beacon

Communications security in a Beacon Platform domain

All external communications traffic to a Beacon Platform domain is always encrypted. For software developed by Beacon, outgoing traffic from a Beacon Platform domain uses encryption where possible.[1]

Where reasonable and practicable, communication traffic within a Beacon Platform domain employs encryption. For example, communication with credentials management or object database is always encrypted. Internally, a Beacon Platform domain is built up of several products and services, many with their own communication protocols. For some of these, such as in-domain log delivery and application telemetry, encryption would add undesirable complexity[2]; for some, adding encryption in transit is not feasible due to performance overheads and/or other contributing factors.[3]

Server-to-server traffic within a Beacon Platform domain is considered trusted. Service-to-service communication is partially trusted, and typically requires authentication.

Beacon controls the network traffic to and from instances within a Beacon Platform domain via the use of cloud provider Security Groups. Beacon strongly recommends that clients refrain from deploying non-Beacon resources within the virtual network and/or VPC used by their domain. If such resources are deployed, their interoperability with the domain is not guaranteed: instances brought up in the same network but as not part of Beacon Platform are not able to communicate with the platform servers.d

---

[1] Eg. outgoing emails generated by the Platform use opportunistic encryption for the transport. This allows the recipient to decline encrypted transport, which in turn will force a fallback to plaintext.
[2] Logs and application telemetry are used for detecting and triaging problems, including encryption related errors. A failure in encryption settings must not prevent such information from being collected or transmitted.
[3] Eg. NFS is a standard Beacon Platform feature, and is unencrypted. While adding encryption to NFS is technically possible, the addition typically requires a separate account management system, and introduces a performance overhead.