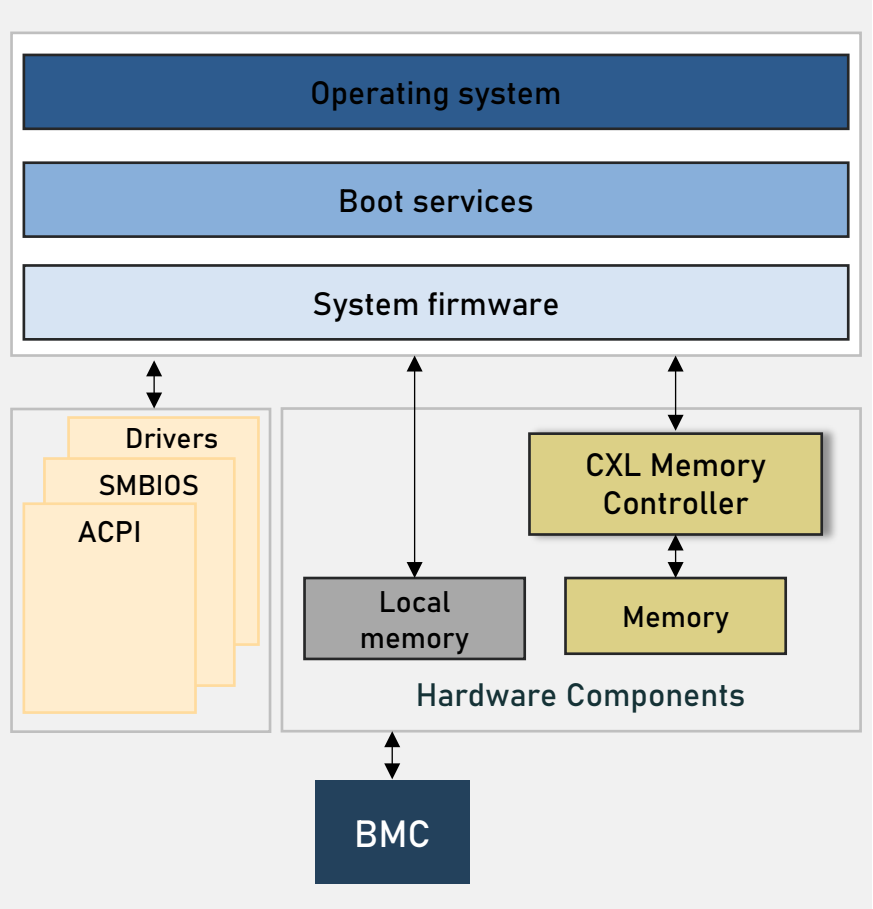
Importance of Pre-boot Process for CXL Type 3 Devices

Presented by Astera Labs for CXL Consortium

August 2024

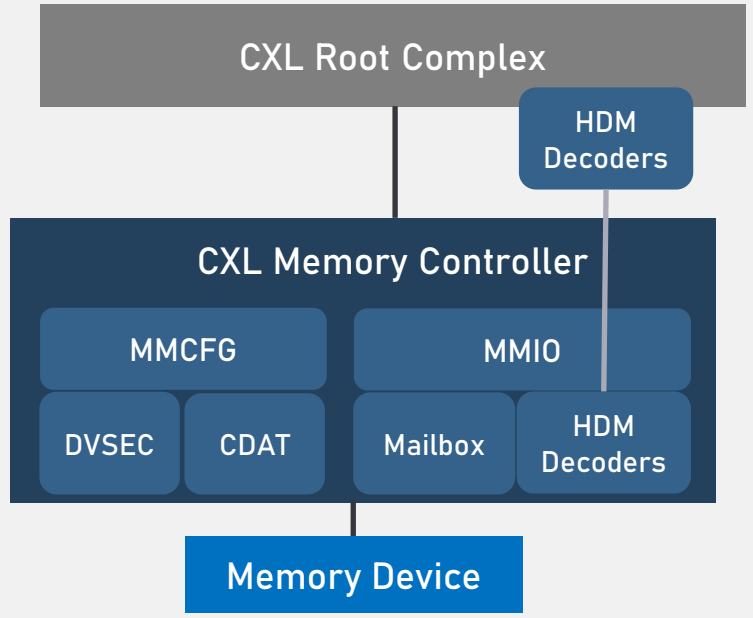
Data Center Server Boot Requirements

- Data center server boot requirements:
  1. Standard-based initialization & configuration routines
  2. RAS testing of device and attached memory
  3. Enable end-to-end security
  4. Enable & configure fleet management capabilities
- Objective
  - CXL Type-3 devices need to conform to above requirements
- Benefits
  - Consistency in operation b/w local and CXL-based memory
  - Lower development time/cost due to std-based methods
  - TCO savings due to high levels of platform reliability



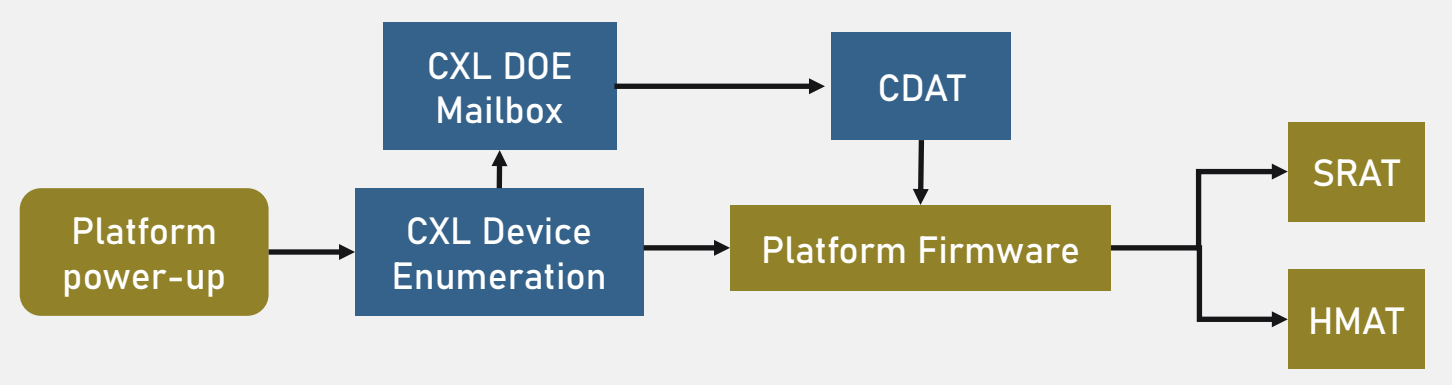
CXL Type-3 Device Initialization

- CXL memory controller initialization
  - PCIe standard defined device mapping mechanisms
    - MMCFG, MMIO, DOE
  - CXL standard mechanism for setting up capabilities, address & capacity
    - Programming HDM decoders, DVSEC & CDAT
    - Set up mailboxes and CXL CCI interface for management
- Memory initialization per JEDEC standard
  - Power-up and initialization
  - Calibration – ZQ, Vref, etc.
  - Read/Write Training



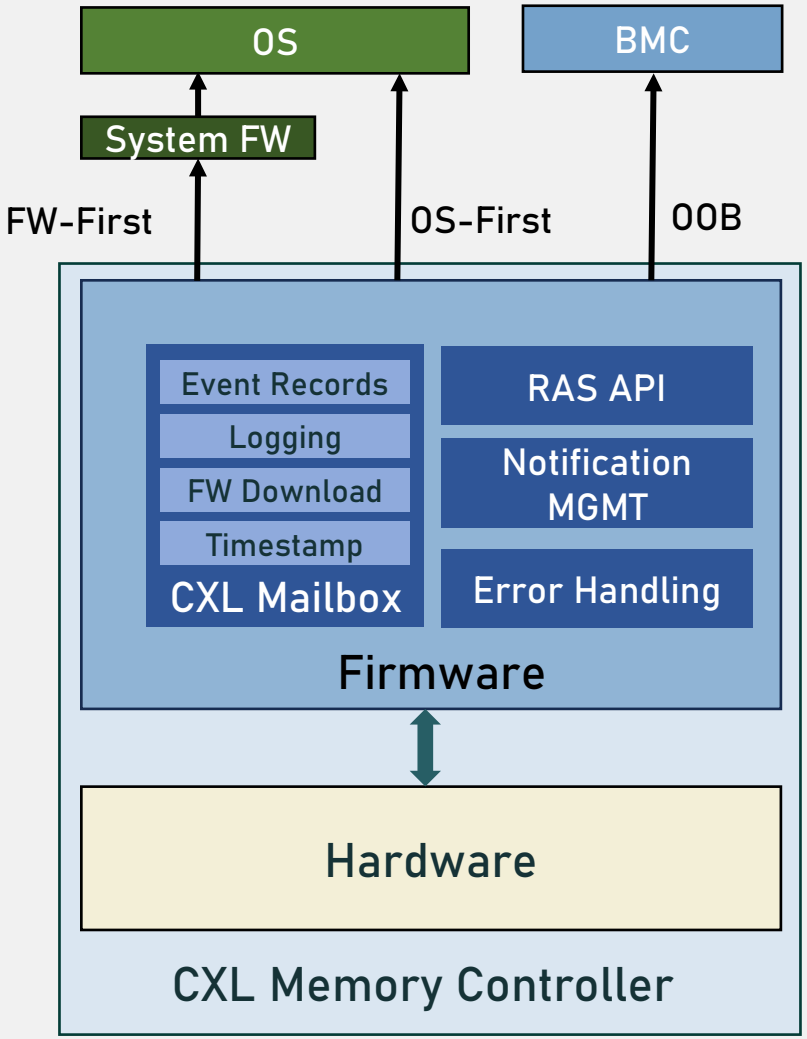
Topology Information During Initialization

- CXL Coherent Device Attribute Table (CDAT) communication
  - System firmware discovers the device performance characteristics at boot time via CDAT
    - Describes the memory & performance characteristics of attached CXL memory controller
    - Information used for construction of SRAT and HMAT ACPI tables
  - Structure includes:
    - Memory size
    - Interleaving scheme
    - Performance characteristics: rd/wr latency, bandwidth



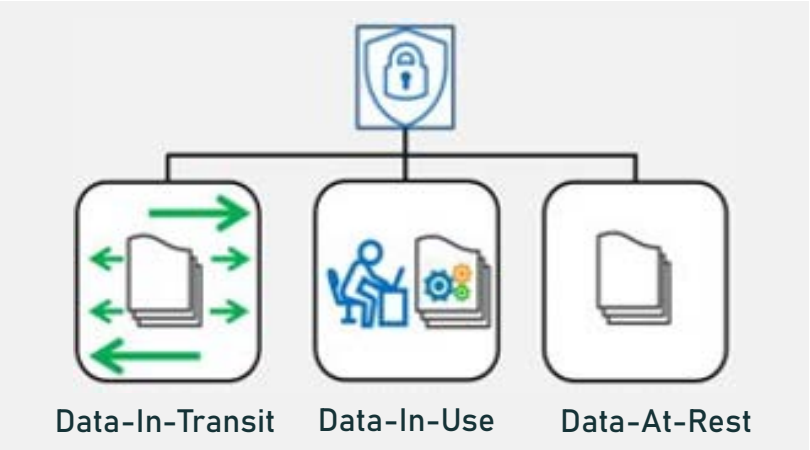
RAS Initialization & Testing

- Configure in-band & out-of-band RAS communication
  - Initialization of CXL mailbox for notification & management
- Pre-boot RAS tests based on PCIe and JEDEC std.
  - Lane margining
  - Link stability → Eye diagram, FOM, Link EQ, etc.
  - Memory testing & repair → MBIST, SDDC, scrub, PPR, etc.
  - Error injection → Data poison & viral injection & detection
  - System firmware event notification → FW-first
- Enablement of OS/Hypervisor communication
  - Error handling
  - Event notification via mailboxes → OS-first
  - Logging

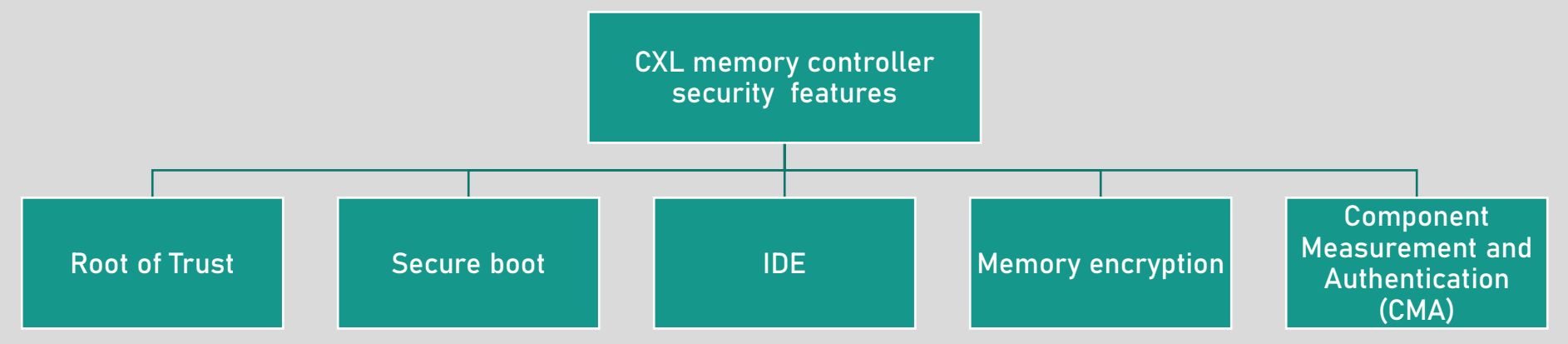


CXL Security Enablement

Security enablement during platform initialization for protecting data-in-transit, data-in-use and data-at-rest

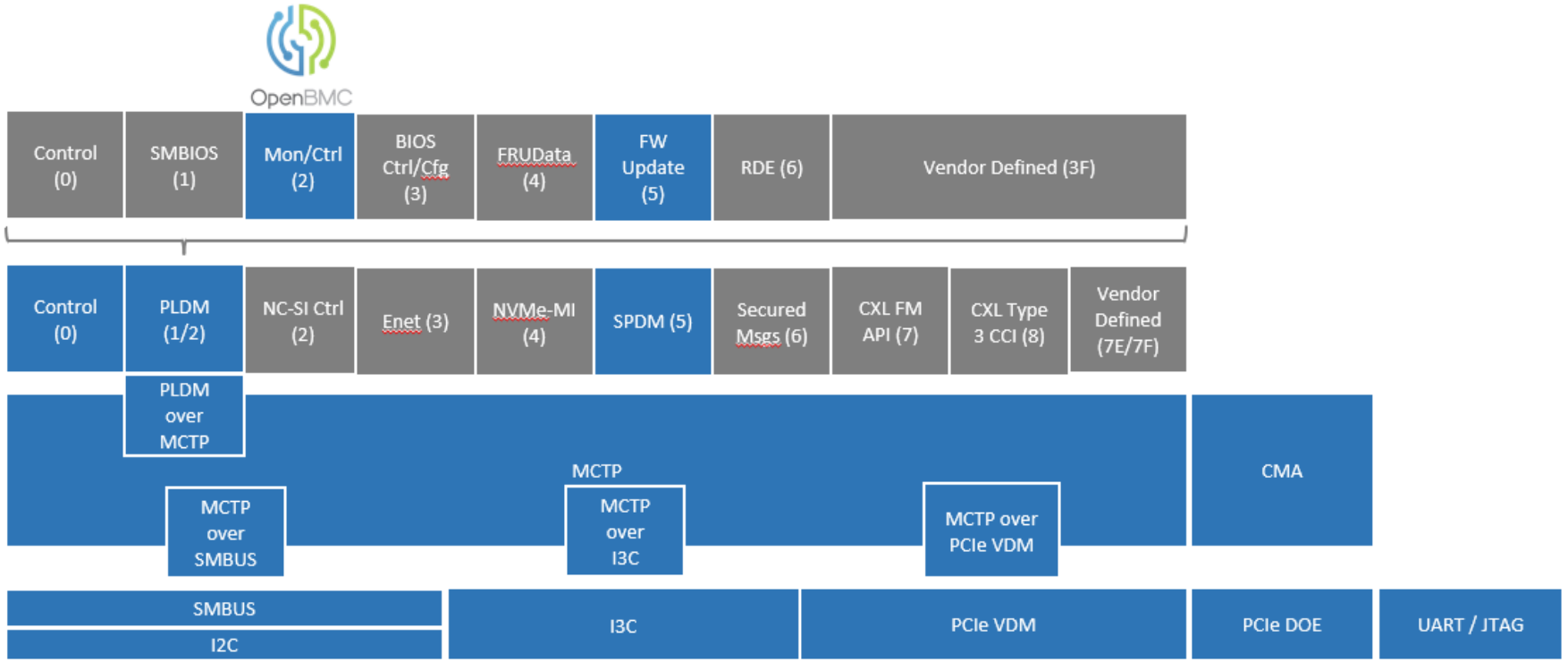


End-to-end platform protection with leading security standard features



Fleet Management Setup

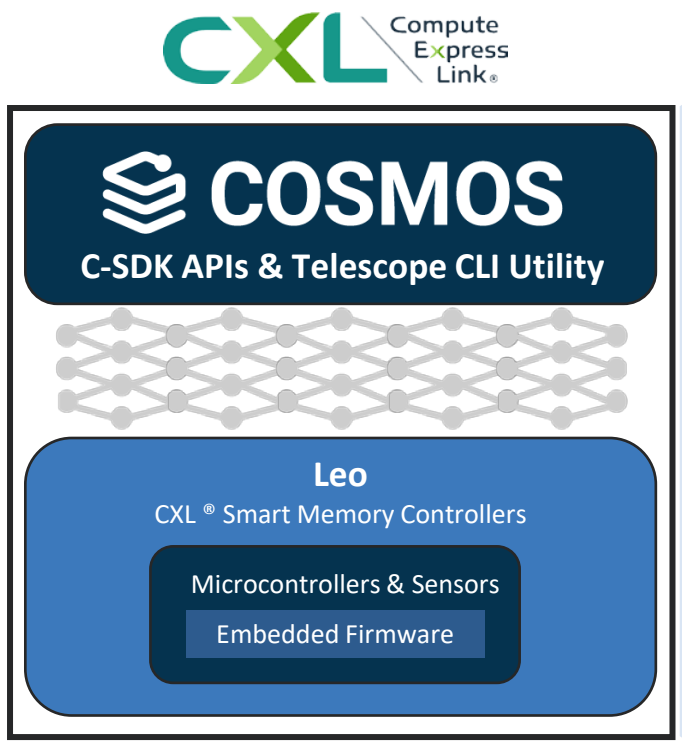
- Configure DMTF defined protocols → MCTP, PLDM, SPDM, etc.
- RAS API framework setup for management functionality



Data Source: OCP – BMC Requirements for Internal Component Communications

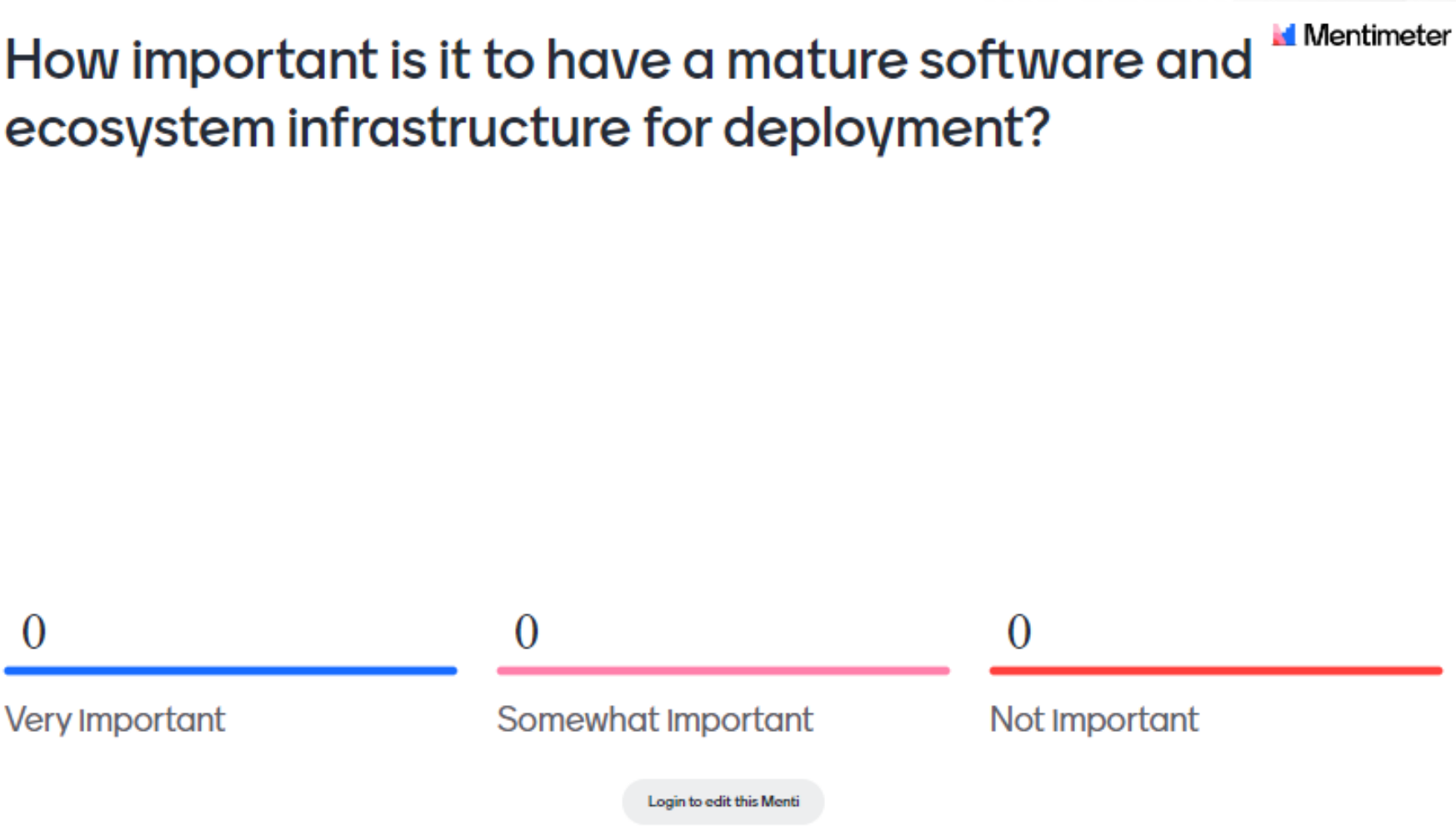
Technology Example

Astera Labs Leo CXL Smart Memory Controller



Standard-based Initialization & Configuration routines
• Supports all system firmware requirements • SW APIs for seamless integration into pre-boot routines • Feature parity between local and CXL attached memory • CXL / PCIe specification defined process • JEDEC defined Memory initialization & training
Reliability, Availability, Serviceability (RAS)
• Device & memory testing • Advanced ECC detection and correction • Error injection, repair & notification • TCO savings due to overall system robustness
Fleet Management
• Support for DMTF protocols – MCTP, SPDM, PLDM, etc. • Management via Inband and Out-Of-Band • Performance & temperature monitoring • Platform customization and configuration • Support for UEFI framework
Comprehensive Security Features
• Supports leading security standards such as OCP, NIST, CXL-IDE etc. • End-to-end protection of data-in-transit, data-in-use and data-at-rest • Immutable RoT and secure boot mechanisms • CXL 2.0 Integrity and Data Encryption (IDE) features • Memory Encryption to protect data-at-rest in off-chip memory devices

Audience Question



Thank You