NEXTLABS®

White Paper

Implementation of Zero Trust Application Protection

In our first whitepaper in this series, Implementation of a Zero Trust Architecture, we examined how organizations can build a Zero Trust foundation by securing their IT environments. That paper emphasized the importance of protecting data, highlighting how the Cybersecurity and Infrastructure Security Agency (CISA)'s Zero Trust Maturity Model (ZTMM) and the Department of Defense (DoD)'s Zero Trust Reference Architecture (ZTRA) position data security as a central pillar of Zero Trust. We also introduced how NextLabs' Zero Trust Data-Centric Security platform, CloudAz, can serve as a foundation for Zero Trust adoption.

Our second whitepaper in the series, Implementation of Zero Trust Data Protection, builds upon the first by exploring the implementation of Zero Trust Data Protection, detailing strategies, technologies, and best practices to safeguard sensitive information in an increasingly complex threat landscape

This paper extends that discussion to the Applications & Workloads pillar. Applications are not only critical to business operations but also serve as gateways to sensitive data. Securing them is essential for a holistic Zero Trust strategy. In the sections that follow, we explore how organizations can apply Data-Centric Security (DCS) principles to protect enterprise applications, workloads, and APIs. This paper complements our earlier focus on data, reflecting both CISA and DoD frameworks that treat applications as essential supports for securing information.

Requirements for Zero Trust Application Protection

CISA: Applications & Workloads Pillar

CISA's Zero Trust Maturity Model identifies Applications & Workloads as one of five critical pillars. This pillar addresses the need to secure the applications and workloads that organizations depend on daily. Applications represent frequent attack surfaces and must therefore be treated as integral components of a Zero Trust strategy.

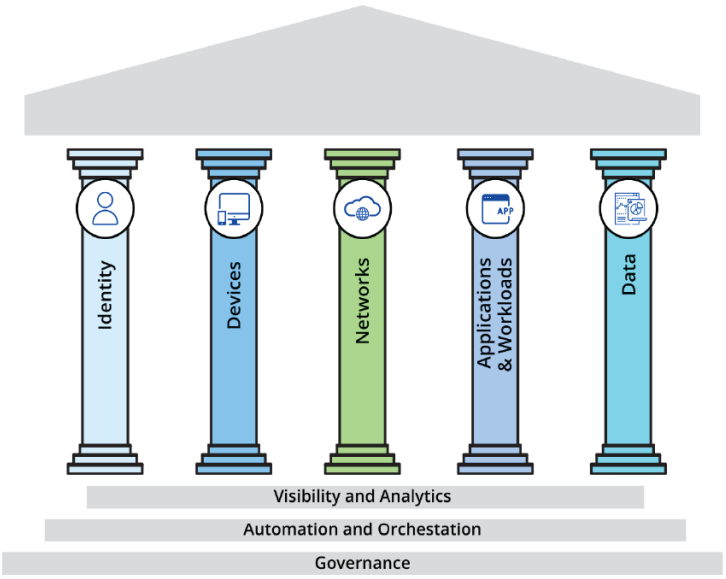


Figure 1: CISA's Zero Trust Maturity Model Pillars

Key practices recommended by CISA include:

- Logical segregation: Dividing application environments into smaller, isolated zones to reduce the risk of lateral movement.
- Application security controls: Implementing runtime application self-protection (RASP) and web application firewalls (WAF) to protect applications during execution.
- Workload isolation: Restricting communications between services and applications to limit propagation of breaches.
- Continuous monitoring: Using real-time analytics to identify and respond to anomalies in workload or application behavior.

DoD: Workloads Pillar

The DoD's Zero Trust Reference Architecture reflects the unique mission requirements of defense operations. The Workloads pillar is focused on securing applications, services, and processes that are essential to military readiness and operations. Given the high-value nature of DoD systems, adversaries are often sophisticated and persistent, making workload protection a top priority.

DoD strategies include:

- Logical segregation: Creating isolated workload segments that contain breaches within non-critical systems.
- Runtime application security: Deploying RASP and WAF technologies to protect applications dynamically.
- Continuous monitoring and response: Ensuring anomalies are detected in real time with automated incident response to mitigate risks.
- Strong policy enforcement: Requiring strict adherence to least-privilege and need-to-know access principles.

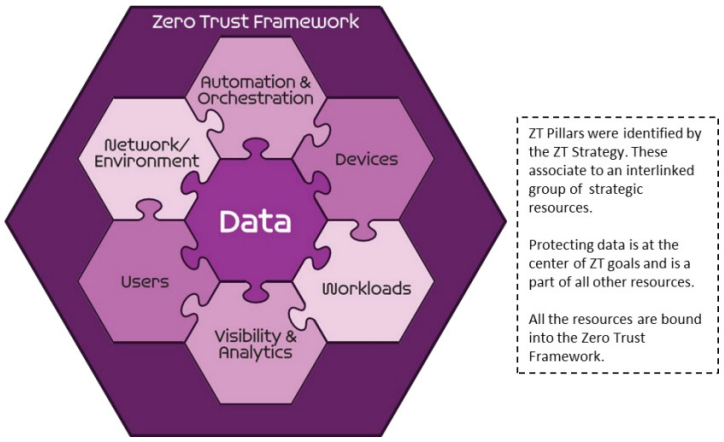


Figure 2: The DoD's Zero Trust Pillars

Comparative View

While CISA and DoD both emphasize Applications and Workloads, their focus reflects their operating contexts:

- CISA emphasizes broad enterprise resilience, scalability, and continuous monitoring for diverse commercial environments.
- DoD emphasizes mission assurance, operational resilience, and defense against advanced persistent threats.

Together, they highlight the necessity of securing applications as a foundational component of Zero Trust.

Why Zero Trust Data-Centric Security is the Best Approach for Protecting Applications

Applications are not only business enablers but also gateways to sensitive data. A breach in an application often provides attackers with direct access to data, making application protection inseparable from data protection. Zero Trust requires that protections extend beyond the network perimeter and follow the data wherever it resides or flows.

Data-Centric Security (DCS) strengthens application protection by ensuring that security policies are enforced consistently at the application and data level. Instead of relying solely on network boundaries or static roles, DCS enforces dynamic policies based on who is accessing the data, from where, under what conditions, and for what purpose.

The core DCS elements—Data, Identity, Authorization, Environment, Policies, Enforcement, and Audit—each play a critical role in protecting applications:

- Data: Encryption, tokenization, and segregation of sensitive data.
- Identity: Strong authentication, including MFA, of individuals and processes
- Authorization: Dynamic access and entitlement controls (PBAC/ABAC)
- Environment: Contextual access decisions considering location, device posture, and risk.
- Policies: Fine-grained rules enforcing least privilege.
- Enforcement: Runtime controls applied consistently at access points.
- Audit: Comprehensive logging and monitoring for compliance and incident investigation.

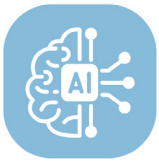
Examples of Data-Centric Application Protection Use Cases

Zero Trust DCS principles can be applied across a wide variety of use cases, strengthening security for both modern and legacy applications:

Protecting Enterprise Applications (ERP, PLM, CRM, etc.)
These applications manage sensitive business data and intellectual property. DCS ensures that access is context-aware, dynamically adjusting based on user identity, role, and behavior. Externalized authorization consistently enforces authorization across all applications, instead of each application managing its own access control rules.

Preventing Unauthorized Access and Lateral Movement
Zero Trust requires restricting movement within applications, using logical segregation and least-privilege policies to contain breaches.

Ensuring API Security and Secure Application-to-Application Communication with Microservices and Containerized Applications
APIs are frequent attack vectors. Applying Zero Trust controls—including authentication, authorization, and encryption—protects data shared between applications. Applying Zero Trust principles allows organizations to secure inter-service communications, prevent lateral movement, and monitor runtime behaviors.



Artificial Intelligence and Data Analytics
As more and more organizations incorporate AI into their business operations, access to the AI systems and models must be secured. In addition to securing the AI applications themselves, applications that use the AI systems must secure both the business and transaction data that is being analyzed as well as the output of the AI systems.

Enforcing Entitlement Controls and Segregation of Duties
Segregation of Duties can be enforced at the application level by applying entitlement controls, such as allowing view access without exporting or enforcing controls that prevent both creation and payment of invoices.

How to Implement Zero Trust Data-Centric Security Controls to Protect Applications

1. **Identify**: Catalog the applications, workloads, and APIs that handle or access sensitive data. Determine which business processes depend on them and classify the data they process based on sensitivity and regulatory requirements.
2. **Understand**: Analyze how applications interact with users, data, and other services. Document access pathways, roles, and dependencies—including who should access what, under what conditions, and through which APIs or integrations. Identify risks such as excessive privileges, unmonitored data flows, or insufficient segmentation.
3. **Control**: Define security policies and governance models that enforce least-privilege and segregation of duties across applications. Establish rules for entitlement management, data flow restrictions, and workload isolation to prevent unauthorized access and lateral movement.
4. **Enforcement**: Implement dynamic and contextual controls to operationalize those policies. Use policy-based and attribute-based access control (PBAC/ABAC) for fine-grained decisions; apply runtime enforcement at the application layer; and secure API communications through strong authentication, authorization, and encryption.
5. **Audit**: Continuously monitor application activity and access patterns. Analyze logs and enforcement events to detect anomalies, validate compliance, and support forensic investigations. Use adaptive analytics to adjust policies as risks and operating conditions evolve.

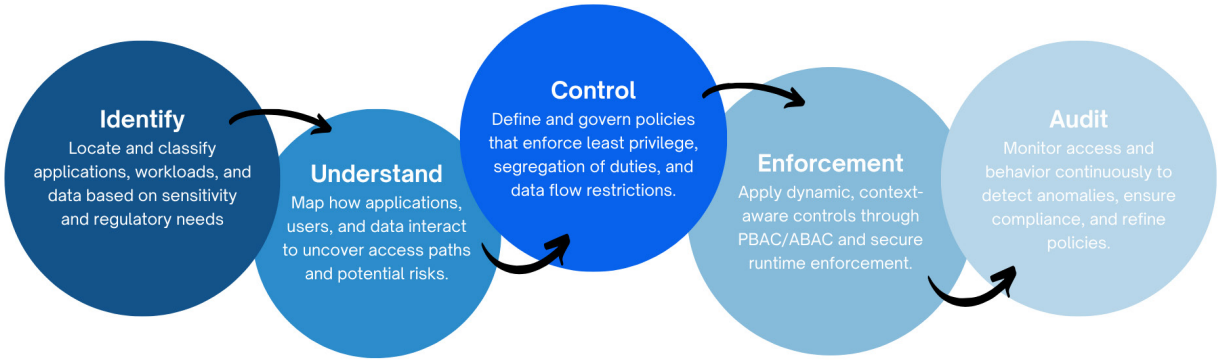


Figure 3: Five Steps to Implement Zero Trust for Applications

Key Zero Trust Data-Centric Security Controls

To consistently enforce Zero Trust principles across all applications, organizations should adopt a standardized set of data-centric controls. These controls ensure that sensitive data remains protected throughout its lifecycle—whether stored, processed, or shared.

Data Segregation: Data segregation provides the foundation by isolating sensitive application data based on its classification. By separating regulated or high-value data from general information, organizations can apply stricter safeguards where they are needed most.

Data Masking and Obfuscation: Data masking and obfuscation further enhance protection by anonymizing sensitive fields during processing or use. This ensures that personal or confidential details are shielded, even in environments where data must be accessed for testing, analytics, or operational purposes.

Data Loss and Extraction Controls: To prevent unauthorized exposure, data loss and extraction controls block attempts to

download, copy, or export sensitive information without approval. These safeguards minimize the risk of both accidental leaks and deliberate exfiltration.

Digital Rights Management (DRM): DRM extends protection beyond application boundaries by applying persistent controls directly to files. Even when data is shared outside the originating system, DRM ensures that usage policies—such as restrictions on editing, printing, or forwarding—remain in force.

Entitlement Management: Effective entitlement management is also essential, enabling organizations to dynamically assign, adjust, and revoke access permissions in real time across all applications across the enterprise. This flexibility supports the principle of least privilege and ensures access reflects the user's current role and context, helping to prevent data loss.

Policy-Based and Attribute-Based Access Control (PBAC/ABAC): Finally, PBAC and ABAC enforce contextual access consistently across applications. By evaluating user identity, attributes, and environmental conditions, these models deliver fine-grained, adaptive access decisions that strengthen data protection at every interaction point.

These data-centric safeguards place protection directly at the data layer, making security portable and persistent. By embedding controls within the data, organizations ensure that sensitive information maintains its integrity and confidentiality wherever it travels.

How NextLabs Helps Implement Zero Trust Data-Centric Security

NextLabs provides solutions that operationalize Zero Trust by mapping capabilities directly to use cases and controls outlined above. Its solutions extend beyond traditional access control to provide dynamic, context-aware, and persistent protections.

CloudAz

Provides dynamic PBAC/ABAC enforcement across enterprise and cloud-native applications, ensuring least-privilege access policies are applied in real time.

Application Enforcer

Delivers runtime enforcement of data security policies and contextual decisioning at the application layer.

SkyDRM

Extends protections to documents and files beyond the application environment through persistent DRM.

Data Access Enforcer (DAE)

Enforces policies at the data access layer, controlling access to data stored in data sources regardless of the application or interface being used to access the data

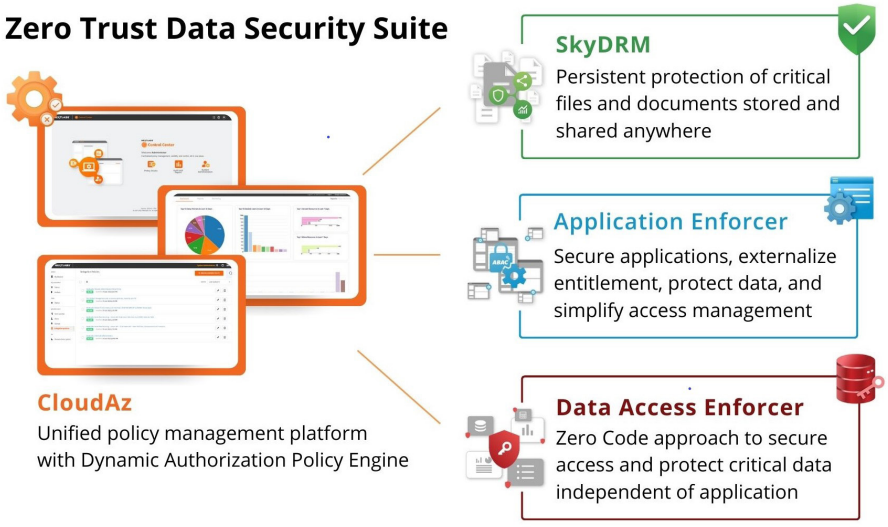


Figure 4: NextLabs Zero Trust Data-Centric Security Suite

Together, these solutions enable organizations to reduce attack surfaces, comply with regulatory mandates, and secure applications while supporting business agility.

Key Takeaways

Zero Trust represents a paradigm shift from perimeter-based defenses to continuous verification and least-privilege enforcement across all enterprise systems. Applications, as gateways to data, are critical to this approach.

By embedding Data-Centric Security principles into application protection strategies, organizations can ensure that controls follow the data wherever it flows, across diverse environments and usage scenarios.

NextLabs extends these principles through advanced authorization, runtime enforcement, and persistent usage controls, helping enterprises secure sensitive applications, achieve compliance, and adapt to evolving cyber threats.

References

- NextLabs White Paper: NIST 800-207: Zero Trust Architecture
- NextLabs White Paper: Implementation of a Zero Trust Architecture
- NextLabs White Paper: Implementation of a Zero Trust Data Protection
- NIST National Cybersecurity Center of Excellence: Implementing a Zero Trust Architecture
- The NIST Cybersecurity Framework (CSF) 2.0
- NextLabs CloudAz
- NextLabs DAE Product Page
- NextLabs SkyDRM
- NIST ABAC Reference Document
- NIST DevSecOps Project

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software & services to protect data anytime and anywhere regardless of where data resides – whether it is across application, database, file or file repository – on-premises or in the cloud. 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 violations. NextLabs software prevents unauthorized access and automates enforcement of security controls and compliance policies to enable secure collaboration and 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 https://www.nextlabs.com/company/.