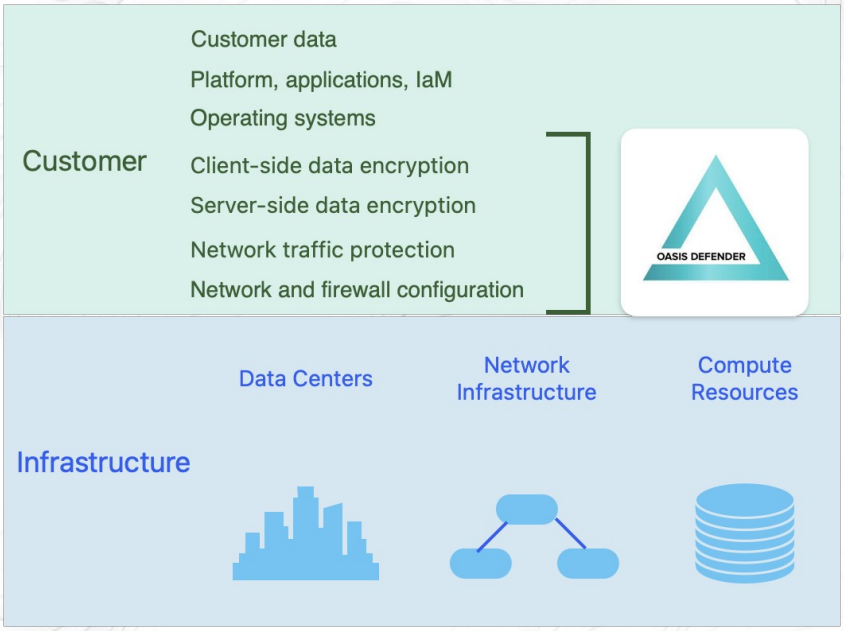
Oasis Defender's place in the AWS Shared Responsibility Model

In accordance with the AWS Shared Responsibility Model, the customer among other things is responsible for [1]:

1. Client-side data encryption;
2. Server-side data encryption;
3. Network traffic protection;
4. Network and firewall configuration.



Oasis Defender helps with these tasks in the following ways [*]:

a) For 1, 2, and 3:

- It ensures that only secure protocols are allowed and only encrypted traffic is transmitted.

b) For 2:

- It ensures that the encryption of the server data is enabled.
- It ensures that security rules are enabled for access to server data.

c) For 3:

- It proactively scans traffic for known attack patterns (signature analysis).
- It creates a traffic profile using AI learning and monitors for deviations from the profile to detect unknown attacks or indicators of compromise (behavioural analysis).

d) For 4:

- It automatically generates a consistent set of firewall rules and applies them to each instance.
- It monitors for changes in a cloud environment to ensure rule consistency throughout the cloud lifecycle.
- It automatically adapts rules to changes in the multi-cloud network, preserving the security policy and maintaining the secure state of the entire multi-cloud.

[1] AWS Cloud Practitioner Essentials, Module 6: Security, AWS Shared Responsibility Model
(*) Some features are under development