Omdia
by informa techtarget

Securing the Modern Enterprise

Confidential computing in private cloud deployments

Author: Roy Illsley

May 2026

In partnership with:

BROADCOM

This Omdia White Paper was commissioned by Broadcom.

Contents

This Omdia White Paper was commissioned by Broadcom.

Summary

Catalyst

Confidential computing (CC) is revolutionizing security by addressing one of the most critical challenges in modern IT: protecting sensitive data while this data is being processed. It is not just in public cloud (hybrid or multicloud) environments but also in private clouds that organizations face increasing risks and threats, such as supply chain vulnerabilities and regulatory pressures. CC capabilities offer a robust solution to these challenges, enabling enterprises to secure workloads in trusted execution environments (TEEs) without compromising operational efficiency.

Omdia view

The CC market is experiencing significant growth, driven by the increasing need for data privacy, regulatory compliance, and secure cloud adoption. Technologies such as AMD SEV-SNP and Intel TDX, integrated into platforms such as Broadcom's VMware Cloud Foundation (VCF), are setting new benchmarks for data security by isolating workloads in hardware-based TEEs. However, challenges such as implementation complexity and cost remain barriers to widespread adoption. The future of CC lies in its ability to integrate seamlessly with artificial intelligence / machine learning (AI/ML) workloads, private (sovereign) cloud, hybrid cloud strategies, and zero-trust architecture, making it a cornerstone of next-generation IT infrastructure.

CC in private cloud environments is a topic customers should prioritize, because it addresses critical concerns around data security, compliance, trust, and innovation and is

simpler to deploy than in hybrid multicloud environments. As threats evolve and regulations tighten, adopting CC is not just a technical decision; it is a strategic imperative for safeguarding business operations and enabling future growth.

Confidential computing is a strategic imperative for private cloud security

A critical capability to ensure data privacy and security

CC in private cloud environments is rapidly emerging as a critical topic for customers because of the increasing need for robust data security, regulatory compliance, and trust in digital operations. As organizations manage sensitive data such as financial records, healthcare information, and intellectual property, the risks associated with data breaches and cyberattacks have grown. CC addresses these challenges by ensuring that data remains protected even while it is being processed in the CPU, which is a traditionally vulnerable stage.

One of the primary reasons why customers should care about CC is its ability to mitigate risks associated with unauthorized access, data leakage, privileged-user attacks, hypervisor vulnerabilities, and hardware exploits. By leveraging technologies such as TEEs and secure enclaves, CC ensures that sensitive workloads are processed in isolated environments, inaccessible to even privileged users or administrators. This is particularly important in private cloud settings, where organizations often retain full control over their infrastructure but still face risks from internal actors or compromised systems. However, for insider threats, it depends on the type of threat: there are still lots of separate ways an attacker can steal data, especially if they have administrator credentials. CC is not going to mitigate a vulnerability in the guest operating system, but it does create isolation between infrastructure layers to protect against unknown and malicious neighboring workloads.

Regulatory compliance is a major driving factor. The EU's Digital Operational Resilience Act (DORA), which became fully enforceable January 17, 2025, mandates strict cybersecurity standards for financial entities and their ICT service providers. A key challenging aspect of DORA is the requirement to protect data, not only at rest and in transit but also in use. Sectors such as financial services, healthcare, and government are also subject to stringent data protection regulations, including the EU’s General Data Protection

Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) in the US, and PCI DSS. CC provides verifiable security measures, such as attestation mechanisms, that demonstrate compliance with these standards. For customers operating in highly regulated sectors, adopting CC in their private cloud strategy is not just best practice; it is often a necessity to avoid legal penalties and reputational damage.

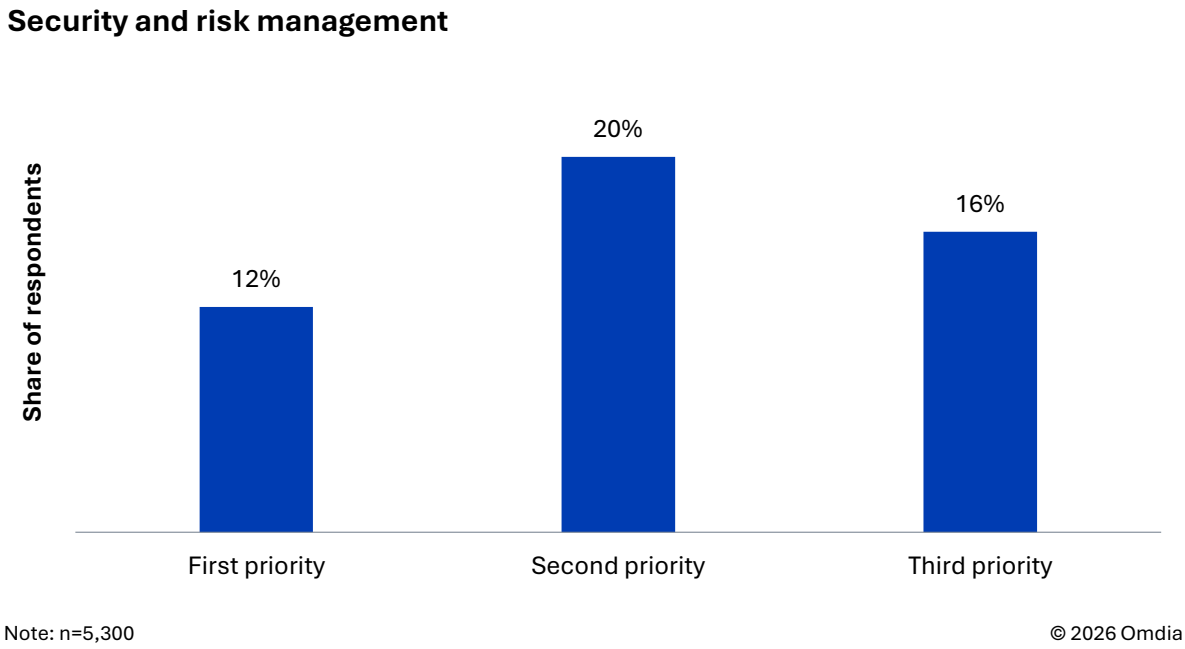
Moreover, CC enhances trust in private cloud environments. As organizations increasingly adopt private clouds alongside public cloud services, ensuring consistent security across diverse platforms becomes challenging. CC technologies, such as those integrated into VCF, enable seamless protection of sensitive workloads, regardless of where those workloads are deployed. This interoperability is crucial for customers seeking to optimize their IT infrastructure without compromising security.

Finally, CC aligns with broader business goals, such as innovation and competitive advantage. By securing sensitive data during processing, organizations can confidently leverage advanced technologies such as AI and ML to extract insights from their data. This unlocks new opportunities for growth while maintaining the highest levels of security.

In summary, CC in private cloud environments is a topic customers should prioritize, because it addresses critical concerns around data security, compliance, trust, risk management, and innovation. As threats evolve and regulations tighten, adopting CC is not just a technical decision; it is a strategic imperative for safeguarding business operations and enabling future growth. **Figure 1** shows that in 2026, CIO attitudes to security and risk remain a priority: 48% of respondents put it as a top-three priority.

This Omdia White Paper was commissioned by Broadcom.

Figure 1: Attitudes to security and risk management in 2026



Source: Omdia ITEI Survey 2025/26

Organizations should adopt the most relevant technological approaches to delivering confidential computing

Once an organization recognizes that CC is a strategic imperative, the next step is to deploy the relevant technologies that will deliver the outcomes desired. This stage requires an understanding of the core capabilities that are needed to deliver CC effectively.

TEEs are hardware-based secure areas within a processor that isolates sensitive data and code during execution. TEEs ensure that data remains encrypted and inaccessible to unauthorized entities, including the operating system, hypervisor, or even cloud providers. Secure enclaves are the isolated “room” where secure processing happens, while a TEE is the “secure environment” established by that isolation. Common implementations include Intel TDX, AMD SEV-SNP, and Arm TrustZone. TEEs are critical to CC, because they protect data in use, addressing a significant gap in traditional encryption methods that only secure data at rest or in transit. However, challenges such as side-channel attacks (e.g., hardware exploits such as Spectre and Meltdown) and compatibility with legacy systems remain areas of concern.

Cryptographic attestation is a mechanism that verifies the integrity and trustworthiness of a TEE before sensitive workloads are executed. It provides cryptographic proof that the TEE

is operating in a secure state and running genuine, unaltered code. This process involves generating attestation reports that external systems can validate, ensuring that only trusted environments manage sensitive data. Attestation is essential for building trust in CC, particularly in private, hybrid, and multicloud environments where workloads may span more than one platform. Recent advances, such as remote attestation protocols, have enhanced scalability and interoperability, making it easier for organizations to adopt CC.

Hardware-based isolation underpins the security of TEEs by creating a physical boundary that separates sensitive workloads from the rest of the system. This isolation ensures that data and code within the TEE are protected from unauthorized access, even if the operating system or hypervisor is compromised. Techniques such as encrypted memory and secure-enclave page caches further enhance this isolation.

Implementing confidential computing requires organizations to understand the choices available

Though CC delivers a robust solution to ensuring data privacy and security, it may not be required for all workloads because CC relies heavily on hardware-based technologies such as TEEs and secure enclaves, which require specialized processors. These hardware requirements mean organizations must consider compatibility between those workloads needing CC and any legacy systems. Organizations must also be aware that implementing CC may require the infrastructure to be upgraded to offset any performance overhead from encrypting and isolating data during processing.

Another aspect of integrating CC into existing environments that organizations must consider is the need for specialized expertise in cryptographic protocols, attestation mechanisms, and secure workload orchestration. Many organizations face a skills gap, and CC is a niche area requiring specialist knowledge, so organizations should look for solutions that reduce the implementation complexity, such as deploying these in private cloud environments rather than hybrid and multicloud environments.

For example, managing encryption keys securely across distributed systems is challenging, especially in hybrid or multicloud setups, but this is less of a challenge for private clouds. Attestation mechanisms are often complex and require coordination between hardware vendors and operating software environment providers. Vendor dependencies in the hardware can also raise concerns about lock-in and long-term support for CC technologies. However, the software layer, such as VCF, is working to eliminate some of the complexities surrounding key management and reduce the concerns about vendor lock-in.

Organizations must exploit the capabilities of the software layer to reduce complexity, optimize workloads, and collaborate with vendors to unlock the full potential of CC. As adoption grows, advances in scalability and standardization are expected to reduce barriers and drive broader adoption.

Recognizing confidential computing's value and identifying its key aspects

Understanding the risk of not using confidential computing

Private cloud environments face unique security and privacy challenges. They offer more control than public clouds, but they are still vulnerable. Traditional security measures, such as firewalls and encryption, protect data at rest (when stored) and in transit (when moving across networks). However, they cannot secure data while it is being processed, leaving a critical gap that attackers can exploit.

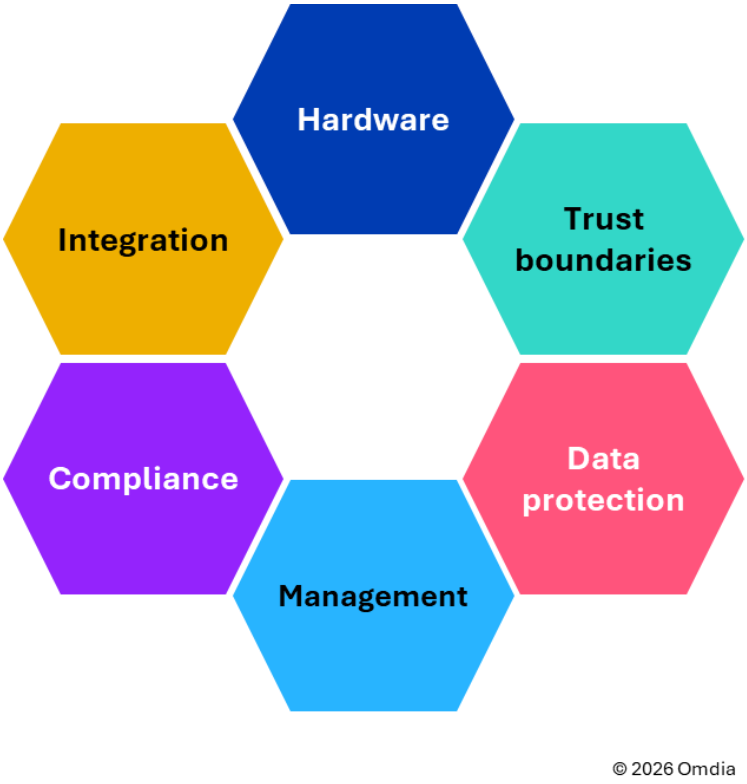
CC fills this gap by ensuring that data remains encrypted even during computation. For example, a healthcare provider analyzing patient data for research can use CC to ensure that sensitive information is protected throughout the process, even from administrators or IT staff managing the infrastructure. Similarly, financial institutions can securely process transactions or run fraud detection algorithms without exposing sensitive customer data.

This technology is particularly valuable for organizations in regulated industries, where compliance with data protection laws such as GDPR or HIPAA is mandatory. It also enables secure collaboration between organizations, allowing them to share and analyze data without compromising privacy. In summary, traditional security measures are no longer sufficient to address modern data protection challenges. CC provides a practical solution by securing data during processing, ensuring privacy, and enabling trust in private cloud environments. For end users, this means greater confidence in the security of their sensitive information and the ability to leverage cloud technologies without compromising privacy. CC also unlocks new opportunities for innovation by enabling secure multiparty computation, where organizations can collaborate on data analysis without exposing their proprietary information. This is particularly valuable in AI and ML, where sensitive datasets can be processed securely to extract insights. Furthermore, CC supports data sovereignty by ensuring that data remains protected even in geographically distributed environments, addressing concerns about jurisdictional compliance.

This Omdia White Paper was commissioned by Broadcom.

What “good” confidential computing looks like

Figure 2: Key considerations in any CC environment



Source: Omdia

Organizations thinking of adopting CC should consider the key aspects shown in **Figure 2**, which are summarized below.

Hardware security foundations

- TEEs and secure enclaves isolate sensitive data during processing, ensuring it remains encrypted and inaccessible to unauthorized entities.
- These technologies are critical for protecting against hardware vulnerabilities.
- Compatibility with legacy systems and performance overhead can be concerns.
- Broadcom VCF supports AMD SEV-SNP, AMD SEV-ES, and Intel TDX & SDX, enabling secure processing in private cloud environments.

This Omdia White Paper was commissioned by Broadcom.

Trust boundaries and attestation mechanisms

- Attestation mechanisms validate the integrity of the hardware and software stack, ensuring a trusted execution environment.
- They provide verifiable proof of security, which is essential for regulatory compliance and customer trust.
- Implementing attestation across diverse hardware platforms can be complex.
- VCF's built-in attestation capabilities ensure secure deployment of workloads.

Data protection layers

- CC protects data while it is being processed.
- Comprehensive data protection is essential for meeting compliance requirements and mitigating risks.
- Balancing security with performance and cost can be difficult.
- VCF integrates secure storage (vSAN ESA) and encrypted communication protocols to protect data.

Management and orchestration components

- In VCF, components such as VMware vSphere and NSX provide centralized management and orchestration of workloads and networks.
- This simplifies deployment and monitoring of confidential workloads, reducing operational complexity.
- Compatibility with existing tools must be ensured, and staff trained on new systems.

Compliance and governance frameworks

- Integrated dashboards and policies ensure that security and compliance requirements are met.
- This is essential for industries with strict regulatory requirements, such as finance and healthcare.
- It is critical to keep up with evolving regulations and ensure consistent enforcement.

- VCF's SecOps dashboard provides real-time insights into compliance and security.

Integration points with existing infrastructure

- VCF's hybrid and multicloud support enables seamless integration with existing IT systems.
- This reduces migration costs and leverages existing investments in infrastructure.
- Operability with existing infrastructure is necessary, and hybrid environments must be managed.
- VCF's compatibility with AI workloads and GPU-level precision makes it ideal for modern applications.

Overview of VCF's confidential computing capabilities

How VCF addresses private cloud security challenges with confidential computing

VMware Cloud Foundation is a unified private cloud platform that combines the scale and agility of public cloud with the security and performance of private cloud to deliver increased productivity and, according to VMware, a lower TCO. The platform modernizes infrastructure with integrated, enterprise-class compute, networking, storage, management, and security across all endpoints. Automated infrastructure and intelligent operations optimize performance, lower costs, and reduce operational overhead.

Organizations can accelerate innovation by using a self-service infrastructure-as-a-service (IaaS) platform that delivers a modern cloud interface to run VMs, containers, and AI workloads. Built-in security and resiliency safeguard businesses, ensure business continuity, and free up teams to focus on innovation rather than responding to security threats.

VCF's support for the latest confidential computing technologies such as AMD SEV-SNP and Intel TDX enables organizations to leverage the newest generation of secure enclaves, encrypted memory, and attestation capabilities, allowing IT teams to deploy confidential workloads across heterogeneous infrastructure while maintaining consistent security policies and operational workflows.

This Omdia White Paper was commissioned by Broadcom.

Appendix

Roy Illsley, Chief Analyst, IT Operations
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B Materials information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.