# Security HW Assist

PR #3319

---

Next (from 25Jan RM call): Rewrite as guidance with recommendations on what to do to get the advantages.

Text WIP before creating PR:

**Chapter 7 (after Platform Access, before Workload Security)**

**Security HW Assist for Data in Use**

Server hardware architectures offer various technologies to assists protecting data in use. From enablement point of view, those technology approaches can be divided into two categories:

- Those exposed as node labels on virtualized software infrastructure, when scheduling can be influenced by those labels:
  - Memory encryption on level of physical server
  - Memory encryption on level of VMs: Where hypervisor manages encryption keys.
- That also requires application modification, and while scheduling the application mapping of HW-support to the application:
  - Secure enclaves within application: To isolate specific application code and data in memory, which are designed to be protected from processes running at higher privilege levels like OS and hypervisor.