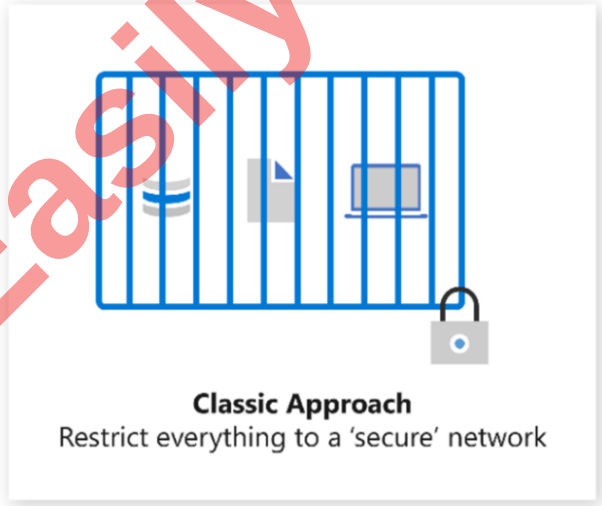
Zero Trust Model

- ✓ Network Security model that verifies each request
- ✓ All users and devices, are considered untrusted until they prove themself.
- ✓ Operates on the principle of "never trust, always verify."
- ✓ The Zero Trust Model is very relevant in today's evolving cybersecurity landscape, where traditional network perimeters are not very efficient



Zero Trust Model

Key Principles & Components

- ✓ **Verify Identity:** All users, devices, and entities must be authenticated & verified
- ✓ **Least Privilege Access:** Users and devices should be granted the minimum amount of access necessary to perform their tasks
- ✓ **Network-Segmentation:** To divide the network into smaller, isolated segments
- ✓ **Continuous Monitoring:** Real-time monitoring and analysis of network traffic and user behavior
- ✓ **Access Control and Policy Enforcement:** Access control policies are enforced at every access request
- ✓ **Encryption:** Data encryption is applied to protect data at rest and in transit
- ✓ **Workload Security:** Security is applied at the workload level
- ✓ **Identity and Access Management (IAM):** IAM solutions are used to manage and govern access to resources
- ✓ **Continuous Improvement:** The Zero Trust Model is an ongoing process that involves continuous improvement