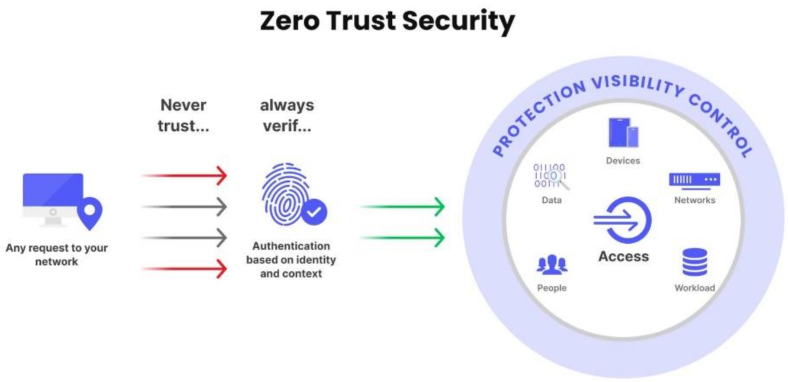
Zero Trust

Zero Trust means trusting no one both from inside and outside of a network by default and requires continuous verification of identity, device security and other contextual factors such as location and behavior to access any resource. This approach shifts away from traditional network segmentation and perimeter-based access to perimeter less access. It also focuses on harder access control and continuous monitoring.



Zero Trust Security
Never trust...
always verif...
Any request to your network
Authentication based on identity and context
PROTECTION VISIBILITY CONTROL
Devices
Data
Networks
Access
People
Workload

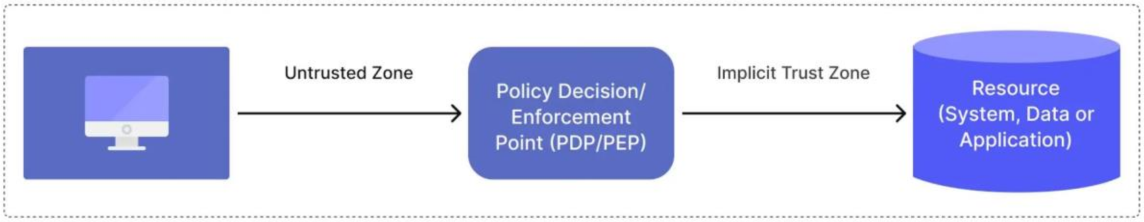
Need for Zero Trust

With the growth cloud computing and evolution of modern network, the complexity of enterprise architecture has significantly increased. It has urged security professionals to add multiple security layers to protect their digital spaces. However, this traditional perimeter-based security model has often lacked in integration and security control.

On the other hand, Zero Trust is a concept where no trust is granted. It enables organizations to create digital transformation where remote connections are secure, integrated and strictly controlled. It stands on a set of policies which prevents all kinds of authorized access and movement across an organization’s network and based on user’s role, location and device.

How it Works

Zero Trust combines the advantages of advanced cloud computing, Identity and Access Management, Next Generation Endpoint Protection and Security. It also establishes secure protocols and policies to improve network hygiene. These Policy Decision Points (PDPs) or Policy Enforcement Points (PEPs) protect cloud resources from untrusted Zone. This is illustrated in a simple diagram below:

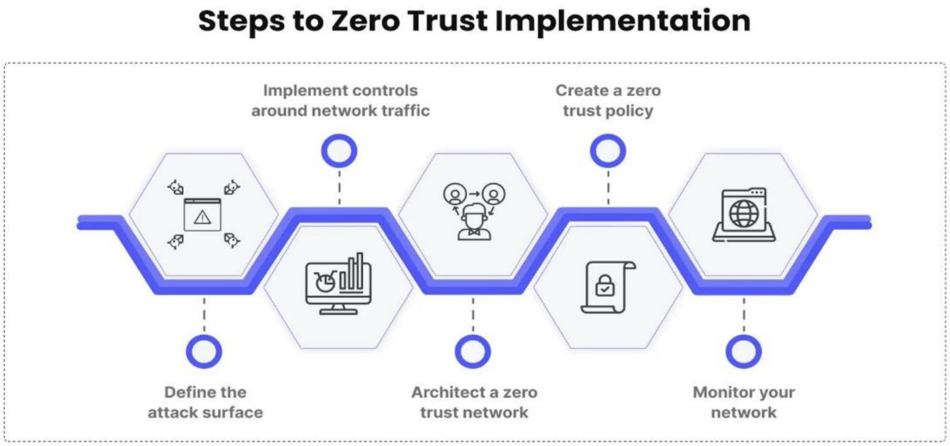

Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Principles of Zero Trust

According to the US National Institute of Standard and technology (NIST), a Zero Trust Model/Solution must follow these principles:

- All access to resources must be governed by company policies and procedures. These can include many factors such as, User, Device, IP address, Operating System, Work Schedule, Location and so on.
- All access to resources must require secure authentication per request basis.
- All resources must require their own authentication to access.
- Every communication must be secure and encrypted.
- All data and devices must be considered as resources and Zero Trust Policies to be applied on them.

How to Implement Zero Trust


Steps to Zero Trust Implementation
Implement controls around network traffic
Create a zero trust policy
Define the attack surface
Architect a zero trust network
Monitor your network

1. **Define Attack Surface:** Identifying Sensitive Data, Critical Application, Assets and Services.
2. **Establish Network Control:** Implementing control around network traffic to prevent any unauthorized access.
3. **Create Zero Trust Policies:** Producing Zero Trust Policies to clearly determine who has access to what resource and based on critical factors such as, user, device, network, time, location etc.
4. **Architect Zero Trust Network**: After policies are well defined and a zero-trust network should be planned and implemented to protect from any unauthorized access. Authentication is required to access any resource in a network. Network should be well protected using next generation firewalls.
5. **Monitor Network**: Observing and analyzing logs, report and data on regular basis to continuously learn and improve security standards. Data analytics provide useful insights into the outcomes of Zero Trust model and help professionals to rethink and redesign the solution.

Google Zero Trust (BeyondCorp)

Google BeyondCorp uses the company's Zero Trust model to create secure environments for its users. It was produced as an extension of Google's security principles introduced in 2011. The purpose behind BeyondCorp was to enable its employees to connect to the workspace remotely without using VPN. Since then, it has been designed to authenticate and authorize Google's employees to securely access corporate resources. It approves access to a resource based on user's role and identities instead of depending on the passwords. Moreover, BeyondCorp facilitates Single Sign On (SSO) and Access Control Policies. As a result, BeyondCorp has emerged as modern Zero Trust solutions for its employees and extended workforce ensuring compliance with security standards and convenient access to resources.

Web References:

1. https://maddevs.io/blog/what-is-zero-trust-network-architecture/
2. https://cloud.google.com/beyondcorp
3. https://www.nist.gov/publications/zero-trust-architecture
4. https://www.strongdm.com/zero-trust