AMD
together we advance_confidential computing

CONFIDENTIAL COMPUTING: A KEY TO ENHANCING SAFETY AND SECURITY IN FINANCIAL SERVICES OPERATIONS

CONFIDENTIAL COMPUTING HELPS PROTECT FSIS

Financial services institutions face an escalating conflict between aggressive modernization—cloud migration, AI deployment, digital assets, and data center consolidation—and stringent regulatory, privacy, and operational-risk requirements. Trading algorithms, fraud models, customer financial records, digital asset keys, and market-risk engines represent both competitive advantage and systemic risk.

Traditional security controls protect data at rest and in transit. But **data in use — when code manipulates sensitive data and models in memory — has remained exposed** to privileged insiders, compromised hypervisors, lateral movement after breach, and increasingly sophisticated supply-chain attacks. Confidential computing closes this gap by using hardware-based Trusted Execution Environments (TEEs) to encrypt memory and isolate workloads while they are actively running. Even the hypervisor, host operating system, cloud operator, or infrastructure administrator cannot access data in clear text. For financial institutions navigating AI expansion, cloud transformation, and escalating regulatory scrutiny, this represents a foundational security upgrade rather than an incremental feature.

WHY CONFIDENTIAL COMPUTING MATTERS NOW

- **Regulatory certainty**: Supervisors increasingly demand demonstrable controls over model governance, risk-data handling, and operational resilience. Hardware-based isolation and attestation provide verifiable evidence that approved workloads ran on approved platforms.
- **Risk reduction:** Insider threats, privilege abuse, and infrastructure compromise are among the most difficult risks to eliminate. Encrypting data in use can materially reduce the blast radius of these scenarios.
- **Security-focused cloud and AI enablement:** Confidential computing allows regulated analytics, AI model training and inference, and digital-asset services to run in public or hybrid clouds without exposing proprietary data, models, or cryptographic keys.
- **Improve TCO while maintaining separation:** Cryptographic workload isolation supports high-density, multi-tenant deployments without weakening logical or regulatory separation requirements.

BENEFICIAL STRATEGIC OUTCOMES

Confidential computing helps financial institutions:

- Accelerate migration of regulated workloads to cloud and hybrid environments.
- Deploy confidential AI systems that protect both sensitive input data and proprietary model parameters.
- Strengthen digital-asset custody by isolating key material and signing services.
- Simplify audit and supervisory engagement using attestation evidence and integrity validation.
- Reduce reliance on costly physical segregation by enforcing separation in hardware.

THE AMD CONFIDENTIAL COMPUTING PLATFORM

AMD EPYC™ Series CPUs with AMD Infinity Guard[1], a sophisticated suite of system-level security features, provide a hardware foundation for confidential computing that supports Zero Trust and high-density FSI data-center designs.

Every AMD EPYC CPU includes an AMD Secure Processor, a dedicated security subsystem that establishes a hardware root of trust and manages key material separately from the main CPU cores. AMD Infinity Guard builds on this with secure boot, memory encryption, and other hardware-based protections. AMD Secure Encrypted Virtualization (SEV), part of AMD Infinity Guard, is built into AMD EPYC 7000, 8000, and 9000 Series CPUs. It lets standard VMs and containers act as trusted execution environments (TEEs).

PORTABILITY FOR EXISTING WORKLOADS

A key advantage of confidential computing with AMD SEV is ease of deployment; no application code changes are required to help enable protection. FSIs can protect existing workloads—fraud models, risk engines, and digital-asset services—by migrating them into confidential VMs, without re-architecting the applications.

SEV focuses on keeping guest workloads private and tamper-resistant, even from the underlying infrastructure:

- **Per-VM memory encryption:** Each VM's memory is encrypted with a unique key; SEV can encrypt DRAM and supports CXL®-attached memory for large models and analytics jobs.
- **Guest integrity vs. malicious hypervisors:** Optional protections help defend against certain interrupt-injection, rollback, and side-channel attacks, reducing the risk that compromised infrastructure can silently observe or modify guest state.
- **Encrypted State and Secure Nested Paging:** Encrypted State helps protect CPU registers when a VM is paused or offline, while Secure Nesting Paging hardens page-table management, so hypervisors are restricted from arbitrarily remapping guest memory.
- **Trusted I/O:** In AMD EPYC 9005 Series CPUs, SEV extends the trusted boundary to PCIe®-attached devices (GPUs, NICs, storage) using the TEE Device Interface Security Protocol (TDISP), helping keep data protected as it moves between CPUs and accelerators, which is critical for AI, trading, and HPC workloads.

Across generations, SEV has strengthened cryptography and scale, moving to 256-bit AES-XTS encryption, supporting more encrypted threads and keys, and adding hardware features that further improve isolation and performance. The result is a platform that can host thousands of confidential VMs per host.

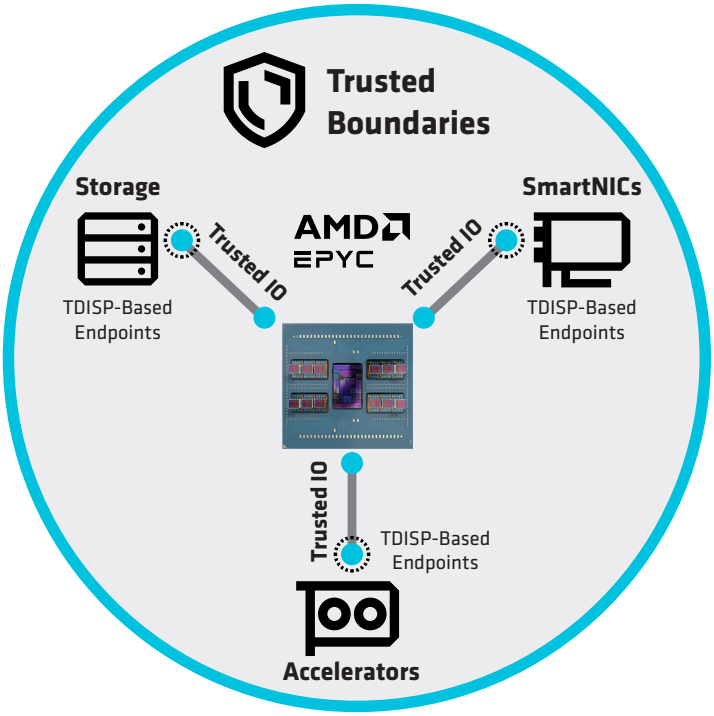

Figure 1: AMD SEV Trusted Boundary extending hardware-enforced isolation across CPU, memory, and TDISP-enabled I/O devices, including storage, SmartNICs, and accelerators.

CLOUD AND ON-PREMISES ECOSYSTEM

AMD EPYC CPU-based confidential computing is available across major public cloud providers and on-premises platforms, enabling flexible deployment models.

Cloud Provider	Confidential Computing Offering*
AWS	https://aws.amazon.com/confidential-computing/
Google Cloud	https://cloud.google.com/security/products/confidential-computing
Microsoft Azure	https://azure.microsoft.com/en-us/solutions/confidential-compute
Oracle Cloud Infrastructure	https://docs.oracle.com/en-us/iaas/Content/Compute/References/confidential_compute.htm

*VM availability and naming may change. Always refer to the cloud service provider's documentation for the latest details. Links to third party sites are provided for convenience and unless explicitly stated, AMD is not responsible for the contents of such linked sites and no endorsement is implied.

DATA CENTERS, MULTI-TENANCY, AND TCO

AMD EPYC™ server CPUs offer high core counts and memory capacity, enabling multi-tenant consolidation without sacrificing performance. Confidential computing can enhance the TCO story by:

- Enforcing strong isolation between tenants, business units, or legal entities sharing the same physical hosts, with a unique key per confidential VM
- Allowing sensitive workloads to run side by side with less sensitive ones while maintaining regulatory separation.
- Reducing the need for over-segmentation at the physical layer, freeing capacity while still satisfying segregation-of-duties and data-separation expectations.

By relying on hardware-based isolation and encryption-in-use rather than dedicated physical segregation, organizations can consolidate workloads, reduce infrastructure sprawl, and increase utilization of existing capacity. This shift helps enable institutions to lower capital and operational costs while increasing available capacity.

KEY FSI SECURITY CHALLENGES AND USE CASES

FSIs face a common set of high-impact security and compliance challenges where confidential computing can provide immediate value.

REAL-TIME FRAUD AND TRANSACTION ANALYTICS

Running fraud detection and transaction scoring inside TEEs helps prevent infrastructure-level access to transaction data during scoring, helps protect proprietary fraud models from insider exposure, and helps reduces risk from lateral movement within shared environments.

MARKET RISK AND TRADING ANALYTICS

Confidential computing helps protect proprietary pricing and risk models during execution, limits exposure of desk-level P&L calculations and supports secure execution in distributed or cloud-based environments.

CONFIDENTIAL AI AND MODEL GOVERNANCE

Using TEEs for AI workloads keeps training data and inference inputs encrypted in use, helps protect model weights and tuning parameters, and supports secure sharing of outputs or audit artifacts without exposing raw data.

DIGITAL ASSETS AND CRYPTOGRAPHIC SERVICES

Confidential computing isolates key material inside TEEs, helps protect signing services from privileged host access, and supports secure control-plane logic governing wallet tier transitions.

SOFTWARE SUPPLY CHAIN

Executing build, signing, and release processes inside TEEs helps protect source code and signing keys, helps reduce tampering risk within build infrastructure, and strengthens the integrity of deployed workloads.

BUSINESS IMPACT AND REGULATORY ALIGNMENT ACROSS FSIS

While regulatory priorities differ by segment and jurisdiction, most financial supervisory frameworks share common expectations around data confidentiality, operational resilience, segregation of duties, model governance, and demonstrable infrastructure integrity. Confidential computing aligns with cross-cutting control objectives across global frameworks, including GDPR, CCPA, GLBA, SOX, PCI DSS, PSD2, Basel III, FRTB, MiFID II, MAS Technology Risk Management guidelines, FedRAMP, and data sovereignty regimes in multiple jurisdictions.

SEGMENT	PRIMARY RISK CONCENTRATION	KEY REGULATORY DRIVERS	CONFIDENTIAL COMPUTING CONTROL	BUSINESS BENEFITS
Capital Markets	Trading algorithms, FRTB risk calculations, desk-level P&L	Basel III / FRTB, MiFID II, SEC reporting	Isolates trading engines and risk workloads in TEEs	Helps protect IP, strengthens reporting assurance
Payments	Transaction data, fraud analytics, key handling	PCI DSS, PSD2, GLBA	Encrypts authorization logic and fraud models in memory	Helps reduce fraud risk, supports secure modernization
Insurance	Health and financial underwriting data	GDPR, HIPAA, regional data laws	Helps protect AI underwriting and claims models in use	Supports secure AI-driven personalization
Retail and Commercial Banking	Credit scoring, AML analytics, customer records	GLBA, SOX, Basel III, GDPR/CCPA	Monitors regulated analytics workloads in confidential VMs	Supports cloud adoption with supervisory confidence
Digital Assets and Tokenization	Private key compromise, signing infrastructure	Emerging custody guidance, operational risk frameworks	Isolates key generation and signing services inside TEEs	Strengthens institutional custody posture

RECOMMENDED NEXT STEPS

1. Identify 3–5 high-value workloads that handle sensitive data or models.

2. Pilot those workloads on confidential VMs (cloud or on-premises) to validate performance and attestation workflows.

3. Engage with your AMD account team to review reference architectures and validated stacks.

Remember: confidential computing is becoming a foundational control for modern financial infrastructure because protecting data in use is essential to reducing operational risk and maintaining supervisory confidence.

AMD EPYC Series CPUs with Secure Encrypted Virtualization provide the hardware-rooted isolation you need to modernize. By supporting encryption-in-use, workload integrity, and cryptographic attestation, AMD confidential computing is designed to help sensitive workloads operate in shared and hybrid environments and supports secure innovation so you can deploy AI, scale cloud infrastructure, and optimize data center utilization with greater confidence.

AMD collaborates with major ecosystem partners to deliver confidential computing at scale. Your AMD representative can provide current information on supported platforms, reference designs, and third-party solutions relevant to your environment. To explore how AMD EPYC™ Server CPUs with SEV can help secure your core workloads, please visit:

- AMD EPYC Confidential Computing Solutions: An overview with use cases and platform information.
- AMD SEV on GitHub: Example code, tools, and community resources for SEV.
- AMD SEV Developer Resources: Documentation, guides, and implementation details for SEV.

1 AMD Infinity Guard features vary by EPYC™ Processor generations and/or series. Infinity Guard security features must be enabled by server OEMs and/or Cloud Service Providers to operate. Check with your OEM or provider to confirm support of these features. Learn more about Infinity Guard at https://www.amd.com/en/technologies/infinity-guard. GD-183A