NEXTLABS®

White Paper

Using NextLabs to Implement the Department of Defense (DoD) Zero Trust Reference Architecture

An Overview by NextLabs

"Implementing a zero-trust architecture has become a federal cybersecurity mandate and a business imperative. We are excited to work with industry demonstrating various approaches to implementing a zero-trust architecture **[NIST SP 800-207]** using a diverse mix of vendor products and capabilities, and share how-to guidance and lessons learned from the experience."

- Natalia Martin, Director of NCCoE

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Purpose

The DoD Zero-Trust Reference Architecture Version 2.0 establishes a framework which provides guidance through architectural Pillars and Principles for implementing a secure, Data-Centric, Zero Trust Architecture. This brief describes how NextLabs, the pioneer in Data-Centric Security and Attribute-Based Policy Enforcement, can help DoD stakeholders implement ZTA in alignment with the DoD ZTA RA with a simplified, automated approach.

Vision and High-Level Goals for the DoD ZTA RA

The growth in cloud computing, the Internet of Things (IoT), business partnerships, and remote work has increased the complexity of managing digital enterprise resources. Traditional network security has focused on securing the perimeter, which has become ineffective as network perimeters become increasingly hard to define. This is due to its limitations and vulnerability resulting from the greater number of points of entry, exit, and data access.

Network perimeters are especially difficult to define in hybrid cloud environments. If subjects (end users, applications, non-person entities that request information from resources) are given broad access to corporate resources within the perimeter, compromising those subjects' credentials can allow malicious actors to gain access to these critical resources, resulting in massive data breaches or other malicious activity.

So how can organizations protect their core data assets from malicious actors in an increasingly digitalized business environment where network perimeters are undefined?

The Department of Defense Zero Trust Architecture Version 2.0 defines five high-level goals (section 1.4.1) that NextLabs capabilities help to address.

• **Modernize Information Enterprise to Address Gaps and Seams**.

NextLabs provides a data-centric external, centralized policy management platform that allows organizations to apply consistent data access policies across the entire enterprise, eliminating the gaps that result from having multiple networks that each have their own security measures. Security policies are defined according to the data they cover, not the networks or devices on which that data resides. This ensures that only the right people can see the right data and take actions they are authorized for, regardless of where and how they are accessing that data.

• **Simplify Security Architecture.**

NextLabs simplifies Security Architecture by allowing administrators to define, manage, and audit all their data security policies from a single interface. NextLabs' natural language policy definitions and out of the box integrations allow for easy deployment and policy enforcement at the database, application, and file level, simplifying the process of enforcing data security policies.

• **Produce Consistent Policy.**

The NextLabs Data-Centric Policy Platform's support for different platforms and provided APIs and SDKs for many different development environments mean that policy enforcement can be integrated with any application. Attributes can be sourced from multiple locations and used across all policies. When combined with products that provide enforcement at the database, application, and file level it is possible to enforce consistent data-centric policies wherever that data is being accessed.

• **Optimize Data Management Operations.**

NextLabs solutions allow enforcement of consistent data security policies at the database, application, and file level, allowing those data-centric policies to be applied to both structured and unstructured data, inside and outside of their originating systems.

• **Provide Dynamic Credentialing and Authorization.**

NextLabs has more patents around Dynamic Authorization and a more robust Policy Engine than any other ABAC provider in this space. Policies are evaluated in real-time with access being granted or denied at the time of request (i.e., at runtime). The policies evaluate the latest user and environment attributes to accurately determine the what, why, when, how, and where of access to the content.

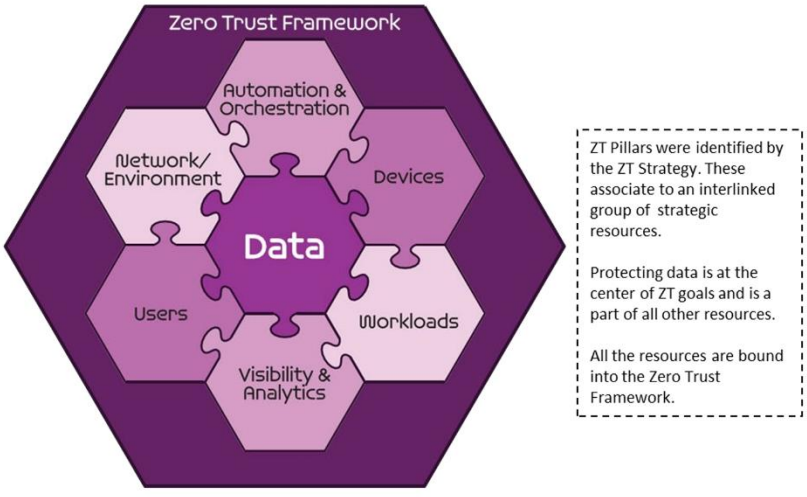
Tenets of Zero Trust (DoD ZT RA Version 2.0, Section 2.2)

Zero Trust has five major tenets that represent the foundational elements and influence all aspects within Zero Trust.

1. **Assume a Hostile Environment.**
2. **Presume Breach.**
3. **Never Trust, Always Verify.**
4. **Scrutinize Explicitly.**
5. **Apply Unified Analytics.**

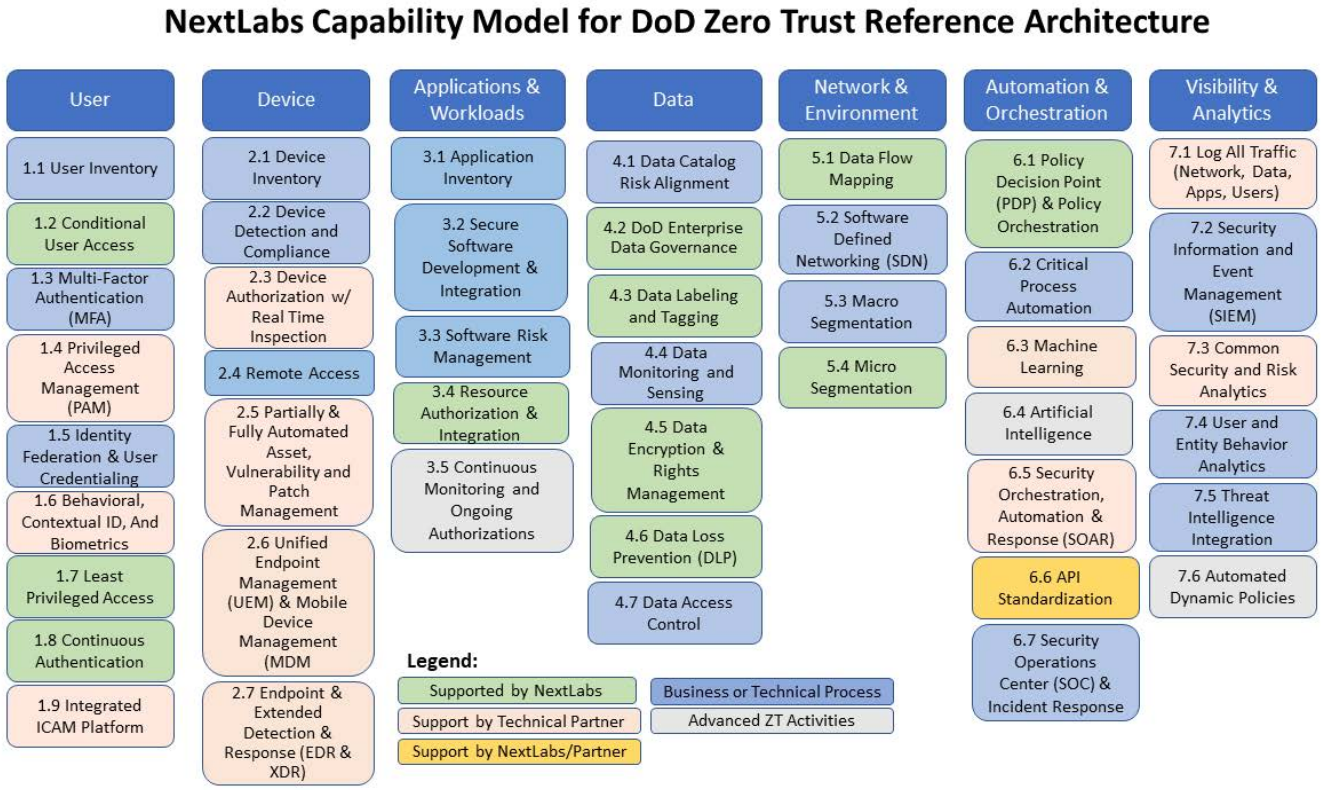
Zero Trust Pillars (DoD ZT RA version 2.0, Section 2.3)

The DoD Zero Trust Reference Architecture defines seven Zero Trust Pillars, each of which map to multiple capabilities. The NextLabs Zero Trust Data-Centric Security Suite addresses many of these capabilities across the seven Zero Trust pillars.



NextLabs Capabilities

The DoD defines capabilities within each of the seven pillars, as shown in the chart below (NextLabs supported capabilities are shown in green). For a definition of each capability, please reference the DoD Zero Trust Capability Execution Roadmap, available for download at https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilitiesActivities.pdf.



User:

- **1.2 Conditional User Access –** Users are only granted access to protected resources if they meet all of the conditions in the NextLabs Attribute-Based Access Control (ABAC) policies which are dynamically evaluated and enforced at the time of the data access request.
- **1.3 Multi-Factor Authentication (MFA) –** NextLabs CloudAz supports MFA for authentication using its internal IDP. MFA can also be enabled on IDP when using an external IDP for SSO.
- **1.4 Privileged Access Management (PAM) –** NextLabs Zero Trust Data-Centric Security Suite allows for access to be controlled not just for standard users but also for users with privileged access. Attributes of the user are used to evaluate access requests, so that data access policies are still enforced for those with elevated privileges.
- **1.7 Least Privileged Access –** NextLabs granular data access policies allow access to be granted on a need-to-know basis, only granting the minimum level of access required, and no more.
- **1.8 Continuous Authentication–** NextLabs data access policies are dynamically evaluated every time there is a data access request, even if the user has already authenticated and has an active connection.
- **1.9 Integrated ICAM Platform -** NextLabs' CloudAz allows for policies to incorporate user attributes from multiple identity providers so that policies can allow access based on information from several sources, instead of being limited to the identity information available through a single source.

Device:

- **2.3 Device Authorization w/Real Time Inspection –** NextLabs policies control access for devices that are accessing resources protected by the policies. Attributes of the device are incorporated into policies so that access to resources can be controlled based on characteristics of the device that is initiating the request or the device where the request is originating from. All of this happens dynamically at the time of the data access request.
- **2.5 Partially & Fully Automated Asset, Vulnerability, and Patch Management –** NextLabs products can detect the update, patch, and vulnerability status of devices and evaluate policies based on the device posture.

Applications and Workload:

- **3.2 Secure Software Development & Integration –** NextLabs reviews component and application security throughout the software development lifecycle (SDLC) as part of our processes of continuous integration (CI) and continuous delivery (CD).
- **3.3 Software Risk Management –** NextLabs reviews component and application security throughout the software development lifecycle (SDLC) as part of our processes of continuous integration (CI) and continuous delivery (CD).
- **3.4 Resource Authorization & Integration –** NextLabs out of the box integrations with enterprise applications as well as its available APIs and SDKs allow organizations to apply data access policies across any application and system within an organization. This secures access to applications, as well as the workloads within those applications with consistent data security policies.
- **3.5 Continuous Monitoring and Ongoing Authorizations –** NextLabs data access policies are dynamically evaluated every time there is a data access request, even if the requestor has already authenticated and has an active connection.

Data:

- **4.1 Data Catalog Risk Alignment –** NextLabs products help organizations automatically discover and categorize data and files, allowing attribute driven policies to be automatically applied.
- **4.2 DoD Enterprise Data Governance –** Policies defined within CloudAz can allow security administrators to appropriately limit access to secured data, enforcing data access controls for enterprise data.
- **4.3 Data Labeling and Tagging –** NextLabs products can automatically discover and classify data so that the correct data access policies are applied.
- **4.4 Data Monitoring and Sensing –** Policies can incorporate metadata for files and data as attribute values in the ABAC policies defined within CloudAz. CloudAz's centralized logging allows administrators to monitor access to any particular data or file to proactively detect any potentially suspicious behavior.
- **4.5 Data Encryption & Rights Management –** NextLabs SkyDRM encrypts files and unstructured data as it is shared within and outside of an organization. The protection stays with the data, so that access can be revoked at any time or at a predetermined time in the future.
- **4.6 Data Loss Prevention (DLP) –** NextLabs products prevent unauthorized access to data through dynamic policy enforcement of data access policies on data at rest, in use, and in transit.
- **4.7 Data Access Control –** NextLabs data access policies are dynamically evaluated and enforced at the time of the data access request. This ensures that policies are evaluated with the attribute values that are current as of the time of the request.

Network/Environment:

- **5.3 Macro Segmentation –** NextLabs policies can be used to create a software defined perimeter (SDP) that controls access to protected resources within that SDP. This is done by incorporating network attributes into the dynamic policy evaluation that happens at the time of the data access request.
- **5.4 Micro Segmentation –** By incorporating network information into the attributes evaluated as part of a data access, NextLabs can virtually segment a network and control access to resources based on that segmentation.

Automation and Orchestration:

- **6.1 Policy Decision Point (PDP) & Policy Orchestration –** The NextLabs CloudAz Policy Controller is the policy decision point (PDP) for CloudAz's unified policy management platform. Policy Controllers can be distributed, and policies and attributes are distributed to each of the PDPs for more efficient evaluation.

- **6.2 Critical Process Automation –** Many of the actions that are part of an organization's security controls can be automated through the use of ABAC policies. Changes to users' group memberships, project statuses, and clearance levels can be automatically incorporated into policy evaluation and enforcement without manual changes to the policies.
- **6.5 Security Orchestration, Automation & Response (SOAR) –** NextLabs' CloudAz is a unified Zero Trust Data-Centric security policy platform that allows administrators to author, manage, and monitor their Zero Trust policies across their entire organizations.
- **6.6 API Standardization –** The CloudAz SDKs and APIs provide a standard an open interface for custom integrations to the CloudAz unified policy platform.

Visibility and Analytics:

- **7.1 Log All Traffic (Network, Data, Apps, Users) –** NextLabs CloudAz logs all policy evaluation activity throughout an organization's network and allows administrators to generate reports from that data for specific data, users, applications, devices or networks.
- **7.2 Security Information and Event Management (SIEM) –** NextLabs CloudAz logs policy evaluation activity and generates reports based on the policy activity logs, monitors and alerts. Monitors can be set for policy activity that meets a predefined criteria and trigger alert to warn administrator when action is required.
- **7.3 Common Security and Risk Analytics –** CloudAz, as NextLabs' unified policy management platform, allows administrators to develop and deploy data protection policies centrally, and collects all activity logs from all policy enforcement points into a single location, so that potentially suspicious activity can be identified by examining activity from across the entire organization.
- **7.4 User and Entity Behavior Analytics –** The centralized reporting in CloudAz allows security administrators to centrally log and audit all data security policy activity, both by the policies being applied as well as by the user, device, or entity that is accessing the protected data.
- **7.5 Threat Intelligence Integration –** NextLabs CloudAz integrates with threat intelligence products so that the centralized policy enforcement data can be used to identify potential threats and proactive mitigate them across the enterprise.
- **7.6 Automated Dynamic Policies –** NextLabs data access policies are dynamically evaluated and enforced at the time of the data access request. Any change in the attribute values that are used in policy evaluation are automatically reflected since current attribute values are retrieved at the time of the request.

Using NextLabs to Implement the DoD's Zero Trust Reference Architecture

NextLabs provides a data-centric security software suite which uses ABAC and dynamic authorization to automate access management, prevent wrongful disclosure, secure data access, and protect data. NextLabs applies an identity-centric approach that utilizes multi-dimensional profiles containing subject and resource attributes to protect and secure access to critical enterprise resources. By ensuring **least privilege access** continuously in real-time, enterprises can enforce secure access to network resources and segregate data. Equally important, is the capability to secure business-critical application and data with externalized authorization management, secure global data access, and persistent protection of data at rest and on the move.

NextLabs' Zero Trust data-centric security suite consists of:

1. **CloudAz**, a unified policy platform that centralizes administration and utilizes the **"never trust, always verify"** principle, ensuring data is protected at any access point.
2. Along with CloudAz, **Data Access Enforcer** helps enterprises protect data access from anywhere, by securing access and protecting critical data stored in databases and data lakes.
3. To protect data on the move and at rest, **SkyDRM** ensures persistent protection of critical files and documents.
4. The next key element is to protect data at the source by externalizing authorization with Attribute-based Access Control (ABAC) principle. A collection of **Application Enforcers** can be used to secure applications, enforce data security controls, and simplify role management.

With a unified policy engine, enterprises can have a cohesive security ecosystem that is flexible, providing consistent policies, monitoring, and audit to protect critical assets both inside and outside of the enterprise. Zero Trust helps the growth of remote workforce and adoption of cloud services, so enterprises can meet the demand of employees working from anywhere, using any point of access, with a 'no default access' criterion, while staying agile and safe.

Next Labs' Zero Trust data-centric security provides not only a more robust cybersecurity infrastructure but also improves business agility. By adopting the **assume breach** mindset, enterprises will be prepared for worst-case scenarios and will be ready for whenever attacks may occur, allowing rapid response to new cybersecurity and business challenges.

Key Takeaways

The Department of Defense's Zero Trust Reference Architecture provides a framework for organizations to implement Zero Trust principles throughout the enterprise. By defining seven core pillars, and the capabilities that make up each of those pillars, the document outlines what is needed for implementation.

NextLabs Zero Trust Data-Centric Security Suite provides many of the capabilities specified within the DoD's ZT RA. NextLabs' unified policy engine that applies dynamic authorization principles through an attribute-based access control (ABAC) model provides greater flexibility and security by allowing the evaluation of real time information to make authorization decisions. In doing this, it enhances business agility and allows for enterprises to scale with ease, allowing them to maintain competitive advantage.

To learn more about implementing a ZTA and the guidelines provided by NIST's National Cybersecurity Center of Excellence (NCCoE) please see our related whitepaper, Implementing a Zero Trust Architecture: NIST National Cybersecurity Center of Excellence.

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 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, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com.

NEXTLABS®