ScreenMeet's Zero Trust Architecture

ScreenMeet's Zero Trust Architecture means it is the most secure remote access solution on the market. A Zero Trust solution is a cybersecurity framework that operates on the principle of "never trust, always verify." Unlike traditional security models that rely on a secure perimeter (e.g., firewalls), Zero Trust assumes that threats can exist both inside and outside the network. It enforces strict access controls, continuously verifying the identity and behavior of users, devices, and applications.

Key Benefits

- **Reduces the risk of data breaches**
- **Improves compliance with regulations (e.g., GDPR, HIPAA)**
- **Enhances security in hybrid or remote work environments**
- **Minimizes the impact of insider threats**

The Major Principles of ScreenMeet's Zero Trust solution include

- **Continuous Verification**
  Always authenticate and authorize users and devices based on dynamic context, such as user identity, location, device health, and activity.
- **Least Privilege Access**
  Grant only the minimum level of access required for users to perform their tasks, reducing the attack surface.
- **Micro-Segmentation**
  Break the network into smaller zones and secure each zone individually to prevent lateral movement by attackers.
- **Assume Breach**
  Design systems with the assumption that breaches have already occurred, focusing on minimizing impact and detection.
- **Device Trust**
  Ensure that devices are secure, updated, and compliant with security policies before granting access.
- **Application-Centric Security**
  Protect applications by enforcing secure access policies and verifying user actions within applications.
- **Visibility and Analytics**
  Continuously monitor and analyze network traffic, user behavior, and access patterns for anomalies.
- **Identity and Access Management (IAM)**
  Tools like multi-factor authentication (MFA), single sign-on (SSO), and role-based access control (RBAC).
- **Endpoint Security**
  Ensures all devices accessing the network meet security standards.
- **Network Segmentation**
  Separates sensitive data and resources from less critical systems.
- **Threat Detection and Response**
  Monitors for unusual behaviors and responds to threats in real time.
- **Cloud Security**
  Secures workloads and data in cloud environments using Zero Trust principles.