NEXTLABS®

White Paper

Applying Zero Trust Principles to NIST 800-53

ABSTRACT

We're in the midst of a key paradigm shift when it comes to security. Instead of focusing on the perimeter like in the old days, attention has now turned to focusing on the data itself. Access can no longer be based on an isolated physical location, statically defined server, or a discrete, segregated network. What with the proliferation of cloud services, mobile technologies, and increasingly globalized workforces, trying to contain and validate access to data within an enterprise-owned network is challenging to say the least. The network is just the first line of defense, with data now viewed as the key asset to secure. The assumption is that all data is compromised (i.e., there is no trust), hence, access to data must be continuously verified.

A Zero Trust Architecture (ZTA) is a framework that is primarily focused on data protection. It presumes threats are constantly originating from both inside and outside the network. A ZTA embraces a data-centric approach that continuously evaluates risks and then enforces controls to mitigate them. In the past, physical boundaries were emphasized, but nowadays, new protections need to be employed due to the presumption of networks being compromised. In other words, data has assumed a role at least as important as the network, if not more.

This paper examines how NextLabs employs a data-centric approach that aligns with the requirements of a ZTA. The NextLabs framework is predicated on automated data classification, granular access control, data protection at rest and in motion, and real-time auditing and reporting.

OVERVIEW OF THE ZERO TRUST ARCHITECTURE[1]

As defined by NIST, a Zero Trust Architecture is "an end-to-end approach to network/data security that encompasses identity, credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure."

In a nutshell, instead of building many security layers from the outside in, ZTA is predicated on protecting resources (aka "data") from the inside out and implementing security controls only where you need them. This is because all networks, no matter how much authentication is used, cannot be trusted and are presumed to be compromised. As a result, the focus shifts downstream, i.e., managing the risks associated with user access and the resources (data) requiring protection.

There are several key tenets of a ZTA, which are explained below.

1. "All data sources and computing services are considered resources."

A network may be composed of several different classes of devices, including personally-owned devices that are allowed to access enterprise-owned resources.

2. "All communication is secure regardless of network location."

Trust should not automatically be granted just because a device is on the enterprise network infrastructure.

3. "Access to individual enterprise resources is granted on a per-connection basis."

With ZTA, a requester's trustworthiness is assessed every time at run time before access is granted.

4. "Access to resources is determined by policy (rules), including the observable state of user identity and the requesting system, and may include other behavioral attributes."

An organization protects resources by defining what resources it has, who its users are, and what level of access to resources those users need.

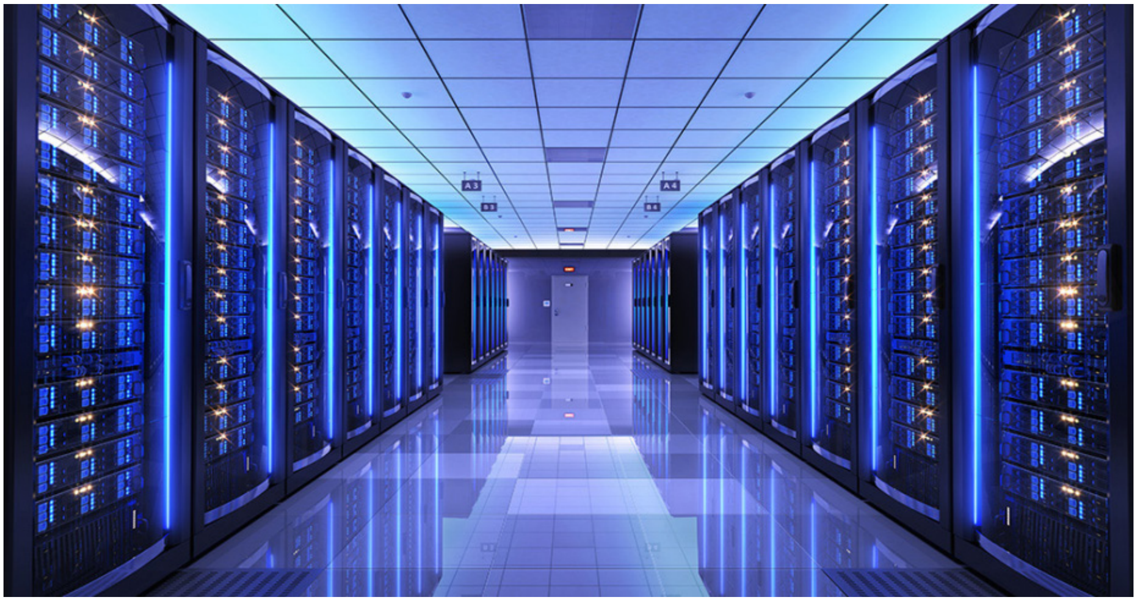
5. "The enterprise ensures all owned and associated systems are in the most secure state possible and monitors systems to ensure that they remain in the most secure state possible."

Enterprises should consider establishing a monitoring and remediation program such that they can continuously monitor and apply fixes as necessary.

6. "User authentication is dynamic and strictly enforced before access is allowed."

Continuous monitoring and re-authentication should occur throughout user interaction, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, etc.) that aims to achieve a balance of security, availability, usability, and cost efficiency.

[1] "Zero Trust Architecture," Draft NIST Special Publication 800-207, September 2019.



How NextLabs Addresses ZTA Requirements

NextLabs' data-centric security approach assumes all data is compromised. Users, data networks, and the transactional environments supporting the data (e.g., location, time, device) must be evaluated at runtime. This method continuously tests and evaluates the risks and then enacts protections and controls to mitigate these risks.

1. Dynamic Access Control

NextLabs supports NIST SP 800-53 Rev. 5, AC-2(6) - Account Management | Dynamic Privilege Management

NIST Supplementary Guidance: "Dynamic access control approaches rely on run time access control decisions facilitated by dynamic privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing mission/business requirements and operational needs of organizations..... Dynamic privilege management can also refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles."

NextLabs uses dynamic authorization management (equivalent to NIST's "dynamic privilege management") to determine access in real-time by evaluating metadata, user attributes, and other factors. Policies are evaluated dynamically, and access is granted or denied during the access request. Policies use detailed attributes to more accurately determine what content should be accessed – the what, why, when, and where. NextLabs' solutions automatically adjust access privileges based upon attributes of the user.

2. Fine-Grained Access Controls

NextLabs supports NIST SP 800-53 Rev. 5, AC-6 – Least Privilege

Control Description: "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

The concept of "least privilege" essentially means that trusted individuals be given only the minimum privileges necessary to carry out organizational or business needs. It often applies to access to sensitive or classified data where not everyone is authorized to view that information.

NextLabs has the unique ability to provide very fine-grained access, including enforcement on a "need to know" basis for data at rest or on the move. It can limit access to the least amount of information required for an individual to do his or her job. NextLabs augments current security infrastructure by only allowing access based on various criteria such as citizenship, certification, security clearance, IP range, department, project, location, file type, etc.

3. Dynamic Evaluation of Users and Devices

NextLabs' solutions are powered by dynamic authorization, whereby policies are evaluated in real-time with access being granted or denied at the time of request (i.e., at runtime). The policies evaluate users and devices, including the most recent user and environment attributes to accurately determine what data can be accessed – basically the what, why, when, and where of access control. This enables NextLabs to meet one of the aforementioned key tenets of the ZTA – that "user authentication is dynamic and strictly enforced before access is allowed."

4. Protection for Data on the Move

NextLabs supports NIST SP 800-53 Rev. 5, AC-3(9) – Access Enforcement | Controlled Release

Description: "The information system does not release information outside of the established system boundary unless the receiving information system or system component provides security safeguards."

NextLabs goes beyond protecting organizational information within the confines of established system boundaries. It provides additional security safeguards needed to ensure that such information is adequately protected once it passes beyond the established information system boundaries.

Example: Data in Motion

1. NextLabs rights management solution has three distinct methods of protecting files in motion: System, Ad-Hoc, and Project. All three operate differently and while they share some features, each has its own unique capabilities.

2. In the "System" mode, the solution selects the required digital rights based and mapped to selected attributes. The content is automatically put in a NextLabs-protected/encrypted wrapper and attributes are applied to that wrapper by the system. This is at the core of a dynamic access solution. This dynamic access is achieved by comparing the attributes of the protected object to the attributes of the requesting subject at the time the request is made. For example, the match may allow the subject to view and print an object today, but a policy change may dynamically change those permissions tomorrow to only allow view access.

3. In the Ad-Hoc method, the user chooses a file and explicitly selects a user using the recipient(s) and applies the appropriate digital rights explicitly to the content. The digital rights are static, unless they are revoked or are expired, as long as either the senders' or recipients' attributes do not change.

4. The Project method is similar to the Ad-Hoc one except that it is designed for larger groups of users. NextLabs does not encrypt the “content.” The content, or protected file, becomes the payload inside of a NextLabs-encrypted wrapper. This is an important distinction when a NextLabs-protected file is passed among systems that recognize the hash of the actual (payload) file being shared.

Alternatively, if the user requests to print a document in an organization-controlled space, procedural means can be employed to ensure that only appropriately authorized individuals can print at that location.

NextLabs goes beyond the NIST requirement for Controlled Release, as outlined above, to have full Access Control and Usage Control (e.g., View, Print/No print, Edit, Watermark, time/location/network/device-specific controls).

Benefits of the NextLabs Platform

The NextLabs platform enhances your security posture and compliance readiness by providing the following benefits:

1. Protect sensitive data

Leverage a data-centric access management system to secure access and protect data across several business-critical applications (e.g., SAP, Siemens, Microsoft) whether the data is at rest or on the move. Control access to business functions and sensitive customer data based on attributes such as data classification, environmental information, user roles and metadata, location, and client system.

2. Ensure compliance

Provide comprehensive visibility as to who is accessing what data and when, identify and proactively intercept anomalies before they become major breaches, and monitor and track events for audit, oversight, and investigation. Create information barriers to segregate regulated data or between confidential projects to avoid data spills or contamination. Manage, educate, enforce, and audit access policies to sensitive corporate data to ensure compliance with regulations such as GDPR, HIPAA, ITAR/EAR, and SOX.

3. Reduce security and compliance management costs

Automate the process of auditing authorization and data access to demonstrate compliance to auditors, regulators, and customers. Eliminate the need to implement and maintain costly customizations to meet security, compliance, and governance requirements. Attribute-driven dynamic authorization reduces the complexity around role management and eliminates the need to maintain multiple SAP instances.

4. Improve business agility

Manage authorization logic through an externalized, standards-based policy framework. Allow secure and non-secure data to reside on the same servers and networks, which greatly reduces complexity and cost and increases ease of use and flexibility. Slash application development time and automate change management processes, thereby enhancing business agility.

ABOUT NEXTLABS

NextLabs®, Inc. provides 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.