**Defense in Depth: A Layered Security Approach**

**What is Defense in Depth?**

* A **multi-layered security strategy** that ensures if **one barrier fails**, another is in place to stop an attack.
* Inspired by **medieval castles**, which used multiple defenses like **moats, stone walls, and watchtowers** to slow down and stop attackers.

**Five Layers of Defense in Depth**

1. **Perimeter Layer (Authentication)**
   * The **outermost layer** that filters **external access** to systems.
   * **Security Controls**:
     + Usernames & Passwords
     + Basic Authentication
2. **Network Layer (Authorization & Firewalls)**
   * Focuses on controlling **who can communicate** over the network.
   * **Security Controls**:
     + Firewalls
     + Network Segmentation
     + Intrusion Detection Systems (IDS)
3. **Endpoint Layer (Device Protection)**
   * Protects **devices** (laptops, desktops, servers) that connect to the network.
   * **Security Controls**:
     + Anti-virus software
     + Device encryption
     + Endpoint Detection & Response (EDR)
4. **Application Layer (User Interaction Security)**
   * Secures **applications and software** that process data.
   * **Security Controls**:
     + Multi-Factor Authentication (MFA)
     + Secure Coding Practices
     + Web Application Firewalls (WAF)
5. **Data Layer (Protecting Sensitive Information)**
   * Focuses on securing **critical data** like personally identifiable information (PII).
   * **Security Controls**:
     + Data Encryption
     + Access Control Policies
     + Asset Classification

**Key Takeaways**

* **Each layer strengthens security** by addressing different vulnerabilities.
* **Data moves through all five layers**, making layered security critical.
* **Organizations use this model** to **reduce risks** and **protect important assets**.