Firmware, the Last Frontier: Open System Firmware (OSF)
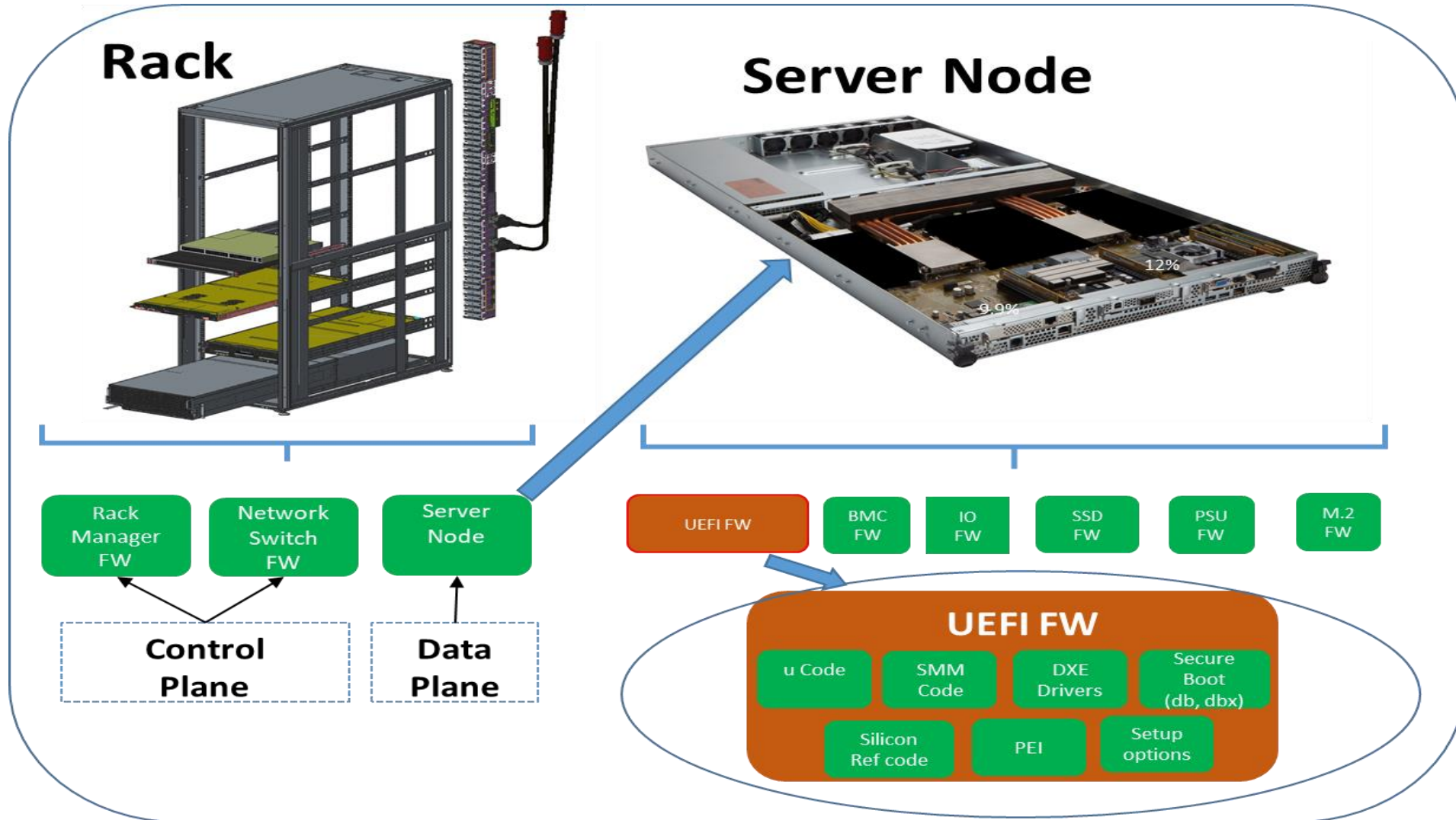
Gundrala "Devender" Goud/Director/Microsoft
Ron Minnich / Google

OPEN. FOR BUSINESS.

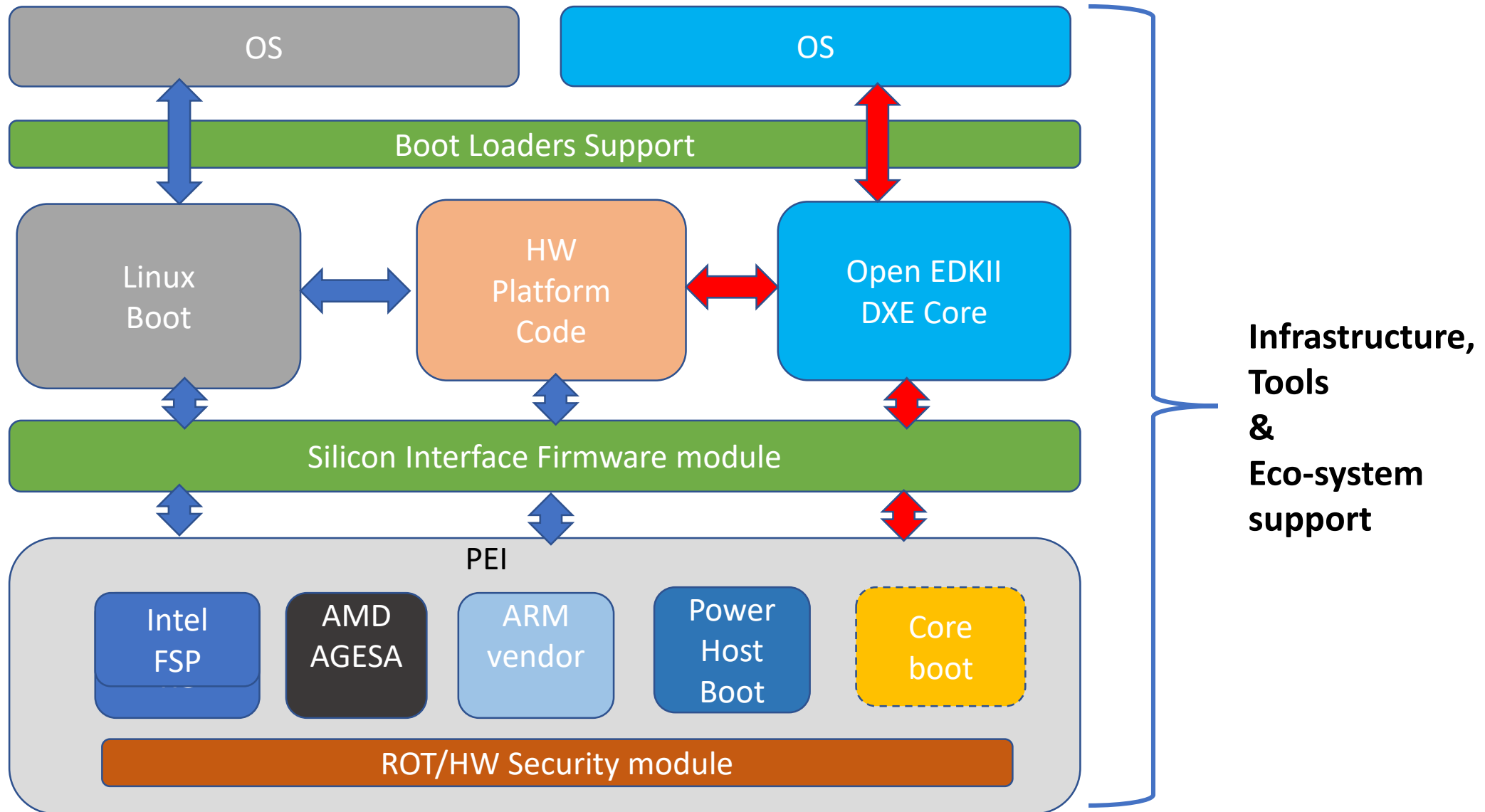OCP SUMMIT

What is this UEFI FW (BIOS)?

Current Challenges 'System Firmware' and Why Open?

- 'Closed' System Firmware **could have impacts to** rapid prototyping of new or derivative products development (NDA, IP, etc.)
- Variance in boot flows of different Silicon vendors', causing inefficiencies in System Firmware development and maintenance.
- Various System Firmware implementations exists, but **not one single implementation** addresses the needs of different CSP use models.
- System Firmware current **development models not able** to keep pace with 'High Octane' Innovation by multiple Cloud HW vendors.

Truly Open 'Solution' = open HW+ open FW

Convergence of Different System Firmware(s) –> Open System Firmware (OSF)

OS

OS

Boot Loaders Support

Linux Boot

HW Platform Code

Open EDKII DXE Core

Silicon Interface Firmware module

Infrastructure, Tools & Eco-system support

PEI

Intel FSP

AMD AGESA

ARM vendor

Power Host Boot

Core boot

ROT/HW Security module

Collaborative Community development model

OSF - Workstreams

Workstream name	Owner (Companies)
PEI	Intel
Intel FSP binary	Intel
AGESA RC binary	AMD
ARM Boot code binary	
Power Host boot	
Core Boot	9 Elements
Silicon Interface Firmware Module	Intel
Linux Boot	Google, FB, Two Sigma, Horizon
Open EDK II DXE core	MSFT, Intel
HW platform modules	HW supplier
Boot loader support	OS vendor(s)
Build tools	Two Sigma
Automated test support	Horizon, Google
Telemetry/Diags	
FW variables standardization	Intel, MSFT
Bug tracking and GitHub source code control	Google, 9 Elements, OCP/Rajeev
HW requirements to comply to OSF boot	Two Sigma, MSFT
Security coding guidelines	

OSF- Open EDKII Workstream

Gundrala Devender Goud/Director/Microsoft
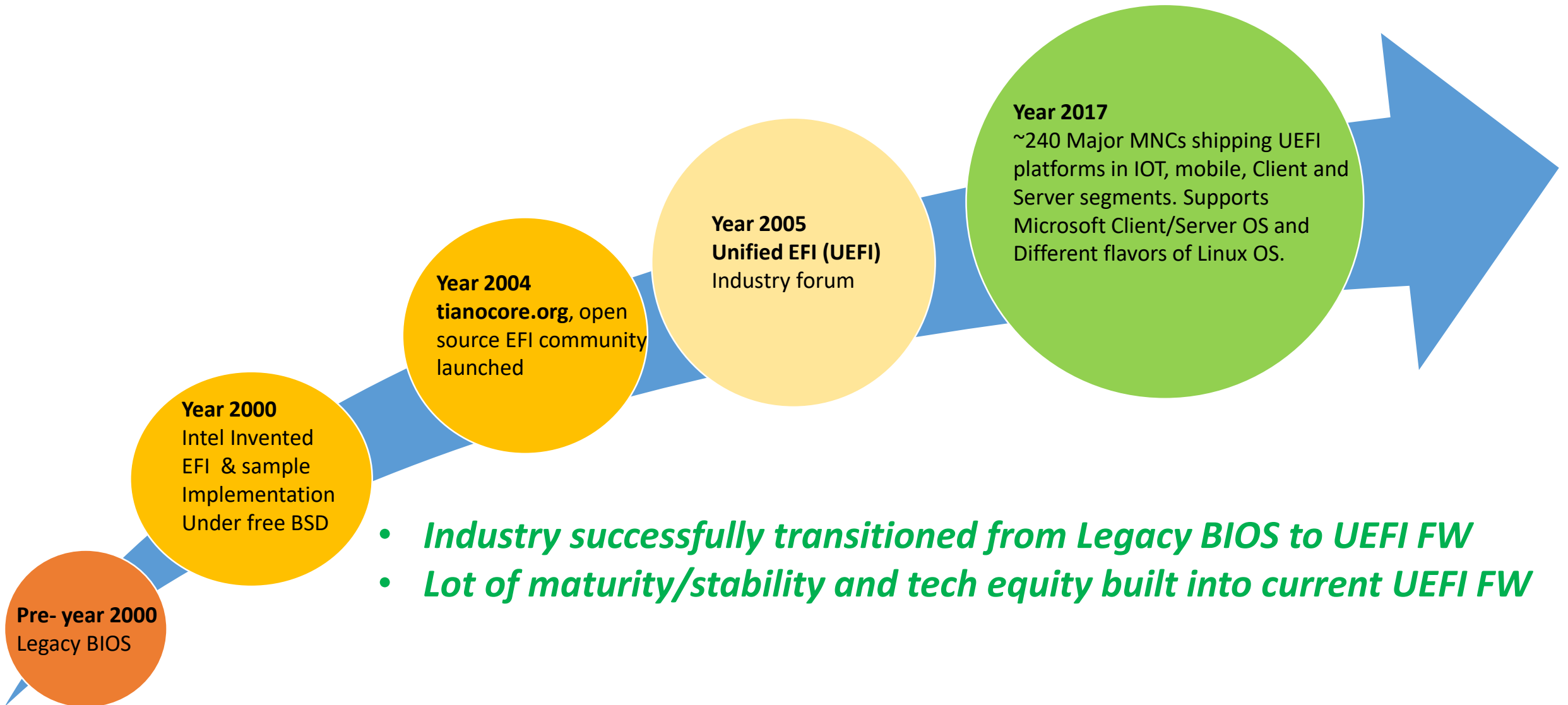Contributor(s): Vincent Zimmer/Sr.PE/Intel
Mallik Bulusu/Director/Microsoft

Background and UEFI FW progression....

Year 2017
~240 Major MNCs shipping UEFI platforms in IOT, mobile, Client and Server segments. Supports Microsoft Client/Server OS and Different flavors of Linux OS.

**Year 2005
Unified EFI (UEFI)**
Industry forum

**Year 2004
tianocore.org**, open source EFI community launched

Year 2000
Intel Invented EFI & sample Implementation Under free BSD

Pre- year 2000
Legacy BIOS

- *Industry successfully transitioned from Legacy BIOS to UEFI FW*
- *Lot of maturity/stability and tech equity built into current UEFI FW*

Let's leverage UEFI learnings to Open System Firmware initiative

Current State of UEFI FW implementation ...
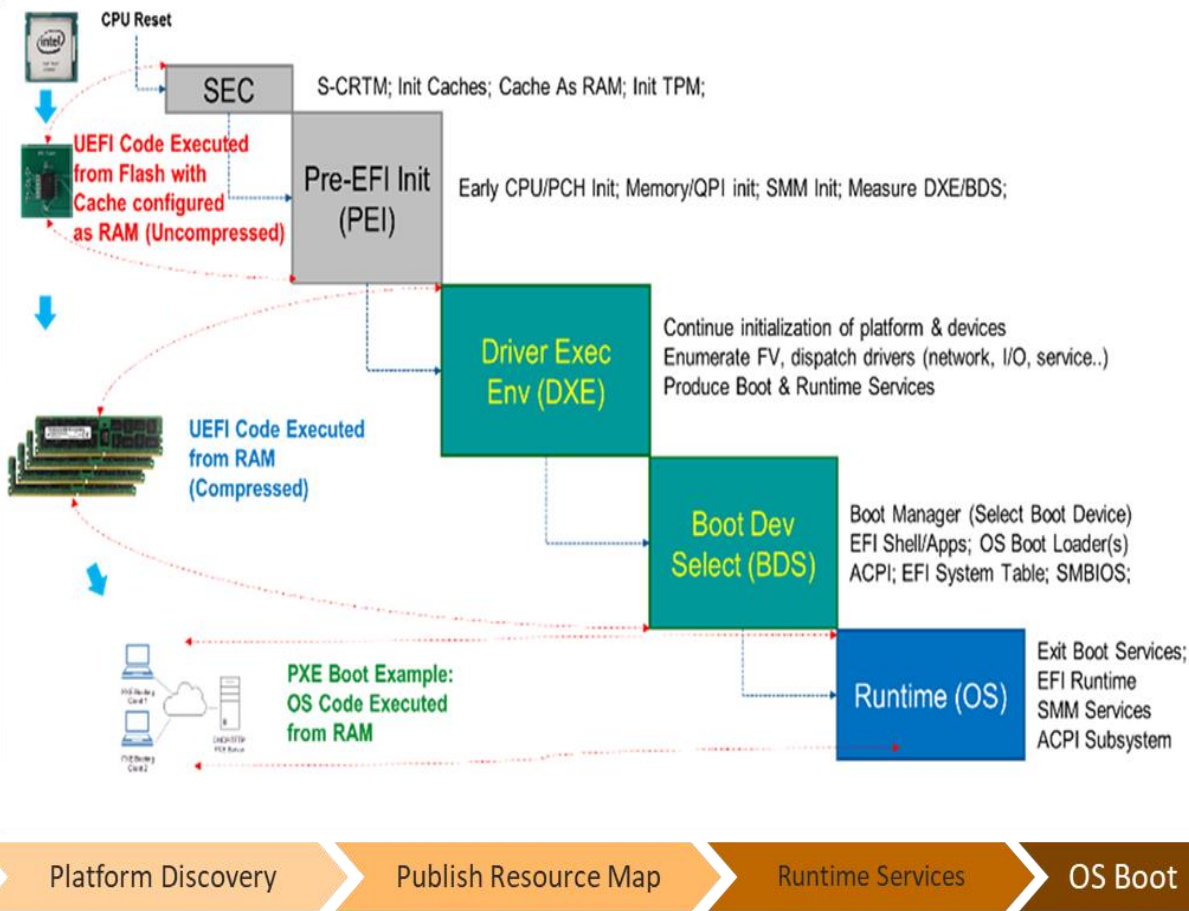
|	
CPU Fetches UEFI Code	
Cache as RAM	
CPU Init	
Interconnect Init	
PCH Init	
Memory Init	
MP Init	
PCI Init	
Platform Init	
RAS Features	
Standards Compliance	
Boot Target Selection	
Windows OS	

Current Gaps:

- **Not truly 'Open' - Commercial products with EDKII core based UEFI FW solutions still shipping with proprietary content**
- **Silicon/Chipset modules are not open**
- **Not Optimized for 'Cloud' Use Models**

Open EDKII workstream is expected to address current gaps and be cloud ready

Open EDK II workstream plans and progress
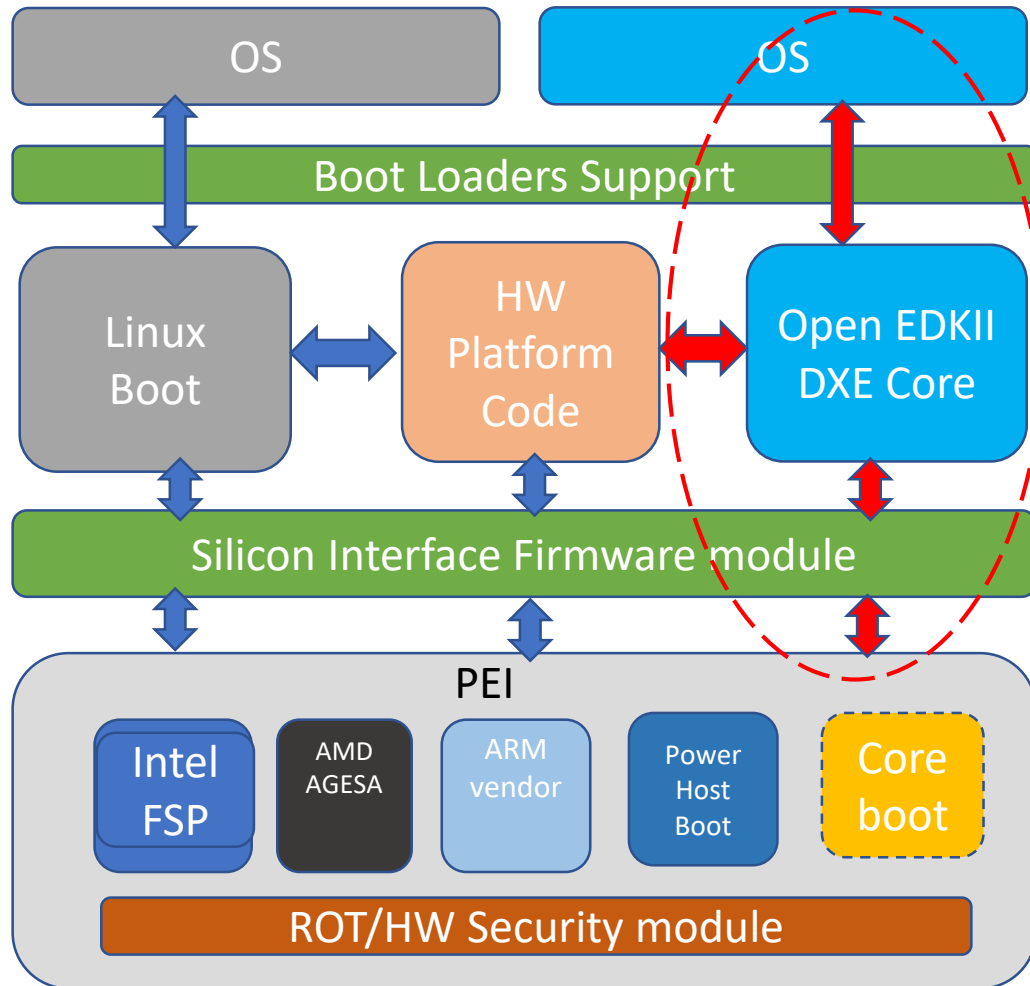
Open EDK II workstream goals:

- Make complete tree open
- Support multi-silicon architectures and multi-OS.
- Standardize the HW ROT interfaces in SEC/PEI modules
- Support new 'Silicon Interface Firmware module interfaces' to open EDKII DXE core
- Simply Setup and make it OOB configurable
- Optimize the solution for Performance, Reliability, Serviceability, Scalability and Deployability.
- **Deliver initial open EDKII based tree to support Mt.Olympus HW - done

Let's together accelerate OSF development

Call for Action(s)

- **Please attend weekly OCP/OSF calls**
- **Encourage each of you to bring-in your challenges, innovative ideas to OSF**
- **Contribute to workstreams->Great opportunity to showcase your passion in open system firmware development**
- **Identify additional workstreams, own them and drive solution**

Questions?