Unlocking the Power of Confidential Computing: Securing Data in Use

Andrej Zdravkovic, SVP and Chief Software Officer

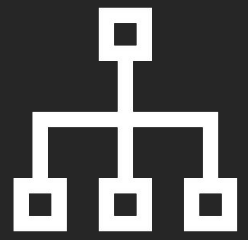
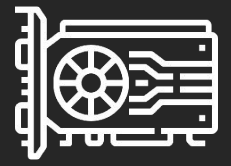
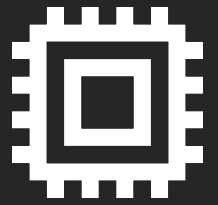
World Summit AI

Montreal, April 15, 2025

AMD

together we advance_

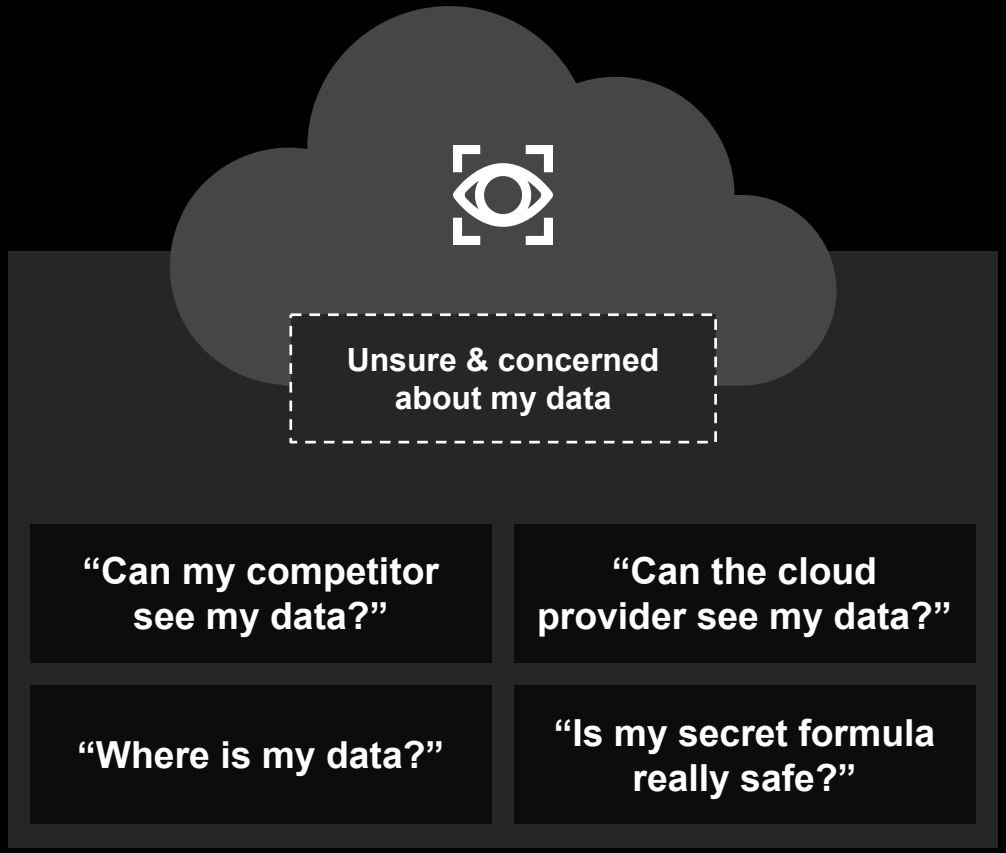
Basics of Data Protection & Confidential Computing

Data in Transit	Data at Rest	Data in Use
		  
Network / Link Encryption	Disk Encryption	Confidential Computing

Unlocking Cloud Opportunities with Confidential Computing

Traditional Cloud

Others can see my data



Confidential Cloud

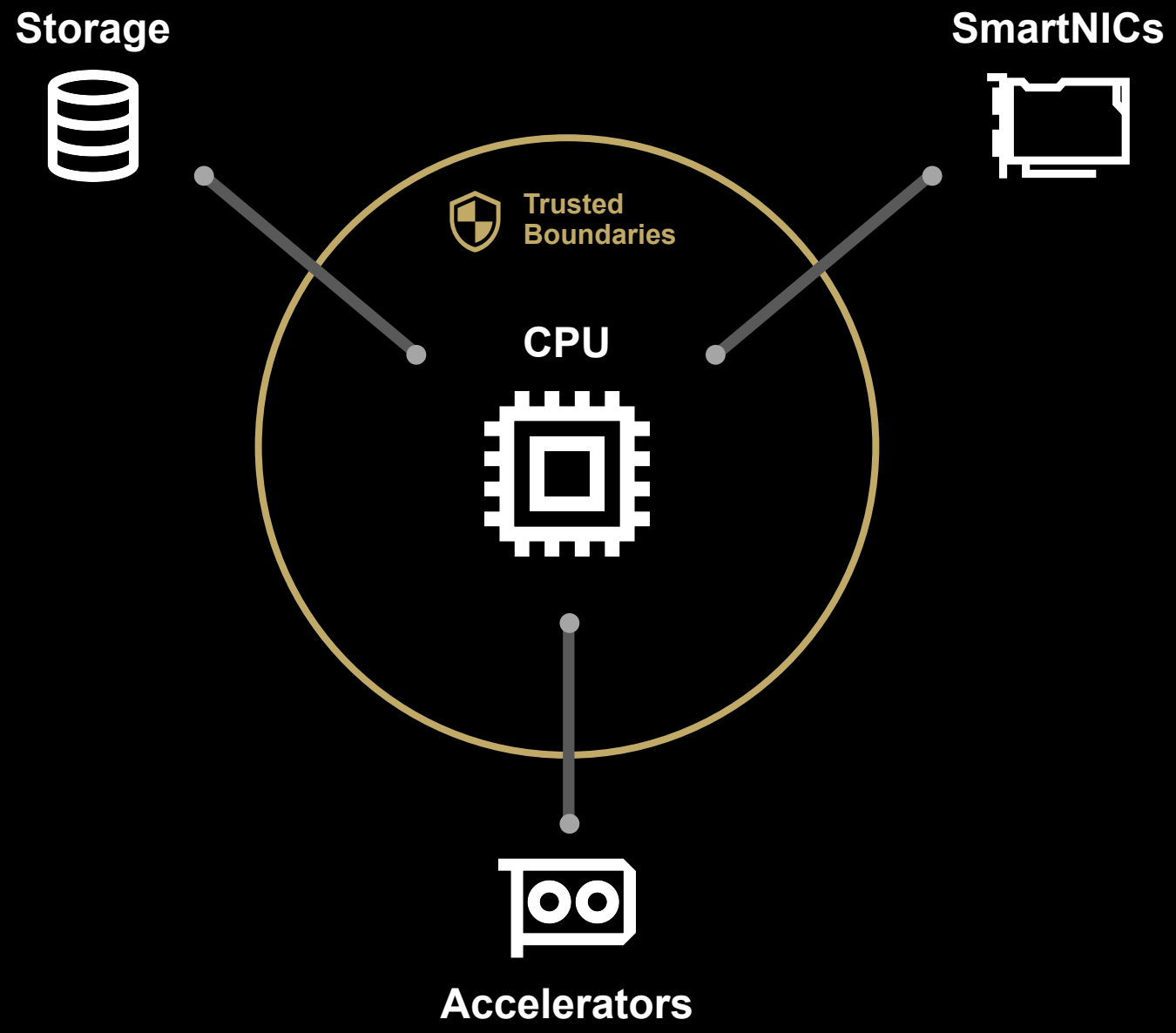
Only I can see my data

AI Will Drive Pervasive Confidential Computing

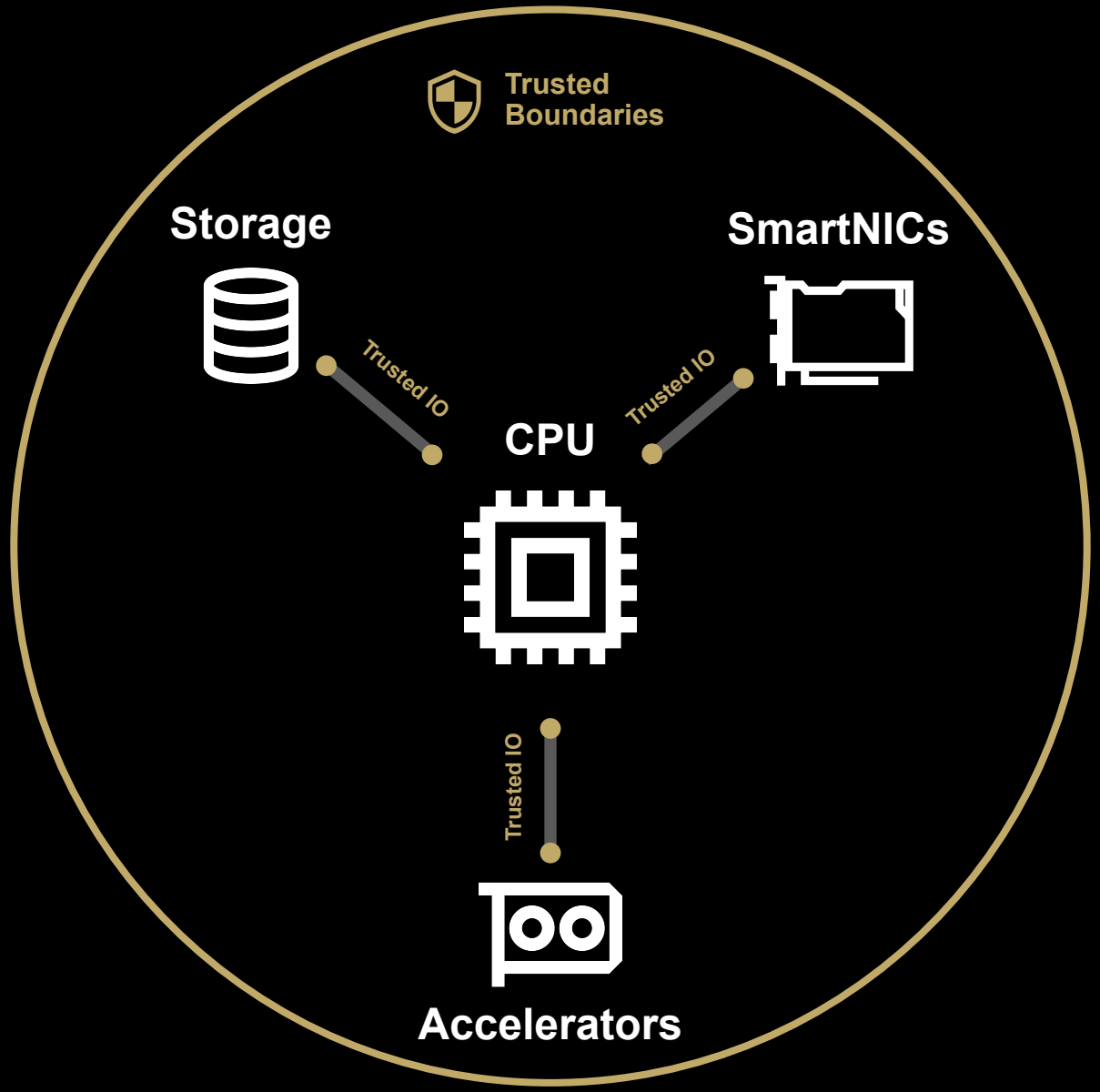
Protecting Data, Models And Weights

Critical at Every Phase of AI Processing

Challenges of Confidential AI



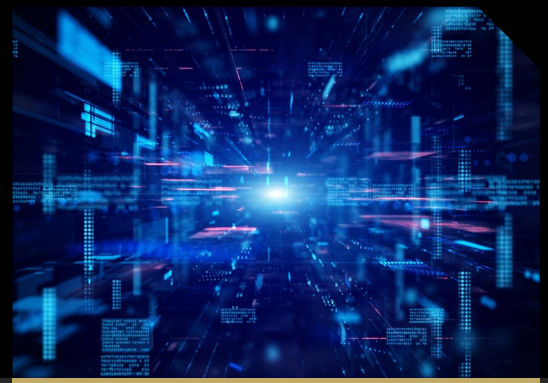
Enabling Confidential AI with Standardized Trusted IO



Why TDISP as Trusted IO for Confidential AI

Enhanced Security

Open Industry Standard



Interoperability

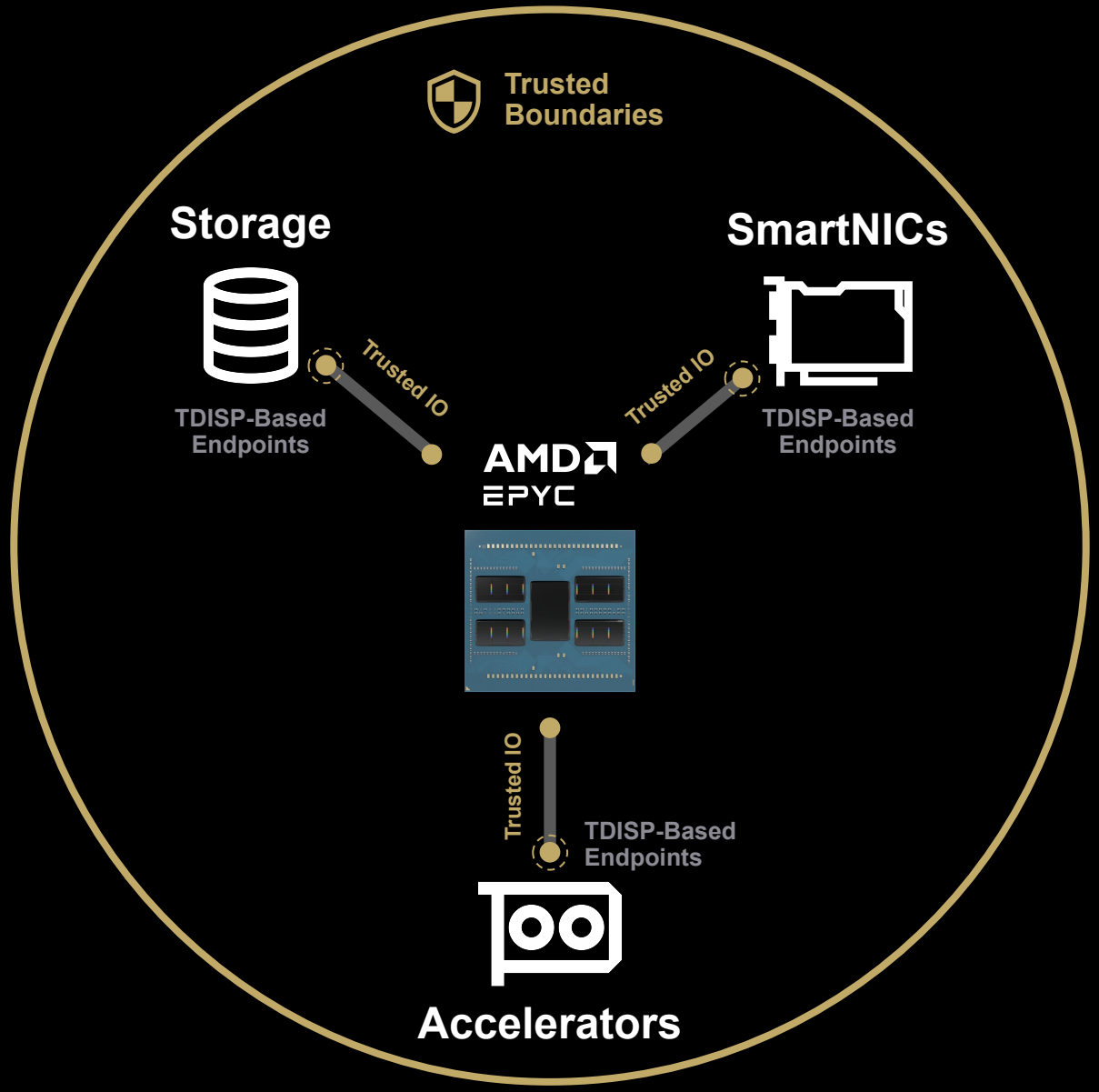
Scalability

PCI SIG

TEE Device Interface Security Protocol (TDISP)

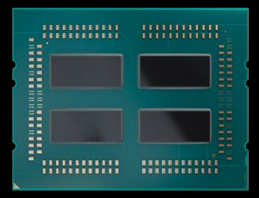
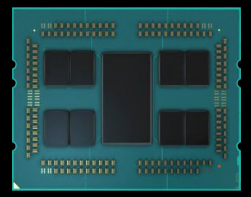
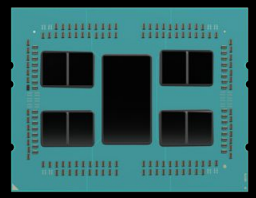
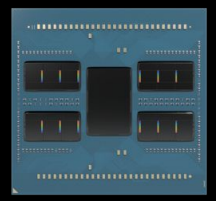
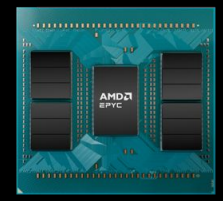
AMD Confidential AI

- **Open Standards and Interoperability**
- **Trust and Transparency**
- **Acceleration of Innovation**



AMD Infinity Guard

AMD EPYC™ CPU Journey

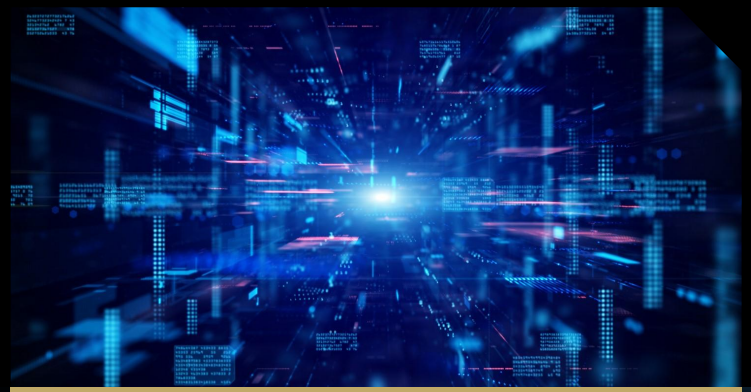
2017	2019	2021	2023	2024
1st Generation AMD EPYC™	2nd Generation AMD EPYC™	3rd Generation AMD EPYC™	4th Generation AMD EPYC™	5th Generation AMD EPYC™
‘Naples’	‘Rome’	‘Milan’	‘Genoa’	‘Turin’
Launched AMD Infinity Guard, including Secure Encrypted Virtualization (SEV)	Added SEV Encrypted State (SEV-ES)	Introduced SEV Secure Nested Paging (SEV-SNP)	AMD published the SEV-SNP firmware source code	World’s first CPU with TDISP Trusted IO

The Next Frontier for Confidential AI

Confidential Cloud

Confidential Computing on Edge & Devices

Open Standards Provide Critical Ingredients for the Success of Confidential AI



Interoperability

Trust and Transparency

Acceleration of Innovation

PCI SIG

CONFIDENTIAL COMPUTING CONSORTIUM

OPEN Compute Project®

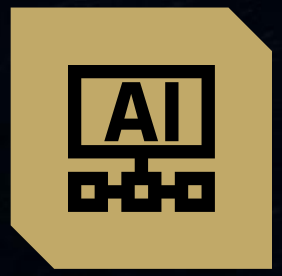
Caliptra

UALink

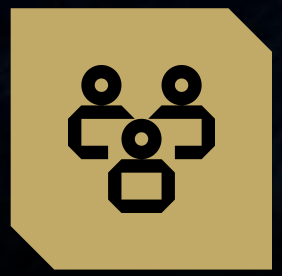
AMD Confidential AI

The Path Forward

AMD Infinity Guard first to deliver "no code touch“ confidential computing, foundational for Confidential AI



AMD has a solid roadmap for Confidential AI with strong industry collaboration



Calling on the ecosystem to build Confidential AI around open standards and trusted supply chain


AMD

Disclaimer

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions and typographical errors.

The information contained herein is subject to change and may be rendered inaccurate for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product releases, product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION.

AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY DIRECT, INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ATTRIBUTION

Other names used herein are for identification purposes only and may be trademarks of their respective companies.