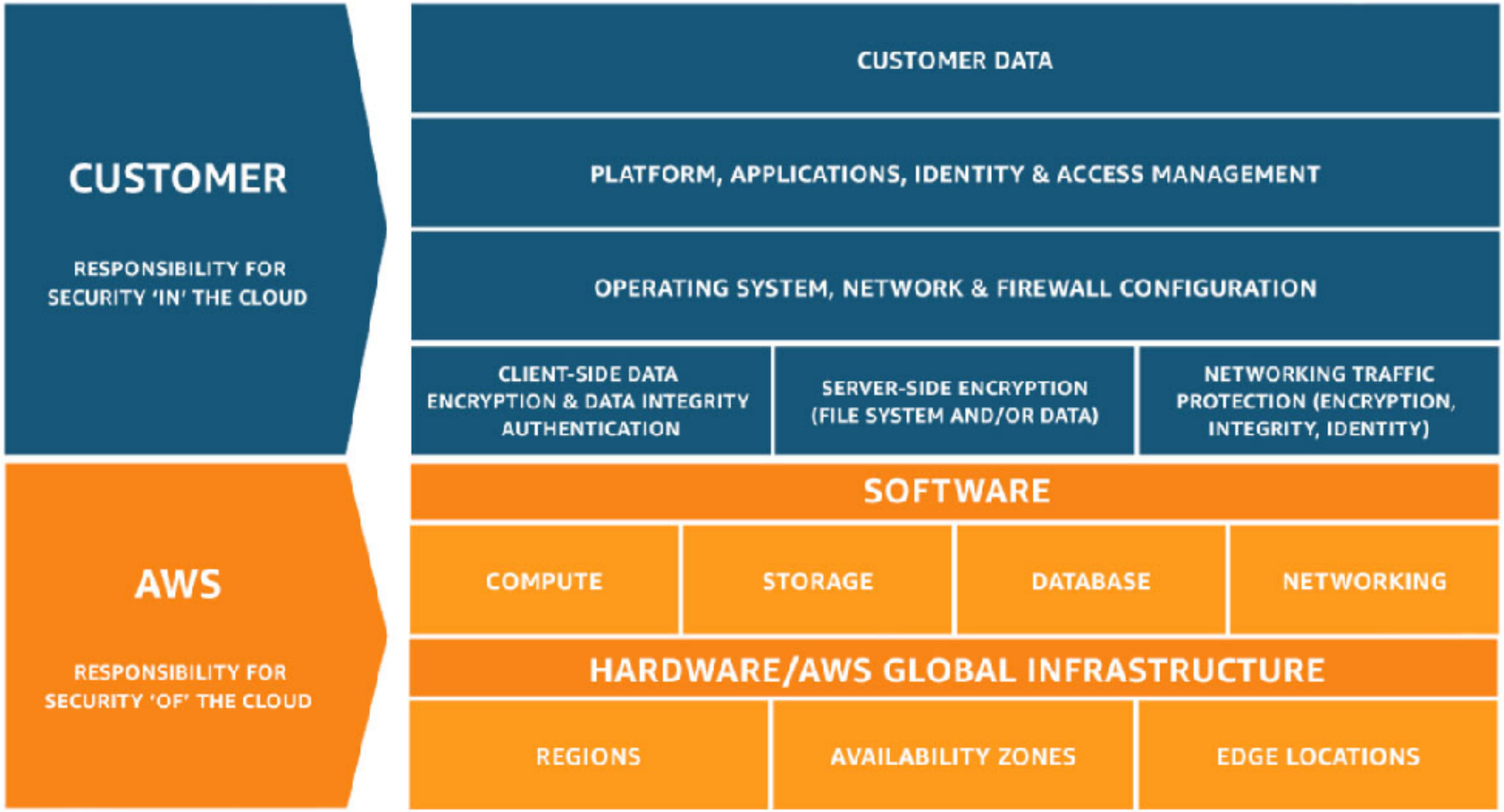
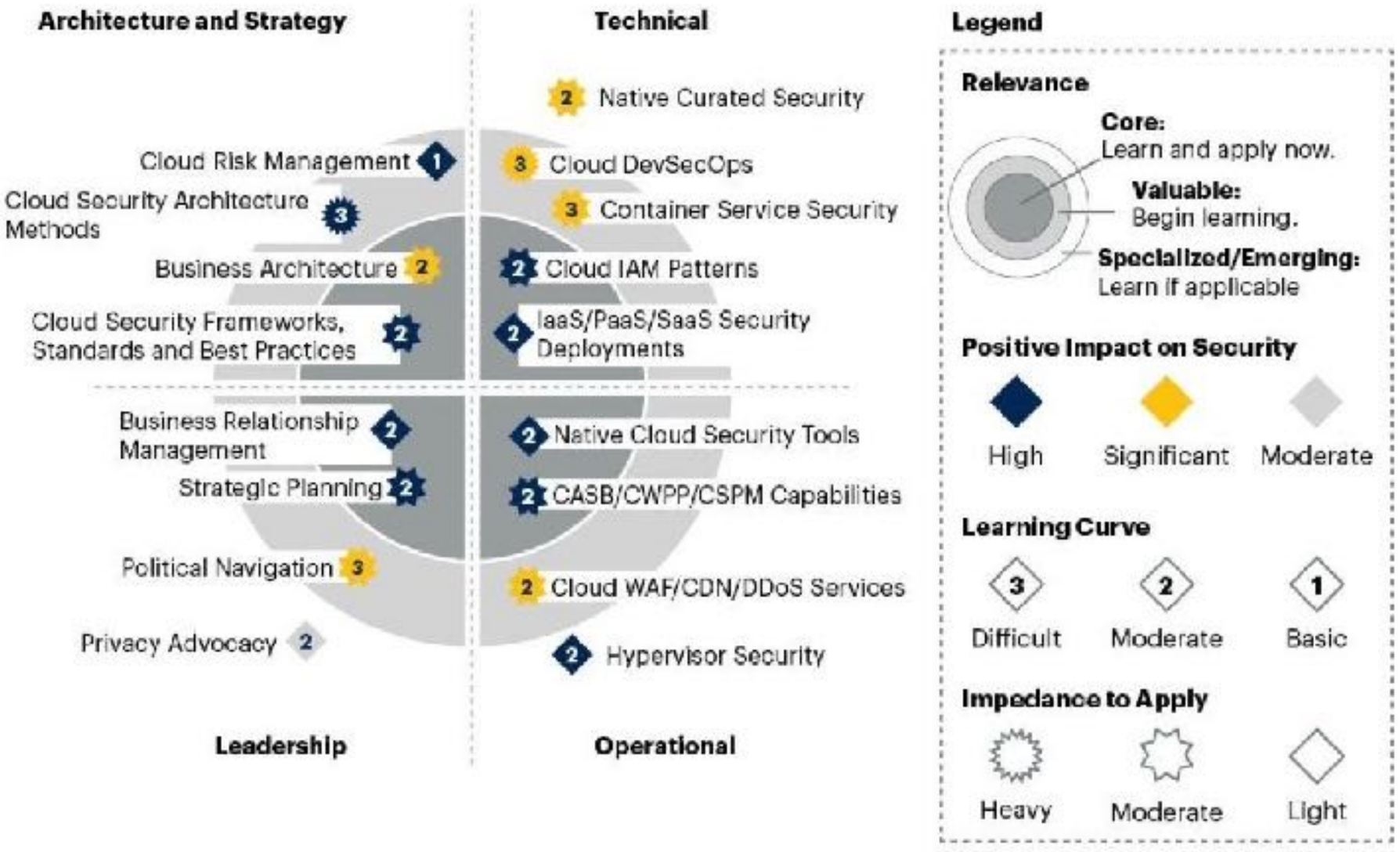
Cloud Security
&
Well Architected Framework

leila.sharifi@gmail.com

Shared Responsibility Model



Cloud Security Architecture



Source: Gartner

Gartner

Conduct a risk assessment and a security audit

- This involves identifying and evaluating the potential risks and threats that may affect the cloud infrastructure and data, as well as the current security posture and gaps. It also involves conducting a security audit to verify and validate the compliance and effectiveness of the security controls and measures in place.

Choose a reputable and trustworthy cloud service provider

- This involves selecting a cloud service provider that has a proven track record and reputation for providing secure and reliable cloud services. It also involves checking the security certifications, accreditations, and guarantees of the cloud service provider, such as ISO 27001, SOC 2, PCI DSS, etc.

Implement backup and recovery plans

- This involves creating and maintaining backup copies of the data and applications in the cloud, as well as having a recovery plan in case of data loss or breach. It also involves testing and updating the backup and recovery plans regularly to ensure their functionality and efficiency.

Educate and train the users and staff

- This involves providing adequate education and training to the users and staff who access or manage the cloud resources, on the security policies, procedures, and best practices. It also involves raising awareness and promoting a security culture among the users and staff to prevent human errors or negligence that may compromise cloud security.

Update and patch the systems and software

- This involves keeping the systems and software in the cloud network up to date and patched with the latest security updates and fixes. It also involves removing or disabling any unnecessary or outdated systems or software that may pose a security risk.

Secret Manager

- Refers to different services or tools that help you store and manage sensitive data such as passwords, API keys, certificates, and tokens.

References

- You can find more examples from various sources, such as Cloud Security Alliance (CSA), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), etc.

Well-Architected Framework

- Operational Excellence
- Security
- Reliability
- Performance Efficiency
- Cost Optimisation
- Sustainability

Operational Excellence

- Perform operations as code
- Make frequent, small, reversible changes
- Refine operations procedures frequently
- Anticipate failure
- Learn from all operational failuresSecurity

Security

- Implement a strong identity foundation
- Maintain traceability
- Apply security at all layers
- Automate security best practices
- Protect data in transit and at rest
- Keep people away from data
- Prepare for security events

Reliability

- Automatically recover from failure:
- Test recovery procedures
- Scale horizontally to increase aggregate workload availability
- Stop guessing capacity
- Manage change through automation

Performance Efficiency

- Democratize advanced technologies
- Go global in minutes
- Use serverless architectures
- Experiment more often
- Consider mechanical sympathy

Cost Optimisation

- Implement Cloud Financial Management
- Adopt a consumption model
- Measure overall efficiency
- Stop spending money on undifferentiated heavy lifting
- Analyze and attribute expenditure:

Sustainability

- Understand your impact:
- Establish sustainability goals:
  - Maximize utilization
  - Anticipate and adopt new, more efficient hardware and software offerings
  - Use managed services
  - Reduce the downstream impact of your cloud workloads