Domain 12 Related Technologies & Strategies

Zero Trust Pillars & Maturity Model:

- the pillars (Identity, Devices, Networks, Applications and Workloads, Data) and cross-cutting capabilities (visibility, automation, governance) in the CISA ZTMM

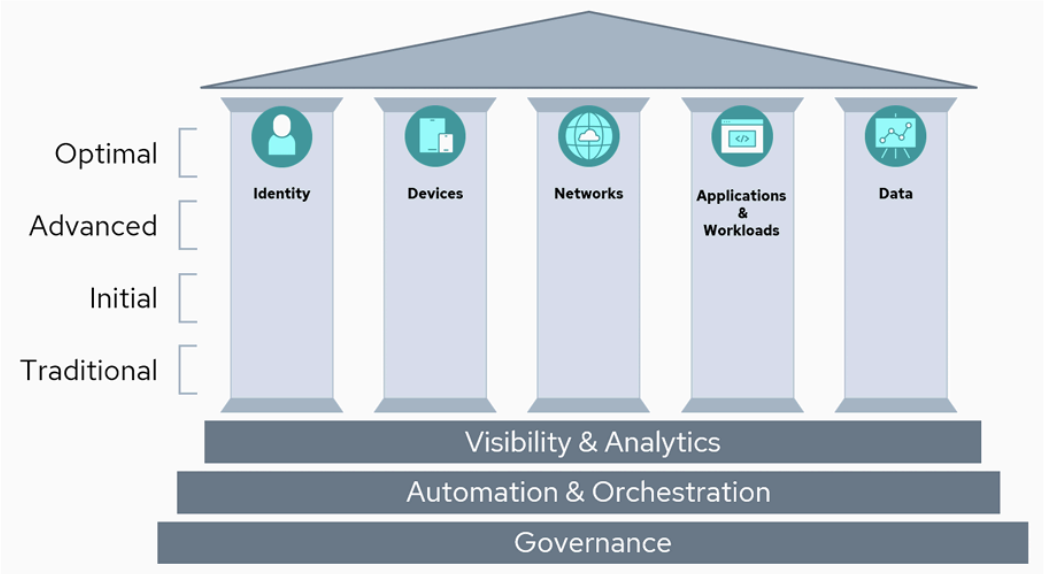

Figure 32: The CISA Zero Trust Maturity Model

- The CISA ZTMM helps organizations enhance their ZT strategies as it outlines maturity stages Traditional, Initial, Advanced, and Optimal– across the ZT pillars and capabilities.
- This maturity model has 4 stages:
  1. **Traditional**: security controls are typically based on firewalls and static policies.
  2. **Initial**: centralized identity management and device security is introduced. Networks start to be segmented.
  3. **Advanced**: continuous and dynamic controls are implemented.
  4. **Optimal**: Functions like identity management and network segregation are fully automated and adaptive.

AI's Role in Cloud Security

AI functions both as a security tool and a potential attack vector in cloud environments. It enhances security by detecting threats and automating defenses but also poses risks by enabling sophisticated cyber attacks.

Characteristics of AI Workloads

AI workloads fall into two categories:

- **Training** – Requires massive data and computing power to create models.
- **Inference** – Runs trained models to analyze or generate data.

Neural networks, particularly large language models (LLMs), are widely used in AI applications.

AI and Cloud Security

AI workloads are substantial and require secure data handling. AI is increasingly integrated into security solutions for better threat detection while also being exploited for attacks.

AI Deployment Models in Cloud Security

1. **AI as a Service (SaaS)** – Fully managed AI solutions (e.g., Claude). Security measures include controlling data access and tracking usage.
2. **AI as a Platform (PaaS)** – Cloud providers offer infrastructure for AI model hosting (e.g., AWS Bedrock). Security involves securing training data, access control, and defending against adversarial attacks.
3. **Bring Your Own Model (BYOM)** – Organizations develop or deploy AI models using cloud resources. Requires in-house expertise and strong security controls.
4. **AI-Enhanced Security Tools** – AI is embedded into security solutions for smarter threat detection, policy enforcement, and access control.

As AI continues to evolve, its impact on cloud security will grow, necessitating robust defenses against AI-driven threats.