NEXTLABS®

CloudAz

Zero Trust Policy Platform

THE SITUATION

In this era of increased virtualization and collaboration, enterprises need a Zero Trust strategy to enable a virtual workforce and facilitate global data access without compromising sensitive data and business integrity. Given the rise of cloud computing and growing regulatory complexities in managing enterprise resources, there is a need for a paradigm shift from network-centric security to data-centric security. Accelerating industry change means a static manual approach to cybersecurity can no longer keep up with today's evolving security, privacy, and compliance requirements.

THE SOLUTION

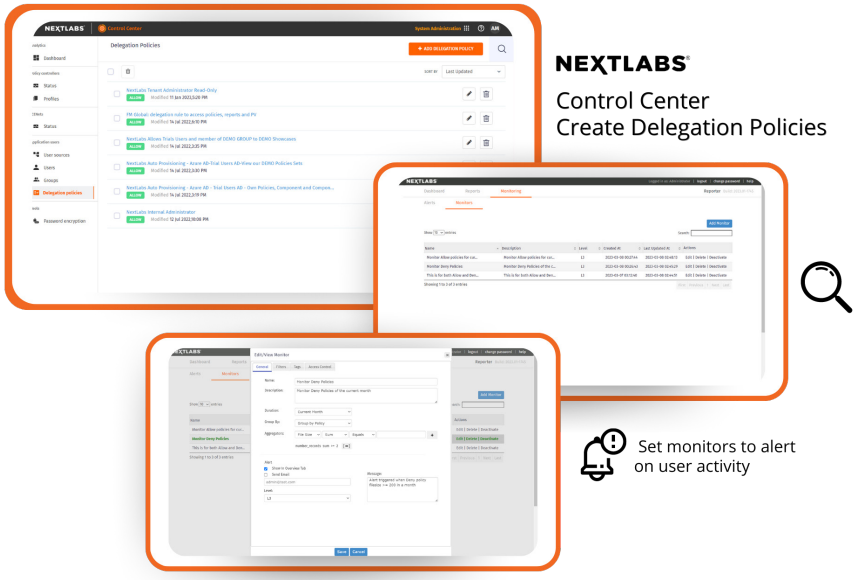
CloudAz is a Zero Trust unified policy platform that centralizes administration of policy with real-time enforcement. CloudAz automates the use of least privilege access, enforcing data-centric security measures and compliance in real time . As the control center of NextLabs' comprehensive Zero Trust Data-Centric Security Software Suite, CloudAz is the foundation to all three NextLabs enforcement solutions to protect data at the source (Application Enforcer), persistently protect files at rest and on the move (SkyDRM) and control global data access (Data Access Enforcer).

Through the enforcement of attribute-based security policies, CloudAz allows organizations to implement fine-grained controls in real-time as required by Zero Trust principles. Dynamic evaluation of data security policies ensures that access and authorization are always granted with up-to-date information, automating policy enforcement, logging, and auditing. CloudAz's zero code and out of the box integrations allow for rapid deployment and ease of maintenance. External attribute sources can be easily integrated into CloudAz, allowing any master data / attribute to be used in the definition and evaluation of policies to secure access and protect data.

KEY BENEFITS

- Implement a Zero Trust unified policy platform across all application and data systems, both on-premises and in the cloud.
- Help secure your organization's data and web applications, microservices, mobile apps, and other applications, regardless of where they are deployed
- Expedite application development and react rapidly to changes in business requirements, market conditions, or regulatory requirements
- Reduce the cost of compliance through more efficient and cost-effective monitoring and audit of your data access activity
- Simplify security management across multiple applications to ensure consistent application of access management and data protection requirements.

KEY FEATURES



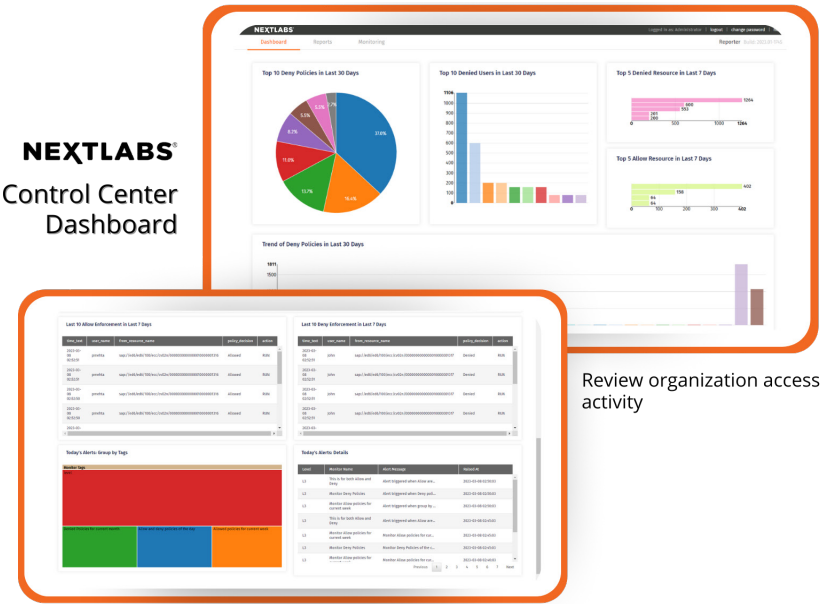
NEXTLABS®
Control Center
Create Delegation Policies

Set monitors to alert on user activity

Feature	Detail
Centralized Authorization Management Both On-Premises and in the Cloud	Centrally manage and review authorization policies across applications and services, whether on-premises, in the cloud, or in hybrid environments.
Externalized Authorization	Centrally manage authorization policies outside of applications, eliminating the need for costly code changes.
Attribute-Based Access Control (ABAC) Policies	Define policies in terms of attributes of the data being accessed, the context of the request, and the identity of the user or entity requesting access. This allows for fine-grained entitlement and security controls to data, regardless of how and where it is being accessed.
Integration with External Attribute Sources	Easy integration with external attribute sources to be used in the definition and evaluation of ABAC policies
Real-time Dynamic Policy Evaluation and Enforcement	Evaluate the attribute-based policies dynamically at the time of the data access request, automatically factoring in any changes to the attributes of the data or user.
Integration with any Application	Integrate with and protect single page web applications, mobile apps, micro-services, and even legacy applications
Application and Data Security	Control access at the application, transaction, data record, and field levels
Simple Policy and test plan creation	Business users can create policies and test plans to validate the policies in the web-based policy platform using 4GPL, without help from IT and without requiring code changes or application downtime
Simple multi-tenant policy enforcement architecture	Simple multi-tenant policy enforcement through policy tags, folders and target deployments
Secured Authentication and ABAC for Permission Management	Supports external identity providers for user authentication through SAML, OIDC, LDAP, and Azure AD/AD with multi-factor authentication. Fine-grained permissions can be set with attribute-based policies to dynamically authorize and delegate permissions to control user actions.
Activity Monitoring & Audit	Track and store real-time user and data access activity across apps and services in a central audit repository, simplifying the process of auditing security controls and demonstrating compliance.

NEXTLABS®

Control Center Dashboard



Review organization access activity

Feature	Detail
Policy Lifecycle Management	Enforce Segregation of Duties (SoD) in policy creation, with approval workflows and version control with policy rollback capabilities allowing seamless migration of policies from policy development to production system
Enterprise Database Support	Support for enterprise databases that include Oracle, MS SQL Server, PostgreSQL, IBM DB2, and cloud database services
Containerized Architecture and Flexible Deployment Model	Support for both Kubernetes-based and non-Kubernetes based cloud platforms to allow for seamless deployment of containers to cloud platforms. CloudAz microservices can be deployed, upgraded, and scaled independently.
Microservice Architecture with REST API	Extensive REST APIs allow external applications to easily integrate with the policy engine and the policy management system.
Distributed Policy Engine Architecture	Distributed architecture allows a single CloudAz instance to manage policies that are evaluated in widespread geographic locations, ensuring consistent application of policies across systems while reducing policy management overhead.
High Availability Architecture	Distributed policy engine architecture allows for seamless scaling and high availability of the solution for mission-critical applications. Continuous availability architecture ensures policies will still be evaluated even if Control Center component is temporarily offline.

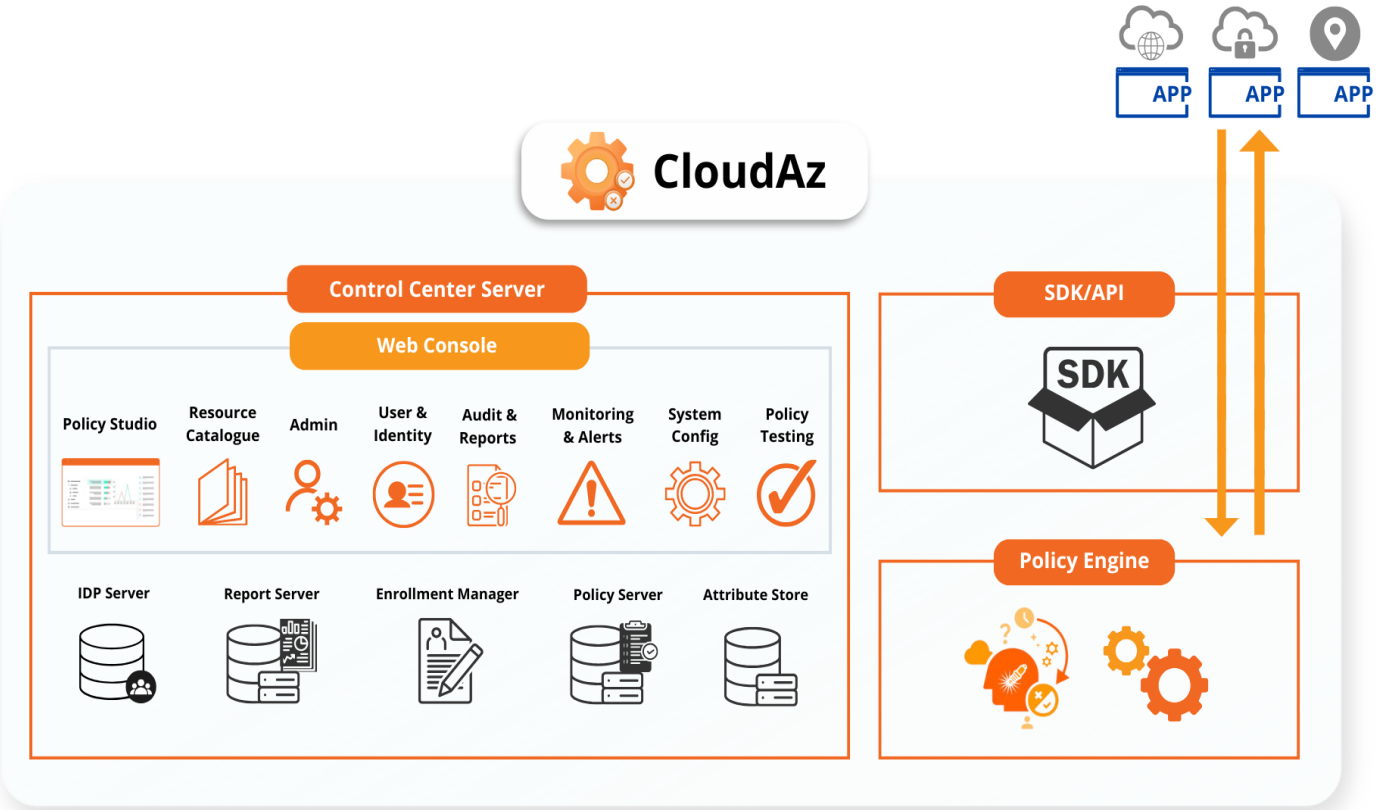
APIS/SDKS

Bespoke and home-grown applications can integrate with CloudAz through REST APIs and SDKs, allowing centralized management of authorization policies to enforce fine-grained access control, data security, and compliance procedures across all applications.

Application	SDK/API
Java	Java SDK
JavaScript	JavaScript SDK
C, C++	C, C++ SDK
C#, .NET	C#, .NET SDK
PHP, Web App	REST API
Microsoft COM	C++ SDK
Cloud services	REST API

KEY COMPONENTS

CloudAz is comprised of the following components. All can be deployed as microservices.



- **Control Center Server –** The central management of all NextLabs enforcement products enables organizations to apply consistent data security policies that are applied at the database layer, application layer, as well as when data is on the move.
  - **Policy Studio** - Web-based application that allows for the authoring and management of data security policies. Policies are defined using a 4th Generation Policy Language (4GPL) that requires no coding by the policy author.
  - **Policy Server** – Store of deployed policies to be accessed by the Policy Enforcement Points (PEPs)
  - **Reporter Application & Report Server** – Web-based application that allows Report Administrators to define and view reports for all policy evaluation and enforcement activity
  - **Audit Log** – Audit log of all activity on the CloudAz server, including all policy and data model changes
  - **Enrollment Manager** – Manages the enrollment of attribute sources so that they can be used in policy definition.
  - **Administrator Application & Management Server** – Web-based application that allows for the management of all CloudAz components, policies, and attribute sources.
- **Policy Engine** – Policy Engine serves as the Policy Decision Point for CloudAz based on the NextLabs' patented dynamic authorization technology. It evaluates the authorization policies whenever a request is made in real-time, using values of the attributes obtained from attribute sources as defined in the policies. Attribute values are retrieved, and policies are evaluated dynamically at the time of the authorization request, so that policy decisions are always based on the current values of the attributes. Since the same policy engine is being used across applications / policy enforcers, the same attributes can be used wherever policies are being enforced.
- **SDK** – Allows customers to integrate their own applications with CloudAz's APIs & SDKs, using Java, JavaScript, C, C++, C#, .NET, or REST. This enables organizations to use CloudAz's Control Center and Policy Engine with their own home-grown applications, ensuring that access control and data security policies are applied as consistently to bespoke applications as they are to enterprise applications with out of the box integrations.

DEPLOYMENT MODEL

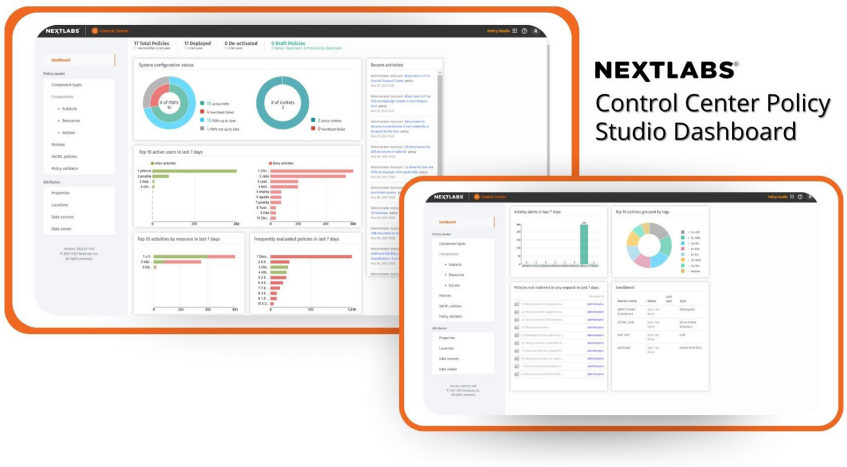
CloudAz can be deployed as a standalone cloud authorization service or in a hybrid model whereby applications and policy enforcement points can be either in the cloud or on-premises.

ON-PREMISES SYSTEM REQUIREMENTS

Component	Supported Platform(s)
Database	**Databases** • Microsoft SQL Server® 2016 and 2019 • Oracle® 19c, 21c • Oracle XE for development environments only • PostgreSQL 12(container), 13 (onpremises), 15 • IBM® Db2 Version 11.5
Control Center Server	**Operating systems** • Microsoft Windows Server® 2016, 2019, and 2022 • Red Hat® Enterprise Linux® (RHEL) 7.9 and 8.8 • Oracle Linux 7.9 and 8.8 • SUSE Linux Enterprise Server 15 SP5
Policy Controller	**Operating systems** • Microsoft Windows Server® 2016, 2019, and 2022 • Red Hat® Enterprise Linux® (RHEL) 7.9 and 8.8 • Oracle Linux 7.9 and 8.8 • SUSE Linux EnterpriseServer 15 SP5 **Application servers** • On Microsoft Windows:Apache Tomcat® 9.0.78 with OpenJDK 11.0.20_8 • On Red Hat Enterprise Linux: Apache Tomcat® 9.0.78 with OpenJDK 11.0.20_8 • On Oracle Linux: Apache Tomcat® 9.0.78 with OpenJDK 11.0.20_8 • On SUSE Linux: Apache Tomcat® 9.0.78 with OpenJDK 11.0.20_8
CloudAz web-based application	**Browsers** • Google Chrome • Firefox • Microsoft Edge • Safari

CLOUD DEPLOYMENT

Using CloudAz's cloud-native Control Center Server, Policy Controller, and web-based applications, organizations can take full advantage of cloud infrastructure, orchestration, data services and application run time. Microservices containerized architecture enables service-based deployment, allowing organizations to utilize cloud-native infrastructure and resources efficiently.



NEXTLABS®
Control Center Policy Studio Dashboard

PRIVATE, HYBRID & MULTI-CLOUD SYSTEM REQUIREMENTS

CloudAz provides private, hybrid and multi-cloud deployment support by leveraging Docker and Kubernetes.

Supported Cloud Platforms

- Google Kubernetes Engine (GKE)
- Azure Kubernetes Service (AKS)
- Amazon Elastic Kubernetes Service (EKS)

Supported Cloud Provider Managed Database Services

- Google Cloud SQL
- Amazon Relational Database Service (AWS RDS)

Supported Multi-cluster container orchestration platforms

- Rancher
- OpenShift

CLOUD DEPLOYMENT SYSTEM SPECIFICATIONS

Service Provider	Specifications
AWS ECS	ECS Cluster, EC2 Worker Nodes, EFS, Auto-Scaling Group, Load Balancer, Route 53, ACM, Cloud Map, ECR
AWS EKS	EKS Cluster, EC2 Worker Nodes, EFS, Auto-Scaling group, Ingress Controller, Load Balancer, Route 53, ECR
AWS EC2 instance	Windows installer, Linux Chef Installer, Kubernetes, Auto-Scaling Group, Load Balancer, Route 53, ACM, ECR
Azure AKS	AKS Cluster, Azure Storage Account, Ingress Controller, Load Balancer, Azure DNS, Azure Container Registries
Azure Virtual Machines	Windows installer, Linux Chef Installer, Kubernetes, Virtual Machine Scale Sets, Load Balancer, DNS Zones, Container Registries
Google GKE	GKE Cluster, Instance Groups, Filestore, Ingress Controller, Load Balancer, Cloud DNS, GCR
Google Compute Engine VM instances	Windows installer, Linux Chef Installer, Kubernetes, Instance Groups, Load Balancing, Cloud DNS, Container Registry
OpenShift	OpenShift Cluster, Worker Nodes, Network File Share Storage, OpenShift Route, Certificates, Load Balancer, DNS Records, Container Registry
Rancher (Kubernetes management platform)	RKE Cluster, AWS EKS, Azure AKS, Google GKE

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.