CENSUS
Cybersecurity Engineering

CONFIDENTIAL COMPUTING OFFERING

ADDRESSING MODERN SECURITY CHALLENGES WITH ADVANCED TECHNOLOGIES

In an era of increasing data privacy regulations and sophisticated cyber threats, organizations must adopt Privacy Enhancing Technologies (PETs) to secure sensitive data throughout its lifecycle. Among these, **Confidential Computing**, coupled with Secure Virtualization, Root of Trust (RoT), and other cutting-edge security technologies, has emerged as a transformative enabler for securing workloads in environments where data privacy and integrity are critical.

For security-conscious organizations and products, integrating Confidential Computing provides a strategic opportunity to deliver robust, scalable, and compliant solutions. This becomes particularly challenging when leveraging a diverse technology stack, in the emerging multi-party business paradigm whose threat model distrusts previously trusted entities. CENSUS enables businesses to adopt these technologies effectively, securing data in use, establishing trust in non-collusive multi-tenant environments, and designing secure-by-default architectures.

CONFIDENTIAL COMPUTING TECHNOLOGIES AND THEIR ROLES IN PRODUCT SECURITY

Confidential Computing leverages a combination of advanced technologies, including Trusted Execution Environments (TEEs), Secure Virtualization, Hardware Attestation, and cryptographic enhancements, to protect sensitive data during computation. By isolating data within hardware-protected environments, Confidential Computing secures data at its most vulnerable state—while it is being processed.

BUSINESS USE CASES EMPOWERED BY CONFIDENTIAL COMPUTING

1. **SECURE MULTI-TENANT CLOUD ENVIRONMENTS:** Mitigate risks of hypervisor-level attacks and cross-VM breaches by isolating workloads in shared cloud environments, enabling industries like financial services to process sensitive transactions securely.
2. **AI/ML WORKLOADS:** Use GPU Confidential Computing to secure AI/ML models and training data in industries such as healthcare and autonomous systems, ensuring that sensitive datasets remain protected during computation.
3. **REGULATED ENVIRONMENTS:** Securely process **PII** and **PHI** while meeting stringent compliance requirements, enabling organizations to adopt cloud and edge platforms without compromising security.
4. **CONFIDENTIAL COLLABORATION ACROSS ORGANIZATIONS:**
   Federated Learning: Facilitate secure, collaborative AI model training across decentralized datasets without exposing raw data.
   Multi-Party Computation (MPC): Conduct secure computations across multiple parties, ensuring all contributions remain encrypted and private.
5. **BLOCKCHAIN AND DECENTRALIZED APPLICATIONS:** Enhance security for smart contracts and DeFi platforms by enabling tamper-proof computations within TEEs.
6. **PROTECTING DIGITAL RIGHTS:** Safeguard intellectual property and proprietary data during content creation and distribution.

HARNESSING CONFIDENTIAL COMPUTING THROUGH CENSUS SECURITY ENGINEERING SERVICES

CENSUS offers a comprehensive suite of Security Engineering Services that integrate Confidential Computing into your organization's product security strategy:

1. **SECURITY FOUNDATIONS CONSULTING (SFC):**
   - Define actionable security building blocks (e.g., **data isolation, secure multi-tenancy, secure edge computing**) powered by Confidential Computing.
   - Develop **Security Architecture Blueprints** to enable scalable and reusable secure product development strategies.
2. **ARCHITECTURE & DESIGN ENGINEERING (ADE):**
   - Design architectures incorporating Confidential Computing to address multi-tenant security, federated processing, and advanced AI/ML use cases.
   - Conduct **threat modeling** to mitigate risks specific to Confidential Computing environments.
3. **SECURITY POSTURE ASSESSMENT (SPA):**
   - Assess the resilience of Confidential Computing implementations against real-world threats, including side-channel and memory-based attacks.
   - Evaluate GPU Confidential Computing deployments for AI and data-intensive workloads.
4. **APPLIED SECURITY RESEARCH (ASR):**
   - Explore cutting-edge capabilities such as hypervisor-backed attestation, execution isolation compartments, and post-quantum cryptography to strengthen your Confidential Computing implementations.

This ensures that sensitive information remains encrypted and inaccessible to unauthorized entities, including privileged users like system administrators, malicious insiders, or even cloud service providers.

Technologies Enabling Confidential Computing

- **Trusted Execution Environments (TEEs):** Hardware-based solutions such as **Intel TME, AMD SME,** and **ARM TrustZone** create isolated environments for secure computation, preventing unauthorized access to data during its processing lifecycle.
- **Confidential Virtual Machines:** Technologies like **AMD SEV-SNP, ARM CCA** and **Intel TDX** extend TEE capabilities to virtualised workloads, enabling multi-tenant cloud environments to operate securely by isolating sensitive workloads.
- **Cryptographic Enhancements:** Confidential Computing integrates with cryptographic tools such as **secure key management**, ensuring seamless encryption and protection for data during processing.
- **Remote Attestation:** A critical feature of TEEs, remote attestation verifies the integrity and authenticity of the computing environment, ensuring workloads are executed in trusted environments.
- **On-the-fly Migration:** Virtualised TEE solutions provide optional VM migration capabilities of encrypted VMs without disclosing image data to the hypervisor layer.
- **GPU Confidential Computing for AI Workloads:** Emerging solutions like **NVIDIA Confidential Computing** extend TEE capabilities to GPUs, enabling secure execution of **AI/ML workloads**. This allows organizations to process sensitive AI datasets—such as healthcare records or financial data—without exposing raw information, while maintaining high-performance computation.
- **Zero Trust Integration:** Confidential Computing complements **Zero Trust architectures** by ensuring continuous verification of workloads, users, and devices, creating a robust and distributed security posture.

Key Benefits of Confidential Computing

- **Enhanced Privacy:** Protect sensitive data during processing, even in shared or third-party environments.
- **Regulatory Compliance:** Simplify adherence to data privacy regulations (e.g., **GDPR, HIPAA, PCI DSS**) by maintaining secure data-handling practices across its lifecycle.
- **Cloud and IoT Security:** Facilitate secure adoption of cloud and IoT technologies, mitigating trust concerns in multi-tenant and edge environments.
- **AI and ML Privacy:** Enable secure training and inference on sensitive AI datasets by leveraging GPU Confidential Computing.
- **Operational Flexibility:** Support secure collaboration and processing across distributed teams without risking exposure of sensitive data.
- **Future-Ready Security:** Address emerging threats in blockchain, decentralized finance (DeFi), multi-tenant cloud, and edge computing ecosystems.

WHY CHOOSE CENSUS CONFIDENTIAL COMPUTING OFFERING?

CENSUS brings together in-depth cybersecurity engineering expertise, a real-world attacker mindset, and innovative applied research to deliver tailored, end-to-end solutions that address your business needs. Whether you're securing AI-powered applications, enabling multi-tenant workloads, or meeting stringent compliance mandates, CENSUS empowers your organization to excel in cybersecurity resilience and innovation.

Our Key Differentiators

1. PLATFORM SECURITY EXPERTISE:

- Extensive experience in security posture assessments, security architecture development, and security controls implementation.
- Applied research and development expertise across virtualization platforms such as AMD SEV-SNP, ARM CCA, ARM (S)EL2 SecureHyp, Intel TDX, KVM, and crosvm.
- Extensive expertise in public cloud Confidential Computing capabilities, developed through ongoing projects and partnership programs with major cloud providers.
- Robust support for private cloud platforms such as OpenStack and vSphere, ensuring secure implementation of Confidential Computing technologies.

2. FUTURE-READY EXPERTISE:

- Proactive strategies to address emerging threats and adopt next-generation technologies, ensuring your organization remains ahead of evolving security challenges.

3. SEAMLESS INTEGRATION:

- Delivery of practical and actionable security architecture blueprints tailored for immediate implementation, minimizing disruption to existing processes while maximizing security impact.

4. COMPREHENSIVE COVERAGE:

- Holistic «shift-left» strategies to protect your data and workloads across all phases of the product lifecycle—from design and prototyping to integration and deployment.
- Expertise in securing edge computing and cloud platforms (public or private), enabling secure operation in complex, distributed environments.

Unlock the potential of Confidential Computing with CENSUS and transform your product security into a strategic advantage. With CENSUS as your partner, you gain access to cutting-edge expertise and practical solutions that enhance security, foster innovation, and build trust across your organization and customer base.

USA
607 Boylston Street,
Suite 165L, Boston, MA 02116
T. +1 8882 029 846
E. usa@census-labs.com

UK
Unit 2.15 Barley Mow Centre
10 Barley Mow Passage
W4 4PH, London
T. +44 1293 324 069
E. uk@census-labs.com

EUROPE
128 A. Siggrou Ave.,
Athens 117 45, Greece
T. +30 210 220 8989-90
E. eu@census-labs.com

ABU DHABI
Office 110 - First Floor
Incubator Building
Masdar City, Abu Dhabi
United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

DUBAI
Unit GA-00-SZ-L1-RT-201, Level 1
Gate Avenue - South Zone
Dubai International Financial Centre
Dubai, United Arab Emirates
T. +971 8003 110 047
E. uae@census-labs.com

www.census-labs.com