NEXTLABS®

White Paper

Implementing a Zero Trust Architecture: NIST National Cybersecurity Center of Excellence

An Overview by NextLabs

Purpose

To address cybersecurity challenges organizations may face, the National Cybersecurity Center of Excellence (NCCoE) part of NIST, collaborates with government agencies, organizations, and academic institutions. In doing this, the NCCoE works to create adaptable cybersecurity solutions showing how standards and best practices can be utilized when using commercially available technology.

To better help federal agencies, in 2018, the Federal Chief Information Officer engaged NIST NCCoE to define what exactly Zero-Trust Architecture (ZTA) is, along with its benefits and limitations. This collaboration resulted in the publication of NIST SP 800-207, Zero Trust Architecture. Said publication, reviews ZTA fundamentals, logical components, case studies, challenges, and how it can be deployed to aid with cyber-security.

From this, NCCoE produced a document on Implementing Zero Trust Architecture, demonstrating proposed architecture(s) for on-premises and cloud environments that inherit ZTA solution characteristics outlined in NIST SP 800-207. The paper also discusses the impacts on the enterprise, administrator, and end-user when a ZTA strategy is employed. In this resource, NextLabs reviews some of the key information of the NCCoE project in a summarized and easy-to-digest format.

> “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

What is ZTA and why is it needed today?

The growth in cloud computing, Internet of Things (IoT), business partnerships, and remote work has increased the complexity of managing digital enterprise resources, as network perimeters become increasingly hard to define. Traditional network security focused on securing the perimeter, which is no longer effective due to its limitations and vulnerability, given the growing number of points of entry, exit, and data access than ever before.

Perimeters are increasingly difficult to define in the current complex hybrid cloud system. Within the network perimeter, subjects (end users, applications, non-person entities that request information from resources) are usually given broad access to corporate resources. If a single subject is compromised, malicious actors can gain access to these critical resources, incurring massive data breaches.

This leads to the question; how can organizations protect their core data assets from malicious actors in an increasingly digitalized business environment where network perimeters are undefined?

A zero-trust architecture (ZTA) shifts from a perimeter-based methodology to one that is data-centric. It focuses on **protecting resources, not perimeters** as these are no longer the prime component to protecting enterprise data. The focus of a zero-trust strategy is on identifying and authenticating users and devices, not on the network location. Zero-trust is a set of cybersecurity principles used to create a strategy that focuses on moving network defenses to focus specifically on subjects, enterprise assets, and resources.

With ZTA, the risk of becoming compromised is greatly reduced. ZTA holds no implicit trust, which means that no access is granted to assets or user accounts based solely on their physical or network location, but rather until a subject, asset, or workload is verified by reliable authentication and authorization. Access privileges are given at a minimum to prevent abuse and misuse.

ZTA assumes that an attacker could be present in any environment, including those owned by enterprises. As such, the enterprise must enact protections to reduce the risks to its assets and business functions through constant monitoring and evaluation.

Principles of ZTA

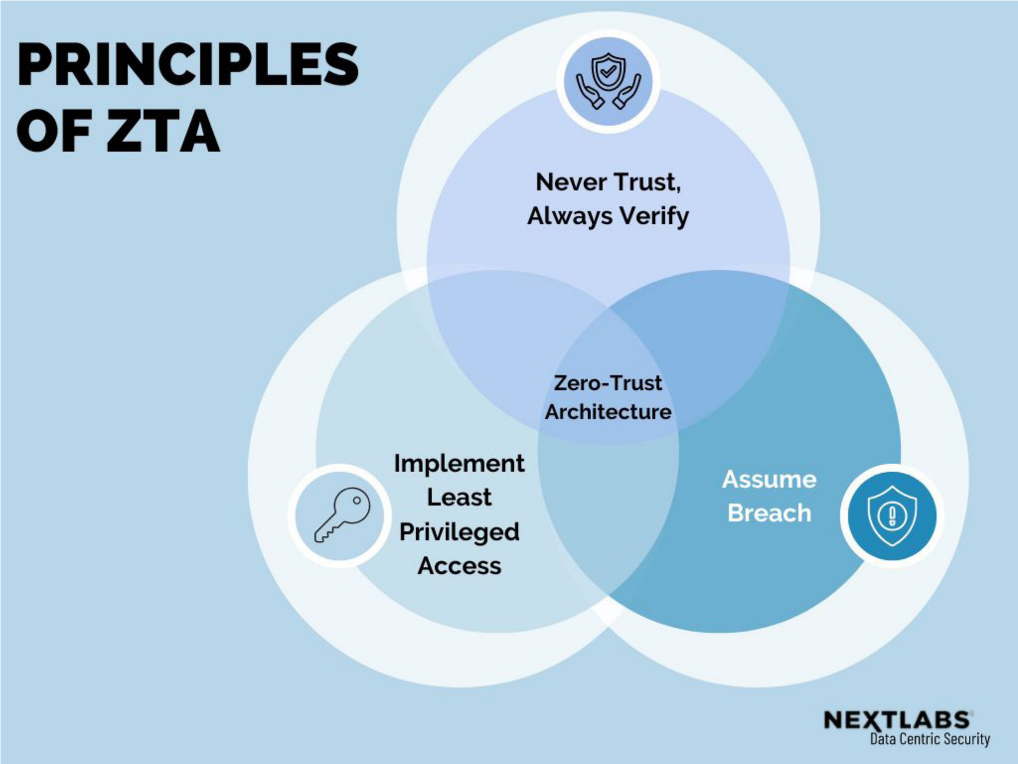
PRINCIPLES OF ZTA
Never Trust, Always Verify
Zero-Trust Architecture
Implement Least Privileged Access
Assume Breach
NEXTLABS Data Centric Security

Figure 1: Principles of ZTA

ZTA comprises of the following three core zero trust principles to plan industrial and enterprise infrastructure and workflows:

1. **Never trust, always verify:** every single time a user, device or application tries to make a new connection attempt, that attempt will be authorized and authenticated.
2. **Implement least privileged access: t**o grant users and applications the minimum amount of access needed to perform their jobs effectively.
3. **Assume breach:** prepare for worse case scenarios and plan when attacks do occur

Incorporation of ZTA into an organization's cyber defense system involves the integration of zero-trust concepts into an existing perimeter-focused cybersecurity system, in which the end goal is to create a database that indexes all assets, as well as their various configurations. ZTA can be used to safeguard data on-premises and in public or hybrid cloud.

Implementation of ZTA can be executed in a general IT infrastructure that combines users including employees, contracts, guests, and non-person entities; assets; and enterprise resources through the extensive network.

The following sections will feature the benefits and challenges of implementing ZTA.

Benefits and Challenges of implementing ZTA

Benefits

ZTA serves a myriad of benefits for the enterprise that adopts the security strategy, such as:

- Real-time access control as users are verified by reliable authentication and authorization before each session.
- Increased visibility over resources as organizations can better monitor user behavior patterns and protect data accordingly.
- Simplified security architecture allows enterprises to easily respond to reports on security events.
- Reduced risk of malicious attacks as there is no "trusted" network or location, all connections would be subjected to verification.

Challenges

Despite the many benefits of implementing ZTA, organizations may face common adoption difficulties such as:

- Lack of vendor product maturity to support ZTA.
- Organization's low ability or willingness to migrate to a ZTA due to:
    - o Lack of proof of concept.
    - o Heavy investment made in legacy technologies.
    - o Lack of identity governance.
    - o Insufficient ability/resources to develop transition plan.
- Security concerns over a compromised zero-trust control plane.
- Lack of evidence to indicate if the ergonomics of the system would improve or worsen users' experience.
- ZTA's interoperability with technologies such as the ability to interact with the enterprise and cloud service ecosystem.

The implementation of a ZTA is dependent on both the available bandwidth of the company and maturity of the current vendors to support ZTA. Implementation of ZTA can cover a broad range of use cases such as evaluating subject access requests to corporate resources hosted on-premises or in the cloud, and through either the public internet or enterprise network. To learn more about how ZTA can be deployed in different scenarios, you may refer to Section 2 Scenarios in Implementing a Zero Trust Architecture document.

Architecture Overview

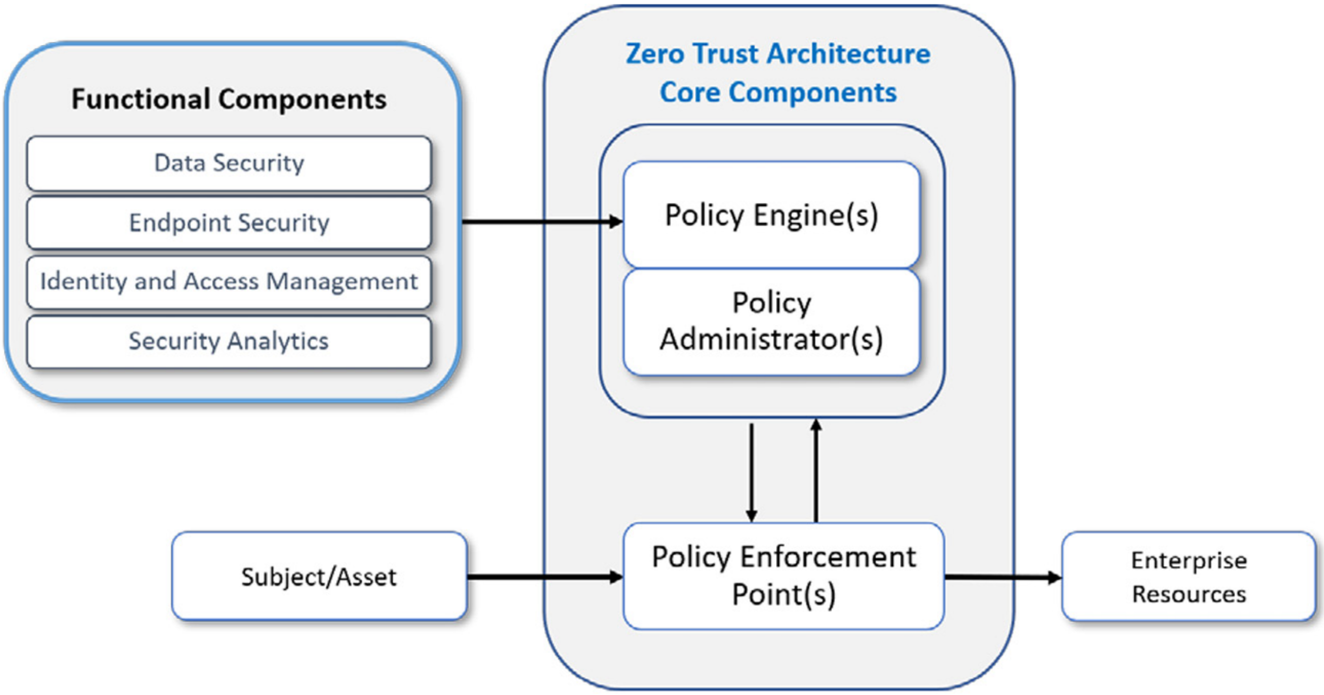

Figure 2: ZTA High-Level Architecture

For a typical enterprise, the technical components required of the ZTA solution(s) include but are not limited to the core, functional, and device and network infrastructure components. The core components act as the brain, where the policy engine (policy decision point) makes decisions to grant, deny, or revoke access to a given subject. The policy administrator (policy administration point) provides a facility to create, edit, and manage authorization policy that is used to grant subject access to the requested resource. It also creates session-specific authentication credentials used by a client to access an enterprise resource. This is closely related to the policy engine and relies on its decision to allow or deny a session. The final aspect of the core components is the policy enforcement point (PEP), which handles enabling, monitoring, and terminating connections between the subject and resource.

The functional components consist of data security, endpoint security, identity & access management (IAM), and security analytics. The data security component includes all of the data access policies that are used to protect data at rest and in transit. While the endpoint security component involves the strategy, technology, and governance to protect endpoints from external threats along with threats from managed or unmanaged devices. The IAM component encompasses the strategy, technology, and governance for creating, storing, and managing subject (user) accounts and identity records, along with their access to enterprise resources. The security analytics component covers all threat intelligence feeds and activity monitoring for an IT enterprise, gathering behavior insights to actively respond to threats.

Finally, the device and network infrastructure components include assets (devices) such as laptops, tablets, and other IOT devices that connect to the enterprise. Along with assets, are enterprise resources which include data, resources, and applications that are hosted and managed on premise, in the cloud, or at the edge. Network infrastructure components include network resources that a large or medium enterprise may deploy in its environment.

It is assumed that the ZTA core and functional components, and devices are integrated into a network infrastructure, as seen in Figure 2. For more information on zero trust architecture, desired characteristics and properties, please refer to Section 3 High-Level Architecture of the Implementing a Zero Trust Architecture document.

Extending ZTA's Efficacy

According to NIST, using a policy engine that applies dynamic authorization principle to implement an attribute-based access control (ABAC) model, is a better and more scalable way to manage access. It provides greater flexibility and security by allowing the evaluation of additional information (attributes) to make authorization decisions.

Dynamic authorization enables ABAC with the use of fine-grained authorization and attributes of subject and resources to evaluate the context of each request. Unlike traditional access control, which typically has static rules for access, attribute-based access control lets you control access beyond the application level and resource level to require that certain conditions are met.

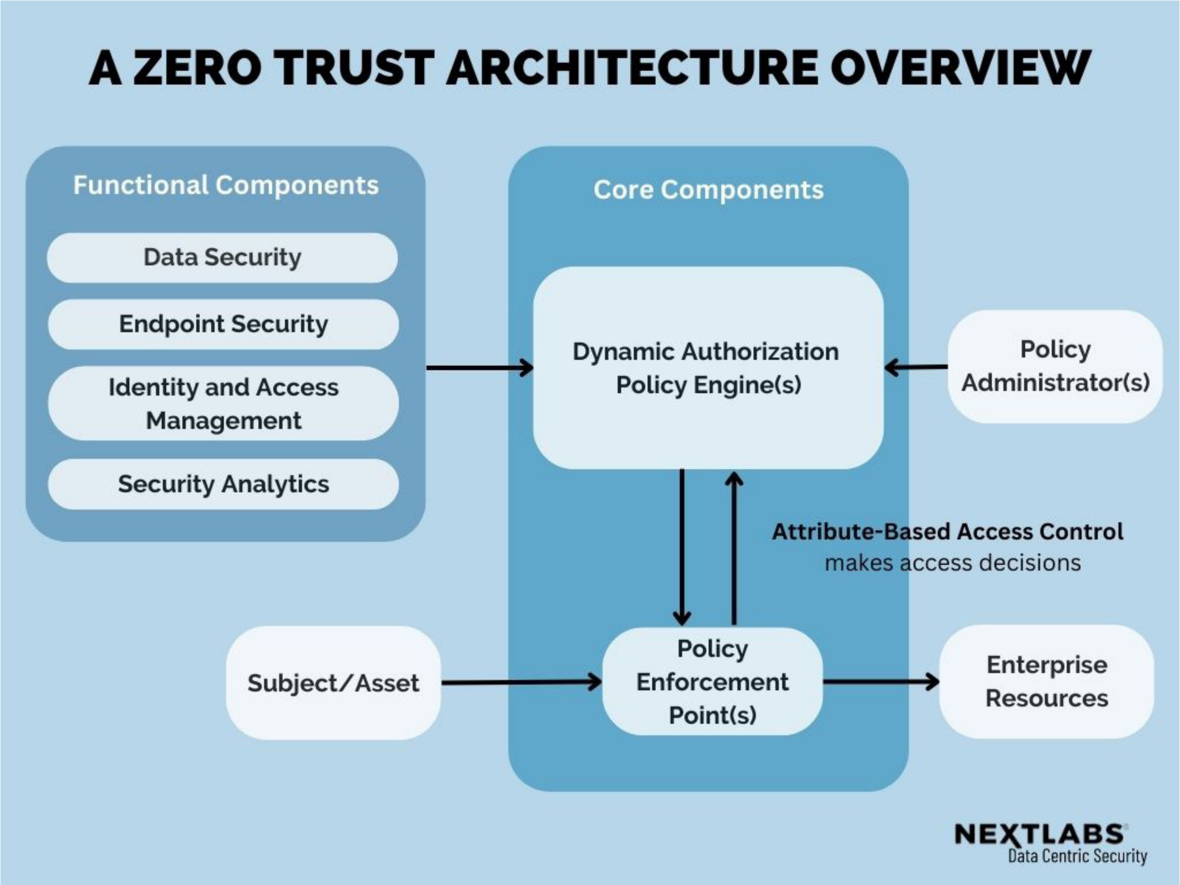

Figure 3: How ABAC can be incorporated into a ZTA

Another key principle of ABAC is the abstraction of business logic from the applications that consume it. Because of the disadvantages of hard-coded, static logic that resides inside applications and is distributed and duplicated across our enterprise, ABAC centralizes access controls instead of incorporating them at the individual application level.

For more information on ABAC, please refer to NIST SP 800-162 and NIST 1800-3 (a collaborative NIST publication that NextLabs contributed to).

NextLabs Solution for ZTA

To address ZTA requirements, 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. ZTA 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.

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

Implementing a zero-trust architecture is essential in today's dynamic digital environment to safeguard critical assets. ZTA is an all-around defense system that can integrate onto an enterprise's existing infrastructure, complementing and boosting its cyber defense. With the implementation of ZTA and data centric security, both workforces and external partners can access application and data securely using any device from any location without compromising integrity.

Furthermore, using a policy engine that applies dynamic authorization principle and attribute-based access control (ABAC) model, it will provide 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 ZTA and its importance, please refer to NextLabs' interview with Alper Kerman, author of the Implementing a Zero Trust Architecture document, on Why is Zero Trust Architecture (ZTA) Important?

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.