NEXTLABS®

White Paper

Why Zero Trust Data-Centric Security is a Better Approach to Protecting Data

In an era where data breaches and cyber threats are more sophisticated and prevalent than ever, traditional perimeter-based security measures are proving insufficient for protecting sensitive information. The rapid adoption of cloud computing, remote work, and the proliferation of connected devices have expanded the attack surface, making enterprises more vulnerable to cyberattacks. Consequently, the market is shifting towards a more resilient and adaptable security model—Zero Trust Data-Centric Security. This approach focuses on protecting data itself rather than relying solely on securing the network perimeter. By assuming that threats can come from both inside and outside the network, Zero Trust enforces strict verification for every access request, minimizing the risk of unauthorized data access.

The drive towards data-centric security is fueled by several factors. Increasingly stringent regulatory requirements, such as GDPR and CCPA, demand more robust data protection and privacy measures. Additionally, the frequency and impact of data breaches are escalating, resulting in significant financial losses and reputational damage for organizations. As enterprises embrace digital transformation, they require a security model that offers greater flexibility, scalability, and control over their data, regardless of where it resides. Zero Trust Data-Centric Security addresses these needs by providing a comprehensive, adaptive framework that secures data throughout its life cycle, ensuring that sensitive information remains protected even in the face of evolving threats.

Enterprises Need to Securely Access Data Anywhere and Everywhere

Modern enterprises are undergoing a profound transformation in how they operate, largely driven by the need for agility, scalability, and global collaboration. This transformation necessitates the ability to securely store and access data anywhere and everywhere. Several key factors are driving this shift, reshaping the traditional data security landscape and pushing enterprises to adopt more flexible data security strategies. One of the primary drivers is the rise of **cloud computing**. Enterprises are increasingly leveraging cloud services to enhance operational efficiency, reduce infrastructure costs, and accelerate innovation. Public, private, and hybrid cloud environments offer the scalability and flexibility needed to handle vast amounts of data. With cloud providers offering global data centers, enterprises can store data closer to where it is generated and consumed, reducing latency and improving performance. This geographical distribution of data is a key component in improving the performance of real-time analytics, machine learning, and other data-intensive applications that require immediate access to vast datasets.

The **proliferation of remote work** and the **need for global collaboration** have further complicated the task of securing data. In today's interconnected world, employees, partners, and customers are often spread across different locations and time zones. To support seamless collaboration and maintain productivity, enterprises must ensure that data is accessible from anywhere, at any

time. This requires a data-centric approach to data security, enabling users to securely access and share information without being constrained by physical location.

Edge computing is another factor contributing to the need for data to be secured wherever it is stored and accessed. As the Internet of Things (IoT) and other edge devices generate massive volumes of data at the network's edge, this data is increasingly processed locally to reduce latency and bandwidth usage. Storing and analyzing data closer to its source enables enterprises to make faster, more informed decisions and enhanceenhances the performance of applications that rely on real-time data processing. This approach not only improves operational efficiency but also opens new possibilities for innovation and customer engagement.

The **rise of multi-cloud strategies** is driving enterprises to store and access data across various platforms and environments. To avoid vendor lock-in and optimize costs, enterprises are increasingly adopting multi-cloud environments, leveraging the strengths of different cloud providers. This approach allows them to distribute applications, workloads, and data across multiple clouds, enhancing redundancy, availability, and resilience against outages or disruptions.

Additionally, as enterprises **store and access data across multiple geographic regions**, they must navigate a complex web of regulatory requirements that govern how data is stored, processed, and shared. Regulations such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and HIPAA mandate strict data privacy measures, while data sovereignty laws in countries like China and Russia impose stringent restrictions on where data can reside. Whether data is structured or unstructured, stored in legacy systems, or resides in distributed environments, organizations must adopt a Zero Trust Data-Centric Security approach for comprehensive protection. By integrating Zero Trust with a data-centric security approach, organizations can ensure that sensitive data is protected at its core, regardless of where it is stored. Moreover, with continuous monitoring and automated compliance tools, enterprises can maintain a real-time audit trail that demonstrates compliance with regional regulations, helping them avoid hefty penalties and legal liabilities.

The Challenge of Securing Data Anywhere and Everywhere

As enterprises increasingly access data from different applications and locations, securing this data becomes an ever more complex challenge. The traditional security model, which focused on fortifying a single, centralized network perimeter, is no longer viable in a world where data exists and is accessed in multiple locations. This shift necessitates a new approach to security, as the sheer volume and diversity of data access requests make it nearly impossible to secure them all effectively using conventional methods.

One of the primary issues with securing data is the inconsistency in security policies and controls across different environments. Each environment where data is located, whether it's a public cloud service, a private cloud, an edge device, or an on-premises server, can have its own set of security tools, configurations, and management interfaces. This fragmentation makes it difficult to maintain a uniform security posture across the entire enterprise. Moreover, managing security policies across these disparate environments is not only time-consuming but also prone to human error, increasing the risk of misconfigurations and vulnerabilities.

Furthermore, the increase in remote work and mobile device usage has expanded the data security perimeter far beyond the corporate firewall. Employees now access corporate data from various locations and devices, including personal smartphones, tablets, and laptops. The risks associated with Bring Your Own Device (BYOD) policies are significant, as personal devices often lack the security controls found in corporate-managed systems. They can become entry points for attackers to gain unauthorized access to data, especially if it is not adequately protected or employees use unsecured public networks.
Another layer of complexity is introduced by the varying security capabilities of different cloud service providers. While leading cloud providers offer robust security features, enterprises often use multiple cloud services, each with its own set of securi-

ty mechanisms and configurations. Ensuring consistent security across multiple cloud platforms requires significant effort and expertise, and any misalignment can lead to vulnerabilities. Attackers are increasingly targeting these multi-cloud environments, looking for weak links in the chain that they can exploit.

Data residency and compliance requirements further complicate data security. Enterprises must ensure that data is stored and processed in compliance with regional regulations, such as GDPR or CCPA. This often means implementing complex data routing and access control mechanisms, which can introduce security gaps if not properly managed.

Advanced Persistent Threats (APTs) are also a growing concern for enterprises, as these sophisticated attacks often bypass traditional perimeter defenses by exploiting vulnerabilities across multiple layers of the IT environment, networks, endpoints, and applications. Many traditional security tools, designed to detect surface-level threats, struggle to identify these persistent, stealthy attacks, which often go unnoticed until significant damage is done. With a Zero Trust model, every access request is verified dynamically in real-time, making it harder for APTs to exploit weaknesses in the system. Additionally, by implementing data-centric security measures such as persistent encryption and dynamic access control, enterprises can significantly reduce the risk of unauthorized data access, even if an APT manages to penetrate the network.

Given these challenges, it becomes clear that a perimeter-based approach, relying on the idea of securing a network at the edge, is inadequate when the network itself is fragmented and constantly changing. Instead, enterprises need to adopt a data-centric security model, focusing on protecting data wherever it resides or is used. This includes encrypting data at rest and in transit, enforcing strict access controls, and continuously monitoring for suspicious activities. By prioritizing the security of the data itself, enterprises can protect data anywhere and everywhere.

Data-Centric Security: The Solution for Protecting Data

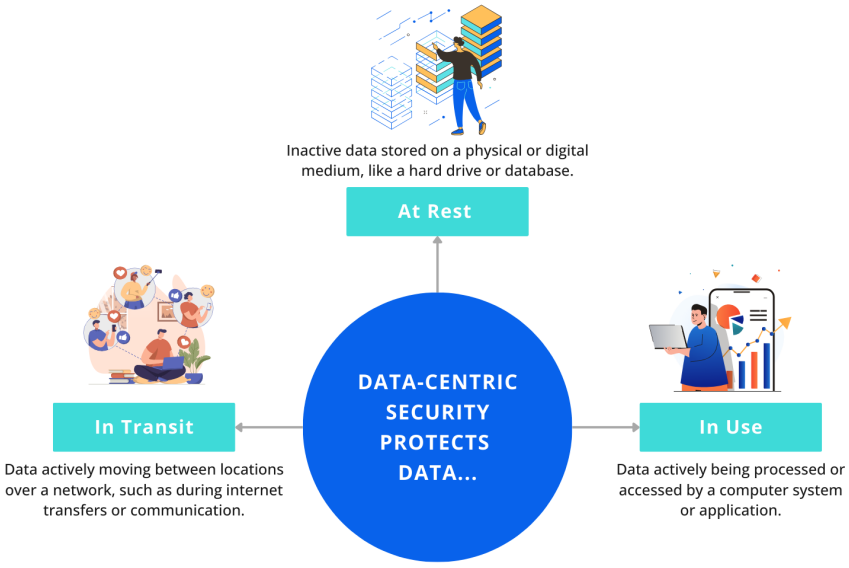

Figure 1: Data-Centric Security Protects Data In Transit, At Rest, and In Use

In an era where data is accessed across an ever-expanding array of environments, from cloud to edge devices, securing the data itself becomes paramount. Traditional network-centric security measures, such as firewalls and intrusion detection systems, are increasingly ineffective in this landscape, as they focus on securing the perimeters of networks rather than the data within them. A data-centric security approach shifts the focus to protecting the data directly, ensuring that it remains secure regardless of its location or the security posture of the environments it traverses.

The core principle of data-centric security is to protect critical data itself. This involves applying security controls, such as encryption, access controls, and monitoring, at the data level. By encrypting data at rest, in transit, and in use, enterprises can ensure that even if unauthorized individuals gain access to the storage environment or intercept the data during transmission, they cannot read or exploit it. Modern encryption techniques, such as Advanced Encryption Standard (AES) and public-key infrastructure (PKI), provide robust protection, making it virtually impossible for attackers to decipher the data without the

appropriate decryption keys.

Access control is another critical component of data-centric security. Instead of relying solely on network-based access controls, such as VPNs or firewalls, a data-centric approach enforces strict authentication and authorization policies at the data level. This means that access to sensitive data is governed by user attributes, identity verification, and contextual factors, such as location or device type. Implementing multi-factor authentication (MFA) and least privilege access ensures that only authorized users can access the data, significantly reducing the risk of insider threats or unauthorized access from compromised accounts.

Data-centric security also involves persistent monitoring and auditing of data access and usage. By implementing data activity monitoring tools, enterprises can continuously track who is accessing the data, when, and for what purpose. This not only helps detect and respond to suspicious activities in real time but also provides an audit trail for compliance and forensic analysis. Advanced monitoring solutions can leverage machine learning and behavioral analytics to identify anomalies that may indicate a security breach or insider threat, allowing organizations to take proactive measures to protect their data.

One of the key advantages of data-centric security is its adaptability to diverse environments. Since the security controls are applied to the data itself, they are enforced wherever it goes, whether it's stored in a public cloud, transferred across a corporate network, or accessed from an edge device. This ensures consistent protection across all environments, regardless of the varying security capabilities of different networks. This gives organizations the benefits of improved performance and global accessibility, without compromising on security. Data-centric security ensures that sensitive information is adequately safeguarded, even when it resides in or moves through regions with different data sovereignty laws.

Moreover, a data-centric approach simplifies compliance with a variety of regulations. By using attribute-based policies, companies can prevent unauthorized access on a fine-grained level. This in combination with a centralized policy platform that monitors, logs, and audits data access attempts, helps enable compliance with regulations like GDPR, CCPA, and HIPAA.

Enhancing Data-Centric Security with a Zero Trust Approach

A Zero Trust approach is a paradigm shift in cybersecurity that complements and enhances data-centric security by adopting the principle of "never trust, always verify." In a traditional security model, trust is often granted based on the location within the network perimeter. However, in today's dynamic environments, where data is stored and accessed across multiple networks, this model is no longer effective. Zero Trust assumes that threats can exist both inside and outside the network, requiring continuous verification and validation of users, devices, and data access requests.

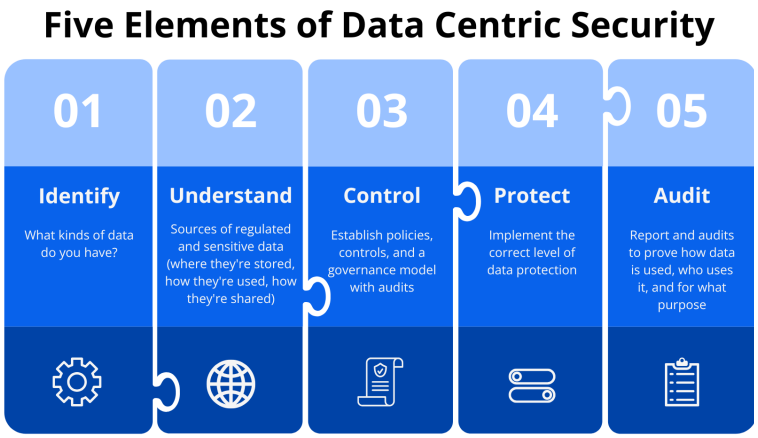

Figure 2: Five Elements of Data-Centric Security

Integrating Zero Trust with a data-centric security approach adds an additional layer of protection by ensuring that only authenticated and authorized entities can access sensitive data, irrespective of their location. The National Institute of Standards and Technology (NIST) has outlined several foundational principles in its guidance on applying a Zero Trust approach to Data-Centric security. These include strong authentication and authorization, least privilege access, continuous monitoring and adaptive security, encryption, and segregation, which are critical for securing modern, distributed environments.

Strong Authentication and Authorization

Zero Trust mandates rigorous authentication mechanisms for all users and devices attempting to access data. This includes MFA to ensure that even if an attacker obtains a user's credentials, they cannot gain access without the second authentication factor. In a data-centric security model, this means that access to data is granted based on verifying the user's identity, their device's integrity, and contextual factors like geolocation and time of access. This granular approach to access control minimizes the risk of unauthorized data access, even in scenarios where the network perimeter has been compromised.

Least Privilege Access

One of the core tenets of Zero Trust is the principle of least privilege, which ensures that users and applications have the minimum level of access necessary to perform their tasks. When applied to data-centric security, least privilege access means that users are granted access only to the data they need and nothing more. This reduces the potential impact of a data breach, as even if a user's credentials are compromised, the attacker would be limited in the data they can access. Implementing attribute-based access control (ABAC) further refines access permissions, ensuring that data access is tightly controlled and monitored.

Continuous Monitoring and Adaptive Security

Zero Trust emphasizes the need for continuous monitoring and adaptive security measures to detect and respond to potential threats in real time. In a data-centric security model, this means continuously monitoring data access patterns, user behavior, and network activity to identify anomalies that may indicate a security breach or insider threat.

Using analytics and advanced machine learning algorithms, enterprises can detect these unusual behaviors and anomalies. With a Zero Trust approach, security teams can implement adaptive security measures, automatically adjusting access controls and enforcing additional authentication steps based on detected risks. Moreover, automated compliance reporting simplifies the process of adhering to complex regulatory frameworks by providing real-time audit trails that track every data access request and action.

Encryption and Data Protection

Zero Trust further reinforces data-centric security by ensuring that data remains encrypted and protected throughout its lifecycle. This includes encrypting data at rest, in transit, and even during processing. Zero Trust ensures that decryption keys are managed securely and are only accessible to authorized users and applications. By integrating encryption with identity and access management (IAM), Zero Trust can enforce strict policies that ensure data is only decrypted in a secure and trusted environment.

Adoption of Zero Trust Data-Centric Security

A Zero Trust Data-Centric approach has been endorsed as the best way to protect data by many different organizations and government agencies, including the United States Department of Defense (DoD) and the Cybersecurity and Infrastructure Security Agency (CISA). This is reflected in the guidance they have published for organizations to adopt a Zero Trust Data-Centric approach as the preferred way to protect data.

United States Department of Defense

To promote the adoption of a Zero Trust approach within its organization, the Department of Defense (DoD) has developed a Zero Trust Reference Architecture (ZTRA), which covers both Zero Trust Data-Centric Security and Zero Trust Network-Centric Security. The ZTRA defines seven key pillars, each playing a critical role in implementing Zero Trust principles effectively within the DoD's environment. The pillars making up the core of Zero Trust Data-Centric Security are Data, Users, Workloads, Automation & Orchestration, and Visibility & Analytics, with the Devices pillar an extension of Data-Centric Security.

Data Pillar

At the heart of the DoD Zero Trust Reference Architecture is Data, the most crucial of the seven pillars. Data is recognized as the core asset, requiring protection at every level, regardless of where it resides. This principle reflects the importance of data-centric security. The DoD ZTRA's Zero Trust Data-Centric approach ensures that protection extends beyond an organization's network perimeters, protecting data as it becomes more distributed and dynamic across multiple environments.

The other six pillars support the protection of data, and can be divided into two categories, resource pillars and foundational pillars.

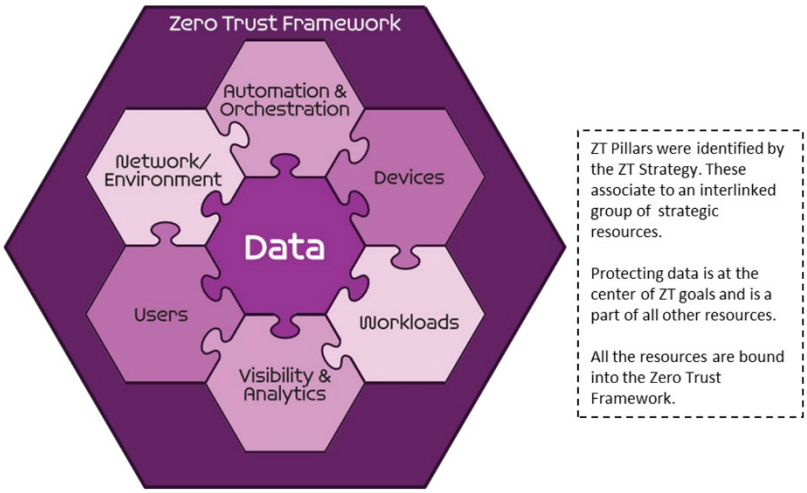

Figure 3: Department of Defense Zero Trust Reference Architecture

Resource Pillars

The resource pillars cover the resources within an organization that should be protected with a Zero Trust approach to protect the data pillar.

The **Users** pillar is a core part of Data-Centric Security as it is critical to verify the identity and role of each individual before granting access to sensitive information. As part of the Zero Trust data-centric security model, this means applying granular access controls based on user attributes like role, location, and device type, ensuring only authorized individuals can interact with critical data.

The **Workloads** (Application) pillar requires that access to applications, and applications themselves be verified before they are allowed to access data, ensuring that only trusted, secure applications that are being used by authorized users or entities can access protected data.

The **Devices** pillar requires continuous assessment of device compliance with security standards before granting access to data. The DoD ZTRA ensures data is protected by restricting access to trusted devices, adding an extra layer of protection.

Foundational Pillars

The remaining pillars cover aspects of Zero Trust Data-Centric security that apply to all of the resource pillars.

The **Visibility and Analytics** pillar highlights the need for continuous real-time monitoring. As part of a Zero Trust Data-Centric approach, real-time monitoring is key to tracking data access patterns and identifying potential threats. Advanced analytics and machine learning tools help detect anomalies, ensuring a rapid response to unusual activity.

The **Automation and Orchestration** pillar highlights the importance of automated dynamic enforcement of security policies. The automation of data protection measures—such as encryption and dynamic access controls—ensures consistent policy enforcement across all environments, reducing the risk of human error and speeding up security responses.

Cybersecurity and Infrastructure Security Agency (CISA)

To promote the adoption a Zero Trust Data-Centric security approach and to help organizations in their implementation journey, CISA has developed a Zero Trust Maturity Model, which explicitly makes the distinction between the resource and foundational pillars defined in the DoD ZTRA, defining data and the resource pillars as the five pillars in the ZTMM and the foundational pillars as three cross-cutting capabilities, all of which are essential for applying Zero Trust principles to the protection of an organization's assets.

CISA's ZTMM also separates out Governance as a key cross-cutting capability that supports the other two capabilities as well as all five pillars. Governance includes the policies, procedures, and controls an organization puts in place to manage their data security. This provides an overarching framework for overseeing how data across the organization is protected and secured using the other cross-cutting capabilities and the five individual pillars.

This split between the five pillars that are being protected and the cross-cutting capabilities of visibility and analytics, automation and orchestration, and governance, make it clear how they combine in Zero Trust Data-Centric Security to provide the best approach to protecting critical data.

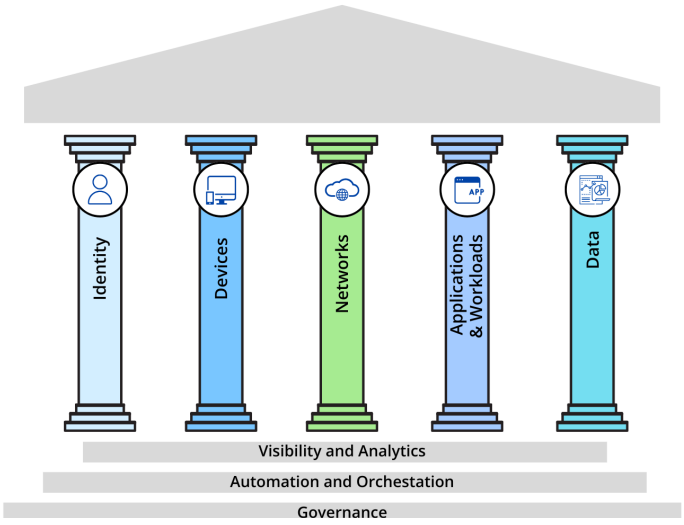

Figure 4: CISA Zero Trust Maturity Model Pillars

Benefits of a Zero Trust Data-Centric Approach

As shown by the adoption by such organizations as the Department of Defense, CISA, and NIST, there are significant benefits to adopting a Zero Trust Data-Centric approach to protecting data.

Granular Access Controls – Attribute-based policies allow organizations to implement the principle of Least Privilege, ensuring users, devices, and applications can only access the data necessary for their roles.

Resilience Against Threats – Continuous authentication, real-time authorization, and fine-grained data security controls reduce the attack surface and mitigate the risk of insider threats. Policy-Based Data Centric Security ensures that protected data is only accessible to the users or entities where all relevant attributes have the required value, reducing the likelihood of inadvertent unauthorized access.

Minimize Impact of Breaches – Policy-Based Access Control (PBAC) implemented with Attribute-Based Access Control (ABAC) can prevent unauthorized access and wrongful extraction of data, even when user credentials have been stolen or otherwise compromised. Logical segregation and obfuscation of data means that even if a network or system is subject to unauthorized access it does not result in other key applications and data systems being compromised as well. Digital Rights Management (DRM) and Encryption ensures that even if the data source is accessed improperly, the protected data remains inaccessible to those unauthorized parties.

Regulatory Compliance – Centralized monitoring and logging of data access requests simplify the process of compliance reporting.

Resource Flexibility – A Zero Trust data security model allows for secure access for remote workers, and the migration to cloud or

hybrid environments. A granular data-centric approach also allows for easier integration of new applications and technologies and allows organizations to scale their security as they grow.

Operational Efficiency – Centralized management of data security policies that can then be enforced throughout the organization reduce the workload required to implement data security. Automated dynamic enforcement of policies reduces the effort required to update policies to account for changes in user, data, and environmental attributes.

How to Implement Zero Trust Data-Centric Security with NextLabs

NextLabs Zero Trust Data-Centric Security offers a comprehensive solution that allows organizations to realize the benefits of adopting a Zero Trust Data-Centric Security approach to protecting their data. NextLabs products leverage dynamic authorization and Attribute-Based Access Control (ABAC) to allow organizations to determine the level of access to be granted based on attributes such as user identity, device type, location, and time of day. This provides organizations with a flexible and granular way of protecting and controlling access to sensitive data.

NextLabs solutions are designed to work seamlessly with existing security infrastructure and are compatible with a wide range of platforms and applications, including cloud-based services and legacy systems. This allows organizations to easily integrate NextLabs' solutions into their existing security infrastructure and take advantage of Zero Trust principles without having to replace their existing systems.

Unified Zero Trust Policy Management Platform

NextLabs provides a unified Zero Trust policy management platform that provides organizations with a Zero Trust Architecture to protect resources across their entire enterprise. Centralized policy authoring enables attribute-based access control (ABAC) policies to be defined and managed centrally for the entire organization, ensuring data security policies are consistent. NextLabs' Zero Trust policy engine evaluates those policies dynamically in real-time with the values of the subject, data, and environmental attributes defined in those policies. A centralized attribute store and out of the box integrations to attribute sources provide the attribute values that the policy engine uses to make access decisions.

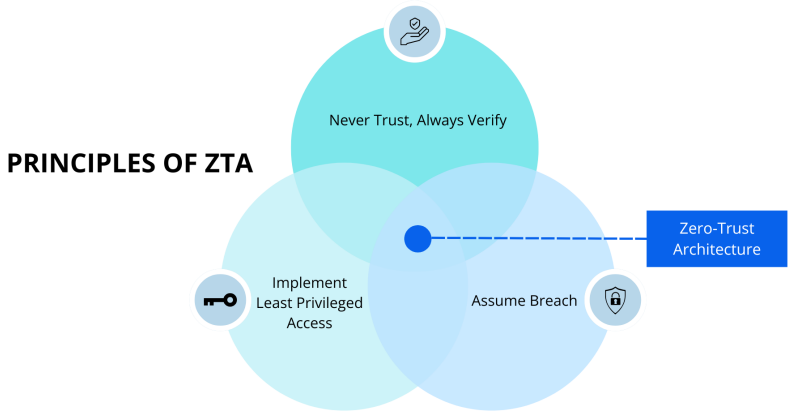

Figure 5: Principles of ZTA

Dynamic Policy Evaluation and Enforcement

NextLabs policies are evaluated and enforced at the time of the data access request, incorporating the current values of the attributes used in the ABAC policies. This dynamic evaluation and enforcement ensure that policy decisions are always based on the most current values of the attributes. By defining policies in terms of dynamic attributes organizations can ensure that updates to user roles, data classifications, and regulations are automatically applied without requiring changes to the policy itself.

Policy-Based Access Control

NextLabs leverages a policy-driven approach to enforce dynamic, context-aware access controls on data. NextLabs policy-based access control implements attribute-based access control (ABAC) and role-based access control (RBAC), allowing organizations to define granular policies based on attributes drawn from MDM, IAM, Threat Intelligence, SIEM, HR, and Configuration Management

systems.

This ensures that access to sensitive data is granted only to authenticated and authorized users under specified conditions. For example, an employee may be permitted to access certain data only during work hours and from a corporate device. These dynamic policies adapt to changing conditions, providing robust security while supporting the flexibility needed in all environments.

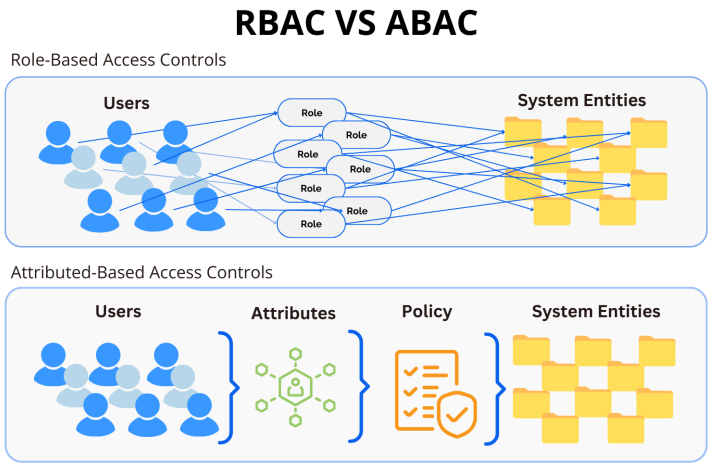

Figure 6: PBAC vs. Traditional Access Control

Data Segregation and Obfuscation

NextLabs helps organizations segregate and segment their data based on sensitivity and compliance requirements. NextLabs allows security policies to be defined based on attributes of the data, applying appropriate security controls and policies to each type of data. This segregation of data minimizes the risk of unauthorized access and limits the potential impact of a breach. By applying different levels of protection to different segments of data, organizations can ensure that their most sensitive information is subject to the highest security standards, in line with the Zero Trust principle of least privilege.

Data Encryption and Secure Collaboration

NextLabs ensures that data is encrypted at rest, in transit, and even during processing. By integrating encryption into its Zero Trust Data-Centric Security model, NextLabs makes sure that sensitive information is protected from unauthorized access, even if it is intercepted or stored in a less secure environment. Moreover, NextLabs enables secure collaboration by allowing organizations to define and enforce policies for data sharing, ensuring that only authorized users can decrypt and access the shared data. This is particularly important in environments where data often needs to be shared across different departments, partners, or locations.

Continuous Monitoring and Risk Analytics

A key component of the Zero Trust model is the ability to continuously monitor data access and usage. NextLabs provides advanced monitoring capabilities that track data interactions in real time, including who is accessing the data, from where, and for what purpose. This real-time visibility into data access helps organizations detect unusual patterns that may indicate a security threat, such as a user attempting to access data they do not normally use or accessing data from an unfamiliar location. NextLabs can automatically trigger alerts or enforce additional security measures, such as MFA, when suspicious activities are detected.

Compliance and Auditing

NextLabs provides robust auditing and reporting tools that help organizations demonstrate compliance with data protection regulations such as GDPR, CCPA, and HIPAA. By maintaining a detailed audit trail of all data access and usage activities, NextLabs enables organizations to conduct thorough compliance reviews and forensic investigations when necessary. The ability to generate reports on who accessed what data, when, and under what circumstances, provides valuable insights and ensures accountability within the organization.

Seamless Integration with Existing IT Landscape

NextLabs Zero Trust Data-Centric Security is designed to integrate seamlessly with an organization's existing environment, including operating systems, cloud platforms, enterprise applications, identity management solutions, and data stores. This allows organizations to implement Zero Trust principles without overhauling their current systems. NextLabs has integrations that work out-of-the-box (OOTB) with hundreds of enterprise applications, such as databases, CAD tools, CI/CD platforms, and ERP solutions, and well as with hundreds of attribute sources, such as identity providers, SIEMs, etc. By integrating with all of these without any coding

required, NextLabs extends Zero Trust policies across all user access points, ensuring a unified and consistent security posture.

Key Takeaways

1. Organizations and enterprises increasingly need to protect critical data anywhere and everywhere
2. The challenges of protecting data in all these potential environments is best met through a Zero Trust Data-Centric Security approach
3. Organizations such as NIST, the United States Department of Defense, and CISA have adopted recommendations that promote a Zero Trust Data-Centric approach as the best way to protect data.
4. NextLabs provides a Zero Trust Data-Centric Security solution that allows organizations to protect their data.

References

- Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model Version 2.0. April 2023.
- Department of Defense. Zero Trust Reference Architecture Version 2.0. September 2022.
- National Institute of Standards and Technology. Special Publication 800-207: Zero Trust Architecture. August 2020.
- NextLabs. Zero Trust Data-Centric Security Solutions.
- NextLabs. Products.
- NextLabs. What is Policy-Based Access Control?
- NextLabs. Policy Engine.

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/.