Security Architecture

Compare and contrast security implications of different architecture models

- **Architecture and Infrastructure Concepts**
    - **Cloud**
        - **Responsibility Matrix**
            - In cloud environments, security responsibilities are shared between the cloud service provider and the customer. It's essential to be clearly responsible for aspects like data protection, application security, and infrastructure management to prevent security gaps.
        - **Hybrid Considerations**
            - Combining on-premises and cloud resources introduces complexities in security management, such as ensuring consistent security policies across environments and securing data in transit between them.
        - **Third-Party Vendors**
            - Relying on external vendors for cloud services necessitates thorough vetting and continuous monitoring to ensure they meet security standards and don't introduce vulnerabilities.
    - **Infrastructure as Code (IaC)**
        - Automating infrastructure provisioning through code enhances consistency and reduces human error. However, it requires secure coding practices and regular code reviews to prevent introducing vulnerabilities into the infrastructure.
    - **Serverless**
        - Abstracting server management to the cloud provider reduces operational overhead but can lead to less visibility and control over the execution environment. Security measures must focus on application code and proper configuration of cloud services.
    - **Microservices**
        - Breaking applications into smaller, independent services improves scalability and resilience. However, it increases the attack surface and necessitates securing inter-service communication, often through robust API security measures.
    - **Network Infrastructure**
        - **Physical Isolation (Air-Gapped)**
            - Completely isolating systems from any network can prevent remote attacks but may hinder operational efficiency and updates.
        - **Logical Segmentation**
            - Dividing networks into segments using VLANs or subnets helps contain potential breaches but requires proper configuration and management to be effective.
        - **Software-Defined Networking (SDN)**
            - Centralizing network controls allows for dynamic management but introduces risks if the control plane is compromised.
    - **On-Premises**
        - Hosting infrastructure on-site provides greater control over security but requires significant resources for maintenance and protection against physical and cyber threats.

    - **Centralized vs. Decentralized**
        - **Centralized**
            - Simplifies management and policy enforcement but creates a single point of failure and potential target for attacks.
        - **Decentralized**
            - Enhances resilience by distributing resources but complicates consistent security policy enforcement.
    - **Containerization**
        - Encapsulating applications in containers ensures consistency across environments. However, it requires securing the container images, orchestrator platforms, and underlying host systems.
    - **Virtualization**
        - Running multiple virtual machines on a single physical host optimizes resource use but introduces risks like VM escape, where an attacker gains access to the host or other VMs.
    - **Internet of Things (IoT)**
        - Connecting numerous devices increases the attack surface, especially if devices lack robust security features. Ensuring device authentication, data encryption, and regular updates is vital.
    - **Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA)**
        - Critical for managing industrial processes, these systems often prioritize availability and may use outdated technologies, making them vulnerable to attacks. Implementing network segmentation and strict access controls is essential.
    - **Real-Time Operating System (RTOS)**
        - Designed for time-sensitive applications, RTOS must maintain strict timing constraints. Security measures must not interfere with real-time performance, necessitating specialized approaches.
    - **Embedded Systems**
        - Often resource-constrained and designed for specific tasks, these systems may lack comprehensive security features. Ensuring secure coding practices and physical security is crucial.
    - **High Availability**
        - Systems designed for high availability aim to minimize downtime. Security measures must be robust yet not impede the system’s ability to remain operational during adverse conditions.

- **Considerations**
    - **Availability**
        - Ensuring systems are operational when needed.
    - **Resilience**
        - Ability to recover from failures or attacks.
    - **Cost**
        - Financial implications of implementing and maintaining security measures.
    - **Responsiveness**
        - Speed at which systems can respond to threats or changes.
    - **Scalability**
        - Capacity to grow and manage increased demand securely.
    - **Ease of Deployment**
        - Simplicity in implementing security measures.

- **Risk Transference**
    - Shifting risk to third parties, such as through insurance or outsourcing.
- **Ease of Recovery**
    - Ability to restore systems and data after an incident.

- **Patch Availability**
    - Timeliness and accessibility of updates to address vulnerabilities.
- **Inability to Patch**
    - Challenges in updating certain systems, often due to legacy technology.
- **Power**
    - Energy requirements and ensuring uninterrupted power supply.
- **Compute**
    - Processing power needed to implement security measures without degrading performance.

Given a scenario, apply security principles to secure enterprise infrastructure

- **Infrastructure Considerations**
    - **Device Placement**
        - Strategically position security devices (e.g., firewalls, IDS) within the network to monitor and protect critical assets effectively.
    - **Security Zones**
        - Segment the network into distinct zones (e.g., DMZ, internal, external) to control access and contain potential breaches.
    - **Attack Surface**
        - Minimize the attack surface by disabling unnecessary services and ports, reducing the number of potential entry points for attackers.
    - **Connectivity**
        - Ensure secure connections between devices and networks, employing encryption and secure protocols to protect data in transit.
    - **Failure Modes**
        - **Fail-Open**
            - In the event of a failure, the system remains open, potentially allowing unauthorized access.
        - **Fail-Close**
            - In the event of a failure, the system shuts down, preventing all access.
    - **Device Attributes**
        - **Active vs. Passive**
            - Active devices (e.g., firewalls) actively filter traffic, while passive devices (e.g., IDS) monitor without interfering.
        - **Inline vs. Tap/Monitor**
            - Inline devices are placed directly in the data path, whereas tap/monitor devices observe traffic without being in the direct path.
    - **Network Appliances**
        - **Jump Server**
            - A secure system used to access devices in a separate security zone.
        - **Proxy Server**
            - Acts as an intermediary for requests, providing anonymity and content filtering.

        - **Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)**
            - Monitor network traffic for malicious activity, with IPS capable of taking preventive action.
        - **Load Balancer**
            - Distributes network or application traffic across multiple servers to ensure reliability and performance.
        - **Sensors**
            - Devices that collect data for monitoring and analysis purposes
    - **Port Security**
        - **802.1X**
            - An IEEE standard for port-based Network Access Control (NAC), providing authentication to devices attempting to connect to LAN or WLAN.
        - **Extensible Authentication Protocol (EAP)**
            - A framework for transporting authentication protocols, commonly used in wireless networks.
    - **Firewall Types**
        - **Web Application Firewall (WAF)**
            - Protects web applications by filtering and monitoring HTTP traffic.
        - **Unified Threat Management (UTM)**
            - Integrates multiple security features into a single device, such as firewall, antivirus, and intrusion detection.
        - **Next-Generation Firewall (NGFW)**
            - Advanced firewalls that provide deep packet inspection, intrusion prevention, and application awareness.
        - **Layer 4/Layer 7**
            - Refers to the OSI model layers; Layer 4 firewalls filter traffic based on protocol and port, while Layer 7 firewalls filter based on application-level data.

- **Secure Communication/Access**
    - **Virtual Private Network (VPN)**
        - Establishes a secure, encrypted connection over a less secure network, such as the internet.
    - **Remote Access**
        - Allows users to connect to the organization’s network from remote locations securely.
    - **Tunneling**
        - **Transport Layer Security (TLS)**
            - Provides secure communication over a computer network.
        - **Internet Protocol Security (IPSec)**
            - A suite of protocols that secure Internet Protocol communications by authenticating and encrypting each IP packet.
    - **Software-Defined Wide Area Network (SD-WAN)**
        - Utilizes software to manage WAN connections, improving performance and security.
    - **Secure Access Service Edge (SASE)**
        - Converges networking and security functions into a single cloud-delivered service model.

Compare and contrast concepts and strategies to protect data

- **Data Types**
    - **Regulated Data**
        - Information subject to laws and regulations, such as health records (HIPAA) or payment card information (PCI DSS).
    - **Trade Secrets**
        - Proprietary business information that provides a competitive edge.
    - **Intellectual Property**
        - Creations of the mind, including patents, trademarks, and copyrights.
    - **Legal Information**
        - Documents related to legal proceedings or advice.
    - **Financial Information**
        - Data pertaining to financial transactions, account details, and fiscal reports.
    - **Human-Readable vs. Non-Human-Readable**
        - Formats intended for human interpretation (e.g., text documents) versus machine-readable formats (e.g., encrypted files)

- **Data Classification**
    - **Public**
        - Data intended for public dissemination.
    - **Private**
        - Personal information meant to be kept confidential
    - **Sensitive**
        - Data that, if disclosed, could cause harm to individuals or organizations.
    - **Confidential**
        - Information meant to be kept secret within a certain group.
    - **Restricted**
        - Highly sensitive information with strict access controls.
    - **Critical**
        - Data essential to the operation of an organization.

- **General Data Considerations**
    - **Data States**
        - **Data at Rest**
            - Stored data not actively in use.
        - **Data in Transit**
            - Data actively moving between locations.
        - **Data in Use**
            - Data currently being processed.
    - **Data Sovereignty**
        - The concept that data is subject to the laws of the country in which it is located.
    - **Geolocation**
        - The physical location where data is stored or processed.

- **Methods to Secure Data**
    - **Geographic Restrictions**
        - Limiting data access or storage to specific locations to comply with regional laws.
    - **Encryption**
        - Converting data into a coded format to prevent unauthorized access.
    - **Hashing**

        - Transforming data into a fixed-size string of characters, which is typically a digest that represents the data.
    - **Masking**
        - Concealing original data with modified content.
    - **Tokenization**
        - Replacing sensitive data with unique identification symbols that retain essential information without compromising security.
    - **Obfuscation**
        - Making data obscure or unintelligible to unauthorized users.
    - **Segmentation**
        - Diving a network into smaller parts to enhance security.
    - **Permission Restrictions**
        - Implementing access controls to limit data access based on user roles.

Explain the importance of resilience and recovery in security architecture

- **High Availability**
    - **Load Balancing**
        - Distributes incoming network traffic across multiple servers to ensure no single server becomes a bottleneck, enhancing performance and availability
    - **Clustering**
        - Involves connecting multiple servers to work as a single system, providing redundancy and failover capabilities to maintain service continuity during hardware or software failures.

- **Site Considerations**
    - **Hot, Warm and Cold Sites**
        - **Hot Site**
            - A fully operational offsite data center equipped with real-time data replication, allowing immediate takeover in case of a primary site failure.
        - **Warm Site**
            - A partially equipped site with some hardware and data backups, requiring time to become fully operational after a disruption.
        - **Cold Site**
            - A basic facility with infrastructure but no immediate hardware or data, necessitating significant setup time following a disaster.
    - **Geographic Dispersion**
        - Distributing data centers and resources across different geographic locations reduces the risk of a single event impacting all operations, enhancing resilience against regional disasters.

- **Platform Diversity**
    - Employing a variety of hardware and software platforms minimizes the risk that a vulnerability in one system could compromise the entire infrastructure, thereby enhancing security and resilience.

- **Multi-Cloud Systems**

    - Utilizing services from multiple cloud providers prevents dependency on a single vendor, offering redundancy and flexibility, and mitigating risks associated with provider-specific outages or issues.

- **Continuity of Operations**
    - Developing and maintaining a comprehensive plan ensures that essential functions can continue during and after a disaster, outlining procedures for emergency response, backup operations, and post-disaster recovery.

- **Capacity Planning**
    - **People**
        - Ensuring adequate staffing with the necessary skills to manage and maintain systems during normal operations and crises.
    - **Technology**
        - Regularly assessing and upgrading technological resources to meet current and future demands.
    - **Infrastructure**
        - Planning for sufficient infrastructure capacity to handle peak loads and potential failover scenarios.
- **Testing**
    - **Tabletop Exercises**
        - Simulated discussions to evaluate the effectiveness of emergency plans and identify areas for improvement.
    - **Failover Testing**
        - Regularly switching operations to backup systems to ensure they function correctly during an actual failure.
    - **Simulations**
        - Conducting realistic drills to test response capabilities and identify weaknesses in procedures.
    - **Parallel Processing**
        - Running backup systems alongside primary systems to ensure they can handle workloads if needed.

- **Backups**
    - **Onsite/Offsite**
        - Maintaining backups in multiple locations protects against data loss due to site-specific incidents.
    - **Frequency**
        - Regularly scheduled backup ensures data can be restored to a recent state, minimizing loss.
    - **Encryption**
        - Encrypting backup data protects it from unauthorized access.
    - **Snapshots**
        - Capturing the state of a system at a specific point in time allows for quick restoration.
    - **Recovery**
        - Establishing clear procedures for restoring data from backups ensures timely resumption of operations.

    - **Replication**

        - Continuously copying data to secondary locations ensures high availability and quick recovery.
    - **Journaling**
        - Recording changes to data in a log facilitates recovery to a specific point in time, enhancing data integrity.

- **Power**
    - **Generators**
        - Provide backup power during extended outages to keep critical systems operations.
    - **Uninterruptible Power Supply (UPS)**
        - Offers immediate, short-term power to protect against sudden losses and allows for safe systems shutdowns or transition to backup generators.