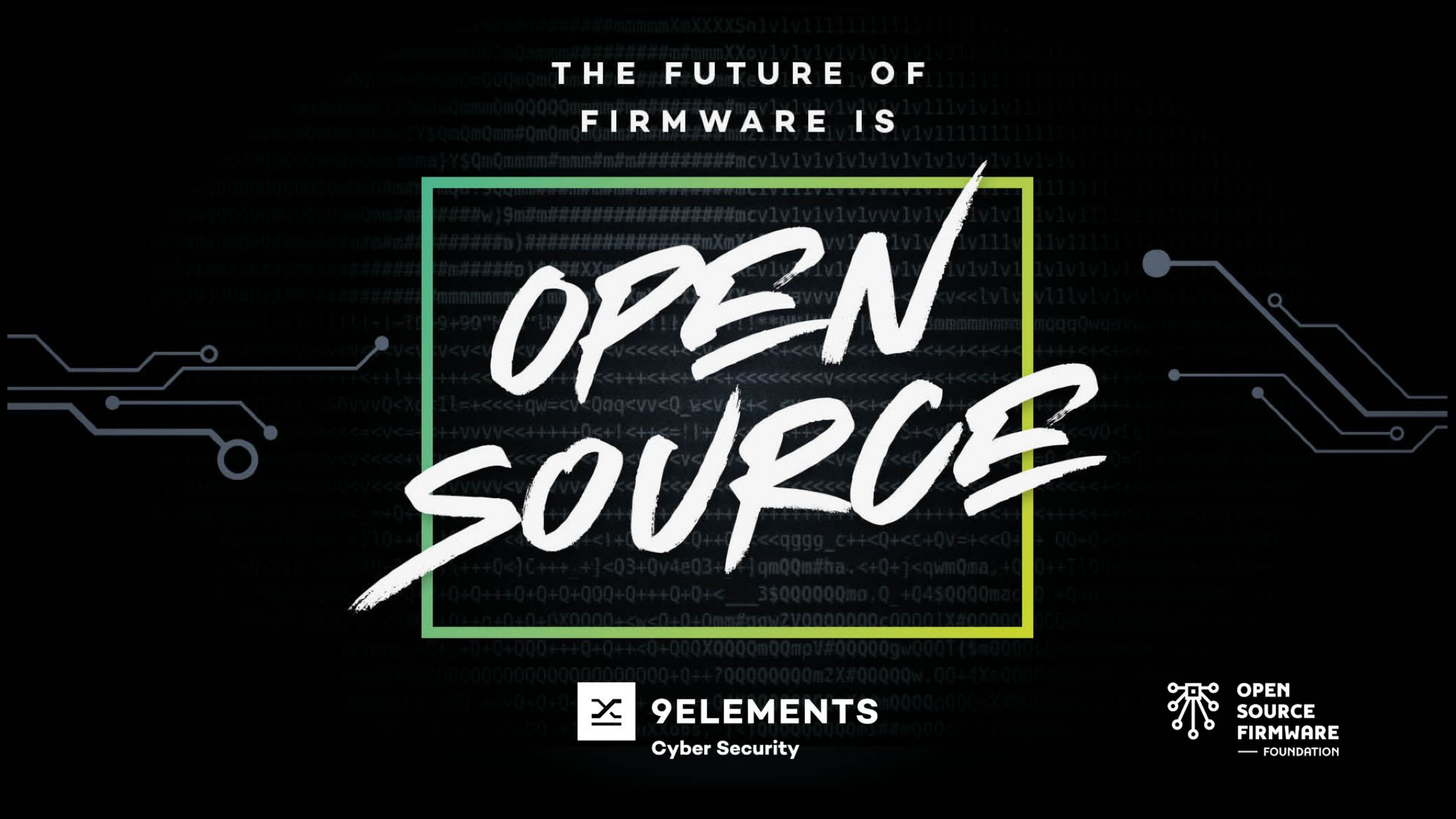

THE FUTURE OF
FIRMWARE IS
OPEN
SOURCE
9ELEMENTS
Cyber Security
OPEN
SOURCE
FIRMWARE
FOUNDATION

The Blindspot of Cyber Security: How to defend cyber attack with open source firmware supply chain

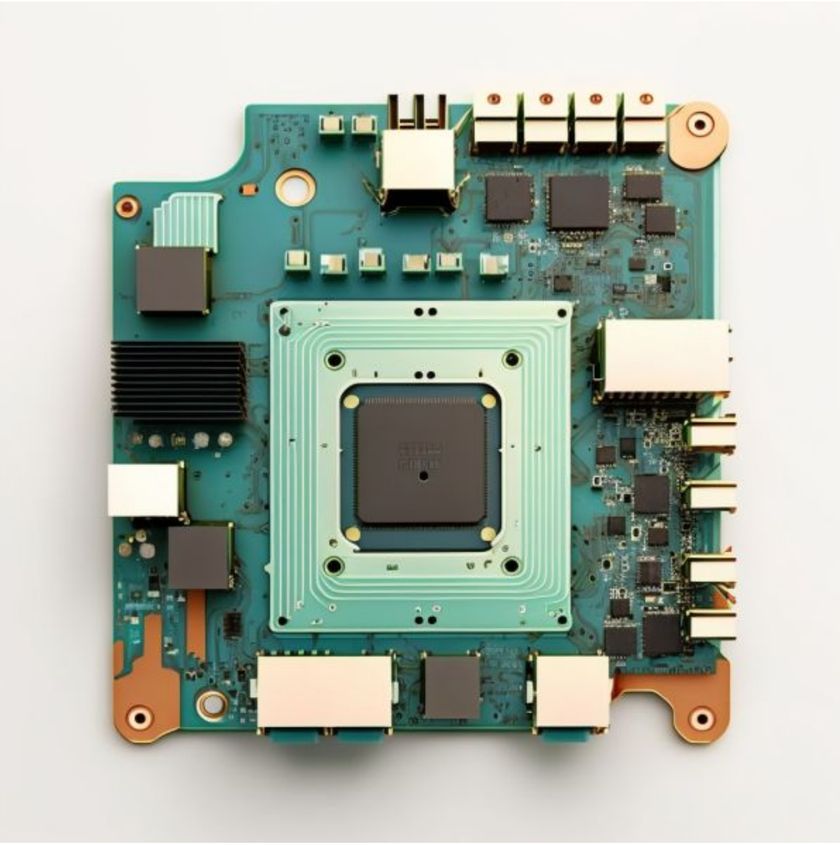
Unlock Open-Source Firmware

Lean Sheng Tan, 9elements

9ELEMENTS
Cyber Security

Firmware: A Specialized Form of Software

- Most privileged
- Firmware has a lot of implications
  - Security
  - Usability
  - Performance
  - Time-to-Market
  - Price (BoM)
- Critical component in each system



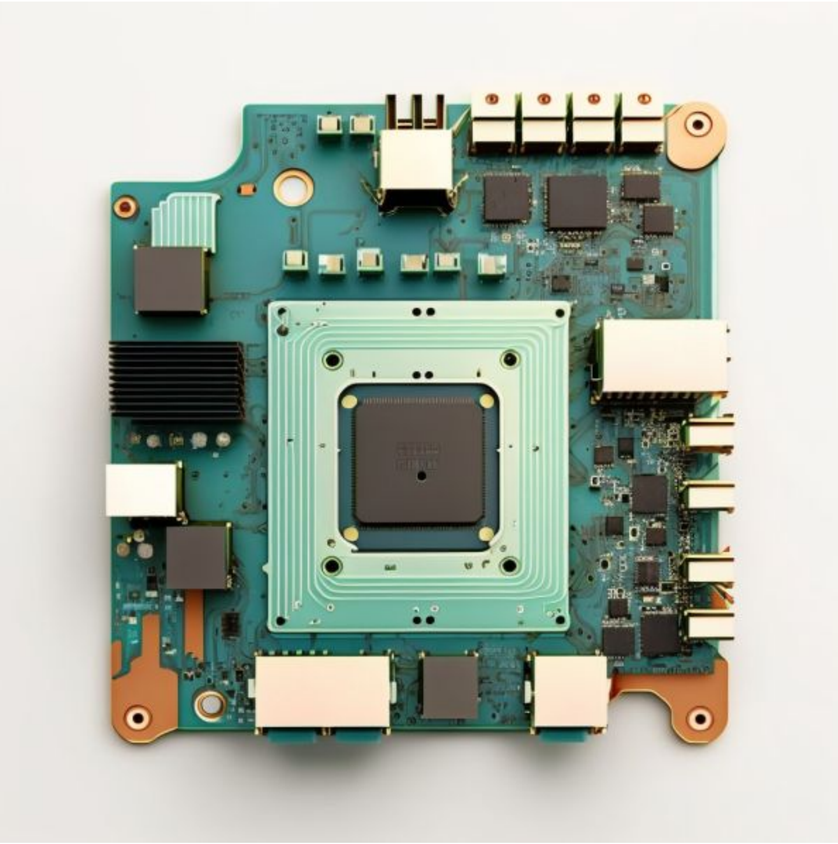
9ELEMENTS
Cyber Security

Firmware: A Specialized Form of Software

- Amanda Brock (openUK)

  “48% to 98% of the Software written today is open-source”

  → Firmware managed to stay away from this… until now!



9ELEMENTS
Cyber Security

Secure by Design

- Secure by Design products are those where the security of the customers is a core business requirement, not just a technical feature
- Secure by Design principles should be implemented during the design phase of a product's development lifecycle
- CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Japan, Australia, Canada, United Kingdom, Germany, Netherlands, and New Zealand jointly developed Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

The Principles of Secure by Design

- The burden of security should not fall solely on the customer
- Embrace radical transparency and accountability
- Build organizational structure and leadership to achieve these goals

CISA: Bolster UEFI Cybersecurity Now

[A Call to Action: Bolster UEFI Cybersecurity Now | CISA]

- "Attackers have a clear value proposition for targeting
- UEFI software" because UEFI subversion can provide malicious software the ability to persist through:
  - System reboot - the malware survives basic defensive actions such as turning the device off and on again.
  - Operating system reinstallation - Malware that persists through reinstallation can evade this standard incident response practice.
  - Partial physical part replacement - A device infected with this level of persistent malware basically needs to be thrown away rather than repaired.

NIST SP 800-218

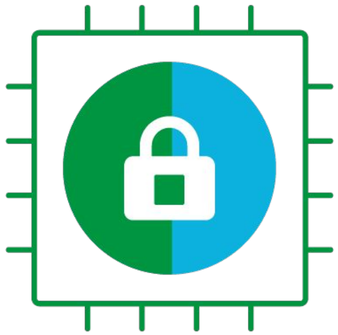
- Executive Order (EO) 14028 - May 2021
  - NIST SP 800 218 Secure Software Development Framework (SSDF) - Feb 2022
  - OMB (M-22-28 & M-23-16) requires all federal agencies to comply with NIST guidance - Sep 2022
    - No later than September 13, 2023, for all software, agencies shall collect attestation letters not posted publicly by software providers for all software subject to the requirements of this memorandum."
    - All Federal gritical software must comply with NIST guidance - Iun 2023
    - All Federal 3rd party software must comply with NIST guidance - Sep 2023

9ELEMENTS
Cyber Security

NIST SP 800-218

- Requirements:
  - A self attestation that the product was built In conformance with NIST 's SSDF.
  - On request, a Software Bill of Materials (SBOM) for the product
  - On request, other artifacts substantiating SSDF conformance, e.g., output of vulnerability scanners, software provenance metadata, etc
  - On request, evidence of participation in a Vulnerability Disclosure Program.

Open-Source in the Firmware Industry



tianocore

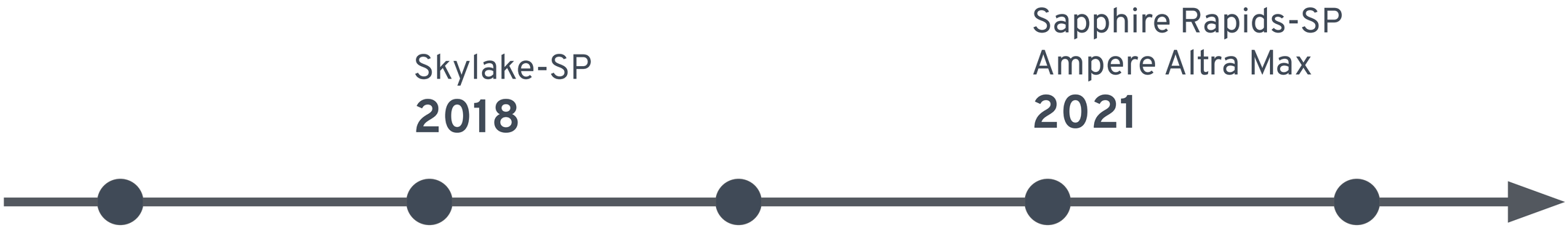
OpenBMC

Open-Source in the Firmware Industry

9ELEMENTS
Cyber Security

Open-Source in the Firmware Industry

All Major Host SoC Vendors Supports Open-Source Firmware



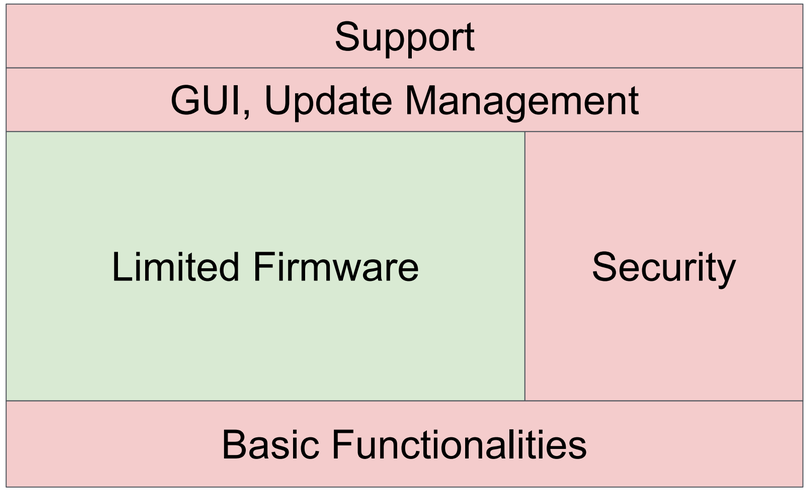
9ELEMENTS
Cyber Security

Open-Source: Why?

- Enhanced security and transparency
- Accelerated innovation through collaboration
- The ability to customize and tailor solutions
- Cost savings

Pseudo Open-Source Solutions?

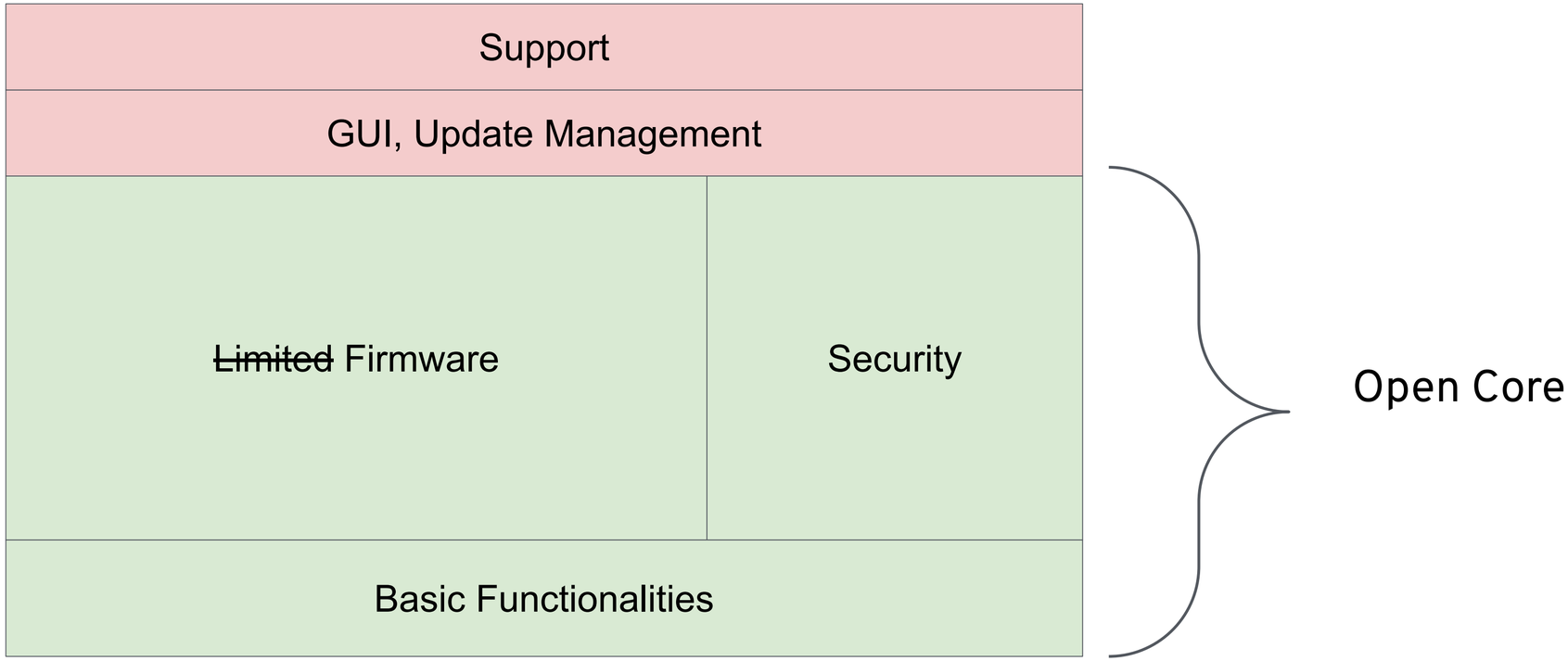
- Companies claim to support open-source
  - Limited Editions
  - Pay for production-ready
- Vendor locked-in versions
- Bad user experience



Pseudo Open-Source Solutions?

- Hindered collaboration and innovation
- Fragmentation within the open-source firmware ecosystem
- Reduced trust in open-source
- Little to no community interaction

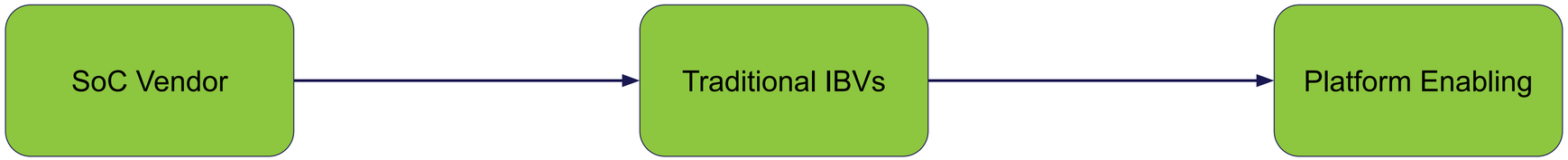
The Open-Source Development Model



Platform Enabling

Traditional Model

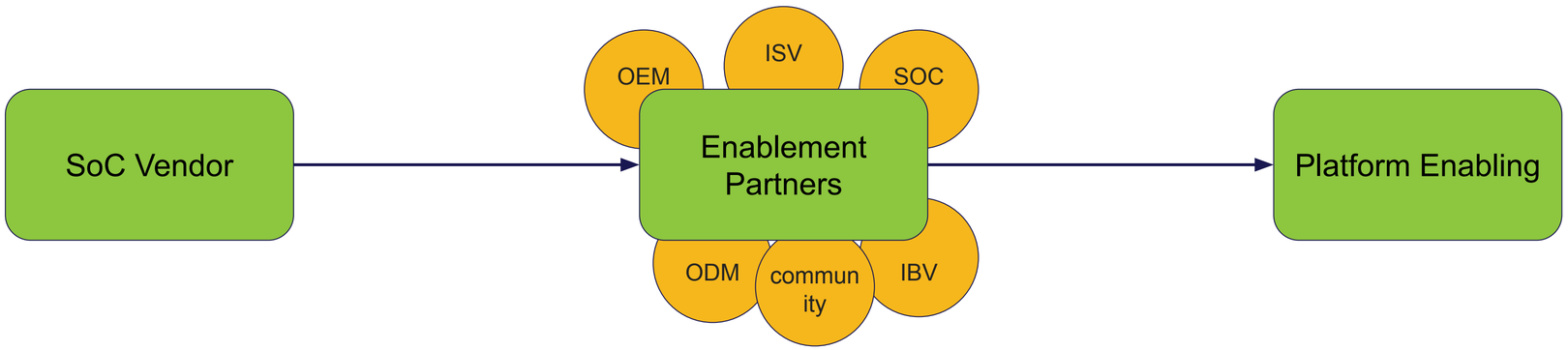
- Controlled by SoC vendors
  - Reference code and documentation only available to IBVs
  - Work closely with IBVs to enable platforms
- IBVs enable ODMs/OEMs
  - Support ODMs/OEMs



The Open-Source Way

Open Development Model

- More scalable approach
  - Community enables platform and features together
- SoC needs to provide the same amount of support



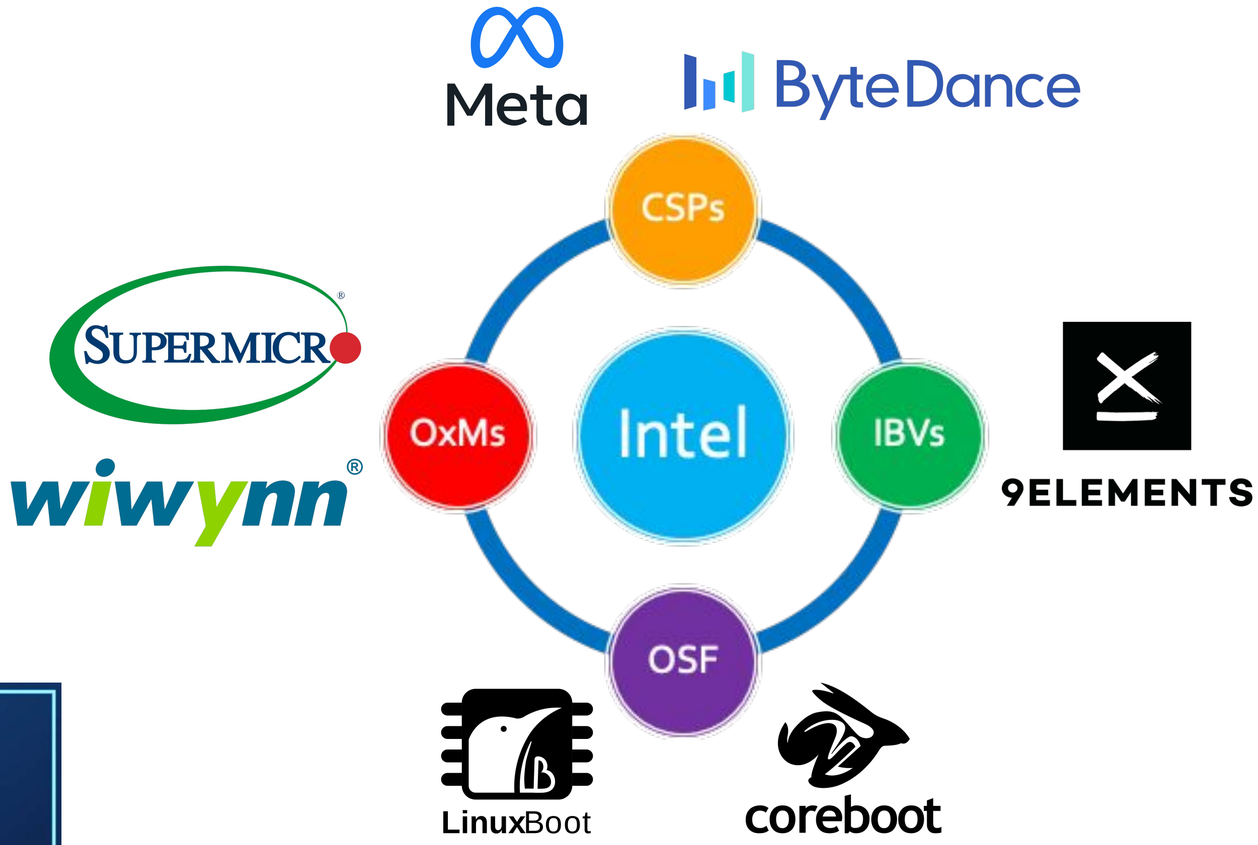
9elements - Embracing Open-Source First

- Part of all major open-source projects
  - coreboot
  - EDKII
  - openBMC

- Upstream first, Open-Source first Development Model
- Unique Business Model
  - Customized to your needs
  - Modular

9ELEMENTS
Cyber Security

9elements - Embracing Open-Source First



OSF Multi Parties Collaboration

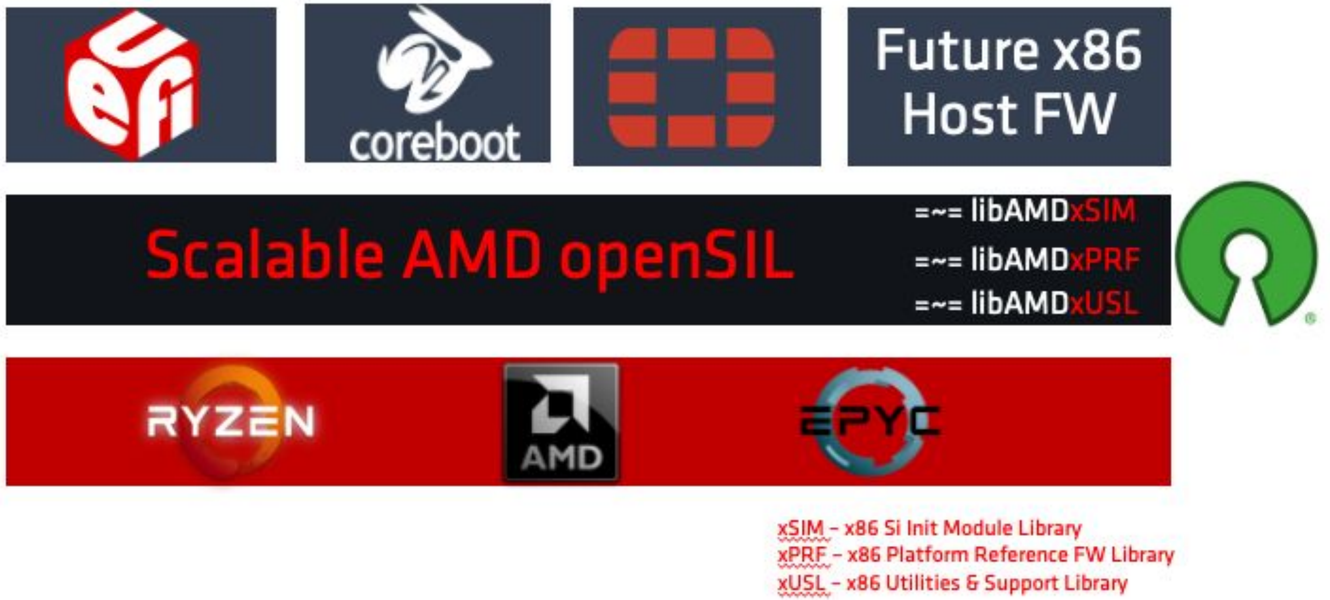
- Intel FSP enables OCP Open System Firmware (OSF) ecosystem
- Enable OSF ready Intel Platforms with Intel partners
- Production-ready platforms:
  - Supermicro
  - ByteDance
  - Wiwynn
- Community driven collaboration
  - Faster development, backporting and bug fixing

intel XEON Accelerate with Xeon

9ELEMENTS Cyber Security

9elements - Embracing Open-Source First

- ✓**Agnostic 3 Static Library** solution written in C-17
  - ✓Silicon, Platform & Utilities
- ✓**Simple & Scalable** integration with any x86 Host FW
- ✓**Flexible** Platform library scalable to customer and x86 host FW needs
- ✓**Lightweight & Low chirp** density for **increased Security**
- ✓**Open Source** – right from the get-go!



xSIM – x86 Si Init Module Library
xPRF – x86 Platform Reference FW Library
xUSL – x86 Utilities & Support Library

Get in Touch!

- https://www.9esec.io
- cybersecurity@9elements.com

9ELEMENTS
Cyber Security