PRODUCT BRIEF

AMD VERSAL™ TAMPER-RESISTANT DEVICES

Setting A New Bar for Tamper-Resistant Compute

AMD
together we advance_security

OVERVIEW

AMD Versal™ tamper-resistant (TR) devices are the industry's first FPGAs or adaptive SoCs with built-in protection against physical attacks on the silicon backside.[1] Through the use of 3D active-on-active technology, tamper-resistant adaptive SoCs[2] build on top of established foundational security elements to deliver backside protection for the entire device along with additional security enhancements to secure boot, key storage, glitch detection, and more. These capabilities help eliminate the need for custom security enclosures or ASICs, allowing developers to protect cryptographic keys, IP, and other critical data without compromising on performance, size, weight, power, or time to market.

Offered as part of the Versal AI Edge Series Gen 2, TR devices combine enhanced security[3] with proven heterogeneous compute engines: programmable logic, AI Engines for both DSP and ML workloads, and high-performance embedded CPUs – all in a single device. Each TR device has a standard, footprint-compatible counterpart, and designs built for the standard counterpart can migrate to the TR device without a redesign.

Versal tamper-resistant devices are backed by AMD design tools, IP, technical support, and partner ecosystem – allowing users to adopt and deploy these devices with confidence in security-critical systems.

HIGHLIGHTS

ENHANCED SECURITY WITH BUILT-IN BACKSIDE PROTECTION

- Full-device backside protection provided by cryptographically bound protection die
- CNSA 2.0 compliant with enhancements to post-quantum crypto secure boot
- Updated countermeasures to help defend against side-channel attacks

PROVEN HIGH-PERFORMANCE COMPUTE

- Up to 543k LUTs / 1.1M system logic cells of programmable logic
- AI Engines for DSP or ML with up to 369 INT8 TOPS (max sparsity)
- Up to 229k DMIPS scalar compute with application and real-time cores
- Standard Versal AI Edge Gen 2 devices in production since 2025

DEPLOY WITH CONFIDENCE

- Scalable device series – target the optimal device for a given use case
- Footprint compatible standard devices – build one board, populate TR device when needed; migrate designs without re-running synthesis, place and route
- Industry-tested AMD Vivado™, Vitis™, and Vitis AI design tools
- Backed by AMD IP, technical support, and partner ecosystem

KEY APPLICATIONS

INDUSTRIAL

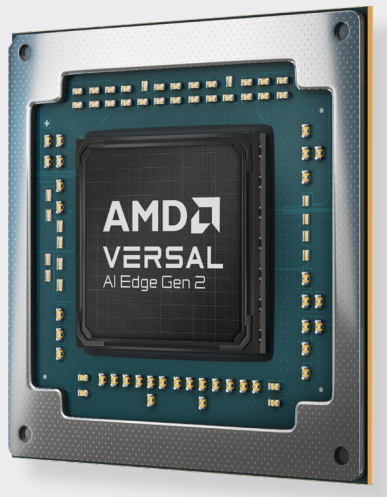
- Critical Infrastructure
- Energy and Grid Systems
- Industrial Control Systems

AEROSPACE & DEFENSE

- Avionics
- Mission Computing
- Communications

DATA CENTER

- Secure Networking
- Bank Infrastructure
- Sensitive IP Protection



FEATURES

FEATURE	HIGHLIGHTS
BUILT-IN BACKSIDE PROTECTION FOR FULL DEVICE	• Sensor-based protection die detects tamper events • Protection die cryptographically bound to user compute die • Detect and respond to physical compromise before sensitive asset exposure
FOUNDATIONAL SECURITY	• Application security unit (ASU) provides run-time HSM security • Platform management controller manages secure boot and device-level services • DDR memory controllers support inline encryption (AES-XTS or AES-GCM)
ADDITIONAL SECURITY ENHANCEMENTS	• New ML-DSA and SLH-DSA post-quantum crypto (PQC) secure boot hardware accelerators • ASU key vault enables enhanced ownership transfer • Improved glitch detection including new orthogonal glitch detector
SECURITY AND FUNCTIONAL SAFETY STANDARDS	• CNSA 2.0 compliant with support for Common Criteria • Support for DO-254/178, ISO26262, IEC61508, and other safety standards • Up to 100k DMIPS scalar compute at ASIL D (random), SIL 3
PROGRAMMABLE LOGIC (PL)	• Low-latency, deterministic, parallel processing • Fully customizable to enable differentiated, proprietary algorithms • Field-upgradeable: adaptable to changing conditions and evolving workloads
PROCESSING SYSTEM (PS) OF INTEGRATED CPUs	• Up to 8x Arm® Cortex®-A78AE application processors – up to 200k DMIPS • Up to 10x Arm Cortex-R52 real-time processors • Support for USB 3.2, DisplayPort™ 1.4, 10G Ethernet, PCIe® Gen5, and more
AI ENGINES	• AIE-ML v2 tile architecture for DSP or ML workloads • Expanded data type options – new FP8, FP16, MX6, MX9 support • MX6 & MX9: Shared-exponent data types designed to boost throughput and perf/watt
IMAGE AND VIDEO PROCESSING	• 4-core Arm Mali™-G78AE GPU supporting up to 4K60 2D/3D rendering • Up to 3 Image Signal Processor (ISP) tiles per device – up to 3.6 Gpix/s throughput, 15 camera streams in largest device • Hard video encode & decode support for HEVC & AVC up to 4K60, 4:4:4, 12-bit
DDR5/LPDDR5X MEMORY CONTROLLERS	• Support for DDR5 @ 6400 Mb/s and LPDDR5X @ 8533 Mb/s • Up to 170 GB/s memory bandwidth in the largest devices • Tightly integrated with high-bandwidth programmable network on chip
PROGRAMMABLE I/O & SERIAL TRANSCEIVERS	• High-performance X5IO for maximum speed; HDIO and MIO support logic levels up to 3.3V • MIPI C-PHY support (4.5 GS/s) and 4.5 Gb/s D-PHY support • Up to PL-facing 20 32G GTYP transceivers per device
100G ETHERNET AND PCIe GEN5	• 100G Multirate Ethernet MAC channelized for 1x100 GE, 2x50 GE, 1x40 GE, 4x25 GE, or 4x10 GE • PL-based support for PCIe Gen5 x4, Gen4 x8, and other configurations • Additional PS-specific PCIe, Ethernet interfaces

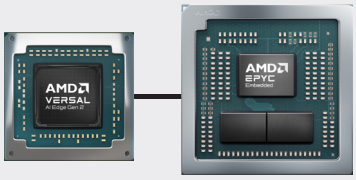
SCALABLE PORTFOLIO FOR SECURE COMPUTING

From Root of Security to Stand-Alone Scalable Secure Compute Platforms

The AMD tamper-resistant portfolio includes solutions that scale from Platform Root of Trust or Root of Security (ROS) devices to stand-alone secure compute platforms. As security and processing requirements increase, these devices offer varying levels of compute, programmable logic resources, and power consumption while maintaining a common trusted architecture.

	2VE3358TR	2VE3558TR	2VE3858TR
SIZE	31 mm x 31 mm	35 mm x 35 mm	40 mm x 40 mm
COMPUTE	229k DMIPS 61 TOPS 94k LUTs	229k DMIPS 246 TOPS 225k LUTs	229k DMIPS 369 TOPS 543k LUTs
USE CASE	ROS Companion	ROS Companion Stand-Alone Secure Compute Platform	Stand-Alone Secure Compute Platform

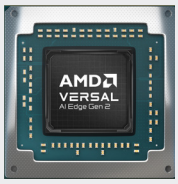
ROOT OF SECURITY COMPANION



ROS **Mission Processor**

- Secure Boot
- Attestation
- Key Storage

STAND-ALONE SECURE COMPUTE PLATFORM



- Trusted Execution
- Secure Processing
- Cryptographic Services

NEXT STEPS

For more information on Versal tamper-resistant devices, visit **www.amd.com/tamper-resistant**

For more information on Versal AI Edge Series Gen 2 adaptive SoCs, visit **www.amd.com/versal-ai-edge-gen2**

ENDNOTES

1. Based on AMD internal analysis in November 2026 of the anti-tamper security features (if any) and standard security features of competing FPGAs and adaptive SoCs. (VER-118)
2. Tamper-resistant does not mean tamper-proof. Protection applies to specified physical attack methods; see product documentation for the applicable threat model and limitations. (GD-256)
3. Based on AMD internal analysis in November 2026 of the security features of AMD Versal AI Edge Series Gen 2 2VE3358TR, 2VE3558TR, and 2VE3858TR devices versus previous AMD FPGAs and adaptive SoCs. (VER-117)

DISCLAIMERS

The information contained herein is for informational purposes only and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale. GD-18u.

COPYRIGHT NOTICE

© 2026 Advanced Micro Devices, Inc. All rights reserved. AMD, the AMD Arrow logo, EPYC, Versal, Vitis, Vivado, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Arm, Cortex, and Mali are registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. DisplayPort and the DisplayPort logo are trademarks owned by the Video Electronics Standards Association (VESA@) in the United States and other countries. PCIe is a registered trademark of PCI-SIG Corporation. Other product names used in this publication are for identification purposes only and may be trademarks of their respective owners. Certain AMD technologies may require third-party enablement or activation. Supported features may vary by operating system. Please confirm with the system manufacturer for specific features. No technology or product can be completely secure. PID5658552