The 7 Pillars of Zero Trust Explained

The emerging Zero Trust framework represents a new standard for organizational cybersecurity. Learning how to implement this approach and get organizational buy-in will better protect companies from insider attacks and help them recover from successful attacks more quickly. This paper covers Zero Trust’s fundamental components and principles, its benefits and challenges, and the seven “pillars”, or key areas, in which Zero Trust practices should be implemented.

What is Zero Trust?

Zero Trust is an approach to cybersecurity that requires a secure authentication for each session in which a private resource is to be accessed. Zero Trust can be usefully contrasted with the older "perimeter" framework, in which a set of trusted in-network devices, often physically located together (e.g., within an office location), is given broad access to many different private resources. With the distinction between in-network and out-of-network devices becoming increasingly porous over the years in light of remote work, bring your own device policies, and related developments, a new approach to cybersecurity is needed, in which institutions "never trust, always verify." The "basic tenets" of Zero Trust, given by NIST SP 800-207 “Zero Trust Architecture”, can be distilled into the following:

- **Eliminate trusted devices in favor of authenticated sessions**. Rather than granting stable and broad permissions to specific devices, secure authentication should be performed each time a user accesses a resource over any device.
- **Minimize access permissions for each session as much as possible**. Access should be granted to the least number of resources needed to complete the relevant task and should also be time-limited.
- **Use a rich body of information to authenticate sessions**. Instead of authenticating solely based on the identity of the requesting device, a broad array of information should be used for greater reliability, including, for example, user identity (itself ensured by Multi-Factor Authentication), time and location of the request, requesting device characteristics (e.g., software version details), and behavioral analytics for previous device/user activity.
- **Continuously monitor network and system activity to improve overall security posture**. Zero Trust eschews the idea of a fixed perimeter with a stable set of permissions in favor of a continuously evolving security policy, requiring network activity analysis to detect threats so that quick and precise permission revisions can be implemented.

How does Zero Trust Work?

The basic tenets of Zero Trust outlined above must be implemented in a concrete Zero Trust architecture. Such an architecture can be described in terms of its essential components and their purposes. These can be divided into the following two categories.

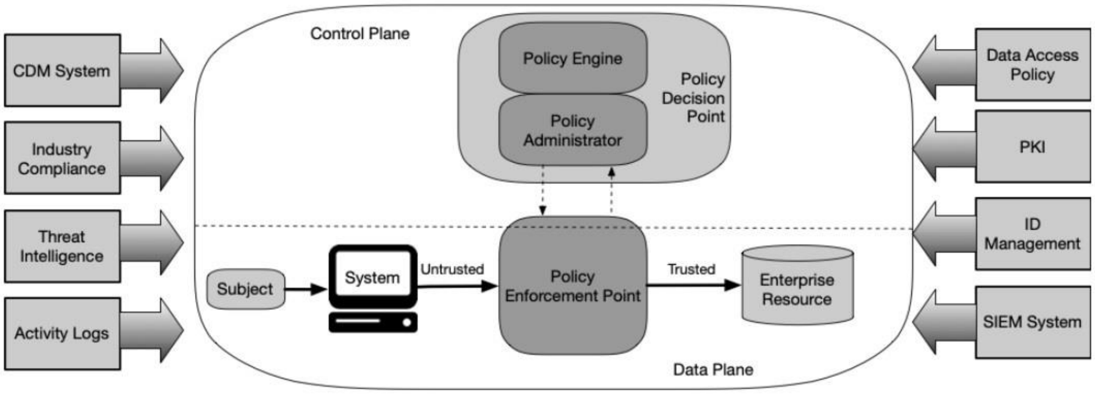

Figure 1: Components of a Zero Trust Architecture. Source: NIST SP 800-207 "Zero Trust Architecture"

Policy Components

The following components administer and implement the actual authentication process and session:

- **Policy Engine (PE)**: Gathers data about the request and implements enterprise policies to determine whether to approve the request.
- **Policy Administrator (PA)**: Takes an authentication decision from the PE and generates, or does not generate, credentials or tokens to allow a session.
- **Policy Enforcement Point (PEP)**: Manages the connection between the requesting device and the private resource based on commands sent by the PA.

Decision Data Sources

The following components supply data to the PE to inform the decision to allow or deny access:

- **Continuous Diagnostics and Mitigation (CDM) System**: Gathers data on the characteristics of the requesting device, including software and operating system version information, presence of non-approved components, and known vulnerabilities. CDM systems also configure and update enterprise assets and software.
- **Industry Compliance System**: Encodes policy rules that ensure compliance with any relevant legal regulations (e.g., FISMA, HIPAA).
- **Threat Intelligence Feeds**: Provides information about attacks or vulnerabilities relevant to the access control process.
- **Network and System Activity Logs**: Records information about events within the network to improve threat detection and measure anomalous behavior.
- **Data Access Policies**: Defines the fundamental rules which determine which subjects are permitted to access a given resource at a given time.

- **Security Information and Event Management (SIEM) System**: Gathers security-centric data inside and outside the context of a session to inform future policy and access decisions.
- **ID Management System**: Manages the identity records, such as names, email addresses, roles, and assigned resources for accounts requesting access to resources.

Benefits of Zero Trust

Zero Trust is designed to eliminate vulnerabilities in the old perimeter approach. In particular, an effective implementation of Zero Trust has the following security benefits:

- **Reduced ability for compromised accounts or devices to access private resources**. In the perimeter approach, accounts and devices within the perimeter are granted broad access to non-public assets. This means that any breach in the perimeter exposes a wide array of private resources. With Zero Trust architecture, each account and device is granted the minimal access permissions it needs to function. If an adversarial agent compromises an account or device, the damage that the adversary can do is minimized.
- **Reduced threat from insider attacks**. Legitimate enterprise actors like employees can intentionally or accidentally damage enterprise resources by exposing or encrypting sensitive data. Zero Trust minimizes the damage from these insider attacks by granting minimal permissions to inside actors and requiring authentication for each session.
- **Reduced duration of successful attacks**. Assuming that an internal or external attack is in progress, a Zero Trust infrastructure can more quickly detect and end the attack because Zero Trust includes continuously monitoring network activity and uses behavioral analytics to detect unusual activity. If unauthorized access occurs or an account or device is compromised, these analytics will be supplied to the PE, which can deny any further access permissions.

Challenges for Zero Trust (and solutions)

No cybersecurity model can completely eliminate vulnerabilities or avoid all challenges. In the case of Zero Trust, these challenges can be divided into three categories: implementation challenges, technical vulnerabilities, and user experience challenges. These are each described below.

Implementation Challenges

For organizations still using older approaches, migrating to a Zero Trust system presents difficulties. This is especially true because such organizations cannot implement Zero Trust from the ground up but must gradually replace existing components and systems with Zero Trust-compliant alternatives. That entails a transitional period in which Zero Trust components must coexist with components still operating on older models. For this to work, the organization must confirm that processes shared between components like event logging and ID management can operate in a hybrid security model.

Another implementation challenge lies in ensuring that the organization collects sufficient data to feed to the PE to enable reliable authentication decisions. This requires detailed knowledge of enterprise assets, subjects, and business workloads and processes. Privileged Access Management solutions are one valuable tool for organizing and managing relevant data.

Technical Vulnerabilities

Although Zero Trust reduces technical vulnerabilities compared to the perimeter approach, these vulnerabilities cannot be eliminated. One crucial chokepoint that must be carefully secured is the policy components, namely the PE, PA, and PEP, as these core components manage all authentication processes for accessing any private resource. Any attack on these components, including, for example, a Denial-of-Service (DoS) attack, could have extremely adverse impacts on enterprise operations. To help protect these components, they can be placed in a secure cloud environment or be replicated in several different environments. The policy components should also be carefully monitored, with any configuration changes logged and audited.

User Experience Challenges

Since Zero Trust requires frequent authentication and minimizes access permissions, users may experience security fatigue. This means that they have to perform so many authentication tasks that productivity is negatively impacted. To reduce security fatigue, user authentication tasks should be streamlined as much as possible.

What are the 7 Pillars of Zero Trust?

The Department of Defense (DoD) "Zero Trust Reference Architecture" lays out seven pillars, or key focus areas, for implementing Zero Trust principles. Each of these Zero Trust 7 pillars comes together to protect important private resources, as seen in Figure 2 below.

1. **User Pillar**: This area involves all processes related to authenticating user identities and managing user access privileges. This could include the use of ID Management Systems, Privileged Access Management, and Multi-Factor Authentication.
2. **Device Pillar**: This area involves authenticating device identities and characteristics, such as ensuring that the device has no non-approved components and up-to-date software. This could include the use of CDM Systems, Mobile Device Managers, and Trusted Platform Modules.
3. **Network/Environment Pillar**: This area involves isolating and controlling the network and both on- and off-site environments through segmentation and fine-grained access permissions. This could include micro- and macro-segmentation, with an eye toward eliminating unnecessarily broad access permissions.
4. **Applications and Workload Pillar**: This area includes all tasks performed at the application layer, consisting of first-party and third-party software. Ensuring Zero Trust-compliance at the application layer means authentication sessions prior to any access of enterprise applications and could include the use of proxy technologies.

5. **Data Pillar**: This area includes all data stored by enterprise applications. Zero Trust involves a comprehensive data management strategy, with data access permissions being granted as minimally as possible for workflows to function.
6. **Visibility and Analytics Pillar**: This area involves the analysis of incoming and outgoing network and system activity. Zero Trust principles require continuous monitoring of network activity to detect active threats and perform audits to improve overall network security, device security, and workforce security, which involves using Network and System Activity Logs, Threat Intelligence Feeds, and SIEM Systems.
7. **Automation and Orchestration Pillar**: This area involves automating security processes, such as authentication and threat detection, as much as possible. Automation improves the speed, scale, and consistency of security policy implementation.

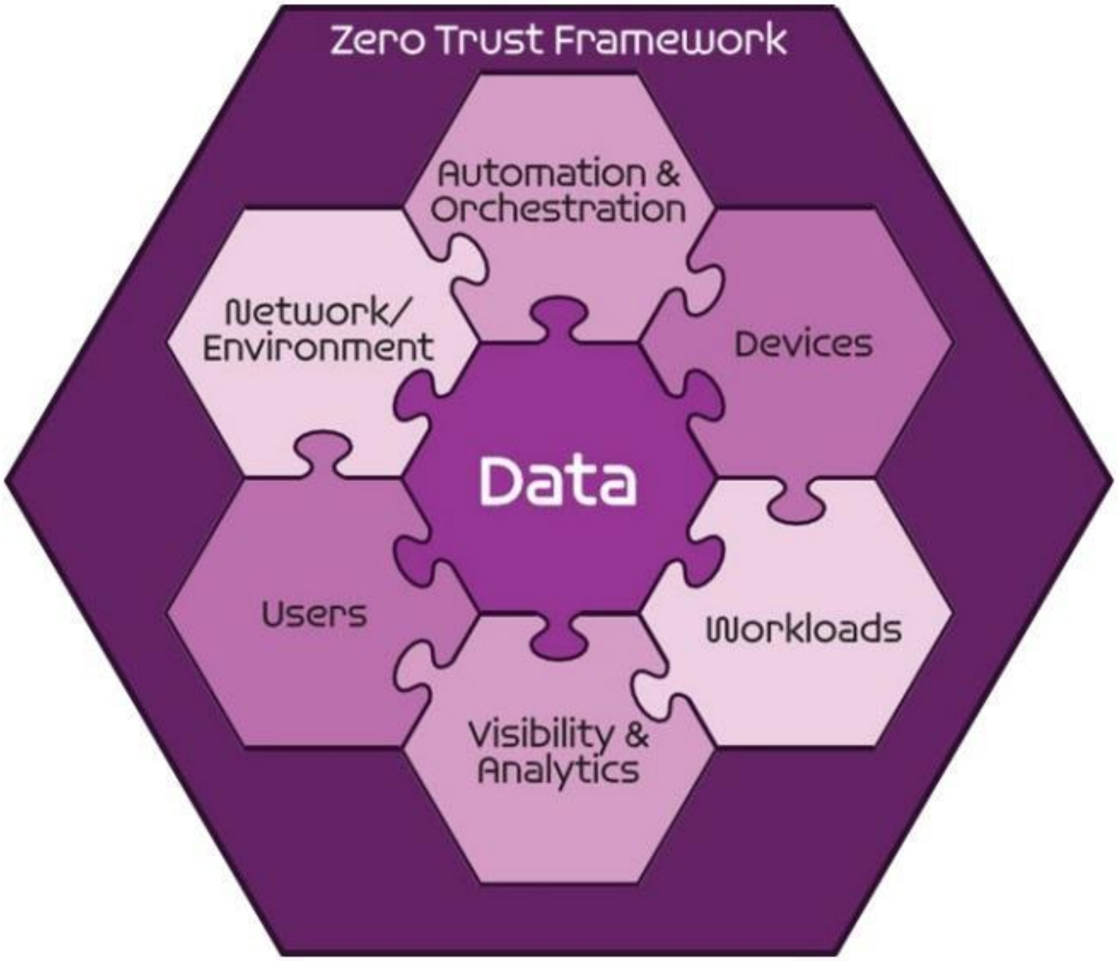

Figure 2: Interlocked Pillars of Zero Trust. Source: Department of Defense (DoD) "Zero Trust Reference Architecture"

Synergizing Zero Trust and Cybersecurity Education

Successfully implementing a zero-trust architecture requires buy-in at all levels of the organization, not just within IT and cybersecurity teams. Replacing older processes and components with Zero Trust-compliant alternatives alters everyday workflows across the enterprise. Users must perform authentication tasks more frequently within a zero-trust environment and may be granted more restrictive access permissions.

To achieve widespread successful deployment of Zero Trust principles, educate users about the motivations for and benefits of the Zero Trust system, as well as the weaknesses of older approaches to cybersecurity. It is also worth clearing up the misconception that "Zero Trust" means a lack of trust in users and employees when "Zero Trust" really means not automatically trusting specific devices and systems marked as inside a perimeter. By synergizing the implementation of Zero Trust with cybersecurity education across the enterprise, organizations can cultivate a successful “Zero Trust mindset”.

Summary

The heart of Zero Trust lies in a paradigm shift away from establishing a network perimeter within which devices and users are trusted and towards a model in which secure authentication is performed before any session in which private enterprise resources will be accessed. It also includes the principle that the access permissions granted for each session should be minimized while preserving the ability to perform the relevant task or workflow.

Such a paradigm shift requires buy-in at all levels of the organization and impacts all major areas in which IT operates. These are the 7 Zero Trust pillars: User, Device, Network/Environment, Applications and Workload, Data, Visibility and Analytics, and Automation and Orchestration. Although it requires a significant change in mindset and business workflows, successfully implementing a Zero Trust architecture comes with several significant security upsides, including reduced attack duration, attack scope, and threat from insider attacks. These benefits follow directly from the basic principles of Zero Trust, which include continuous network monitoring, access minimization, and frequent authentication.

As with any major IT change, Zero Trust has its challenges. Organizations must ensure that shared processes can exist within a hybrid security environment during the transition process and maintain detailed knowledge of enterprise assets and subjects. Organizations should also carefully guard the crucial policy decision-making components of Zero Trust systems, for example, by placing them in a secure cloud environment and replicating these components in different environments. Finally, organizations should take steps to streamline user authentication processes to minimize the risk of security fatigue.

With the successful deployment of a Zero-Trust approach to cybersecurity, organizations can significantly reduce their vulnerabilities and protect their most important assets and resources.