Built in security function of cloud product

Built-in Security Features:
Many cloud platforms offer built-in security features and tools that can help users secure their applications without needing to develop everything from scratch.

This can include
identity and access management,
encryption,
and monitoring tools.

1. **Shared Responsibility Model**:

In cloud environments, security is often a shared responsibility between the cloud service provider (CSP) and the user.

The CSP typically handles the security of the cloud infrastructure, **while users are responsible for securing their applications and data.**

2. Application Type:
The level of security required can depend on the type of application being deployed.

For example, applications that handle sensitive data (like personal information or financial data) may require more robust security measures compared to less sensitive applications.

3. **Compliance Requirements**:
Depending on the industry and the data being processed, there may be specific compliance requirements (like GDPR, HIPAA, etc.) that necessitate additional security measures.

4. **Development Practices**:

Implementing secure coding practices and regular security assessments can help mitigate risks.

Users should consider integrating security into the development lifecycle (DevSecOps) to ensure that security is a fundamental aspect of application development.

In summary, while users may not need to develop security features for every application from the ground up,

they do need to be proactive about security, leveraging available tools and practices to protect their applications effectively.

What are the security function of cloud system by cloud product

The security functions of major cloud products include various features

tailored to protect data and applications.

1. **AWS** offers encryption for data at rest and in transit, DDoS protection through AWS Shield, and compliance with standards like ISO 27001 and GDPR1.

2. **Azure** provides advanced threat protection via Azure Security Center, encryption for data at rest and in transit, and identity management through Azure Active Directory2.

3. **Google Cloud** includes default encryption for data at rest, tools like Google Cloud Armor for application protection, and compliance with various security standards4.
   These features collectively enhance the security posture of cloud environments across different providers.

Users are responsible for securing their applications and data.

The level of security required can depend on the type of application being deployed.

For example, applications that handle sensitive data (like personal information or financial data) may require more robust security measures compared to less sensitive applications