5 Key Pillars of Zero Trust Architecture

1 IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity verification is at the core of Zero Trust. This ensures that only authenticated and authorized users and devices can access systems and data.

KEY ELEMENTS:

- Multi-Factor Authentication (MFA): Reinforces user identity verification.
- Single Sign-On (SSO): Simplifies access management across multiple applications.
- Role-Based Access Control (RBAC): Access is granted based on user roles.

2 DEVICE SECURITY

Every device (laptop, mobile, IoT) accessing the network must be validated before access is granted. Device posture checks are essential.

KEY ELEMENTS:

- Device Compliance Checks: Ensuring that devices meet security requirements (e.g., anti-virus, encryption).
- Endpoint Detection and Response (EDR): Protects against malware and other attacks on endpoints.

3 MICRO-SEGMENTATION

Dividing the network into smaller, controlled zones to limit lateral movement of threats.

KEY ELEMENTS:

- Network Segments: Creating isolated zones to reduce exposure.
- Granular Access Control: Restricting access between zones based on need.

4 LEAST-PRIVILEGE ACCESS

Only the minimum access required is granted to users, devices, and applications to perform their tasks.

KEY ELEMENTS:

- Access Control Lists (ACLs): Managing who can access what resources.
- Time-Based Access: Limiting access to specific times.
- Just-In-Time (JIT) Access: Providing temporary access as needed.

5 CONTINUOUS MONITORING AND ANALYTICS

Zero Trust requires continuous monitoring of all users, devices, and network activity to detect and respond to threats in real time.

KEY ELEMENTS:

- Behavioral Analytics: Analyzing behavior patterns to detect anomalies.
- Threat Intelligence: Gathering real-time threat data to prevent attacks.
- Incident Response: Rapid response and mitigation of detected threats.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com