ZeroTrust Architecture

Framework to Strengthen Structural Security of Modern Enterprise

Edited by **MOHAN DAS VISWAM**

Zero Trust Architecture or ZTA is an infrastructure design philosophy based on the principle of 'never trust, always verify'. It debunks the typical 'castle-and-moat' style perimeter security and intends to handle newer threats of privilege misuse, internal breaches and lateral movement from within the trusted inside. Zero Trust Architecture defines a framework for structural cyber security of modern enterprises. It combines some of the already well known and established security guidelines and highlights them as the basic of tenets of the framework.

Ashish Agarwal
Sr. Technical Director
ashish@nic.in

Syed Hasan Mahmood
Scientist-'C'
hasan@nic.in

Traditional security in based on the concept of trusted and untrusted zones. These zones are defined by physical or logical perimeter protected by security devices like firewall. Any device/ user inside the perimeter is treated as trusted and is allowed access to internal resources by default. An example of such a design is a typical office network local area network (LAN). Any device/ user inside the office LAN is allowed access to the internal office resources like eOffice, eFiles, eHRMS, network printers, or any other computer/ server within the LAN. This design assumes that all devices/users within the office LAN are genuine and authorised. It also assumes that all programs running within these devices are safe and non-malicious. However, with high speed internet access on these devices, we have seen time and again that these trusted devices/ programs can very easily be compromised by the well-resourced adversaries to launch various attacks on the internal resources like unauthorised access, data exfiltration, internal network control, etc. They take advantage of the design which implicitly trusts anyone and everyone which happen to get an entry into the trusted zone.

Zero Trust design principle aims to overcome this weakness and create a design based on actual verification of devices/users and continuous monitoring of resource accessed by them. The first step is to identify and enumerate internal resources and define micro-perimeters (also called Software-defined Perimeter or SDP) around them. The idea is to verify each and every request for the resources, continuously monitor and change access control policies based on change in access parameters. The request for resources can originate from either the internal LAN or remote workers using Virtual Private Network (VPN). The concept of Zero Trust has been there for a long time in silos. However, the term was coined by John Kindervag in 2010, during his tenure as a vice president and principal analyst for Forrester Research, for the complete framework encompassing various IT operation silos and technologies to achieve new age structural security.

Tenets of Zero Trust

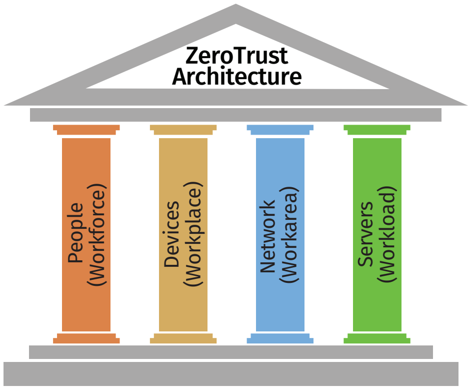
Zero Trust Architecture defines a framework for structural cyber security of modern enterprises. It combines some of the already well known and established security guidelines and highlights them as the basic of tenets of the framework. The basic tenets of the ZTA are enumerated below,

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per session basis
- Access to resources is determined by dynamic policy - including the observable state of client identity, application, and the requesting asset - and may include other behavioural attributes
- The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible
- All resource authentication and authorisation are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture

Pillars of Zero Trust Architecture

We need to understand the type of resources in an IT ecosystem in order to be able to protect them and move toward zero trust.

Typically, an environment consists of people (workforce), devices (workplace), network (work-area) and servers (workload). A zero trust model has to identify and separate these components and define dynamic/adaptive policies around them. The pillars of ZTA as defined by Forrester's Zero Trust eXtended model are as follows,



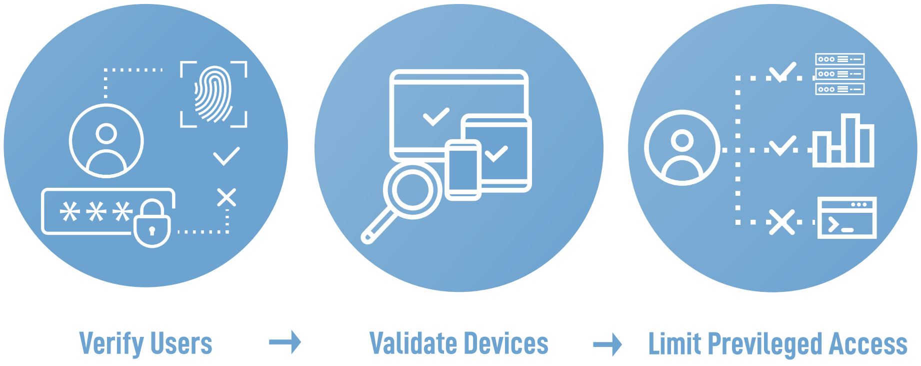
- **Data security:** encryption and secure access

Take a zero-trust approach to securing data by protecting the new, extended perimeter: classify and categorise data; authorise user and device access to data; prevent data loss and exfiltration; and encrypt emails and device data.

- **Network security:** **prevent and contain breaches on the network**

By segmenting access across your network, you can better isolate and control critical areas of your network to contain breaches and prevent lateral move-

Key Steps to Zero Trust Model



ment. Get more visibility into what's on your network so you can secure it with a zero-trust approach.

- **Workforce security:** control who gets access

Assume zero trust until you can verify the trust-worthiness of your users' identities and the security of their devices. Protect against phishing and other identity-based attacks.

- **Workload security:** protect the entire application stack

Secure access for APIs, micro-services, or containers accessing a database within an application, no matter where it's located--in the cloud, data centres, or other virtualised environments. Segment access and identify malicious behaviour to contain breaches and protect against lateral movement.

- **Device security:** control user and IoT devices

Get visibility into, better secure, and control every device accessing your applications and network at all times. That includes Internet of Things (IoT), network-enabled devices, and (managed and unmanaged) user devices like APIs, cameras, HVAC systems, printers, medical equipment, and more.

- **Visibility and analytics:** gain insight to enforce security

Improve or increase visibility and analytics for your users and admins by gaining insight to unknown or unidentified assets on your network, across workloads or applications. Integrate with other data sources to use information intelligently to create and enforce policies that strengthen your overall security posture.

- **Automation and orchestration:** respond to threats quickly

The ability to integrate and automate security across your entire IT environment - for applications, networks, and workloads - is key for the success of your zero-trust strategy. By automating policy enforcement consistently across your environment, you can prevent a breach and also automate your threat response to more quickly contain a breach.

Implementation of Zero Trust in Government ICT Environments

The government can benefit greatly from implementing zero trust architecture because of the following reasons:

- Criticality of the data
- Variety and volume of data
- Importance of availability of services
- Diversity of environments
- Shortage of skilled resources

Typical environment in a government setup includes data centers housing data & services and office networks housing users & devices. Zero trust has to be planned for both the environments separately with necessary tools, policies and procedures in place. The steps to zero trust can be:

- **Identify resources** – data, assets, applications and services
- **Authenticate and authorize users** – user access policies should be based on identity
- **Contextualize request** – grant access to resources from users not only based on identity but other environment parameters like device used, network hooked on to, date and time of request, past history and pattern of access, etc.
- **Adaptive policy** – define access policies based on context to grant/deny access
- **Grant least privileges** – grant access to resources explicitly requested by user rather than resources by virtue of user identity or network
- **Monitoring and audit** – monitor all access requests and patterns for establishing normal and identify anomalies based on normal.

> **Zero Trust Architecture defines a framework for structural cyber security of modern enterprises. It combines some of the already well known and established security guidelines and highlights them as the basic of tenets of the framework.**
>
> **R S MANI**
> **Deputy Director General, NIC**

Zero trust can be achieved using most of the existing tools and technologies already deployed in the environment with augmentation of a few new ones. It has more to do with design change rather than technology change. The technologies which can be used for achieving zero trust in a data center can include (not limited to) disk encryption, database encryption, database access management, privilege identity/access management using multi-factor authentication, network micro-segmentation, next-gen firewall, network intrusion prevention, host intrusion prevention, virtual private network, log monitoring and analysis. The tools for office network can include user identity management with multi-factor authentication, network access control, endpoint protection solution, network micro-segmentation and next-gen firewall with anti-advanced persistent threat.

Advantages of Implementation of Zero Trust

Various advantages of implementation of zero trust can be,

- Decreases risk by discovering assets and improving visibility into them
- Protect data
- Reduce time to breach detection and gain visibility into enterprise traffic
- Reduce the complexity of the security architecture
- Deliver both security and an improved end-user experience

Summary

Zero trust is not a technology rather an infrastructure design principle built on security. It takes care of the modern threats faced by enterprises at the hands well-resourced and persistent adversaries. It begins with concept of isolation of resources and access based on requests after proper verification. Adoption of zero trust requires modification of policies and tweaking user behaviour to achieve the desired goals. It does not require a complete replacement of existing tools and technologies. New infrastructure being created can be designed on zero trust from the beginning. Existing infrastructure can be migrated gradually. Zero trust is not a choice any more, it is the way future infrastructure has to be designed to survive the cyber threats.

For further information, please contact:
R S Mani
Deputy Director General & HoG
National Informatics Centre, A-Block, CGO Complex
Lodhi Road, New Delhi - 110003
Email: rsm@nic.in, Phone: 011-24305397