**Zero Trust Security:**

* Zero trust security model also known as zero trust architecture (ZTA), zero trust network access (ZTNA) and perimeter less security.
* Approach to strategy, design, and implementation of IT systems.
* Concept: “never trust, always verify”.
* users and devices should not be trusted by default, even if they are connected to a permissioned network such as a corporate LAN and even if they were previously verified.
* Implemented by establishing strong identity verification, validating device compliance prior to granting access, and ensuring least privilege access to only explicitly authorized resources.
* Most modern corporate networks consist of many interconnected zones, cloud services and infrastructure, connections to remote and mobile environments, and connections to non-conventional IT (IoT).
* Reasoning: traditional method not sufficient.
* Advocates mutual authentication, checking the identity and integrity of users and devices without respect to location, and providing access to applications and services based on confidence of user and device identity and device health in combination with user authentication.
* Applied to data access, and to the management of data. Every request should be authenticated dynamically and ensure least privileged access to resources.
* To grant the access, the policies can be applied based on the attributes of the data like, who the user is and the type of environment using Attribute-Based Access Control.
* Elements to implement ZTA:
  + Using enhanced identity governance and policy-based access controls
  + Using micro-segmentation
  + Using overlay networks or software-defined perimeters
* Key principles:
  + Single strong source of user identity
  + User authentication
  + Machine authentication
  + Additional context (policy compliance and device health)
  + Authorization policies to access an application.
  + Access control policies within an application
  + Verify explicitly: authenticate and authorize based on all available data points. Assume all the network traffic is a threat at all the times.
  + Use least privileged access: Limit user access with Just-in-time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
  + **Assume breach: Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.**
* The approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy.
* Where this affects: Different organizational requirements, existing technology implementation and security stages.
* Moving towards trust-by-exception from trust-by-default. Zero trust is a network security philosophy that states no one inside or outside the network should be trusted unless their identification has been thoroughly checked. Zero trust operates on the assumption that threats both outside and inside the network are an omnipresent factor.
* Every attempt to access the network or an application is a threat.
* To solve the zero-trust problem, the recommended solution is Segmentation gateways (SG), which could be installed on the heart of the network. The SG model incorporating several different protection measures and using a packet-forwarding engine to dispatch protections where they are needed in the network.
* The verification for user applies whether the device or user is already within the network perimeter. User or device identity verification can be triggered by events such as changes in the devices being used, location, log-in frequency, or the number of failed login attempts.

|  |  |
| --- | --- |
| **Name** | **Description** |
| The protect surface | **Data**: which data to be protected?  **Applications**: Which application has sensitive info?  **Assets**: what are the most sensitive assets?  **Services**: Which services can a bad actor exploit in interrupt IT operation.  Preferable to trying to guard the attack surface, which constantly increasing in size and complexity.  Regulating traffic around critical data and components by forming micro perimeters.  At the edge of micro perimeter Zero trust networks employs a SG, which monitors the entry. Applies security measures that are designed to thoroughly vet users and data before to granting access using a Layer 7 firewall and Kipling method. |
| Multi-factor authentication | Identity verification by multiple credentials.  Without anyone factors user cannot access the data or gain the access.  Aids a zero-trust network by increasing # user-specific credentials required for access.  Increase difficulty for hackers. |
| Endpoint Verification | To make sure that the one is being controlled by the right person by sending verification out to the endpoint. And user sends the response to the device.  The data sent from endpoint is used to check the validity and a successful receipt and transmission process earns the status as “Trustworthy”.  it requires both the user and the endpoint itself to present credentials to the network. |
| Micro segmentation | Creating zones within the network to isolate and secure the element.  once the secured area has been micro segmented, it’s protected from threats. |
| Least privilege access | Allowing users to access only those resources which are essential for performing their duties.  It limits #point of entries to sensitive data or infrastructure.  Saves time and resources because fewer MFA measures have to be employed, which limits the volume of credentials. |
| Zero-Trust Network Access | Focus on controlling access to application.  Verify users and devices before every application session to meet the organizations policy to access the application.  Supports MFA for verification.  Location independent and no matter the user is on the netork or off network.  For off internet: secure encrypted tunnel for connectivity to application. |

**Benefits:**

* Protection of customer data
* Reduced redundancy and complexity of the security stack
* Reduced need to hire and train security professionals.
* Increase visibility.
* Limit the blast radius of breaches.
* Access control in modern IT environments.
* Continuous Compliance.

**How to implement Zero Trust Security:**

Define a protect surface.

Limit access to data.

Give the team visibility.

**Challenges of Zero trust:**

* Being Consistent
* Inhibiting productivity
* Combating insider
* Maintaining policies and architecture.

**Pillars of Zero Trust:**

* Identity
* Device
* Network
* Application workload
* Data
* Visibility and analysis
* Automation and orchestration