

NEXTLABS®

Zero Trust
Data-Centric Security

CloudAz

A Zero Trust Policy Platform





Virtual Workforce

In this era of increased virtualization and collaboration, enterprises need a **zero trust strategy** to enable a virtual workforce without compromising sensitive data and business integrity.



Single Global Instance

The global workforce and business partners need to access data from anywhere in a way that is simple and secure.



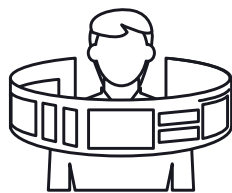
Regulatory Landscape

A shifting geopolitical landscape has spawned regulatory complexities in managing digital enterprise resources.



Cloud Computing Paradigm

Adoption of cloud computing necessitates a paradigm shift from network-centric security to **data-centric security**.



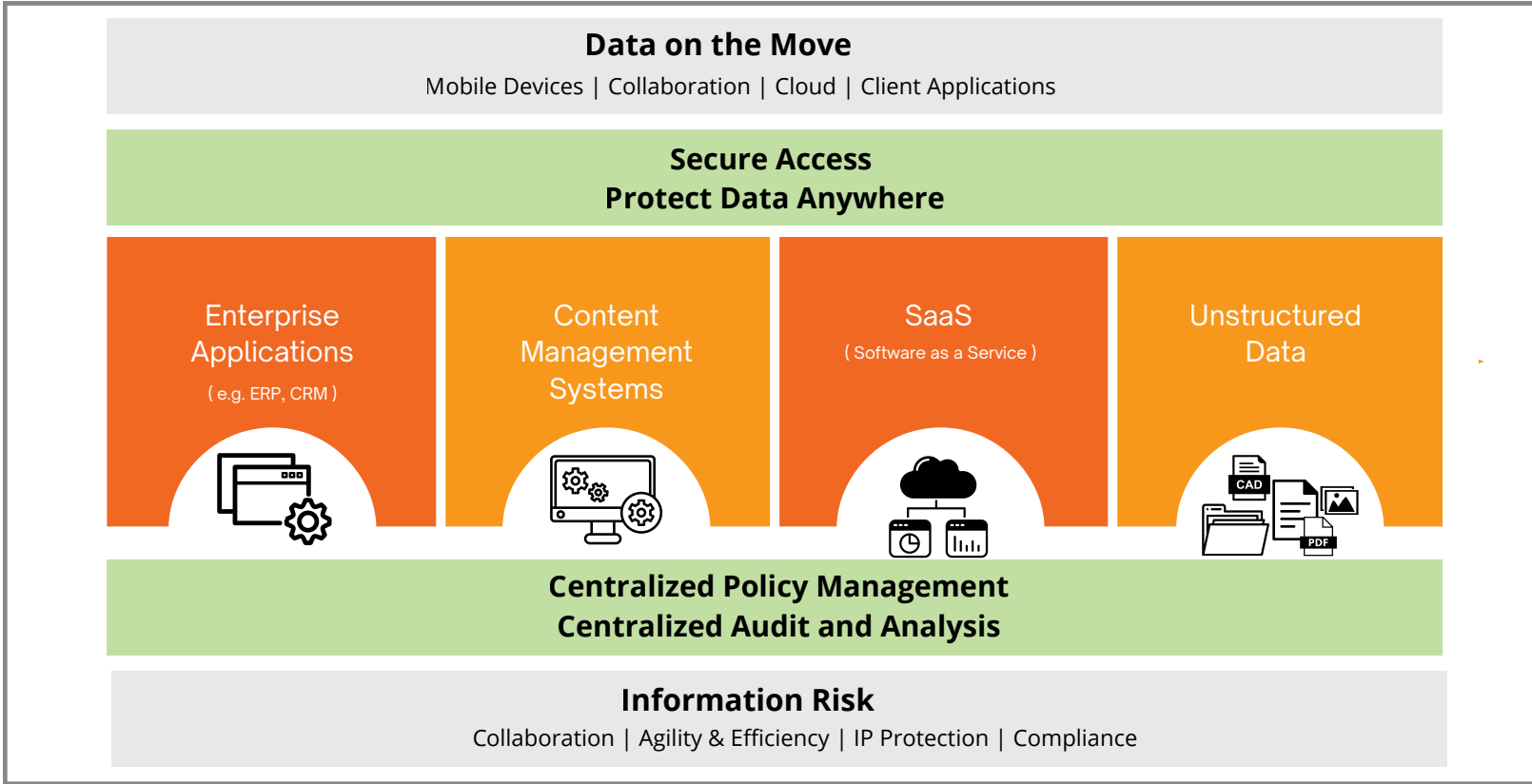
Industry Evolution

Accelerating industry change means a static manual approach to cybersecurity can no longer keep up with today's evolving security, privacy, and compliance requirements.

 How can enterprises modernize IT, ensure compliance, and protect data while reducing cost, complexity, and breaches?

 It is inevitable for enterprises to progress from silos toward a unified approach for access management and data security.





Requirements of a unified approach:

- Centralized policy platform working with existing infrastructure and applications
- Native integration with key applications
- Dynamic authorization technology to secures structured and unstructured data anywhere
- Automated and centralized audit and compliance reporting
- Protect data everywhere – whether it is on premises or in the cloud
- Safeguard sensitive information throughout its entire lifecycle

At the core of the unified approach is a **unified policy platform** that applies the zero trust principle to to secure access and protect data across silos using **attribute**-based **policies**. Key elements of the platform include:

1 Zero Trust Architecture

A cybersecurity model designed to secure resources by eliminating implicit trust and verifying every stage of a digital interaction.



2

Data-Centric Security

An approach to safeguarding sensitive information by protecting the data itself with real-time enforcement.



3 Dynamic Authorization

Enforce zero trust data-centric security controls in real-time, using policy to ensure least privilege access and safeguard data.

Attributes represent information about the user, data or environment.
Policy is a rule that uses attributes to decide whether to grant or deny access to a resource.

Automation

Automates data security, compliance procedures, and internal controls to enhance competitiveness and business agility.

Integration

Out-of-the-box integration with enterprise applications (eg. ERP, PLM, databases), microservices and business processes without disruptions.

Enforcement

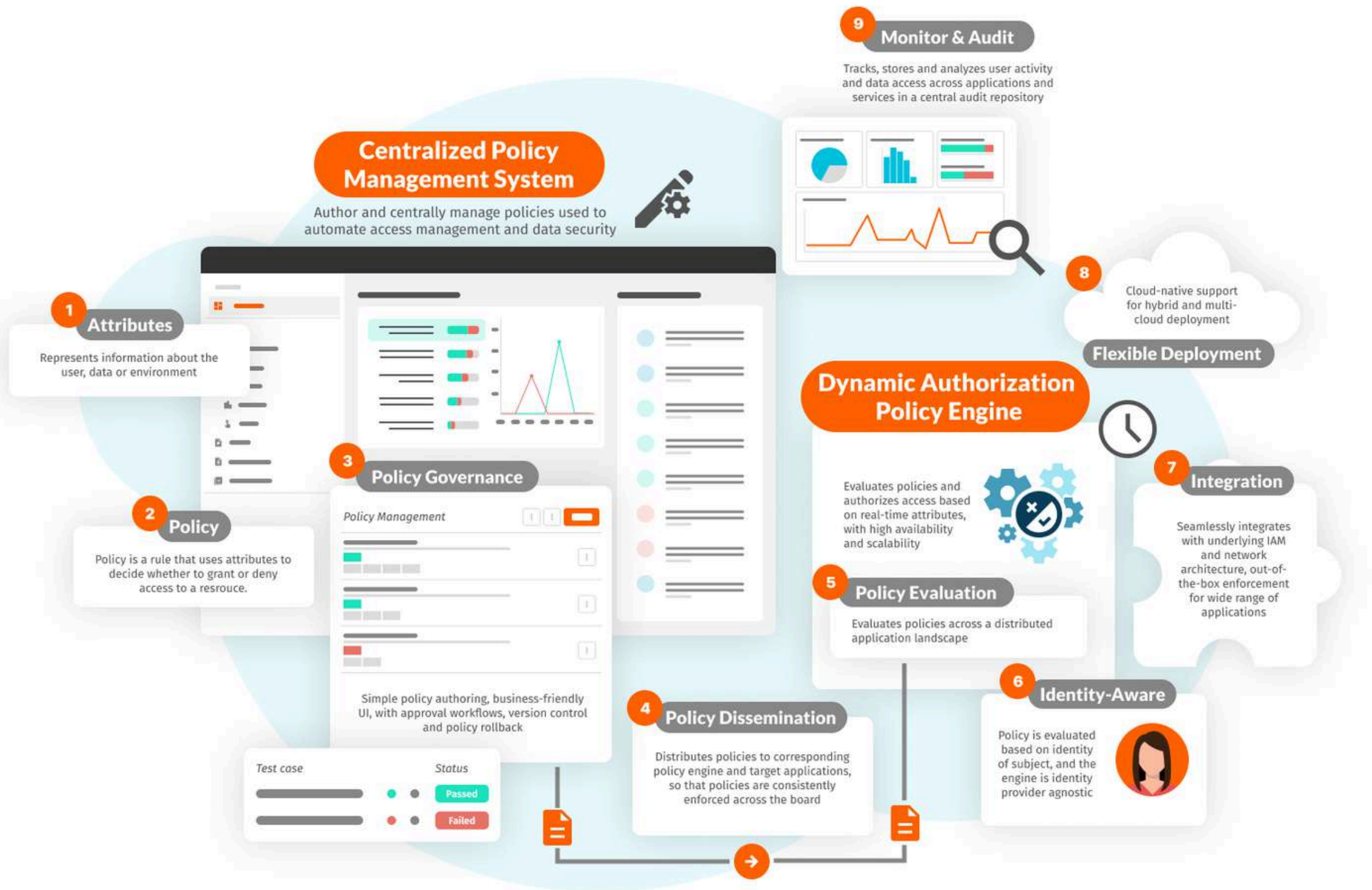
Detects, alerts and applies preventive controls to enforce policy in real time.

Deployment

Runs in cloud natively, deploys using containers in a hybrid and multi-cloud environments.



CloudAz is a **unified policy platform with real-time enforcement** that centralizes administration and employs zero trust principle to enforce data-centric security measures and compliance in real time, by automating least privilege access and securing applications and data.



CloudAz Benefits:

Unify & Modernize it

Streamline IT infrastructure, unify application and business services under a shared services model, expedite system consolidation and eliminate security silos, accelerate cloud adoption without compromising security coverage and total cost of ownership.

Improve Business Agility

Accelerate time to market and enhance competitive advantage through automation and simplified change management; easily incorporate new business models without code changes and application downtime.

Enhance Cybersecurity

Prevent data leakage and cyber-attacks by automating least privilege access to eliminate implicit trust and safeguard data across business-critical applications (e.g. SAP, Siemens, Microsoft, ServiceNow, Oracle), whether the data is at rest or on the move.

Increase Collaboration

Safeguard trade secrets and sensitive information to ensure secure data sharing and accelerate collaboration through central access control and data segregation policies.

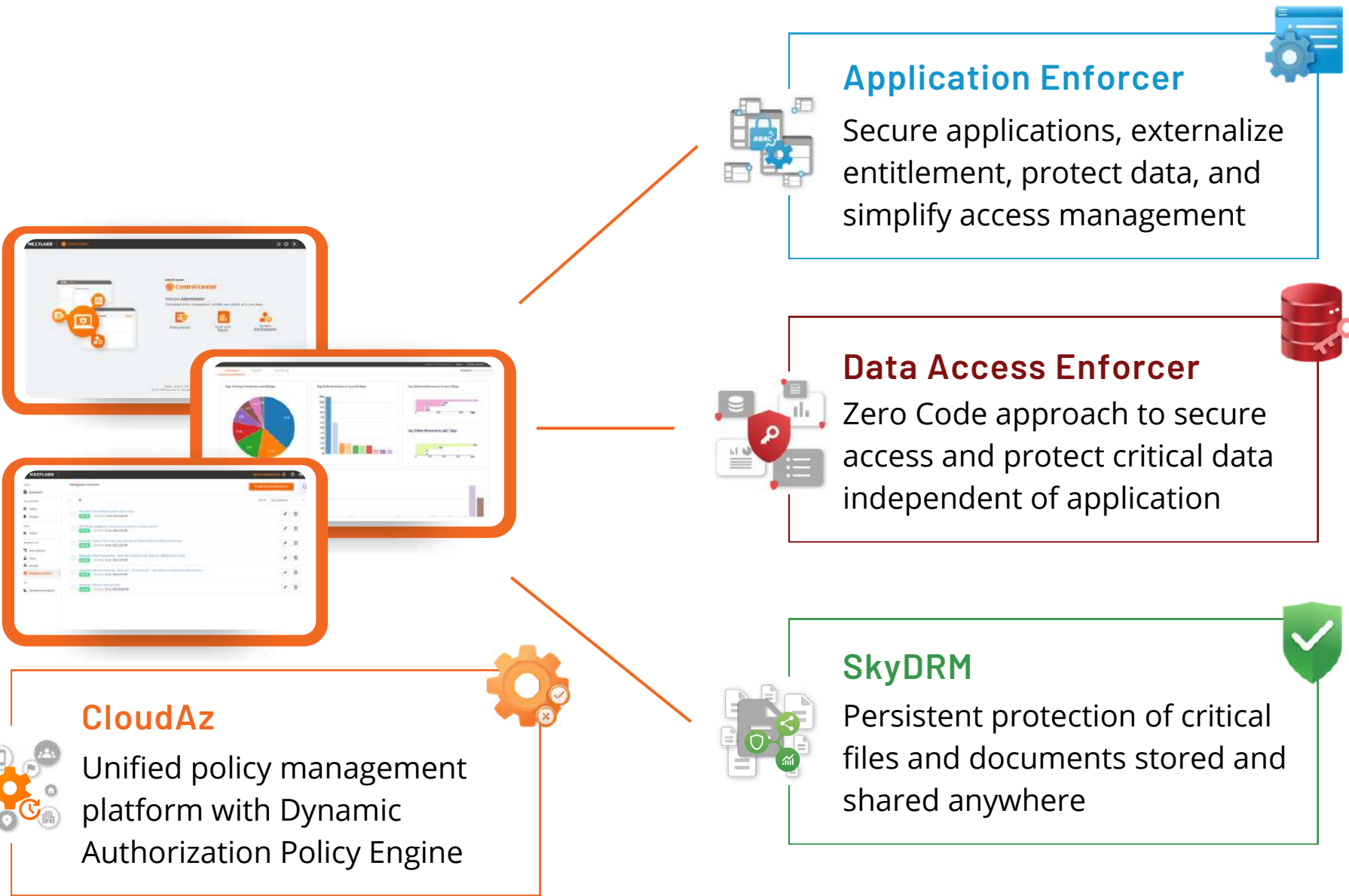
Ensure Compliance

Ensure compliance with regulations such as GDPR, ITAR, SOX and EH&S, simplify audit processes with centralized logging and reporting of all data access activity and authorization decisions.



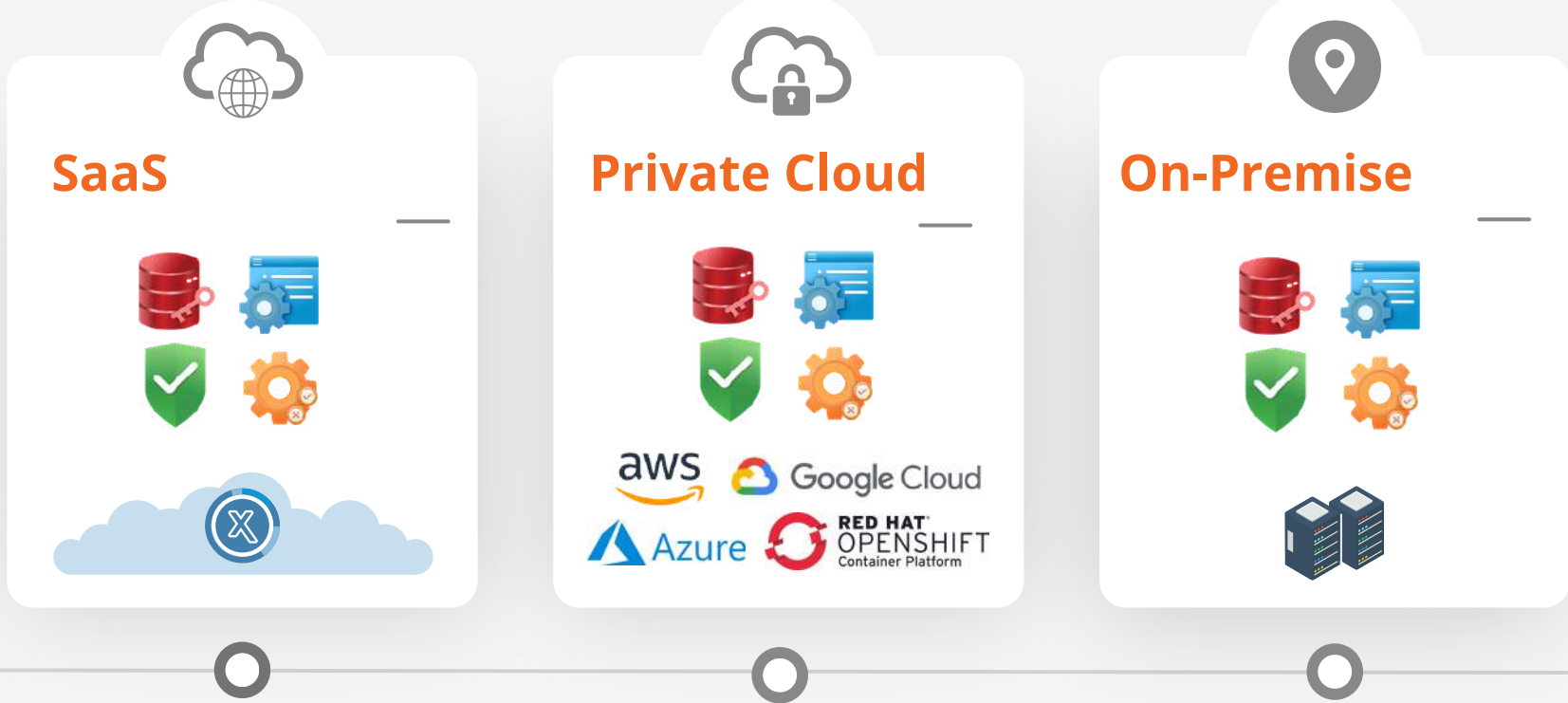
CloudAz is the control center of the NextLabs comprehensive Data Security Software Suite, which includes three enforcement solutions to protect data at the source (Application Enforcer), persistently protect files at rest and on the move (SkyDRM), and control global data access (Data Access Enforcer).

Data-Centric Security Enforcement



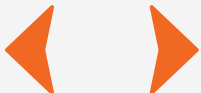
Flexible Deployment Options

CloudAz can be deployed anywhere, be it on-premises, in private cloud, or as a SaaS. CloudAz runs natively on AWS, Azure, OpenShift and Google Cloud. With support for multiple deployment models, it gives you the freedom to choose the right cloud deployment strategy, whether it is hybrid or multi-cloud. With the ability to create new instances across multiple landscapes - set up development, test, and production environments can be done quickly. Policies can be transported between cloud and on-premise deployments, ensuring consistent policy enforcement across all environments.



Cloud Deployment System Specifications:

Service Provider	Specifications
AWS ECS	ECS Cluster, EC2 Worker Nodes, EFS, Auto-Scaling Group, Load Balancer, Route 53, ACM, RDS, Cloud Map, ECR
AWS EKS	EKS Cluster, EC2 Worker Nodes, EFS, Auto-Scaling group, Ingress Controller, Load Balancer, Route 53, RDS, ECR
Azure	AKS Cluster, VMs, Azure Storage Account, Ingress Controller, Load Balancer, Azure DNS, Azure SQL, Azure Container Registries
OpenShift	OpenShift Cluster, Worker Nodes, Network File Share Storage, OpenShift Route, Certificates, Load Balancer, DNS Records, External DBMS, Container Registry
Google Cloud	GKE Cluster, Instance Groups, Filestore, Ingress Controller, Load Balancer, Cloud DNS, Cloud SQL, GCR





NEXTLABS®

**Zero Trust
Data-Centric Security**

Follow us



www.nextlabs.com/contact-us

© NextLabs Inc. All Rights Reserved

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>.

