addressing the root causes, automate and prevent is proactive, scalable, and more cost-efficient.
- **CI/CD and Continuous Monitoring**: Integrating security into the DevOps pipeline through Continuous Integration and Continuous Deployment (CI/CD) practices emphasizes security automation and continuous assessment. This approach enhances the ability to detect anomalies and enables security analytics regarding access data consumption patterns, ensuring proactive threat management and continuous improvement of security postures.

HOW NEXTLABS PROVIDES DYNAMIC SECURITY TO PROTECT DATA IN THE CLOUD

NextLabs Zero Trust Data Security is a comprehensive suite of access enforcement and data protection applications powered by CloudAz, a Zero Trust policy platform. It consists of policy enforcers to proactively prevent unauthorized access of data across applications, file repositories and databases, even in compromised systems. It employs the following features:

- **Zero Trust Policy Platform**: Business and security needs are digitized and stored as centrally managed, attribute- based policies. These policies allow organizations to define who can access what data and what actions are permissible. By centralizing policy management, NextLabs ensures that security protocols are consistent and adaptable across diverse environments, protecting data anywhere and everywhere, regardless of enclave (database, app, file) and location.
- **Dynamic Authorization Policy Engine:** The policy engine evaluates and authorizes access in real time based on user, device, resource, and contextual attributes. By aligning with the 'Least Privileged Access' principle of Zero Trust Architecture, the policy engine ensures that access rights are granted only when necessary and are re-evaluated dynamically with each new request.
- **Real-Time Enforcement:** Once the policy engine makes an access decision, it is communicated to policy enforcers that implement data-centric security controls. These controls include:
    - **Digital Rights Management (DRM)**: Restrict access to digital content through encryption and permissions to prevent unauthorized usage.
    - **Data Segregation**: Separate data based on sensitivity, access, and functional requirements, ensuring appropriate security controls and access policies are applied to each category.
    - **Data Masking**: Obfuscate sensitive information by replacing it with fictitious data, ensuring data privacy.
    - **Attribute-Based Access Control (ABAC)**: Tailor access permissions based on user attributes and environmental factors, allowing for granular and context-aware security.
- **Policy Governance & Orchestration:** The policy platform provides facilities for policy lifecycle management and strong policy governance support, to secure policy administration and ensure policy integrity. Policy orchestration capabilities enable customers to adopt Continuous Integration and Continuous Deployment (CI/CD) practices to continuously improve and deploy policies.
- **Continuous Monitoring and Centralized Audit:** A centralized audit facility, along with continuous monitoring, ensures full oversight of security policies and data access activities. This facilitates compliance with regulatory requirements and enhances overall security posture. Continuous monitoring allows for the detection of anomalies and supports security analytics, enabling proactive threat management.

NextLabs can be deployed anywhere, be it on-premises, in private cloud, or as a SaaS. Running natively on AWS, Azure, OpenShift and Google Cloud, NextLabs offers organizations the freedom to choose the right cloud deployment strategy, whether it is hybrid or multi-cloud. Policies can be transported between cloud and on-premises deployments, ensuring consistent policy enforcement across all environments.

CASE STUDY- A GLOBAL MANUFACTURING COMPANY

- **Company:** XYZ Industries
- **Industry**: Manufacturing
- **Business Driver**: Export Compliance and Cloud Security
- **Products**: Electronics, Industrial Machinery, Automotive
- **Employees**: 100,000+

As companies pursue Industry 4.0 and the 'Factory of the Future' status, manufacturers are modernizing their IT infrastructure for cost-cutting and improved supply chain management. XYZ Industries, a Fortune 1000 manufacturing powerhouse, has adopted a hybrid cloud infrastructure to drive digitization and streamline operations across 50+ countries. This strategic move enhances collaboration among global teams and accelerates time to market by eliminating manual processes. By leveraging hybrid cloud technology, XYZ Industries ensures cost-efficiency and sustains a competitive advantage in 21st- century manufacturing. dynamically with each new request.

CHALLENGES

However, storing data in the cloud across international servers poses significant risks for XYZ Industries. Export-controlled design files or production data might be accessed in foreign locations without proper authorization. Additionally, the globally shared data often includes protected IP critical for market differentiation and competitiveness. Data leakage could result in millions of dollars. in compliance violation fines and the loss of business-critical ideas to competitors. To prevent such catastrophic consequences, XYZ needs a solution that addresses the following challenges:

- **Privileged Users in Foreign Countries**: To ensure export compliance, including ITAR and EAR policies, XYZ must secure its technical data such as design blueprints and manufacturing processes from unauthorized personnel. This is especially crucial for privileged users, such as offshore system administrators in foreign countries, who can access data directly at the system level, bypassing application-level security measures and controls.
- **Multi-Use Environments**: Engineering design, development, and manufacturing resources at XYZ Industries are utilized for both ITAR-regulated projects and commercial endeavors. In a cloud-based infrastructure, this multi-use environment increases the risk of accidental disclosure and cross-contamination of technical data. For example, an American engineer might inadvertently enter ITAR-restricted technical specifications for a drone project into a cloud database that is accessible to a foreign engineer working on a commercial drone delivery project.
- **IP Loss across Supply Chain**: A significant risk in supply chain collaboration is the inability to control how partners, employees, and third parties handle shared data, especially Intellectual Property (IP). XYZ Industries needs to share critical product designs with their tier- one supplier, AVA, while ensuring that AVA cannot accidentally or intentionally share these designs with their subcontractors.
- **Wrongful Disclosure in Remote Work Environments:** XYZ Industries must prevent data leakage while sharing sensitive data in the cloud, particularly R&D information, customer data, CAD/CAM models, and crucial go-to- market (GTM) plans. The ease of sharing, especially under WFH/BYOD policies, increases the risk of accidental disclosure. For instance, an unauthorized family member could access sensitive customer contracts from an employee's workstation at home.

SOLUTION

To address the cloud security challenges faced by XYZ Industries, NextLabs provided Zero Trust Data Security, a comprehensive suite of dynamic cloud security solutions, ensuring compliance and protection across their global operations. Here's how each element of NextLabs' solution overcomes the above obstacles:

Protect Export-Controlled Data from Privileged Users: To prevent unauthorized access by privileged users, NextLabs' solution safeguards data at rest in the cloud. It controls access dynamically using ABAC, based on policies driven by attributes such as user citizenship, certification training, computer system, and physical location. The solution ensures data integrity by implementing proper governance processes and maintaining comprehensive audit trails to track any access and modifications to policies and data.

Segregate Data in Multi-Use Environments: NextLabs' logically segregates data subject to export controls by using ABAC to dynamically control user access based on, for example, export license or ECCN. It identifies data based on locations such as cloud applications, repositories, and devices, as well as data attributes like export jurisdiction, to actively prevent deemed export and unauthorized transfers. For instance, ITAR- restricted technical data for a drone project can be segregated from commercial drone delivery systems data, even though both reside within the same cloud application.

Secure IP Across the Supply Chain: NextLabs' solution enables XYZ Industries to safeguard the sharing of IP data by persistently protecting documents and files with DRM encryption. DRM allows data owners to control access and usage of data after it is shared. By securing the file with DRM, it remains protected after being shared, preventing unauthorized access and use, including printing, downloading and forwarding. For instance, if an AVA engineer mistakenly forwards the design to a subcontractor, the unauthorized recipient will not be able to access the design due to the permissions specified in the DRM policy.

Safeguarding Data During Remote Work: With DRM encryption, XYZ Industries can ensure that access and usage of sensitive data is verified in real time, even on personal devices and home workstations. For example, if an employee's family member at home tries to copy a customer contract document into a thumb drive, the action would be blocked according to DRM policies, keeping the sensitive file unviewable.

Automated Logging and Reporting: NextLabs' solution continuously collects logs across multiple cloud systems and applications to monitor and audit authorized exports in accordance with approved licenses and business policies. It automates the documentation of who has access to controlled technical data and provides comprehensive reports detailing technical data exports, ensuring compliance and meeting governance requirements.

BENEFITS

This case study highlights the importance of a dynamic, integrated security strategy for protecting sensitive manufacturing data in a complex multinational environment. By implementing NextLabs Zero Trust Data Security, XYZ Industries has greatly improved its data protection and regulatory compliance, enabling secure and efficient global collaboration. Consequently, XYZ Industries is now able to achieve enhanced global collaboration.

- Streamlined data security and compliance across all business units, reducing complexity and administrative overhead.
- Reduced operational costs by integrating seamlessly with existing ERP, PLM, CRM, and BI systems in the hybrid cloud.
- Reduced time and labor-intensive manual audit processes through automated compliance reporting.

Enhanced Security and Export Compliance

- Automated data-centric controls, ensuring only authorized personnel access sensitive data.
- Ensured full compliance with ITAR and EAR regulations, preventing unauthorized access to export-controlled data across international borders.
- Enabled right-shoring practices by protecting sensitive data from privileged IT system and cloud service.

Accelerated Time to Market

- Supported faster decision-making by quickly providing authorized personnel access to data on a need-to-know basis with dynamic access control.
- Enhanced supply chain efficiency and collaboration by eliminating data loss while enabling the seamless and rapid exchange of information.
- Gained a competitive advantage and increased revenue potential through quicker product launches and streamlined operations.

Improved Workforce Collaboration and Innovation

- Reduced the risk of IP leakage and compliance violations in the cloud, supporting safe and efficient global collaboration.
- Improved product quality and reduced manufacturing defects by ensuring integrity of data throughout the manufacturing process.
- Fostered innovation by enabling seamless sharing of critical information across teams and partners.

CONCLUSION

This white paper highlights the critical need for a comprehensive, dynamic security strategy to manage global data access in today's complex cloud environments. The rise of hybrid and multi-cloud ecosystems introduces challenges such as export compliance, privileged user access, and IP protection, and requires a dynamic approach to protect sensitive data at rest, in use, and in transit. Organizations must adopt solutions that seamlessly integrate across diverse platforms while ensuring consistent security measures are in place to address these challenges.

For enterprises at large, the message is clear: embracing a Zero Trust approach and leveraging advanced technologies can lead to stronger security and compliance postures, reduced risk of data breaches, and greater business agility. This strategic focus on cloud security not only safeguards critical assets but also fosters innovation and collaboration on a global scale. Prioritizing comprehensive and integrated cloud security solutions will empower organizations to thrive in the digital age.

NEXTLABS | Zero Trust Data-Centric Security

ABOUT NEXTLABS

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