Solution Brief

Proactive Protection with Zero-Trust Data-Centric Security

OVERVIEW

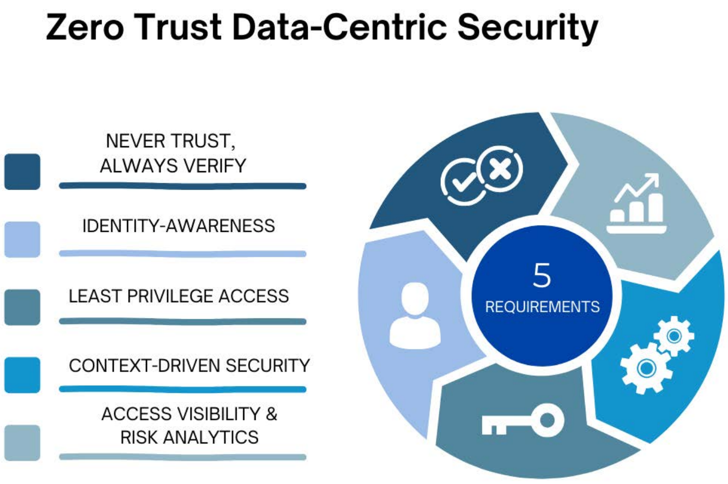
In today's world where the surge in data sharing collides with the increasing sophistication of cyberattacks, preserving data security and integrity has become a pressing challenge. Organizations have to secure a digital core that lies beyond traditional network boundaries, while ensuring a seamless flow of data across different environments, from cloud services to mobile devices.

To address the challenge of securing an expanding digital core, organizations should turn towards Zero-Trust Data-Centric Security, a strategy that applies Zero Trust principles to focus on data, applications and their usage, location, collection, storage, and visibility.

Zero-Trust Data Security fosters a proactive approach to safeguarding sensitive data by eliminating implicit trust, implementing fine-grained access controls (also known as Attribute-Based Access Control or ABAC), and prioritizing data protection over network boundaries. By adopting Zero Trust Data-Centric Security, organizations can prevent breaches and ensure that data remains protected regardless of its location, surpassing the limitations of traditional perimeter defenses.

The rapid adoption of cloud services, remote workforces, Bring Your Own Device (BYOD) policies, and microservices architecture has eroded the traditional network perimeter that once provided a sense of security for organizations. The dissolution of this perimeter has resulted in security vulnerabilities that have incurred huge financial costs. According to an IBM report, in cases of remote work-related breaches, the average cost is nearly 1 million USD higher than breaches caused by other means.

Furthermore, the growing volume of data and prevalence of data sharing are expanding the attack surface for security breaches. Traditional static access controls and manual change management struggle to keep pace with the dynamic nature of such data flows and access requirements. At the same time, they also pose a significant hurdle for compliance and audits, where role explosion and the lack of centralized visibility make it difficult for organizations to demonstrate regulatory compliance.


Zero Trust Data-Centric Security
NEVER TRUST, ALWAYS VERIFY
IDENTITY-AWARENESS
LEAST PRIVILEGE ACCESS
CONTEXT-DRIVEN SECURITY
ACCESS VISIBILITY & RISK ANALYTICS
5
REQUIREMENTS

REQUIREMENTS FOR ZERO TRUST DATA-CENTRIC SECURITY

Enterprises must wield zero trust strategy in the right direction: to prioritize securing data and applications over the network perimeter. This entails implementing principles such as:

Never Trust, Always Verify

Requires continuous verification of user identity, device and network integrity, nature and importance of resources & data before granting access. This ensures that only authorized entities can access sensitive information, minimizing the risk of unauthorized exposure.

Identity-Awareness

Authentication process goes beyond the traditional username, password, and ID token, incorporating a holistic validation of the individual's identity, such as device, the location, the times, the purpose of access, and the assigned access privileges.

Least Privilege Access

Grants users the minimum level of access necessary to perform their tasks. By limiting permissions to only what is essential, organizations mitigate the potential risks of security breaches, maintaining data confidentiality and integrity.

Context-Driven Security

Considers the specific context of each access request, enabling granular access decisions that improve the precision of data and application security. Contextual details create deeper comprehension of performance, behavior, and activity, which would aid in analyzing anomalous activity.

Access Visibility & Risk Analytics

Access visibility enhances anomaly detection and enables organizations to respond swiftly to potential security incidents. This goes hand in hand with data-driven analytics, which are utilized to monitor and identify risks, allowing realtime optimizations of security policies and access decisions.

HOW TO IMPLEMENT ZERO TRUST DATA SECURITY

To implement zero trust data-centric security, the solution should comprise of two key parts: zero trust policy platform and enforcement of consistent access and data protection measures across applications and data sources. Architecturally, it is achieved through a unified policy management system, policy engine and a collection of policy enforcers.

Centralized Policy Management

On the policy platform, business and security requirements are digitized and stored in the form of centrally managed policies. During an access attempt, these digital policies are evaluated in real time by the policy engine, which makes its authorization decision based on identity, context and user behavior. By unifying authorization and access policies, a zero trust policy platform allows organizations to eliminate security silos, prevent role explosion and enhance visibility of access activity across systems.

The policy platform works hand in hand with the consistent enforcement of data protection measures, enabling organizations to secure data across diverse systems beyond the network perimeter and shift away from manual security controls. Instead of an error-prone process that detects and mitigates unauthorized access after occurrence, organizations can automatically prevent breaches before they happen.

Enforcement of Data Protection Policies

With a **centralized policy system**, security policies can be enforced consistently across the entire organization, managing rapidly increasing data volumes amidst rising access requirements.

Policy enforcement helps to control access to the source of data, before implementing controls over what can be seen and done with the data. These data security controls include data segregation, data masking, data loss prevention and persistent digital rights file protection.

Many data sources incorporate **data classification** to organize data according to its value and toxicity, to determine the right level of protection for each category. To apply proper security enforcement based on metadata and attributes, a data-centric security solution must possess a comprehensive understanding of the underlying data, identity and attribute models of the data source.

One of the most implemented security measures is **data segregation**, which physically or logically separates data based on its classification, so that appropriate security controls can be applied to different data categories. By enabling granular control over access permissions and other security measures, it helps organizations preserve the confidentiality and integrity of sensitive information, especially in the realm of regulatory compliance.

Other strategies include:

Data masking: Uses attribute-based policies to dynamically replace sensitive data (such as Personally Identifiable Information) with fictitious or obfuscated data.

Data loss prevention: Detects and prevents unauthorized access, transmission, or exfiltration of data.

Digital rights management: Uses policy-driven encryption to secure data at rest and in transit throughout its lifecycle, automatically applying various access rights to documents in real-time.

Policy enforcement also serves as a crucial tool in the automation of access control, data protection, business and compliance procedures. Digital policies allow organizations to enforce preventive controls over traditional detective ones. The policy engine, through dynamic authorization can automate security procedures to eliminate human error and proactively prevent breaches before they occur. By identifying and neutralizing threats beforehand, businesses can significantly strengthen their security posture.

Finally, a Zero Trust Data-Centric Security solution involves smart auditing and risk analytics. A core tenet of data-centric security is the visibility of access activity and authorization decisions. The policy platform should contain a central activity log, where risky access activities can be monitored, tracked and reported. This simplifies compliance reporting and enables the fine-tuning of security procedures. The solution should also be seamlessly integrated with various applications, identity providers, and attribute sources, to facilitate quick time-tovalue and user adoption.

HOW NEXTLABS DELIVERS THE SOLUTION

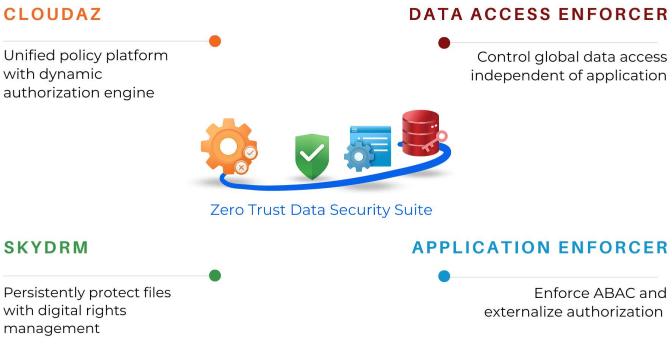
Enterprises must wield zero trust strategy in the right direction: to prioritize securing data and applications over the network perimeter. NextLabs' Zero Trust Data Security Suite is a comprehensive suite of access enforcement and data protection applications powered by a zero trust policy platform. The Suite enables organizations to protect critical data at the source, on the move and at rest. The applications include:

CloudAz: Centrally author and manage zero trust policies

Application Enforcer: Simplify access and protect data across applications and services

SkyDRM: Secure unstructured data and files stored and shared anywhere

Data Access Enforcer: Enforce need-to-know data access on a global scale

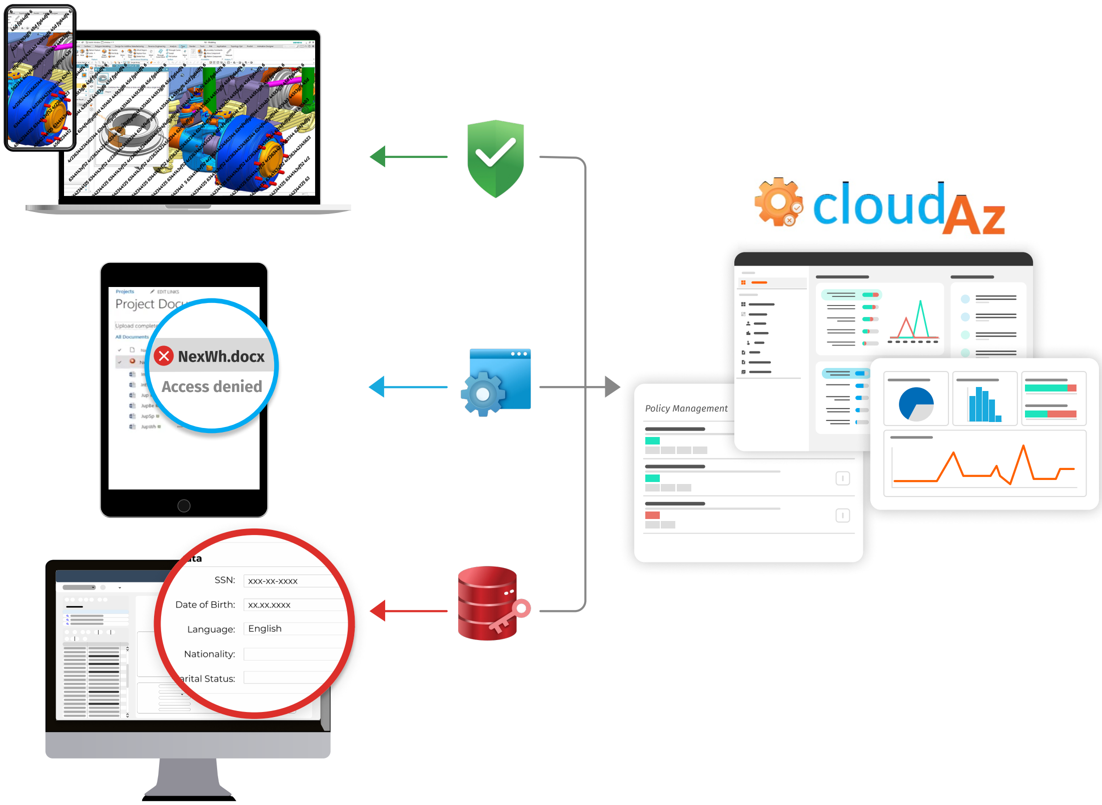

CLOUDAZ
Unified policy platform with dynamic authorization engine
DATA ACCESS ENFORCER
Control global data access independent of application
Zero Trust Data Security Suite
SKYDRM
Persistently protect files with digital rights management
APPLICATION ENFORCER
Enforce ABAC and externalize authorization

CloudAz, the unified policy platform, offers centralized policy management that allows users to create and manage attributebased policies. It works with NextLabs' patented Dynamic Authorization Policy Engine to automate zero trust data security controls, where the policy engine authorizes access in real-time based on attribute-based policies. User activity, policy logs and data access records are stored in CloudAz's centralized audit repository, enabling organizations to easily monitor, track, and audit for compliance and reporting purposes.

Application Enforcer enhances the existing security model of an application, offering an additional layer of controls that cater to organizations with extensive security and compliance needs. This augmentation is achieved without the necessity for custom coding, making it a convenient and efficient solution.

Data Access Enforcer delivers dynamic data-level security controls and fine-grained data access governance, all while remaining independent of the user interface, API, service, and application. With Data Access Enforcer, businesses can enforce data obfuscation and segregation policies on a global scale, without custom coding.

SkyDRM offers persistent access control and usage management for digital information, ensuring comprehensive protection regardless of its location. Whether the data is stored in a file, regardless of its whereabouts, SkyDRM empowers organizations to safeguard and monitor critical documents such as intellectual property and product designs.



SSN: xxx-xx-xxxx
Date of Birth: xx.xx.xxxx
Language: English
Nationality:
rital Status:

CONCLUSION

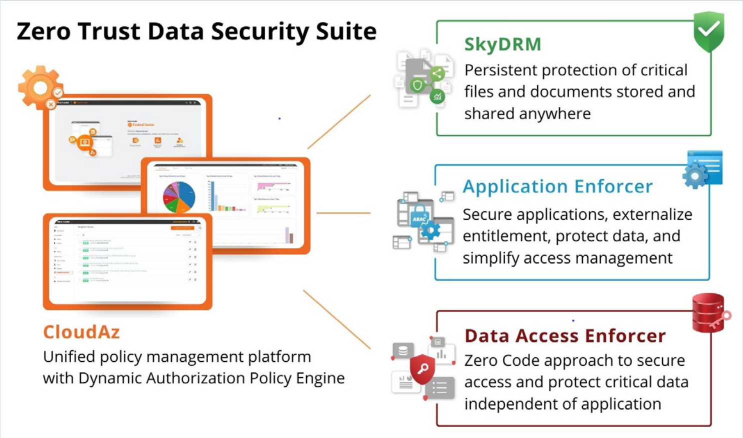
Zero-Trust Data-Centric Security, with its focus on access management and data protection over securing network boundaries, addresses the escalating cybersecurity challenges of expanding digital environments. The approach rests on principles of continuous verification, identity-awareness, leave privilege access, context-driven security and access visibility. In doing so, the strategy enables proactive breach prevention, streamlined compliance reporting, and improved access visibility, thereby significantly enhancing data security and integrity.

By leveraging NextLabs' Zero Trust Data Security Suite, organizations can implement a unified policy management and enforcement system to protect data at the source, use, transit, and rest, while integrating seamlessly with existing infrastructures. With quick time-to-value and seamless user experience, the Zero Trust Data Security Suite emerges as a highly effective solution inthe everchanging cybersecurity landscape.

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**.



Zero Trust Data Security Suite

CloudAz
Unified policy management platform
with Dynamic Authorization Policy Engine

SkyDRM
Persistent protection of critical files and documents stored and shared anywhere

Application Enforcer
Secure applications, externalize entitlement, protect data, and simplify access management

Data Access Enforcer
Zero Code approach to secure access and protect critical data independent of application