SEQUITUR LABS

Securing Smart Devices:

Protecting AI at the Edge

SEQUITUR LABS | Securing the Connected World

Chip-to-Cloud Security Solutions for the Network Edge

Sequitur Labs Security Platform

Software, Cloud Services and Ecosystem

EmSPARK™

EmSPARK™ Security Suite

Device Security Software

EmPower™

EmPower™ Security SAAS

Trust as a Service

Top Markets

Industrial Automation | Machine Vision | Building Automation | Smart Home | Intelligent Video Analytics

Customers

Johnson Controls | boundary | Fairmount Automation

Silicon Platforms

Premier Microchip Third-Party Partner | Registered Partner NXP | NVIDIA Preferred Partner | ST life.augmented

Today's Webinar

- Edge Device Security & AI at the Edge - Overview
- Device Security Basics: Secure Boot, Firmware Updates, Failure Recovery, and Cloud Integration
- Methods for Protecting AI at the Edge
- AI at the Edge: Demo
- Resources
- Q&A

Problem: IoT Devices are at HIGH SECURITY RISK

- ***75B*** connected devices by 2025
- ***48%*** of firms experienced an IoT security breach at least once
- Cost of an IoT Breach can exceed ***10%*** of revenues
- AI at the Edge Increases IP exposure
  - **75%** of all data will be generated at the Edge

Sources: Researchgate, Poneman Institute, Altman Vilandrie & Company, Gartner

Why Isn't the IoT Secure?

- Specialized skills
- Steep learning curve
- Fragmented silicon and software options
- Time-to-market pressure

ZDNet

THURSDAY, MARCH, 18, 2021

Your insecure Internet of Things are putting everyone at risk for an attack

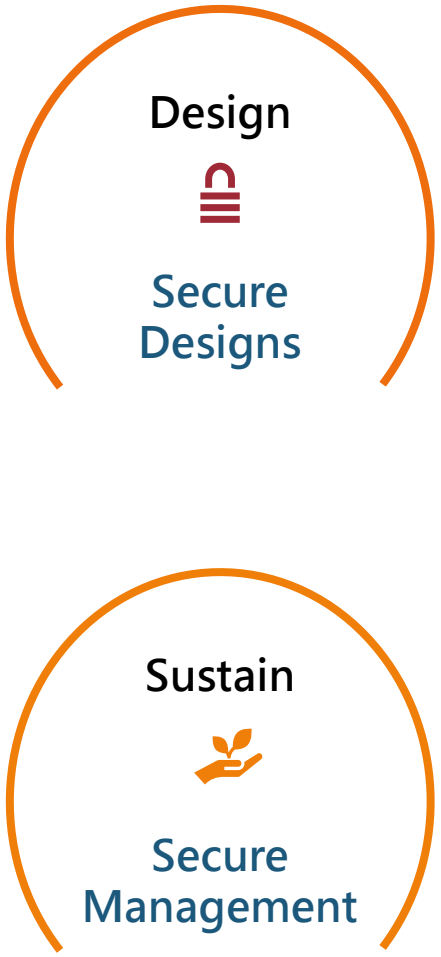
IoT devices are becoming more and more popular but many of the products people are installing don't come with adequate security—and that's something cyber criminals can take advantage of.

ZDNet

TUESDAY, APRIL, 13, 2021

These new vulnerabilities put millions of IoT devices at risk, so patch now

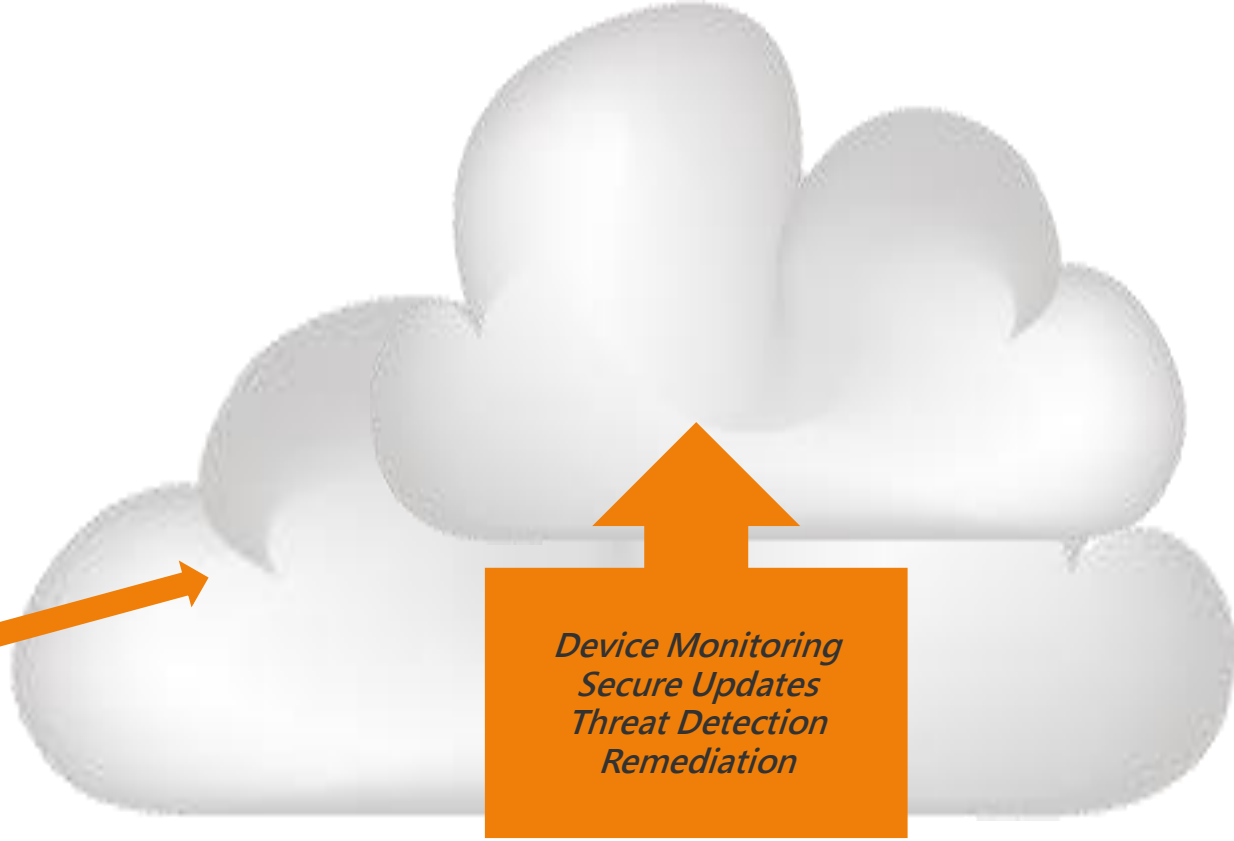
Edge Device Security - from Design to End-of-Life



- Implement a solution comprising a strong device security framework ensuring end-to-end, chip-to-cloud trust.
- This solution must:
  - Simplify security deployment
  - Work across a fragmented silicon landscape
  - Enable secure manageability
  - Provide a trust anchor for cloud services

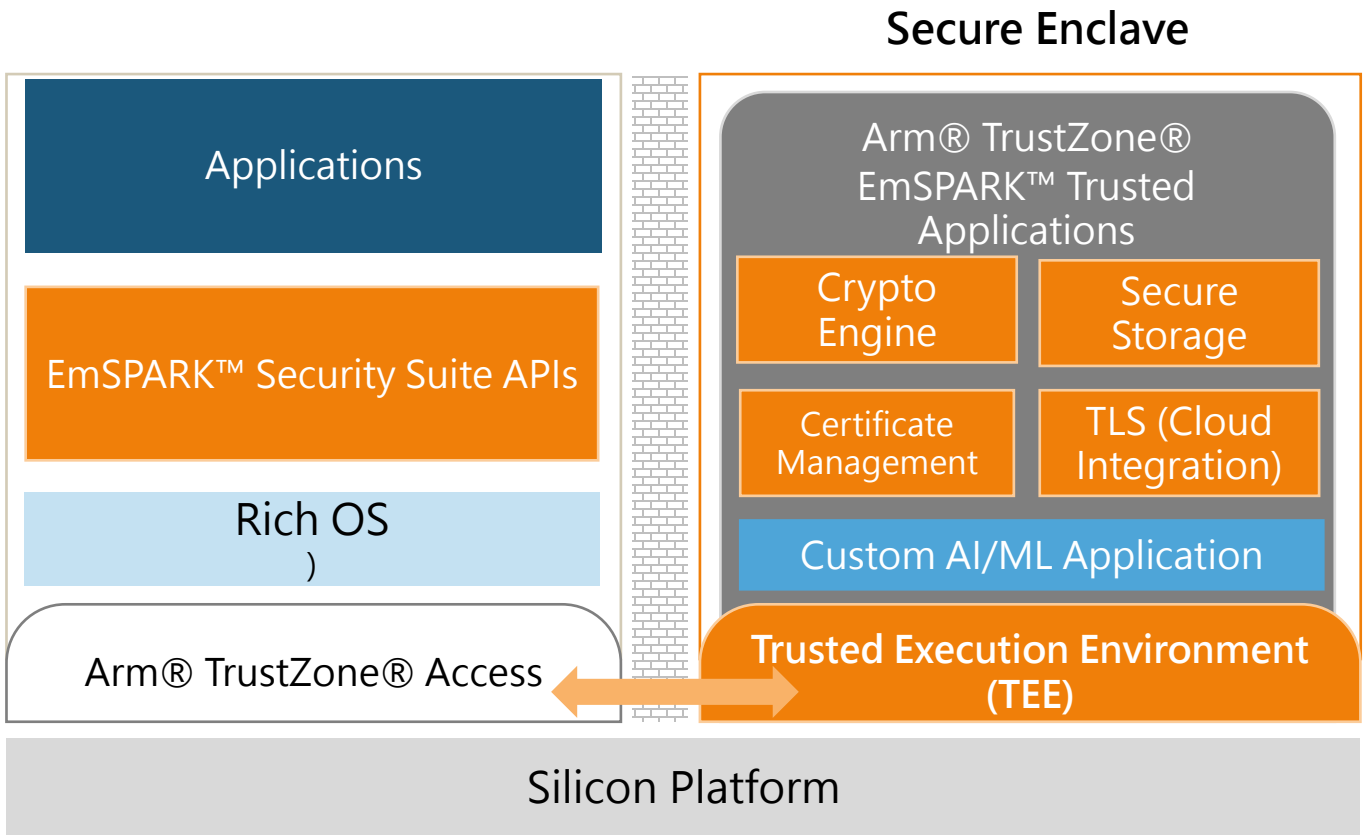
Edge Device Security End-to-End

- Device security using ARM TrustZone®
- Secure Cloud Integration
- Cloud Services for management and updates
- Consistent implementation across silicon platforms



Secure Boot
Failure Recovery
Key & Certificate Mgmt
Software Provisioning
AI Model Protection

Understanding ARM TrustZone®



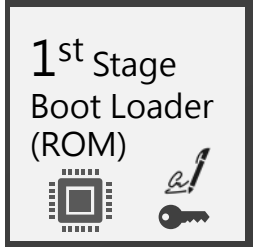
Pre-packaged Security

Anti-Piracy	+ Protect critical IP (ex. AI/MP algorithms) at the edge
Firmware Update	+ Authenticated, encrypted single API call for secure OTA update
Cloud Integration	+ MQTT based cloud connectivity with TLS
Secure Boot	+ Application authentication, memory isolation, payload encryption/decryption
Secure Storage	+ Protection for files and data streams
Failure Recovery	+ Authenticated, encrypted single API call for secure update
Software Provisioning	+ Diversified device IDs, secure manufacturing facility not required

Secure Boot

Step 1: ROM Boot Loader

- Boot is initiated by Read-Only Memory (ROM)
  - Enabled by hardware (Fuses and Pins)

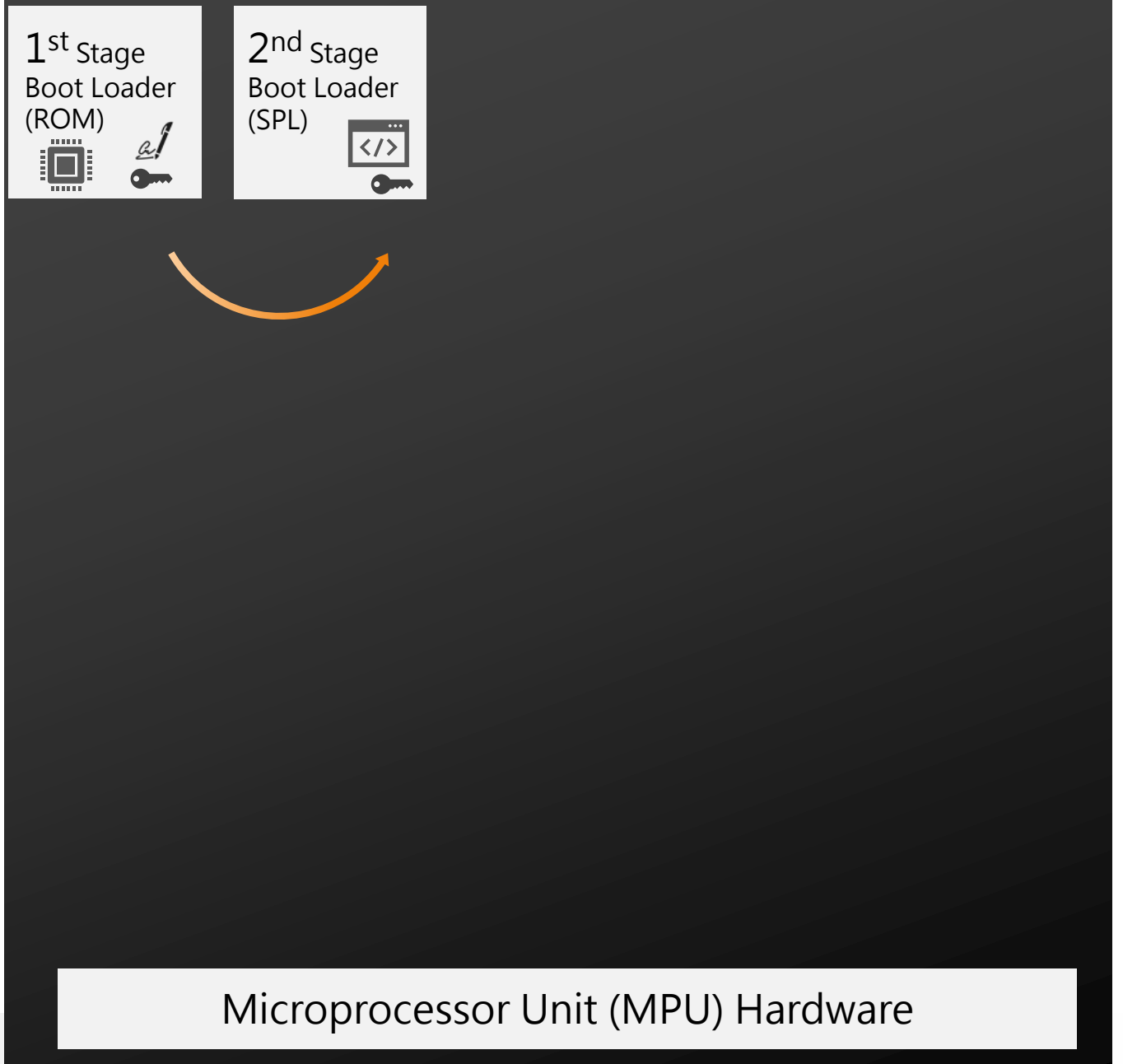


Microprocessor Unit (MPU) Hardware

Secure Boot

Step 2: Secondary Program Loader (SPL)

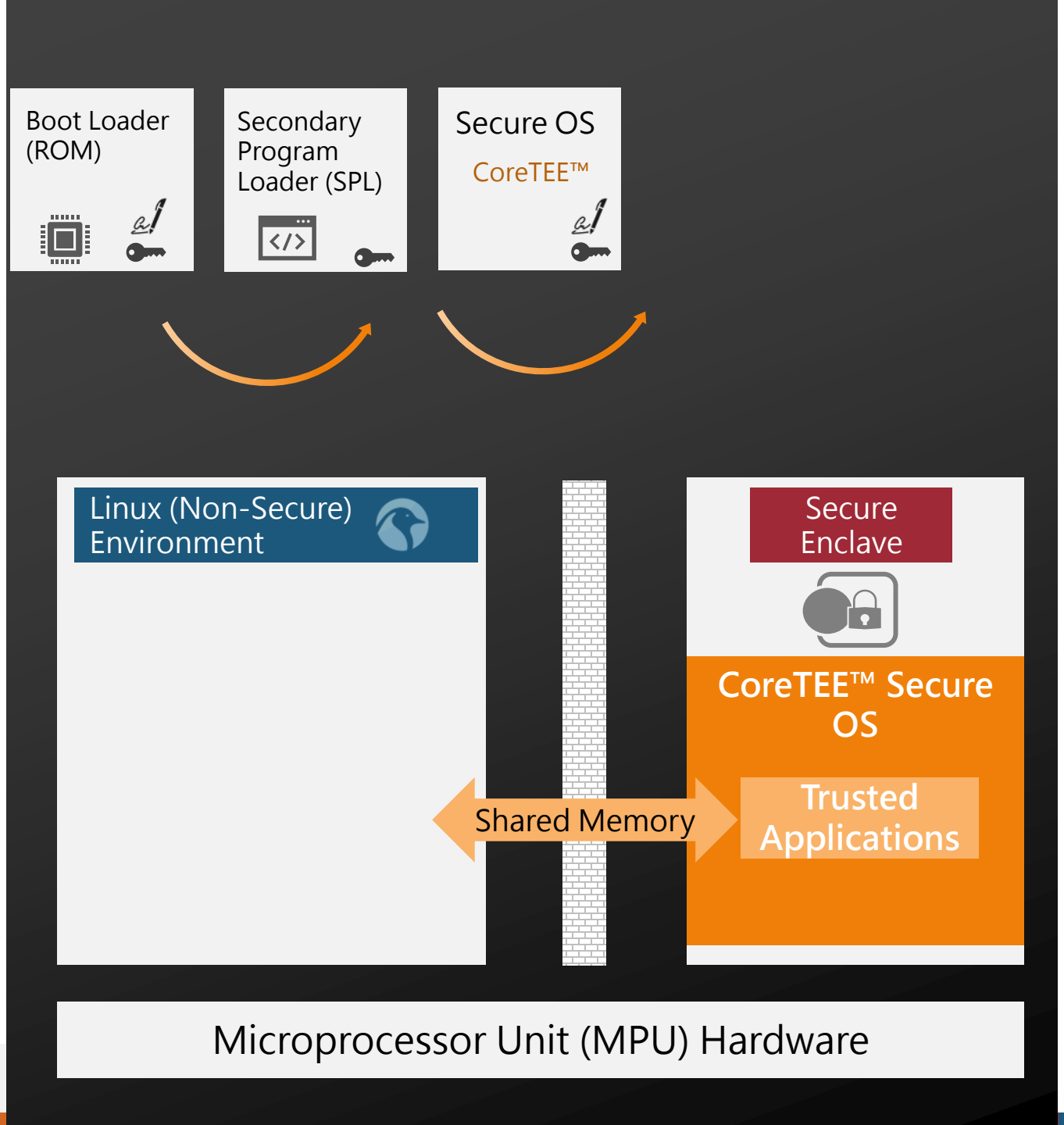
- ROM Loads the first software – Secondary Program Loader (SPL)
  - Loaded from Flash Memory (NVM) to Random Access Memory (RAM)
  - Signature is verified using a cryptographic key
  - ROM verifies key by comparing it to value set in fuses
- After verification, software is loaded and process of decrypting and locating OS and Application software begins



Secure Boot

Step 3: Memory Isolation, Secure Environment (TEE) Establishment

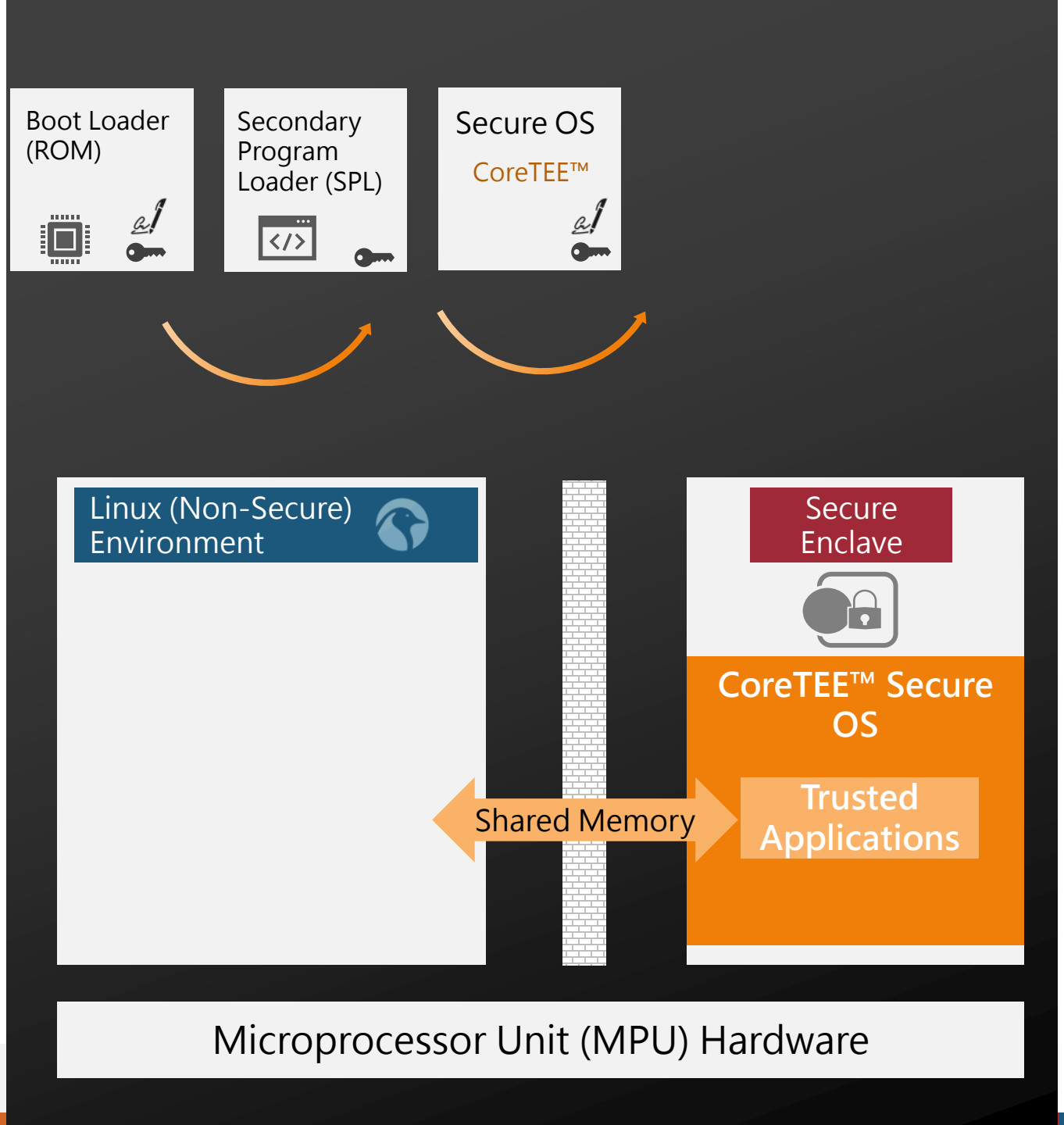
- Secondary Program Loader Separates RAM into two partitions
  - Secure Environment (secure Enclave)
  - Rich-Environment (Non-Secure)
- Secure OS software is verified, decrypted and loaded



Secure Boot

Step 3: Memory Isolation, Secure Environment (TEE) Establishment

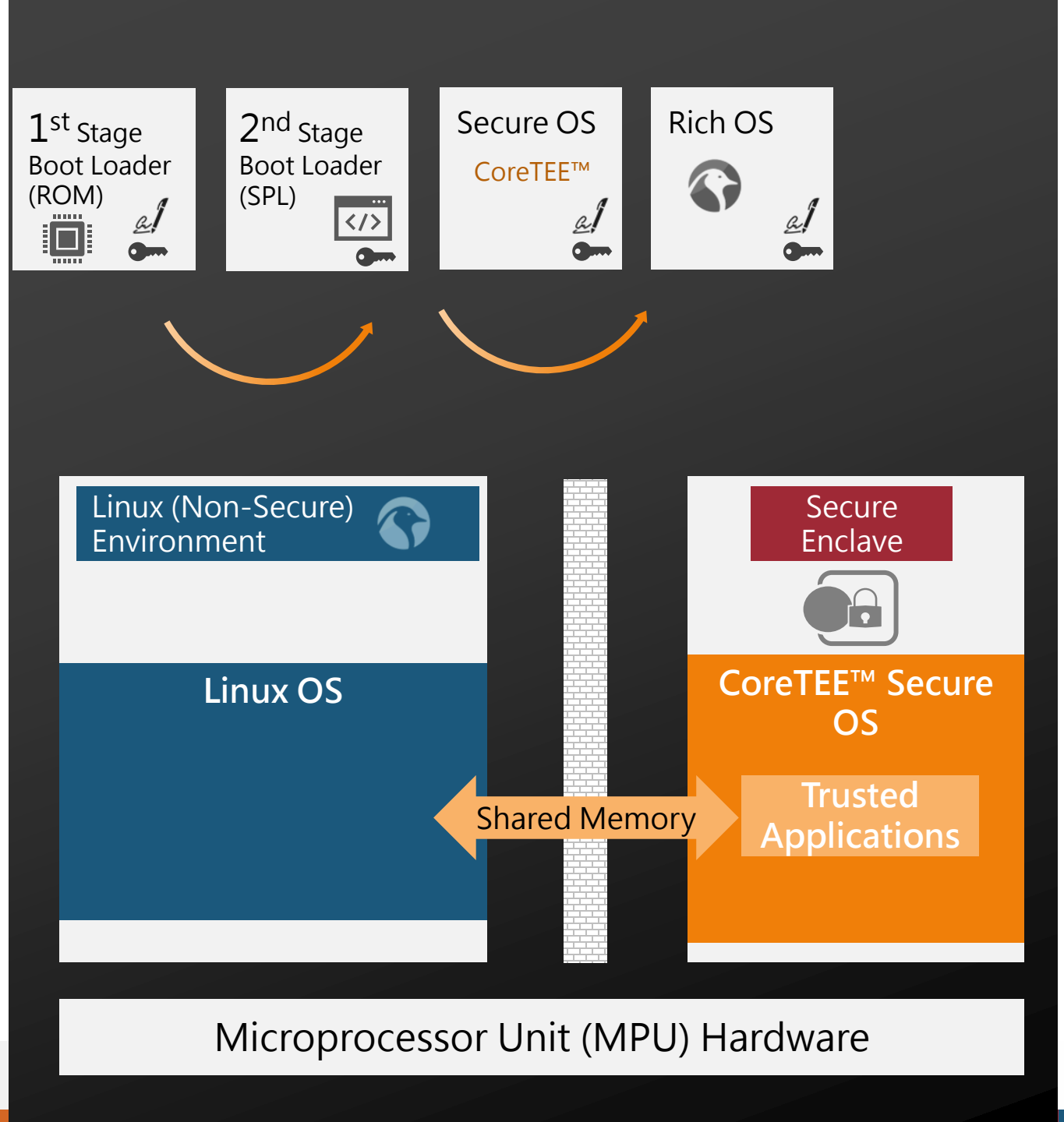
- Secure OS – called the Trusted Execution Environment (TEE), is set up
  - EmSPARK™ CoreTEE™ Secure OS supports this
- CoreTEE™ loads Keys and Certificates for use by Trusted Applications



Secure Boot

Step 4: Establish Rich (Non-Secure) Environment

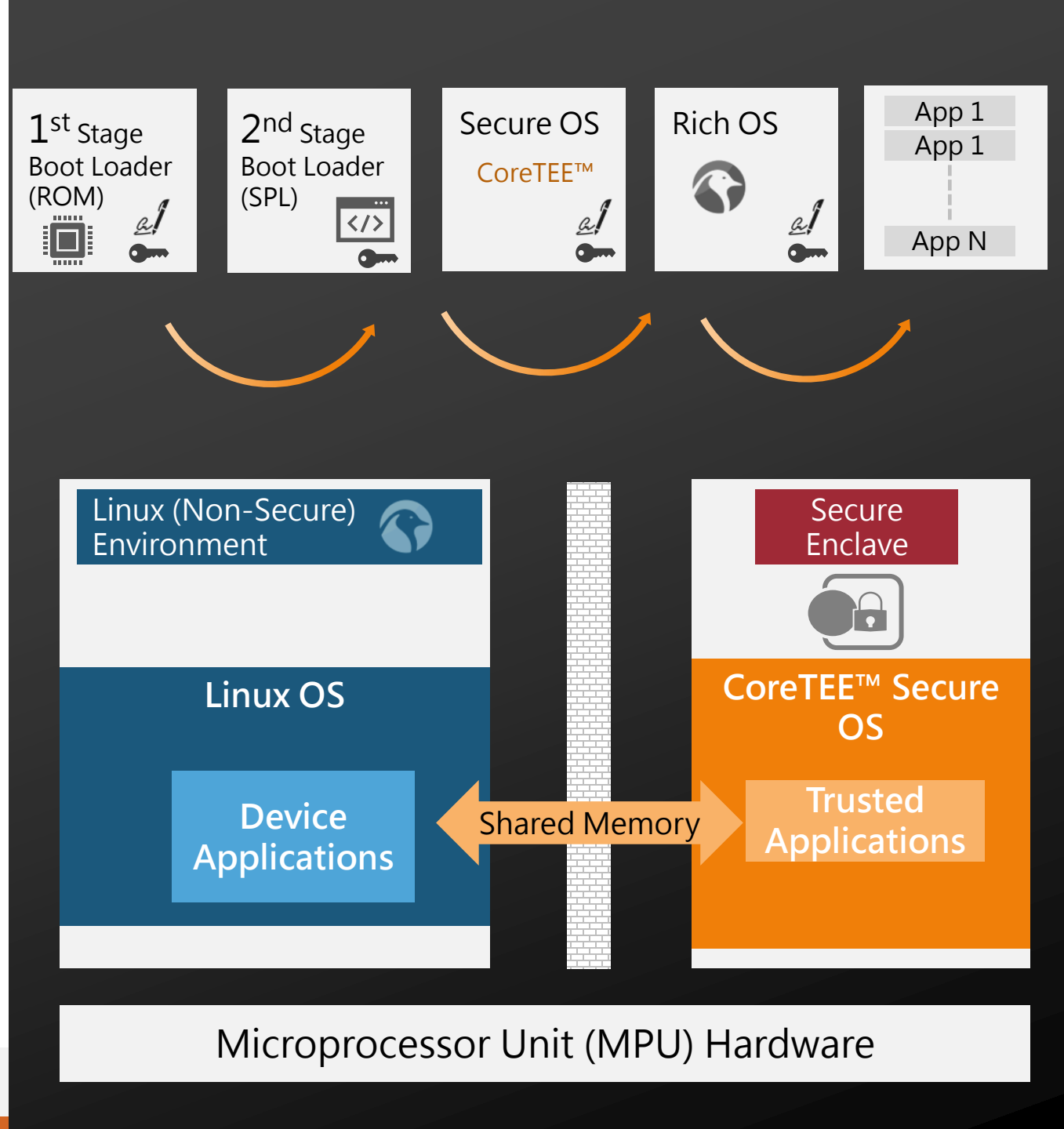
- CoreTEE™ passes control to Secondary Program Loader (SPL)
- SPL sets up the Rich (Non-Secure) environment OS (ex. Linux)



Secure Boot

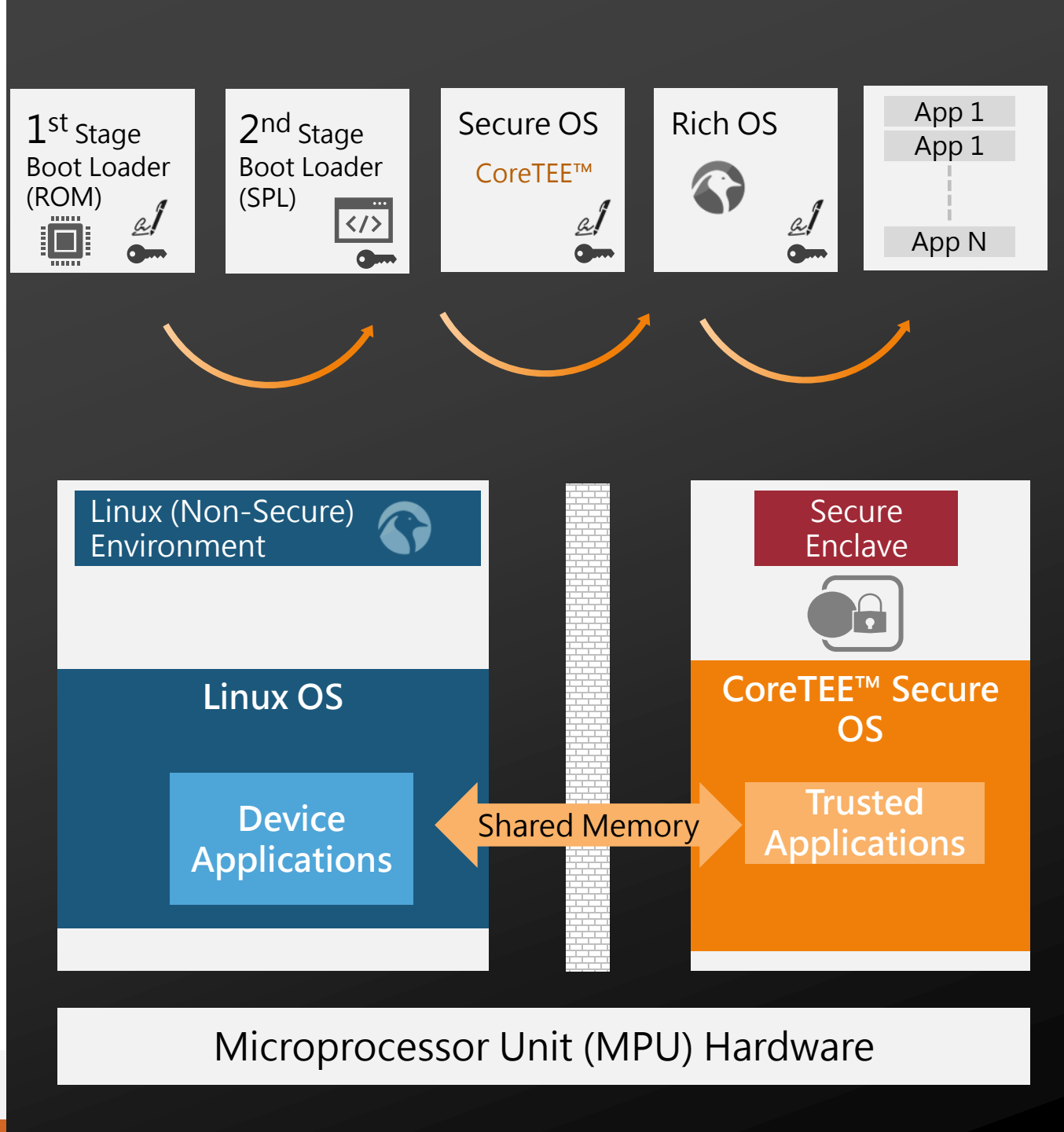
Step 5: Load Device Applications

- Rich OS (ex. Linux) sets up device applications
- Applications are loaded and decrypted



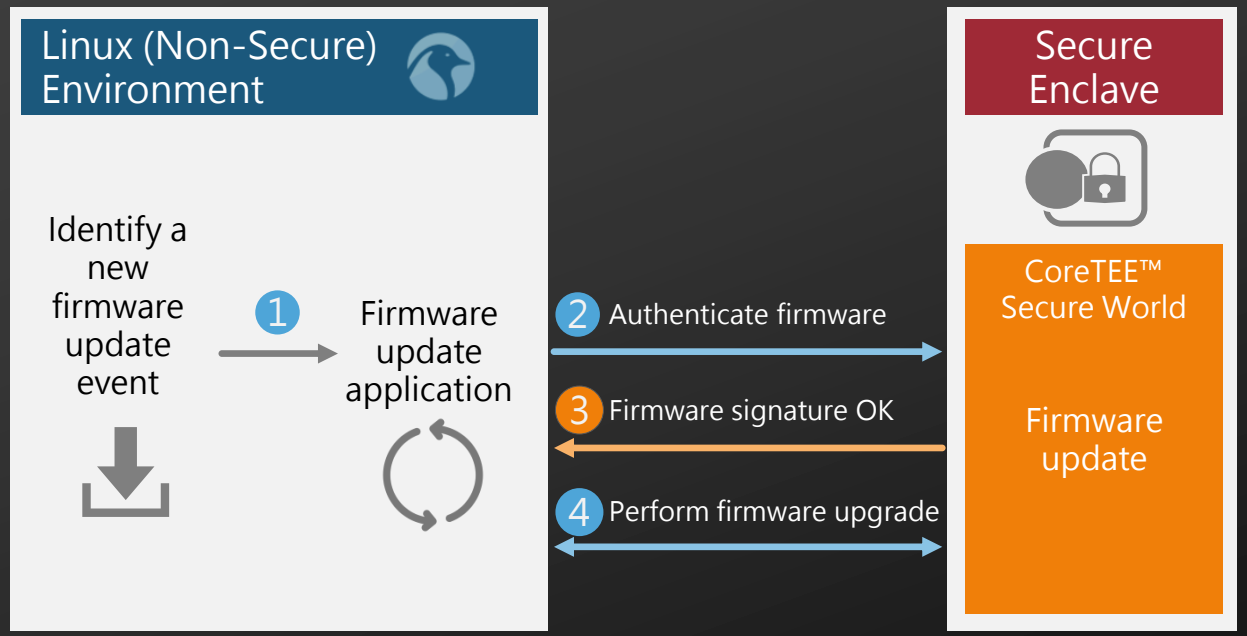
Secure Boot - Summary

- Provides authentication and protection for all applications and functions in the boot process
- Isolates critical security resources
  - Memory addresses reserved for rich OS (Linux) and secure OS (Trusted Execution Environment)
  - Shared memory for coordination between OS
- Verifies fidelity of firmware
- Encrypts/Decrypts boot payloads
- Creates Unique Device ID, Tied to Hardware Root of Trust (RoT)



Secure Over-the-Air (OTA) Firmware Updates

- Risk of compromise is HIGH during the update process!
  - Incoming payloads need to be authenticated
- Critical functions
  - Key and certificate-based payload authentication
  - Coordination with Linux encrypting file system
  - Location for storing update payloads
  - Customizable enforcement of rollback prevention
  - Generation, signing, and encrypting of a new firmware image



Secure Over-the-Air Updates - Example

Device sends periodic/event-driven status messages
To Cloud Server

Cloud Server provides update details (ex. Location)

Device retieves update and authenticates firmware

Device performs update, sends new status to Cloud

Chip-to-Cloud Integration

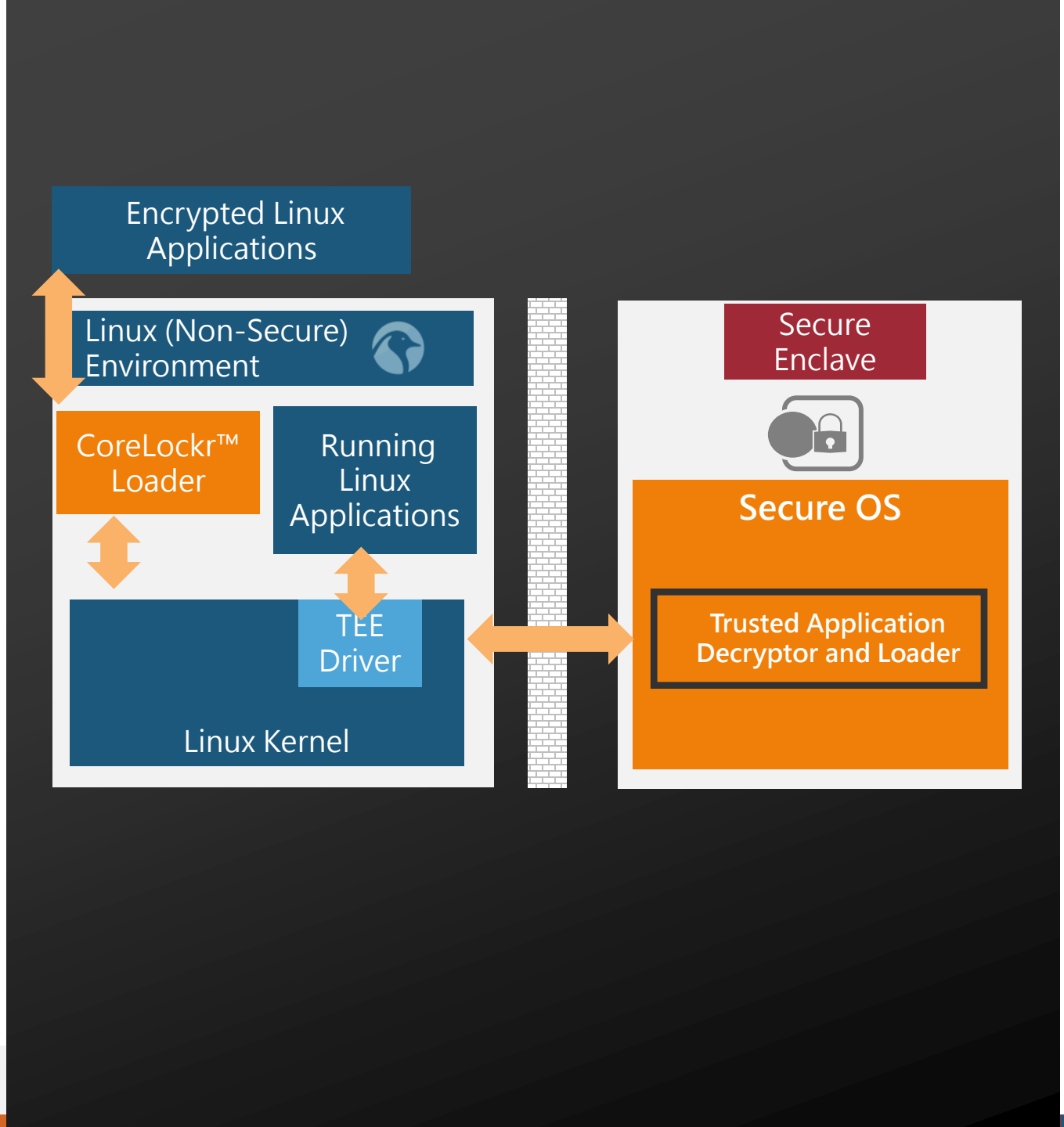
- **Mutual** authentication between device and cloud is required
  - Tied to hardware root-of-trust (RoT), verifying identity
  - Credentials (cert/key) protected storing and verifying in secure domain
- All device data has strong audit trail to source
- Device Tampers and faults can be collected for analysis

Protecting AI Models at the Edge

- Machine Learning and AI at the edge present new challenges for security
- Applying the principles of device security at the edge becomes critical
- Key principles for protecting AI Models:
  - *Ensure the model is authentic*
  - *Hide the model from attackers*

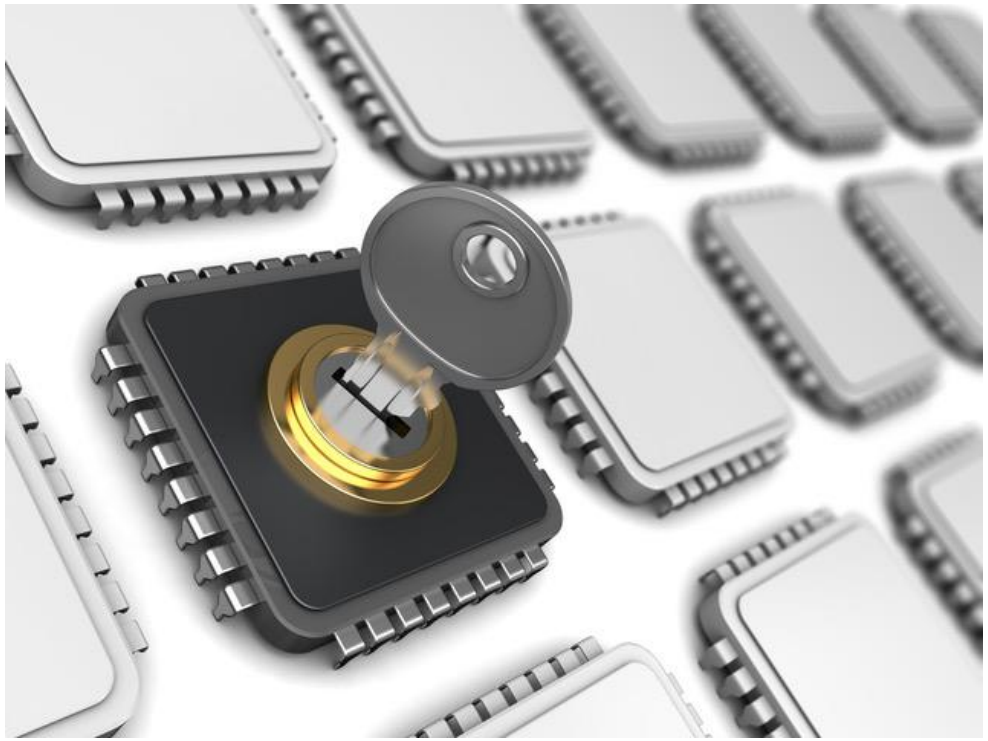
Protecting IP: Encrypting Rich OS Applications using Trusted Applications

- Applications encrypted and locked to device in storage
- Special CoreLockr Loader to handle protected applications
- Trusted Application verifies permissions and decrypts application
- Trusted Application loads Linux App direct to RAM and runs



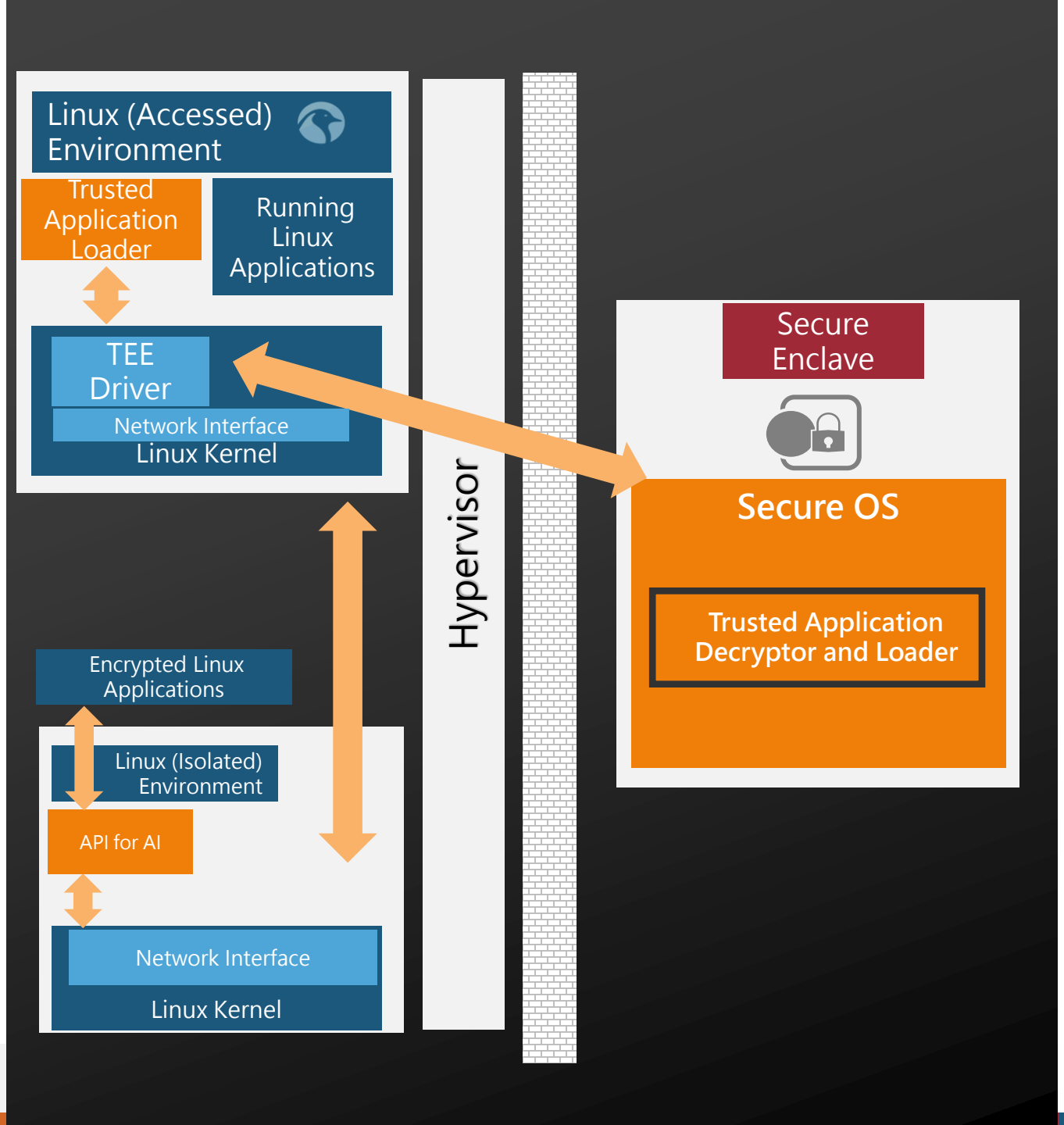
Opaque Keys and Objects
How do I protect content on the device?

- EmSPARK™ provides two mechanisms to send confidential information to a device
  - Opaque Keys – Device specific encrypted and signed key to be loaded to key store in TEE
  - Opaque Objects – Device Specific encrypted and signed Data to be decrypted on device
- Protecting an application or model
  - Deliver as an Opaque Object
  - Decrypt with Opaque Object to volatile memory
  - Use application or model
  - Clear memory



Protecting IP: Protecting Rich OS Applications that Rely on Dedicated Hardware

- Applications encrypted and locked to device in storage
- Special CoreLockr Loader to handle protected applications
- Trusted Application verifies permissions and decrypts application
- Trusted Application loads to Isolated VM to run securely



Virtualization (SECURING THE AI Hardware)

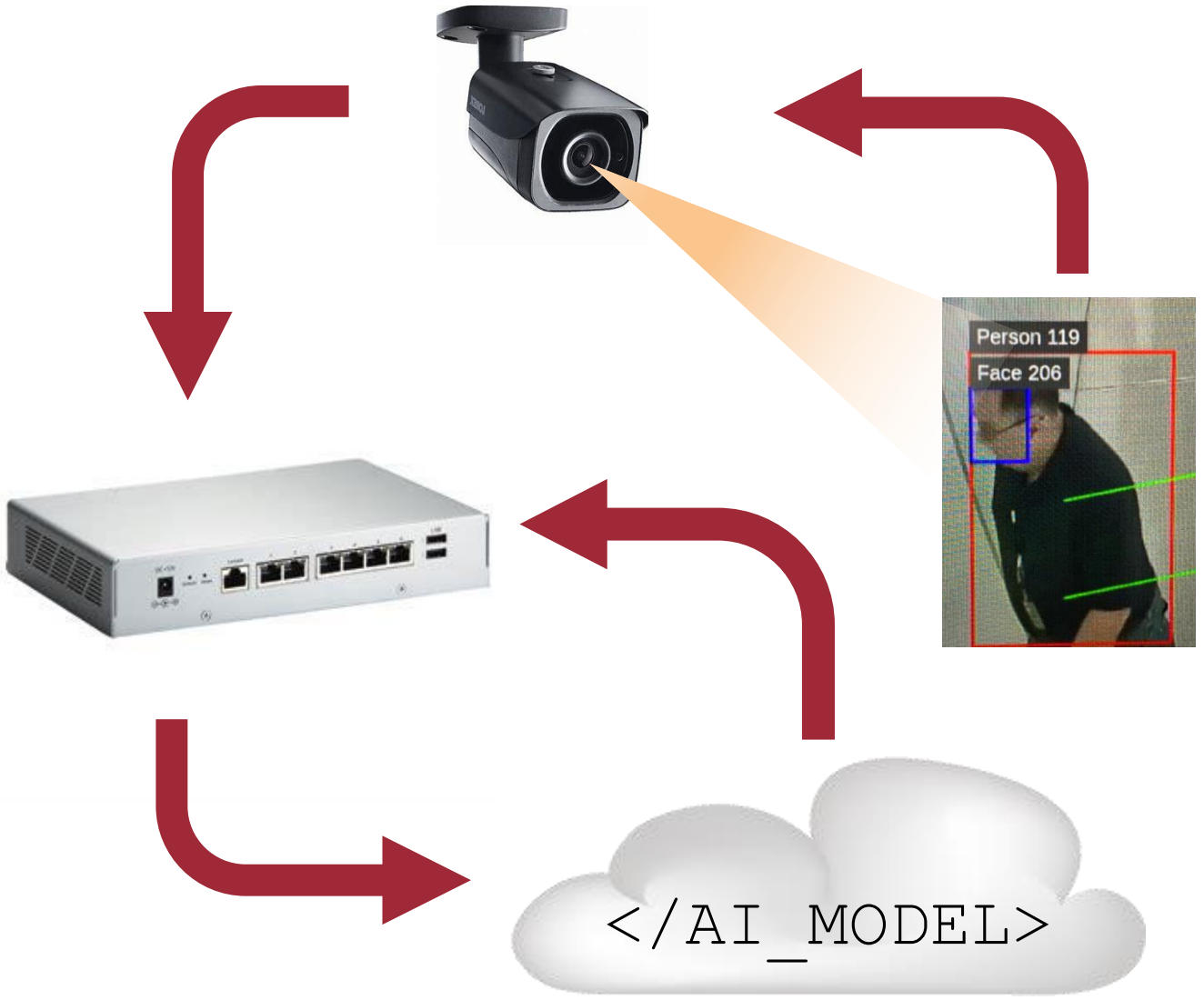
Challenge – Sometimes moving the software and hardware to the secure enclave is too much. How do you protect assets without moving to the secure enclave?

Virtualization is the answer!

- Create a virtualized set of guest OS instances to separate domains in the non-trusted side
  - One isolated Linux to run the primary application and user code, but restricted hardware access.
  - One Linux to access the protect hardware and assets
- The isolated Linux is where the primary application, user data, and other less critical applications run

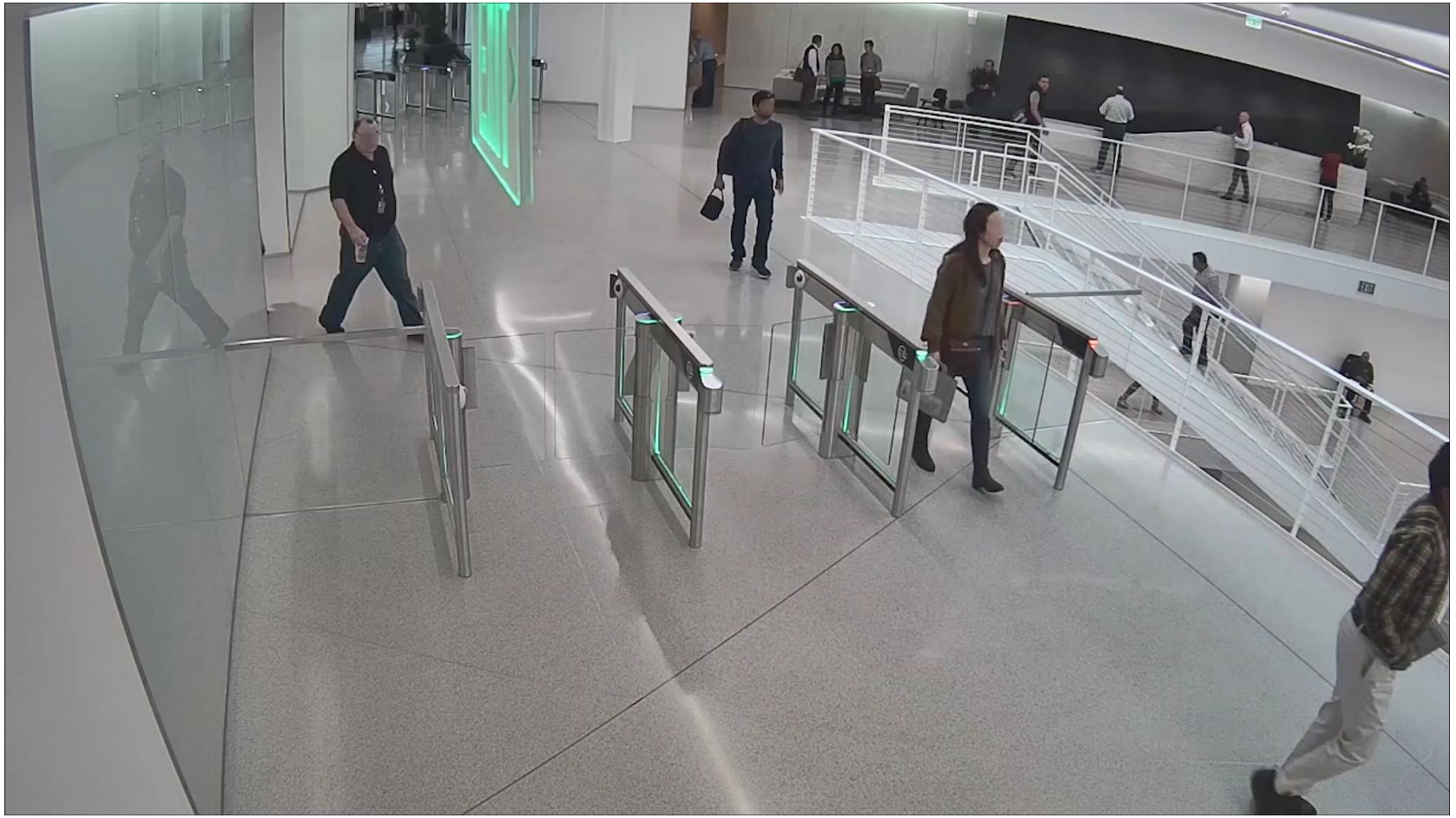
Today's example

- Appliance that applies AI models for camera feeds
  - Different models can be loaded (ex, store demographics, intersection traffic, etc)
- Secure communication between the device and the cloud
- AI Models are delivered to the device



Video Feed

- Office traffic
- Key areas of inference:
  - Entry/Exit
  - Faces
  - People
  - Bags

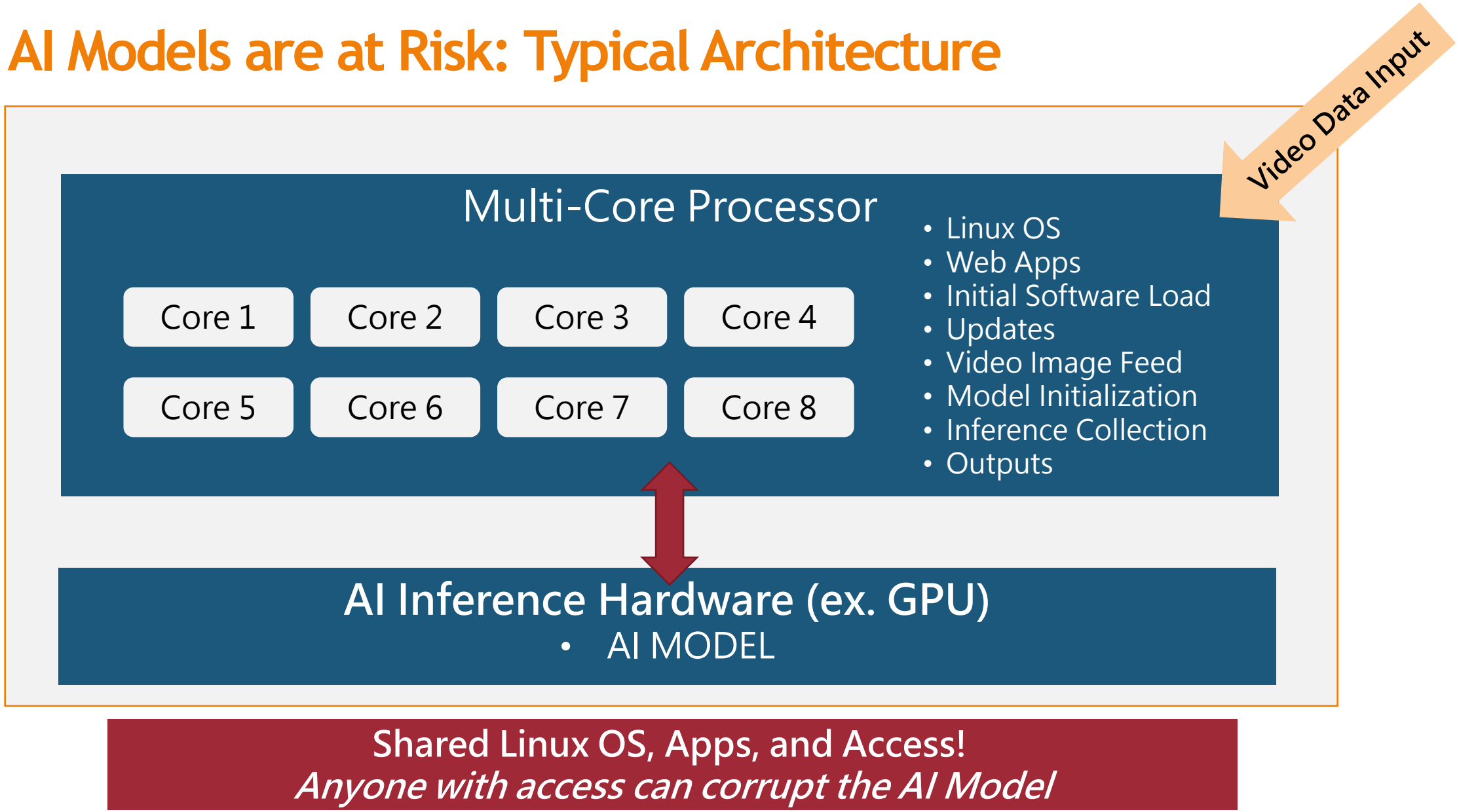


AI model applied

Entry/Exit are incremented as people cross

People, faces and bags are counted

Why AI Models are at Risk: Typical Architecture



Shared Linux OS, Apps, and Access!
Anyone with access can corrupt the AI Model

Accessing and Corrupting the Model

```
# The values in the config file are overridden by values set through GObject
# properties.

[property]
enable=1
#Width height used for configuration to which below configs are configured
config-width=1920
config-height=1080
#osd-mode 0: Dont display any lines, rois and text
#         1: Display only lines, rois and static text i.e. labels
#         2: Display all info from 1 plus information about counts
osd-mode=2
#Set OSD font size that has to be displayed
display-font-size=12

[line-crossing-stream-0]
enable=1
#Label;direction;lc
# Direction: 2 coordinates of direction followed by 2 coordinates of virtual
line
# Label ; direction;direction; line;line
line-crossing-Entry=750;670;800;750;300;850;1350;650;
line-crossing-Exit=900;1000;850;900;300;1000;1550;760;

# class-id: 0=> people 1=> bag 2=> face
class-id=0

#extended when 0- only counts crossing on the configured Line
#              1- assumes extended Line crossing counts all the crossing
extended=0
```

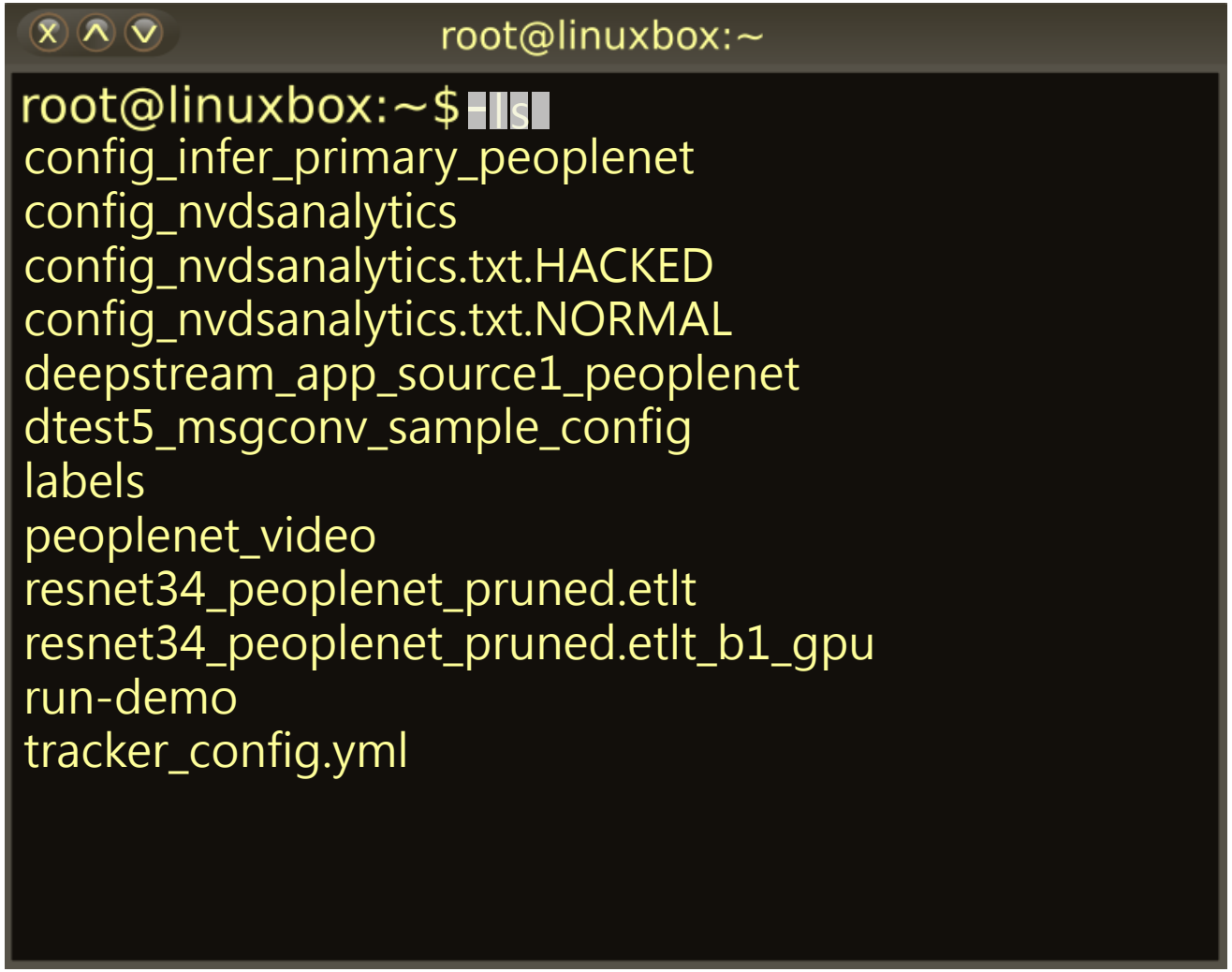
```
# The values in the config file are overridden by values set through GObject
# properties.

[property]
enable=1
#Width height used for configuration to which below configs are configured
config-width=1920
config-height=1080
#osd-mode 0: Dont display any lines, rois and text
#         1: Display only lines, rois and static text i.e. labels
#         2: Display all info from 1 plus information about counts
osd-mode=2
#Set OSD font size that has to be displayed
display-font-size=12

[line-crossing-stream-0]
enable=1
#Label;direction;lc
# Direction: 2 coordinates of direction followed by 2 coordinates of virtual
line
# Label ; direction;direction; line;line
line-crossing-Entry=750;670;800;750;300;850;1350;650;
line-crossing-Exit=900;1000;850;900;300;1000;1550;760;

# class-id: 0=> people 1=> bag 2=> face
class-id=5

#extended when 0- only counts crossing on the configured Line
#              1- assumes extended Line crossing counts all the crossing
extended=0
#LC modes supported:
```

Change to script renders model useless!

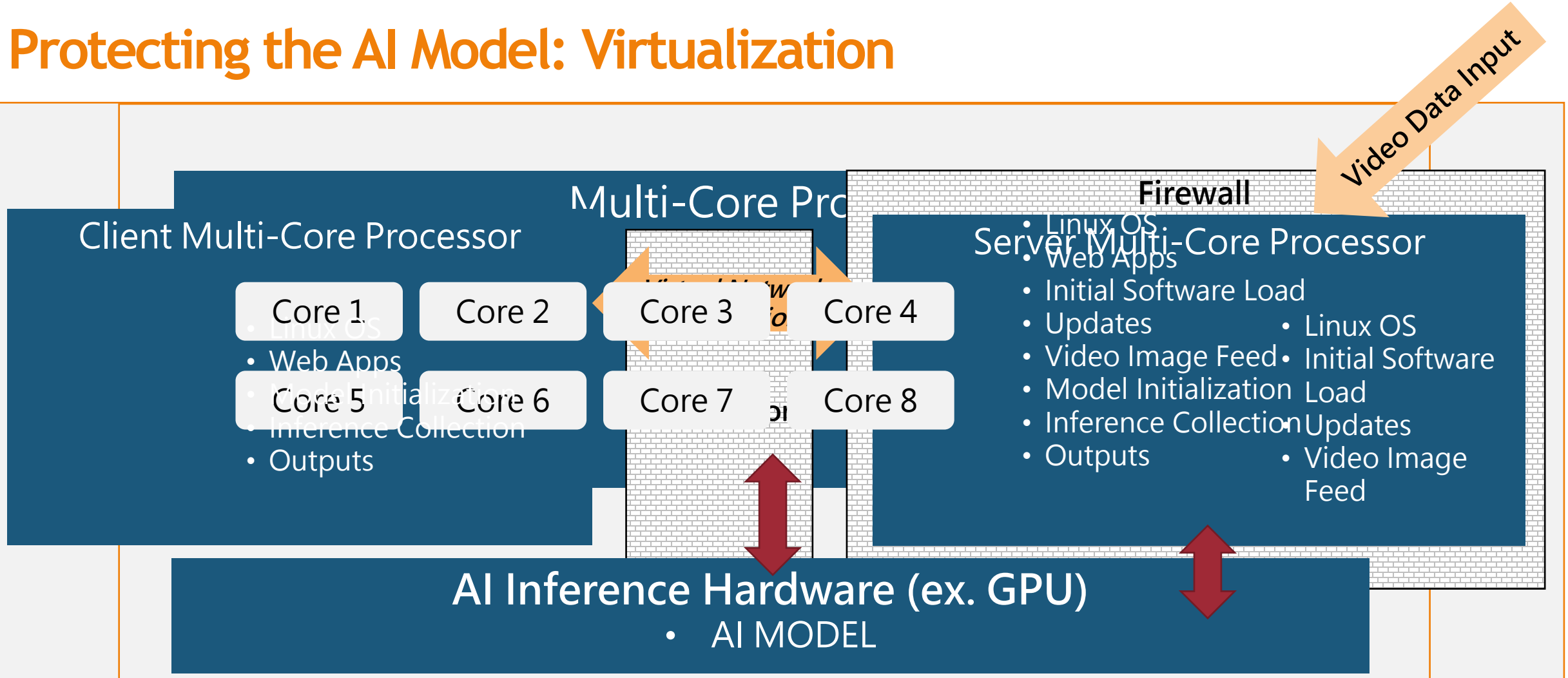
AI Corrupted!

Entry/Exit no longer increments

Intellectual Property (Models and Data) are Exposed!

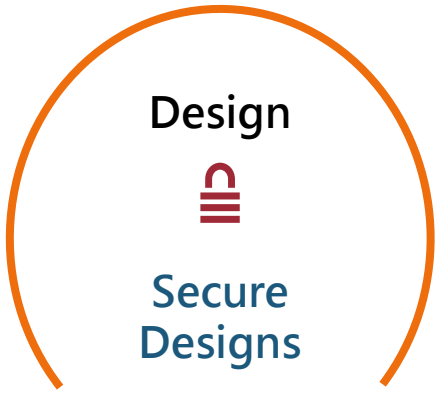


Protecting the AI Model: Virtualization



Server Cores and GPU are isolated!
Cannot be seen or accessed by the Client Cores

Sequitur Security Platform: The Next Logical Step



EmSPARK™

EmSPARK™ Security Suite
Device Security

- 40% reduction in security deployment time
- Fraction of in-house development risk
- Consistent implementation across silicon platforms

EmPOWER™

EmPOWER™ Cloud Services
Trust as a Service

- Secure updates, management
- Threat detection and remediation
- Authenticated device events and metrics

Sequitur Labs Security Platform

EmSPARK™ Security Suite

- **CoreTEE™**
  - Secure OS enabling access to TrustZone® secured resources
- **CoreLockr™**
  - APIs
  - Trusted applications
  - Code examples
- **Integration Tools**
  - Firmware packaging tool
  - Linux patches
- **Software Development Kit**
  - Software for Custom Trusted Application Development
- **Trusted Provisioning Tools**

EmPOWER™ Device Managment

- **Available NOW**
- **Contact us at info@sequiturlabs.com for a demo or free trial**

Platforms Supported:

Microchip SAMA52

Microchip SAMA5D2-SOM

NVIDIA Jetson AGX Xavier

NVIDIA Jetson TX2 / NX

NXP i.MX6/7/8

NXP Layerscape

ST Micro STM32MP1

Empowering Product Creators to Harness Edge AI and Vision

The Edge AI and Vision Alliance (www.edge-ai-vision.com) is a partnership of 100+ leading edge AI and vision technology and services suppliers, and solutions providers

Mission: To inspire and empower engineers to design products that perceive and understand.

The Alliance provides low-cost, high-quality technical educational resources for product developers

Register for updates at www.edge-ai-vision.com

The Alliance enables edge AI and vision technology providers to grow their businesses through leads, partnerships, and insights

For membership, email us: membership@edge-ai-vision.com

Join us at the Embedded Vision Summit

May 16-19, 2022—Santa Clara, California

The only industry event focused on practical techniques and technologies for system and application creators

- *"Awesome! I was very inspired!"*
- *"Fantastic. Learned a lot and met great people."*
- *"Wonderful speakers and informative exhibits!"*

Embedded Vision Summit 2022 highlights:

- **Inspiring keynotes** by leading innovators
- High-quality, practical **technical, business and product talks**
- Exciting **demos**, **tutorials** and **expert bars** of the latest applications and technologies

Visit www.EmbeddedVisionSummit.com to learn more

Q&A

SEQUITUR LABS

Thank You

https://www.sequiturlabs.com/