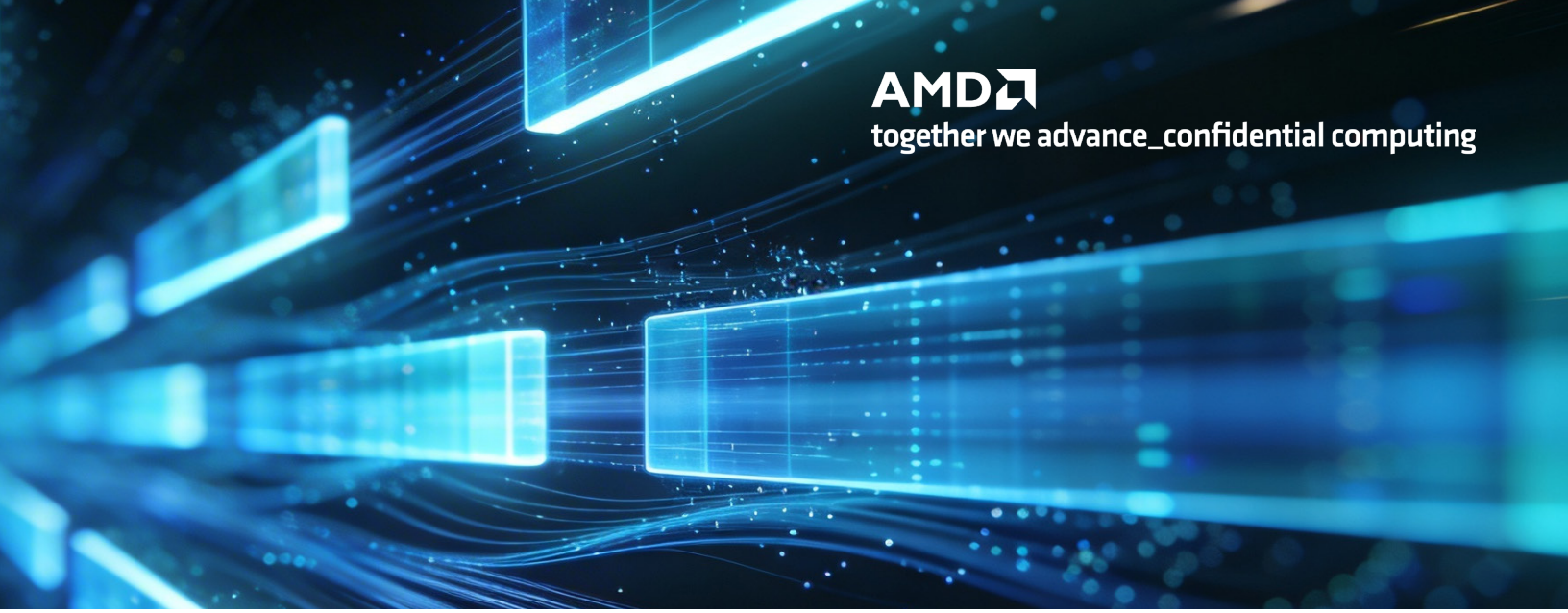
AMD
together we advance_confidential computing

PROTECTING THE PUBLIC SECTOR WITH CONFIDENTIAL COMPUTING



EXECUTIVE SUMMARY: CONFIDENTIAL COMPUTING HELPS SAFEGUARD THE U.S. PUBLIC SECTOR

Public sector organizations manage mission-critical systems and sensitive data in both connected and disconnected environments. Traditional security protects data at rest and in transit, but not data-in-use during computation. Confidential computing narrows this gap with hardware-based Trusted Execution Environments (TEEs) that isolate workloads and encrypt memory while code executes—including protections against access from privileged system software such as hypervisors and host administrators. It aligns with Zero Trust principles (NIST SP 800-207) and federal mandates (e.g., Executive Order 14028), supporting secure cloud adoption, privacy-preserving analytics, and resilient AI across the public sector.

AMD Confidential Computing, especially as implemented via its **Secure Encrypted Virtualization (SEV)** and related technologies built into AMD EPYC™ Series CPUs, offers these capabilities to address the security and compliance challenges public sector agencies face. This hardware-rooted isolation helps reduce the risk of unauthorized access.

PORTABILITY FOR EXISTING WORKLOADS

A key advantage of the AMD approach is that no application code changes are required to help enable protection; existing workloads can often be "lifted and shifted" into confidential VMs, an important consideration for agencies that commonly run legacy systems alongside modern analytical and AI-driven applications, systems that historically have been slow to move into cloud environments due to security concerns.

MARKET TRENDS DRIVING CONFIDENTIAL COMPUTING ADOPTION

Government agencies are modernizing legacy systems and accelerating the adoption of hybrid cloud, AI, and advanced analytics. These initiatives can increase exposure to insider threats, malware, and nation-state adversaries, especially when workloads run on shared or untrusted infrastructure. Confidential computing uses silicon-rooted isolation to help protect sensitive workloads during processing, supporting inter-agency collaboration and secure multi-tenant operations.

- **Cloud migration of regulated workloads:** Public sector organizations are moving critical applications to public and hybrid clouds and need strong assurances and controls for confidentiality and compliance.
- **Zero Trust architectures:** Modern security strategies assume breach and require hardware roots of trust and strict workload isolation.
- **Ecosystem maturity:** Major cloud providers now offer confidential VM services powered by AMD Secure Encrypted Virtualization (SEV), making adoption practical.

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 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 by incorporating secure boot, memory encryption, and other hardware-based protections.

AMD SEV, part of AMD Infinity Guard, is built into AMD EPYC 7000, 8000, and 9000 Series CPUs. It lets standard VMs act as TEEs. Containers running inside those VMs are designed to inherit the same protections without requiring application code changes, allowing agencies to migrate existing workloads into confidential VMs.

CONFIDENTIAL COMPUTING: CAPABILITIES AND EVOLUTION

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 encrypts DRAM and can operate with platforms supporting CXL®-attached memory expansion 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 potential for compromised infrastructure to observe or modify guest state.
- **Encrypted State and Secure Nested Paging:** Encrypted State is designed to help protect CPU register state during VM exits, limiting hypervisor visibility into guest registers, while Secure Nesting Paging helps harden page-table management to reduce the risk of arbitrary guest-memory remapping by the hypervisor.
- **Trusted I/O:** In AMD EPYC 9005 series CPUs, SEV can extend protections to devices through emerging PCIe® confidential-computing mechanisms such as TDISP and PCIe IDE (depending on platform and device support), helping support data protection as it moves between CPUs and accelerators, which is an important consideration for AI 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.

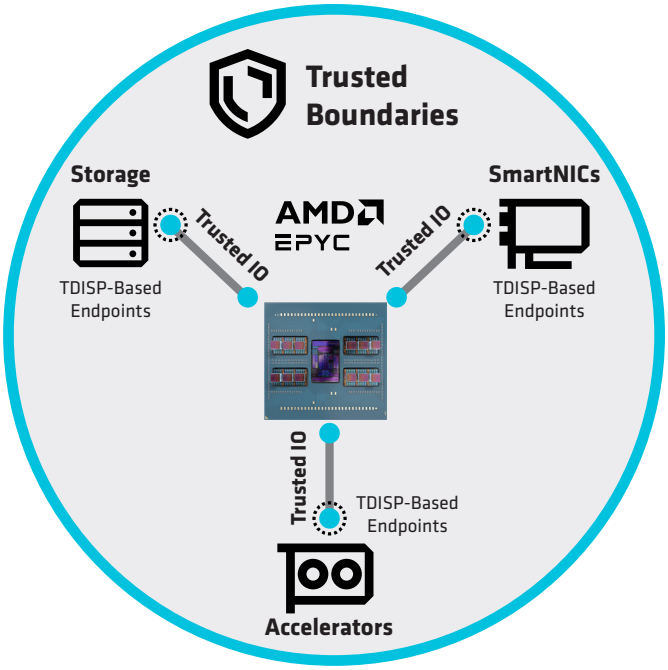


Figure 1: AMD SEV Trusted Boundary extending hardware-enforced isolation across CPU, memory, and TDISP-enabled I/O devices, including storage, SmartNICs, and accelerators.

CLOUD AND ON-PREMISES ECOSYSTEM

AMD Confidential Computing is available across major cloud and on-premises platforms, allowing public sector agencies to choose the deployment model that best fits each workload. Examples of SEV-powered confidential VM families include:

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.

USE CASES IN THE PUBLIC SECTOR

ZERO TRUST ARCHITECTURE: TRUST NO ONE AND ATTEST

Confidential computing supports silicon-level isolation and attestation, enabling policy-based access that treats hosts, networks, and administrators as untrusted. Identity-bound encryption, just-in-time keys, and inbound and outbound controls are designed to support least-privilege principles across multi-cloud and on-prem environments.

CYBERSECURITY: PROTECTING AND REDUCING THE ATTACK SURFACE

Security operations can analyze sensitive telemetry (endpoint events, network flows, and identity logs) within TEEs to detect advanced threats without exposing raw data. Cross-agency collaboration on indicators of compromise becomes feasible while preserving privacy. AMD SEV's confidential computing features are designed to improve cybersecurity by helping reduce the attack surface around data-in-use and strengthening protections at lower layers of the stack.

SUPPORTING SECURE MULTI-TENANCY AND CROSS-DOMAIN SOLUTIONS

AMD Confidential Computing is well-suited for secure multi-tenancy, using hardware-based isolation mechanisms designed to separate tenants from one another and from the underlying hardware layer, rather than relying solely on policy or hypervisor trust. AMD SEV encrypts each VM's memory with unique keys, helping limit the risk of lateral access by compromised hypervisors or co-resident tenants. An IT administrator could set up multiple confidential VMs, each having its own unique key, which provides protection via isolation of each user group in a multi-tenant scenario. This approach can support shared infrastructure and consolidation efforts while helping maintain strict data boundaries.

CRITICAL INFRASTRUCTURE OPERATIONS

Energy, water, transportation, and election applications benefit from confidential analytics that fuse OT telemetry, IT logs, and intelligence data. Responders can run playbooks inside attested enclaves, reducing the risk of key exfiltration and supporting trustworthy forensics and remediation.

DATA SECURITY AND PRIVACY

Agencies can process PII, PHI, and CJIS data in ways that help limit exposure of plaintext data to the underlying platform. Attestation evidence and audit trails can support compliance activities, while privacy-preserving joins may facilitate inter-agency data sharing (e.g., benefits eligibility, fraud reduction) with reduced data movement.

CRYPTOGRAPHY AND KEY MANAGEMENT

Confidential computing supports split-key operations, threshold signatures, secure key generation, and sealed storage as part of a design intended to help limit exposure of key material outside the TEE. Hardware-bound secrets and attested KMS integrations are designed to help protect tokens and certificates while supporting FIPS-aligned cryptographic services.

SOFTWARE SUPPLY CHAIN SECURITY

AMD takes a risk-based approach to managing our supply chain and utilizes third-party risk analytics to conduct an overall supply chain risk analysis. We also take measures to mitigate geopolitical risks by collaborating with leading semiconductor suppliers on a global diversification strategy that includes increased manufacturing in the U.S.

CONFIDENTIAL AI

Agencies can train and perform inference on sensitive datasets—such as health records, tax data, or intelligence sources—in ways designed to help limit exposure of raw data. Confidential computing is intended to help protect AI prompts, model parameters and inputs, supporting approaches such as federated learning and privacy-conscious multi-party analytics across agencies. The AMD Instinct™ MI400 family extends the confidential AI trusted domain to encompass the GPU, via TDISP.

REGULATORY COMPLIANCE AND FEDERAL MANDATES

Confidential computing supports compliance frameworks, including FedRAMP, CJIS, HIPAA, IRS Publication 1075, and GDPR for cross-border data. It aligns with U.S. Executive Order 14028 (Improving the Nation's Cybersecurity) and NIST SP 800-207 (Zero Trust Architecture). Attestation logs, encrypted memory, trusted I/O, and verifiable isolation contribute to least-privilege enforcement, data minimization, and auditability.

YOUR NEXT STEPS

By helping protect data in use, AMD supports public sector agencies and organizations in addressing regulatory requirements, mitigating insider and external threats, modernizing data centers, and pursuing cloud and AI-driven initiatives. Here are seven suggested next steps:

1. **Assess current risk exposure:** Identify workloads that process sensitive or classified data and evaluate relevant insider-threat and misuse scenarios.
2. **Align with applicable mandates:** Map confidential-computing capabilities to frameworks such as NIST SP 800-207 and EO 14028, and evaluate alignment with FedRAMP and FIPS 140-3 requirements for relevant systems.
3. **Engage ecosystem partners:** Explore cloud-based confidential-computing offerings for near-term use cases and consider on-premises Proofs of Record (POR) for mission workloads.
4. **Integrate into modernization roadmaps:** Prioritize confidential computing in procurement and architecture decisions, including secure AI initiatives.
5. **Communicate strategic value:** Position confidential computing as a risk-reduction, compliance, and agility enabler across agencies and shared services.
6. **Lean on Zero Trust:** Identify workloads and processes that are most vulnerable and build a zero trust model to integrate them.
7. **Test and Deploy:** Spin up a confidential VM on your cloud service provider of choice and deploy your existing workload without any software modifications.

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 Series CPUs with SEV can help secure your core workloads, we encourage you to dive deeper into our solutions and technical resources and engage with your AMD account team.

- 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.

Use these resources to identify candidate workloads, plan proof-of-concepts, and bring confidential computing into use across your environment.

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