White Paper

Unlocking the Future of Data Security: Confidential Computing as a Strategic Imperative

Sponsored by: Confidential Computing Consortium

Philip Bues
November 2025

IN THIS WHITE PAPER

Executive Summary

In today's interconnected world, organizations of all sizes across industries face unprecedented challenges in safeguarding sensitive data. From healthcare providers managing patient records to financial institutions processing transactions, and from manufacturers protecting intellectual property to governments securing national infrastructure, the risks of data breaches, compliance violations, and operational disruptions are escalating. Traditional security measures, such as encrypting data at rest and in motion, remain foundational and are effective for many use cases, but they do not secure data being actively processed or analyzed, potentially creating a risk of inadvertent exposure or sophisticated cyberthreats. Confidential Computing emerges as a promising solution, addressing this vulnerability by securing data in use through hardware-based and cryptographically attested trusted execution environments (TEEs). This security gap has become urgent, accelerated by the massive data-processing demands of AI and LLMs. These technologies expose the limitations of traditional security and underscore the critical need to protect data and intellectual property (i.e., proprietary models) during computation. As a result, Confidential Computing recognition is growing as a modern business enabler fostering trust in data-driven business models.

This white paper presents findings from IDC's July 2025 *Confidential Computing Study* of 600 global IT leaders. The results show rapid adoption: 75% of organizations are already using Confidential Computing, with 18% in production and 57% actively piloting Confidential Computing. The paper explores its transformative potential in addressing modern security challenges, driving regulatory compliance (like EU DORA), and enabling innovative use cases such as secure AI and multiparty data collaboration.

November 2025, IDC #US53866125

The 600 global study respondents represent a manager role or higher across 15 industries varying in size from 500 to 10,000 employees. Most importantly, all respondents are involved in specifying or developing technology systems to process confidential or regulated data on a weekly basis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Definition

Confidential Computing is defined as the protection of data that is actively in use by performing computation in a hardware-based, attested trusted execution environment (TEE). These secure and isolated environments prevent unauthorized access or modification of applications and data while in use, thereby increasing the security assurances for organizations that manage sensitive and regulated data. Confidential Computing is intended to be used in conjunction with storage and network encryption, thereby protecting data at rest, in transit, and in use. No technology provides a security "cure-all", but Confidential Computing delivers new capabilities that significantly strengthen existing use cases and enables new deployment models.

Evolution of Data Security Technologies

The journey to Confidential Computing represents an evolution in data security technologies, driven by the increasing complexity of digital ecosystems, the proliferation of sensitive data, and the need for robust privacy and compliance measures. This evolution can be categorized into three additive stages: encryption of data at rest, encryption of data in motion, and encryption of data in use.

- **Stage 1: Encryption of data at rest** focuses on securing data stored on physical devices. Technologies like file and disk encryption ensure sensitive information remains protected when not actively accessed and remain a best practice for many organizations.
- **Stage 2: Encryption of data in motion** protects data during transmission across networks, such as emails, web traffic, and API calls. Protocols such as TLS and SSL safeguard data as it moves between endpoints. While effective for securing data in transit, encryption is removed during processing, potentially leaving data exposed.
- **Stage 3: Encryption of data in use** addresses the remaining security gap by protecting data actively being processed in the CPU and memory. Confidential Computing leverages TEEs to isolate sensitive workloads, ensuring data integrity and confidentiality during computation. It is important to note that some organizations may address these risks through alternative privacy-enhancing technologies, such as secure multiparty computation or homomorphic encryption, depending on their specific requirements and risk profiles. Confidential Computing enables a foundational rethink of identity not just for users but also for chips, workloads, and other entities by providing independent attestation. This attestation delivers verifiable proof of both the TEE's security state and the unique identity of participating components,

significantly enhancing trust and compliance. This approach embodies the principles of zero trust.

A TEE is a foundational component of Confidential Computing — it is an isolated view within a processor designed to protect sensitive data and code while being processed. As a hardware-based technology, TEEs can isolate critical workloads from unauthorized access, tampering, or exposure, even if the broader system is compromised. TEEs offer several key features, including:

- **Isolation** ensures that sensitive data and code are executed independently from the host operating system or hypervisor. This isolation is hardware enforced, adding to its resiliency.
- **Confidentiality** is maintained by encrypting data within the TEE, so external entities cannot access it.
- **Integrity** is protected by safeguarding data and code against tampering or malicious modifications, ensuring that only authorized changes can occur.
- **Attestation** allows the TEE to provide cryptographic proof of its security state to external systems, enabling third parties to verify that the environment is operating securely and as intended.

Each stage builds on the previous, evolving to address emerging vulnerabilities in increasingly complex digital ecosystems. Confidential Computing represents the latest advancement, focusing on securing data throughout its life cycle, particularly during computation. IDC believes that investing in Confidential Computing is not just a security measure but a strategic enabler for business resilience, regulatory compliance, and competitive differentiation, particularly in industries handling sensitive data or leveraging AI-driven innovation.

FINDINGS

Confidential Computing

The Confidential Computing Consortium, established in 2019, has played a pivotal role in advancing the security of data while it is actively being processed commonly referred to as "data in use." According to IDC research, market awareness of Confidential Computing is rising rapidly: 73% of surveyed organizations are either familiar with the concept (42%) or report being very familiar (31%). This growing awareness is being accelerated by regulatory frameworks such

- Confidential Computing Consortium was founded in 2019 to advance data security in use.
- IDC study reveals that 73% of respondents are familiar with confidential computing, 31% of which are very familiar.
- Regulatory frameworks like EU DORA are driving adoption, mandating high standards for data confidentiality, integrity, and availability.

as the European Union Digital Operational Resilience Act (EU DORA), which mandates stringent standards for data confidentiality, integrity, and availability across all states at rest, in motion, and in use. These regulations are driving organizations to seek out solutions that can meet these high standards, especially as data privacy and sovereignty requirements become more complex and costly to manage. In addition, leading security organizations such as the Cloud Security Alliance (CSA) and the Center for Internet Security (CIS) have recognized the importance of TEEs to further strengthen data protection during active processing.

Finding 1: Adoption Accelerates as Awareness Hits Critical Mass

Confidential Computing is gaining traction as organizations recognize the urgent need to secure sensitive data during computation, not just at rest or in transit. IDC data shows that 44% of organizations conduct analyses where sensitive data sets must be combined in a privacy-preserving fashion. Confidential Computing is highly relevant to this practice because it enables computation, collaboration, and analytics across data sets without exposing raw information to any party. As a result, organizations are increasingly exploring or planning initiatives in this space (see Figure 1). 75% of organizations are already in production (18%) or piloting/testing (57%), with another 19% planning deployment within 24 months. This momentum reflects a broader shift toward securing data in use, driven by the need to mitigate urgent threats and enable secure collaboration in environments where sensitive data is routinely handled.

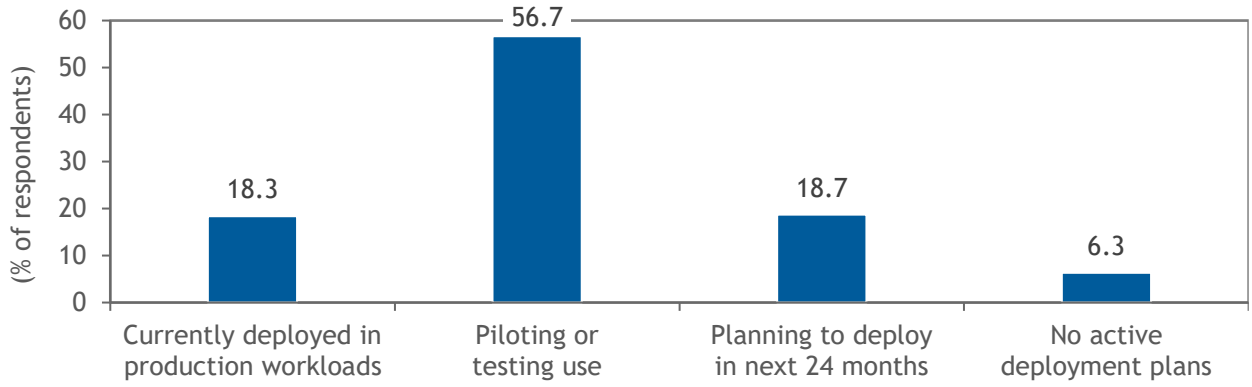
However, IDC research also highlights widespread unpreparedness for emerging threats. Organizations face significant gaps in multitenancy security, compliance readiness, and mitigation of human error. These challenges are compounded by the complexity of modern IT environments, the proliferation of AI-powered applications, and the need to balance innovation with robust security controls. As organizations combine sensitive data sets for advanced analytics, the risk of exposure increases, making privacy-preserving computation and hardware-based protections essential.

IDC believes that the current adoption trend is in part a direct response to these pressures and growing maturity of Confidential Computing solutions. Organizations are seeking to not only comply with regulatory mandates but also recognize the importance of mitigating against evolving threats and risks, including insider threats, ransomware, and the challenges posed by AI and quantum computing. Confidential Computing, with its ability to protect data during active processing, is emerging as a critical component of a holistic data security strategy enabling secure collaboration, safeguarding intellectual property, and supporting compliance in highly regulated industries.

FIGURE 1

Deployment Environments

Q. Which of the following best represents your organization's adoption stage of this technology?



n = 600

Source: IDC's *Confidential Computing Study,* July 2025

Finding 2: Public Cloud Leads, While Sovereignty Drives Hybrid/ On-Prem Growth

Confidential Computing is rapidly gaining traction across a variety of deployment environments, with public cloud emerging as the leading platform for adoption. According to IDC research, 71% of organizations deploy Confidential Computing in public cloud environments, drawn by the scalability, flexibility, and advanced security features offered by major cloud providers. Public cloud platforms are particularly well suited for Confidential Computing, as they enable organizations to leverage container-based application security and real-time encryption of data in use, protecting sensitive information even during active processing.

However, the landscape is evolving. Hybrid and distributed cloud deployments are increasingly common, with 45% of organizations adopting Confidential Computing in these environments. This trend reflects the growing complexity of enterprise IT architectures, where workloads are distributed across multiple clouds and on-premises infrastructure to balance performance, cost, and compliance requirements. Private and on-premises cloud deployments also remain significant, accounting for 36% of adoption. These environments are often chosen by organizations with stringent data sovereignty, privacy, and regulatory mandates, such as those in government. IDC's historical research shows that hybrid multicloud is the reality for most organizations.

IDC's October 2024 Government Buyer Intelligence Survey underscores this trend, revealing that 34% of respondents have repatriated workloads from public cloud back

to on-premises environments in the past 12 months. Of those, 33% cited data privacy, compliance, and regulatory concerns as their primary drivers. This repatriation trend highlights the importance of maintaining control over sensitive data and meeting evolving regulatory requirements, which can be more challenging in public cloud settings.

While edge adoption of Confidential Computing remains nascent, the proliferation of powerful endpoint devices and the need for real-time, local data processing are expected to drive future growth in this area.

Confidential Computing adoption is accelerating across public, hybrid, and private cloud environments, driven by the need for scalable security and compliance with evolving regulatory requirements. As organizations increasingly balance performance, cost, and data sovereignty, the trend toward hybrid and repatriated workloads highlights the importance of flexible deployment strategies and robust data protection measures.

Finding 3: Benefits Evolve from Incremental Security to Strategic Enablement

Confidential Computing delivers two distinct and complementary forms of value for organizations: it strengthens existing cybersecurity portfolios with unique protections and it unlocks new strategic capabilities that were previously out of reach. Both dimensions are essential and transformative, offering organizations a broader and deeper approach to data security and innovation.

Distinctive Protections

IDC research shows that organizations anticipate significant benefits from Confidential Computing, including improved data integrity (88%), confidentiality with proven technical assurances (73%), and enhanced regulatory compliance (68%):

- **Improved data integrity:** Confidential Computing provides robust data privacy, reducing the risk of exposure to insider threats and malicious actors. Hardware-based attestation ensures that code runs in a trusted environment, safeguarding data and code from tampering and enhancing overall integrity.
- **Confidentiality with proven technical assurances:** Real-time encryption and isolation, grounded in zero trust principles, assuming "never trust, always verify" continuous verification, is especially critical in multitenant environments, protecting data and code even from privileged administrators and cloud providers.
- **Regulatory compliance:** Confidential Computing helps organizations meet stringent data protection regulations and future-proof their operations,

supporting requirements such as data, model and application sovereignty and residency under frameworks like EU DORA.

Strategic Enablers

Beyond strengthening existing defenses, Confidential Computing opens the door to new possibilities:

- **Secure multiparty collaboration:** Organizations can collaborate with external partners by sharing data, code, or models without exposing proprietary logic, enabling secure joint innovation along with unlocking the value of data.
- **Increased trust in remote environments:** Sensitive data and logic can be deployed in public cloud datacenters or remote edge devices, with higher levels of control and confidence. IT leaders should still ensure remote locations and third-party infrastructure providers are reputable and maintain proper physical security, as sophisticated open-chassis physical attacks are a consideration.
- **Expansion of use cases:** Use cases have expanded rapidly over the past three years, particularly in AI, including GenAI and agentic AI, and ML workflows. Confidential Computing is increasingly recognized as a best practice for protecting proprietary algorithms and models and sensitive data throughout the entire AI life cycle from pretraining and training to inference. In the case of large language models, this includes securing proprietary architectures, data sets, and outputs at every stage. During inference, Confidential Computing enables organizations to run proprietary AI models on external data without exposing either the model or the data, mitigating risks such as inference-time data leakage and reverse engineering. This capability not only facilitates secure data collaboration and model monetization but also supports compliance with healthcare and financial regulations. Independent attestation mechanisms further enhance trust by validating the integrity of the execution environment and ensuring tamper-proof processing.
- **Foundational re-think:** Confidential Computing enables a foundational rethink of digital identity, provenance, and traceability, extending trust from chips to workloads to entities. This paradigm shift allows organizations to establish verifiable chains of trust across hardware, software, and participants, supporting secure digital interactions and robust accountability.

Confidential Computing's strategic value is evident across a wide range of industries and use cases. In finance, it plays a critical role in supporting regulatory compliance and audit, enabling secure blockchain operations, asset digitalization, advanced data analytics, anti-money laundering efforts, and the secure movement of digital assets. These capabilities are essential for financial institutions that must navigate stringent regulatory environments while protecting sensitive transactional data. In healthcare,

Confidential Computing empowers organizations to securely manage electronic health records, optimize supply chains, facilitate federated learning for collaborative AI model training, and enable secure cross-boundary data exchange. It also accelerates clinical research, drug discovery, data aggregation, and genomics, helping healthcare providers maintain patient privacy and comply with complex regulations.

Beyond these sectors, Confidential Computing is being adopted in retail for payment and transaction fraud detection across multiple retailers or payment processors, returns fraud, account takeover, and loyalty programs; in IoT and edge computing for secure device management and data processing; and in telecom for safeguarding sensitive communications and infrastructure.

IDC observes that Confidential Computing is also commonly leveraged for data clean rooms. Data clean rooms are privacy-preserving environments for secure multiparty analytics, AI model training, fraud detection, supply chain optimization, and cross-industry collaboration, all while maintaining privacy and compliance. These are rapidly expanding in advertising, healthcare, financial services, and market research.

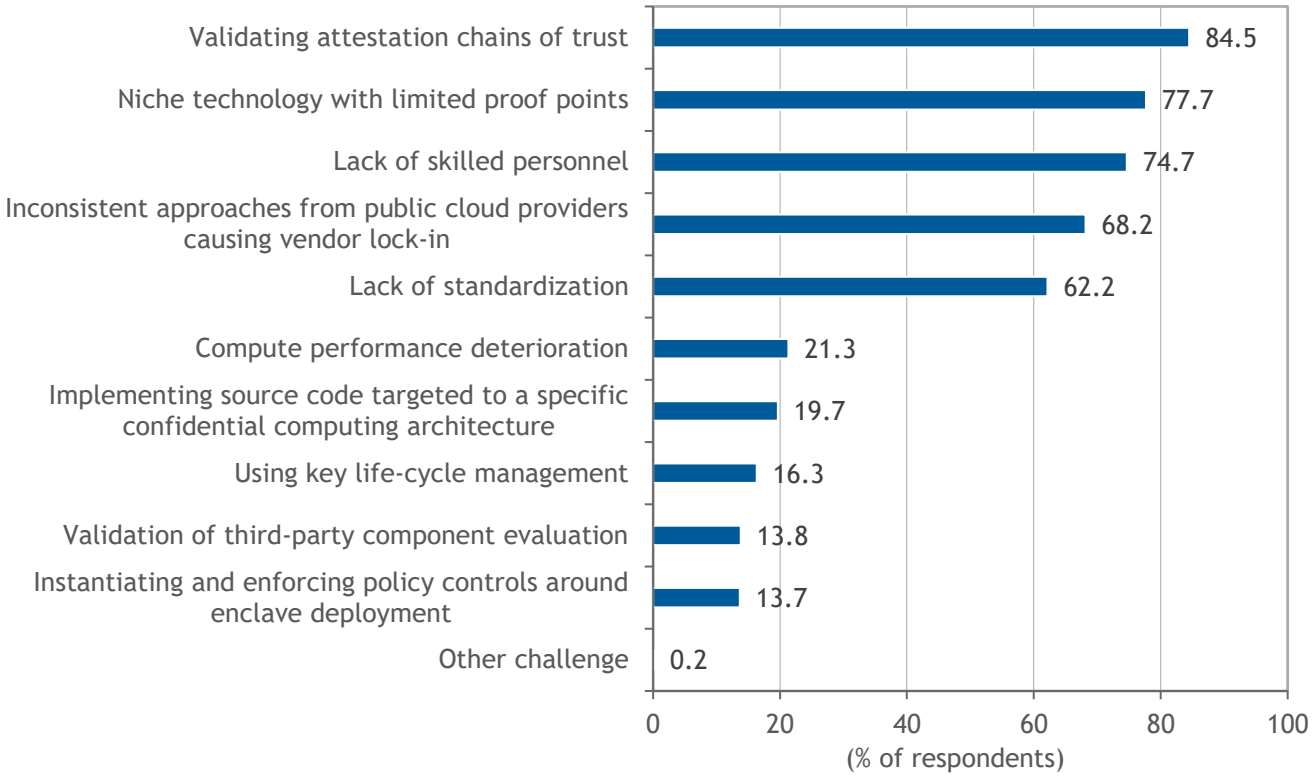
Finding 4: Key Barriers Are No Longer "Why?" But "How?"

Organizations seeking to adopt Confidential Computing face a range of challenges that can hinder implementation and long-term success. One of the most pressing issues is the validation of attestation chains of trust, cited by 84.5% of respondents (see Figure 2). This process is critical to ensuring the integrity and security of confidential workloads, but it remains complex and can be difficult to manage at scale. The primary challenges are no longer about the value of Confidential Computing, but the implementation specifics. Attestation validation (84%), the perception of it being a niche technology (77%), and a skills gap (75%) top the list. These are actionable, solvable hurdles. However, these perceptions contribute to hesitancy among decision-makers, especially in industries that rely on well-established security frameworks.

FIGURE 2

Challenges: Overcoming Adoption Hurdles

Q. What are the key challenges or risks that you see in adopting confidential computing?



n = 600

Source: IDC's *Confidential Computing Study,* July 2025

These challenges are evident when healthcare organizations begin to consider Confidential Computing, initial evaluation challenges, and technical concerns are commonly shared. IDC research confirms that finding the right balance between risk and security requirements is a primary evaluation challenge across all sectors. IDC has commented that a top technical concern is ensuring that user access to data is secure, compliant with regulations, and kept up to date whether the data is protected inside a secure, isolated environment or managed through different ways of deploying Confidential Computing (such as in the cloud, on premises, or at the edge)The lack of skilled personnel adds to these concerns. Robust access control presents a unique opportunity for cloud service providers, managed service providers, and consulting partners to engage early and educate organizations during the solution vetting process, helping them navigate the complexities of secure data management and regulatory compliance.

While some technical challenges such as compute performance deterioration (21.3%) and key life-cycle management (16.3%) are less frequently cited, they still represent important considerations for organizations aiming to optimize performance and security. The relatively low percentages for issues like enclave policy enforcement (13.7%) and third-party component validation (13.8%) suggest that while these are not widespread concerns, they may become more prominent as adoption scales.

Finding 5: Regulatory Mandates (Like EU DORA) Create Compelling Events for Adoption

Regulatory frameworks such as the EU DORA are playing a pivotal role in accelerating the adoption of Confidential Computing, particularly within the financial sector. DORA mandates that financial entities must maintain high standards of availability, authenticity, integrity, and confidentiality of data whether the data is at rest, in use, or in transit. This comprehensive requirement directly aligns with the core capabilities of Confidential Computing, which uniquely protects data during processing, a traditionally vulnerable phase.

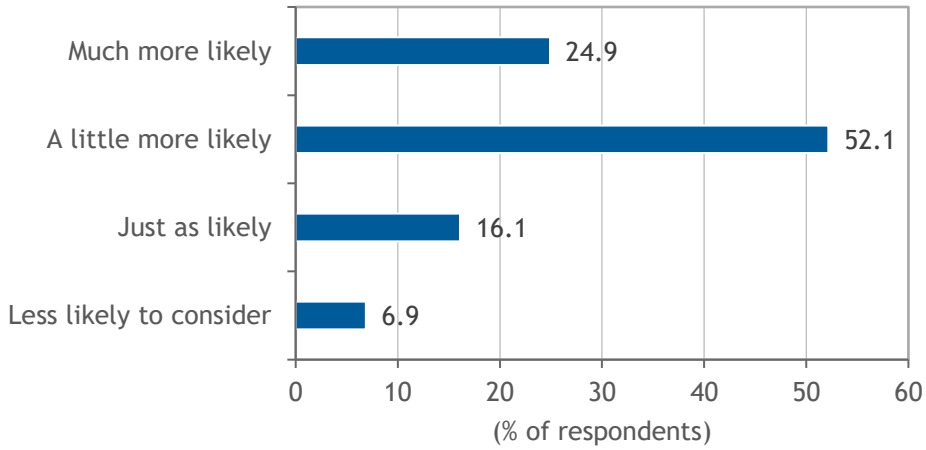
The impact of regulation is clear: 77% of organizations are more likely to consider Confidential Computing specifically due to DORA (see Figure 3). The act's mandate to protect data "at rest, in use, or in transit" explicitly names the vulnerability that Confidential Computing solves. This strong majority underscores how compliance requirements are not just encouraging adoption, they're becoming a strategic imperative. Only a small fraction (6.9%) indicated they are less likely to consider Confidential Computing, suggesting again that regulatory pressure is broadly viewed as a positive catalyst.

The implications are significant: as regulations including DORA become more stringent and widespread, organizations will increasingly seek technologies that can demonstrate compliance while enhancing security posture. This regulatory momentum is also likely to influence vendor road maps, industry standards, and cross-sector collaboration, helping address earlier adoption challenges such as lack of standardization and technical expertise.

FIGURE 3

Deployment Environments

Q. How have the confidential data requirements within DORA impacted your consideration of confidential computing as part of the solution? Are you …



n = 600

Source: IDC's *Confidential Computing Study,* July 2025

Finding 6: Security and Privacy Priorities: Handling Sensitive Data

Organizations today are under increasing pressure to safeguard sensitive data against a growing array of external threats, comply with evolving regulations, and maintain trust with customers and partners. Survey results reveal that the top security and privacy priorities for enterprises handling sensitive data include workload security and protection against external threats (56%), safeguarding personally identifiable information (PII) (51%), compliance with data privacy regulations (50%), and cloud privacy (45%). These priorities reflect a landscape where threat prevention, data protection, and regulatory adherence are not just operational requirements but strategic imperatives. Further:

- **Workload security and protection against external threats (56%):** Confidential Computing enables organizations to run sensitive workloads in hardware-isolated environments, reducing risk for applications and data from external threats such as ransomware, advanced persistent threats, and unauthorized access. This ensures that even if the underlying host stack is compromised, the integrity and confidentiality of workloads can be maintained.
- **Protection of personally identifiable information (51%):** By encrypting data in use, Confidential Computing provides support for PII and other sensitive information, remaining protected throughout the entire data life cycle not just at

rest or in transit. This minimizes the risk of exposure to both insider and external threats, supporting robust privacy practices.

- **Compliance with data privacy regulations (50%):** Confidential Computing provides verifiable technical assurances, such as hardware-based attestation and real-time encryption, which help organizations meet stringent regulatory requirements for data privacy, sovereignty, and residency. This is essential for compliance with frameworks such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and EU DORA.
- **Cloud privacy (45%):** In cloud and hybrid environments, Confidential Computing isolates sensitive data and workloads from cloud providers and privileged administrators, ensuring that organizations retain control over their data governance and privacy. This supports secure cloud adoption and mitigates risks associated with multitenant architectures and multinational cloud providers.

As auditors increasingly factor threats like ransomware, insider risk, and data recovery practices into corporate risk assessments, the implications extend beyond compliance to budgeting, licensing, and even cyberinsurance premiums. In sensitive, multiparty environments such as medical research and bio-innovation spanning multiple jurisdictions, the need for secure data collaboration is paramount. Confidential Computing offers a distinctive advantage by enabling secure processing of sensitive data without exposing it, backed by attestation and hardware-based isolation.

Finding 7: Alternative Privacy-Enhancing Technologies

While many privacy-enhancing technologies (PETs) offer strong theoretical guarantees, Confidential Computing stands out as a practical and scalable alternative especially when compared with more complex or resource-intensive methods. It is also applicable for standard computing workloads, without requiring rewriting of applications or algorithms.

However, organizations may find that other PETs, such as fully homomorphic encryption (FHE), zero-knowledge proofs (ZKPs), secure multiparty computation (SMPC), or federated learning, are better suited for specific use cases, particularly where regulatory requirements, performance, or data sharing models differ.

According to Figure 4, a majority of respondents expressed reluctance to adopt these advanced PETs:

- **FHE:** 67.3% would not consider it. FHE allows computation on encrypted data but at the moment is recognized to be more computationally expensive than Confidential Computing, making it impractical for latency-sensitive applications.

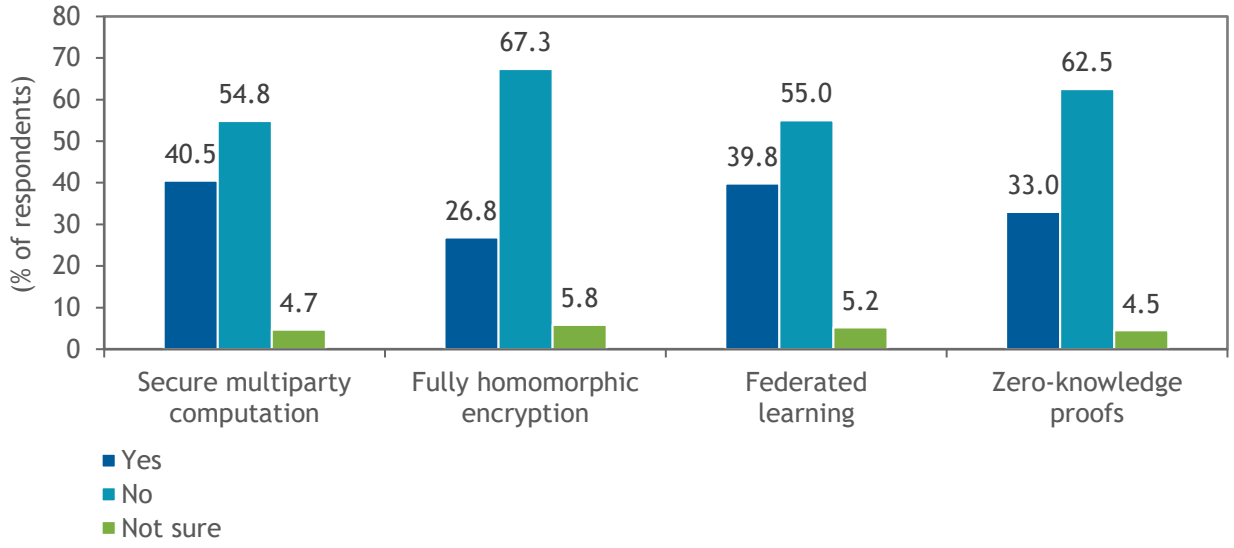
- **ZKPs:** 62.5% would not consider it. ZKPs are powerful for proving data validity without revealing the data itself but require specialized cryptographic expertise and may be difficult to integrate into existing systems.
- **SMPC:** 54.8% would not consider it. SMPC involves splitting data across multiple parties for joint computation, which can introduce network overhead, synchronization challenges, and scalability issues.
- **Federated learning:** 55.0% would not consider it. Federated learning, while useful for decentralized model training, may struggle with data heterogeneity, model drift, and privacy leakage risks.

These high rejection rates are likely due to performance limitations, complexity of implementation, and lack of tooling or standardization. Nevertheless, some organizations continue to invest in these technologies where their unique properties align with business or compliance needs

FIGURE 4

Alternative Privacy-Enhancing Technologies

Q. Which privacy-enhancing tech is your org currently using or considering to help manage and control sensitive data?



n = 600

Source: IDC's *Confidential Computing Study,* July 2025

Recommendations: Strategic Actions for Decision-Makers

Best Practices

By following these steps, organizations can systematically address the barriers to Confidential Computing adoption, build trust in new technologies, and unlock the new potential of secure data processing across cloud, on-premises, and edge environments:

1. **Identify and prioritize sensitive workloads:** Begin by pinpointing your most sensitive workloads (e.g., AI model training, PII processing, multiparty analytics). Assess where data is exposed during computation; this will guide your initial focus.
2. **Initiate targeted pilot projects:** Don't try to boil the ocean. Start with a single, high-value use case (such as securing a RAG pipeline for an internal LLM or a specific analytics workload). Pilot initiatives allow you to demonstrate the practical benefits of Confidential Computing, build internal expertise, and generate stakeholder buy-in. Successful pilots lay the groundwork for broader adoption and help overcome initial skepticism. Piloting with one of the growing number of solution providers can significantly reduce the time, effort, and expense of pilot projects versus building in-house.
3. **Leverage third-party attestation solutions and open source tools:** Attestation validation is often the top challenge. Utilize independent attestation services and open source tools from organizations such as the Confidential Computing Consortium (CCC) to validate the integrity of Confidential Computing environments and simplify the process from day one. This is especially critical in multicloud or hybrid environments.
4. **Engage with vendors supporting open standards and interoperability:** To avoid vendor lock-in, prioritize cloud providers and vendors that support open, interoperable standards for Trusted Execution Environments and attestation. This approach enables integration across diverse platforms, simplifies deployment, and ensures compatibility with existing security and data management tools.
5. **Participate in industry initiatives and collaborate with key stakeholders:** Join collaborative efforts such as the Confidential Computing Consortium, engage with your cloud providers and hardware vendors, and participate in industry groups. These connections help you stay informed about evolving standards, share lessons learned, and contribute to best practices, accelerating the maturity of Confidential Computing technologies.
6. **Invest in skills development and training:** Address the skills gap by investing in training programs, certifications, and hands-on workshops. Use resources, training, and best practice guides from the CCC, vendors, and industry groups to

upskill your team and build internal expertise in Confidential Computing concepts, deployment models, and operational management.

CONCLUSION

Conclusion and Call to Action: Embracing Confidential Computing

The findings from this IDC survey underscore that Confidential Computing has evolved from a niche security enhancement into a foundational enabler of modern data-centric innovation. While it strengthens existing infrastructure delivering improved data integrity, confidentiality, and regulatory compliance, it also unlocks new possibilities in AI, multiparty collaboration, and privacy-preserving analytics that were previously out of reach. This dual role is what makes Confidential Computing so compelling: It can serve as both a critical layer of defense in depth and a strategic accelerator for digital transformation.

Key Takeaways

Adoption is accelerating, with 75% of organizations either piloting or planning deployment within 24 months.

Many respondents are most compelled by Confidential Computing benefits to their overall cybersecurity. Many also appreciate its role in enhancing regulatory compliance. A substantial number also see promise in new use cases and business capabilities enabled by Confidential Computing, such as confidential AI and privacy-preserving data collaboration.

IDC research supports the following business outcomes from Confidential Computing including:

- **Accelerated innovation:** Organizations can tap into previously inaccessible data, sharing across industries and speeding up product development and decision-making.
- **Regulatory momentum:** Stronger data protection helps meet GDPR, HIPAA, DORA, and other mandates reducing risk of fines and reputational damage particularly in highly regulated sectors like finance and healthcare.
- **Revenue growth:** New services and data monetization models become viable through secure collaboration and analytics. IDC highlights use cases such as cross-brand collaboration, audience segmentation, and predictive analytics, which leverage secure data sharing to create innovative services and business opportunities.

- **Customer trust:** Enhanced privacy and data governance improve brand reputation and customer loyalty.

Barriers such as attestation complexity, skill gaps, and inconsistent cloud approaches must be addressed through industry collaboration, standardization, and product improvements. While it strengthens existing infrastructure and delivers improved data integrity, confidentiality, and regulatory compliance, it is most effective when integrated with traditional security measures.

To fully realize its potential, CCC members, stakeholders, and the broader cybersecurity community must continue investing in education, interoperability, and real-world proof points to hasten the adoption of Confidential Computing as a trusted and foundational security layer.

APPENDIX A

Table 1 shows definitions of use cases and value propositions.

TABLE 1

Definitions of Use Cases and Value Propositions

Use Case/Value Proposition Name	Description
Security of workloads from outside attackers	Confidential Computing can strengthen the security of workloads from outside attackers by running them inside a hardware-protected trusted execution environment, verified with remote cryptographic attestation.
Protection of personally identifiable information (PII)	Confidential Computing can cryptographically protect all personally identifiable information, user profiles, authentication credentials, and other sensitive user information from outside and insider threats while it is actively in use.
Compliance with relevant compliance regulation	Confidential Computing can strengthen compliance with data protection regulations like GDPR, HIPAA, DORA, and certain government defense agencies that demand data confidentiality and control by processing regulated data in a hardware-protected and attested trusted execution environment.
Maintaining privacy of workloads from public cloud providers	Confidential Computing can help ensure the privacy of your workloads in the public cloud by using hardware-based controls to prevent workload or data access by the cloud provider's software stack or system administrators.
Workload integrity verification	Using remote cryptographic attestation, Confidential Computing can verify that a workload has not been modified or tampered with. This helps provide assurance that the software has not been compromised before interacting with it.
Adherence to data sovereignty requirements	Confidential Computing can strengthen data sovereignty programs by helping prevent unencrypted or unprotected data from being accessed by the cloud provider even if they are subject to authorities outside the targeted sovereign area.

TABLE 1

Definitions of Use Cases and Value Propositions

Use Case/Value Proposition Name	Description
Improved security via workload compartmentalization and containment	Confidential Computing can protect the security and resilience of the enterprise by running containerized workloads in access-controlled trusted execution environments. A breach in one workload, such as a compromised third-party app, can be prevented from spreading to workloads shielded by Confidential Computing.
Analysis of multiple sensitive data sets in a single workload	Confidential Computing can enable privacy-preserving environments where multiple sensitive or regulated data sets can be analyzed without the original data being exposed to the host or any other party. Examples include multiple hospitals collaborating on joint disease research or marketing firms combining leased data from multiple sources for ad targeting.
Security and compliance of data sets used for AI model training	Confidential Computing can help improve AI model accuracy by enabling training on sensitive or regulated data sets while maintaining confidentiality and compliance safeguards.
Assurance of integrity of digital supply chains	Confidential Computing can help ensure the integrity of digital supply chains by creating and evaluating provenance data inside a hardware-protected trusted execution environment verified by remote cryptographic attestation, particularly important as AIBOMs are increasingly requested.
Security of public cloud workloads from malicious cloud tenants	Confidential Computing can help ensure the security and privacy of your workloads in the public cloud by using hardware-based controls to prevent workload or data access by malicious tenants in the cloud.
Unlocking sensitive data sets safely for wider analytic use	Confidential Computing enables utilization and combination of sensitive structured and unstructured data sets that might otherwise be restricted due to privacy or security concerns driven by risks of unauthorized access.
Digital Operational Resilience Act (DORA) compliance	Confidential Computing can help meet the DORA requirement to "maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit" by processing relevant data in a hardware-protected and attested trusted execution environment.
General security of AI systems	Confidential Computing can be used to protect critical AI systems from many types of model manipulation, API abuse, poisoned training data, or model theft.
Personal key management for users	Confidential Computing enables secure personal key management on behalf of your users, such as in blockchain. This equips each user with their own keychain to sign and/or encrypt their own information in a way that enables completely new secure experiences while protecting both keychains and information from data breaches and insider threats.
Retrieval-augmented generation (RAG) security and confidentiality in AI analysis	When using AI with retrieval-augmented generation, Confidential Computing can help control access to sensitive and private data used to generate AI responses from third-party LLMs.

Source: IDC, 2025

APPENDIX B

Figures 5A-5C show survey results in total and by industry and country.

FIGURE 5A

Survey Results in Total and by Industry and Country

	Industry					Country						
	Total	Fin Serv	Healthcare	Gov	Other	Canada	China	France	Germany	India	United Kingdom	United States
Unweighted base	600	100	100	100	300	65	100	65	100	100	70	100
Thinking about the quantity and sensitivity of confidential or regulated data, what is the level of urgency in your organization around protecting data from theft, tampering, or misuse? Is it ...												
Higher sensitivity than most organizations	52%	91%	81%	88%	17%	52%	46%	55%	52%	47%	57%	57%
Similar to the sensitivity in most organizations	36%	8%	15%	11%	61%	38%	40%	34%	38%	39%	33%	29%
Lower sensitivity than most organizations.	12%	1%	4%	1%	22%	9%	14%	11%	10%	14%	10%	14%
How prepared is your organization to protect your confidential and regulated data through investments in tools, processes, and training? Are you ...												
More prepared than our industry peers	18%	38%	28%	16%	8%	23%	20%	9%	17%	12%	20%	21%
Similarly prepared to our industry peers	67%	51%	62%	75%	71%	60%	65%	74%	69%	75%	64%	59%
Less prepared than our industry peers	16%	11%	10%	9%	22%	17%	15%	17%	14%	13%	16%	20%
Does your organization manage or contribute to projects that combine sensitive data sets from multiple sources for analysis, AI training, or multiparty collaboration?												
Yes	44%	87%	79%	73%	9%	42%	38%	45%	43%	41%	56%	49%
Piloting or testing	25%	13%	15%	18%	35%	34%	25%	29%	22%	25%	20%	23%
Planning to start in next 12 months	20%	0%	6%	7%	35%	17%	25%	15%	19%	20%	19%	21%
No	11%	0%	0%	2%	21%	8%	12%	11%	16%	14%	6%	7%
In which of these areas does your organization's threat preparation need improvement?												
Data breach by a remote outside attacker	87%	95%	94%	85%	83%	89%	84%	91%	88%	87%	81%	91%
Loss of service or downtime due to ransomware	85%	88%	85%	95%	80%	89%	82%	97%	85%	79%	79%	87%
Data breach by a malicious insider	83%	94%	91%	93%	74%	88%	80%	91%	83%	78%	87%	81%
Data breach by a system administrator in your public cloud provider	81%	88%	80%	88%	77%	85%	78%	89%	82%	74%	89%	78%
Reputational or brand damage due to data breaches	81%	90%	86%	91%	72%	85%	78%	85%	79%	76%	84%	82%
Accidental data breach due to user error or inadequate training	71%	21%	89%	95%	73%	62%	75%	68%	71%	74%	64%	76%
Fines or sanctions due to data privacy compliance violations	66%	82%	87%	7%	74%	68%	65%	66%	70%	58%	63%	73%
Data breach by another tenant in your public cloud provider	40%	85%	82%	4%	23%	40%	37%	37%	42%	37%	41%	44%
Other threats you feel are high urgency.	10%	18%	9%	4%	10%	12%	0%	0%	0%	17%	20%	23%
How familiar are you with the concept of "confidential computing"? Are you ...												
Very familiar	31%	56%	31%	35%	22%	34%	28%	22%	22%	29%	57%	33%
Familiar	42%	37%	61%	56%	33%	32%	42%	51%	51%	42%	30%	44%
Somewhat familiar	14%	6%	8%	9%	21%	29%	13%	15%	7%	21%	6%	12%
Not very familiar	9%	1%	0%	0%	17%	5%	11%	11%	12%	6%	6%	9%
Not familiar at all	3%	0%	0%	0%	7%	0%	6%	2%	8%	2%	1%	2%
Based on the definition of confidential computing, which of the following best represents your organization's adoption stage of this technology? Is it ...												
Piloting or testing use	57%	58%	64%	73%	48%	52%	46%	74%	65%	53%	60%	52%
Planning to deploy in next 24 months	19%	3%	5%	1%	34%	15%	27%	8%	13%	29%	19%	15%
Currently deployed in production workloads	18%	37%	29%	21%	8%	26%	20%	15%	13%	12%	20%	24%
No active deployment plans	6%	2%	2%	5%	10%	6%	7%	3%	9%	6%	1%	9%

Source: IDC, 2025

FIGURE 5B

Survey Results in Total and by Industry and Country

		Industry				Country						
	Total	Fin Serv	Healthcare	Gov	Other	Canada	China	France	Germany	India	United Kingdom	United States
Unweighted base	600	100	100	100	300	65	100	65	100	100	70	100
What do you anticipate as the main benefits of confidential computing?												
Improved data integrity	88%	93%	89%	91%	85%	92%	82%	95%	90%	73%	97%	94%
Data confidentiality with proven technical assurances	73%	72%	66%	70%	76%	75%	82%	91%	77%	77%	39%	65%
Improved code confidentiality	70%	70%	69%	74%	69%	71%	97%	68%	40%	92%	47%	67%
Better regulatory compliance	68%	74%	66%	69%	65%	72%	64%	65%	62%	63%	77%	73%
More secure platform	65%	72%	70%	62%	62%	78%	63%	49%	56%	58%	77%	76%
Attestability/authenticate officially	63%	43%	57%	70%	70%	40%	85%	65%	62%	81%	31%	61%
Reduced risk of data leakage/breach	60%	63%	61%	62%	57%	72%	65%	65%	56%	55%	44%	62%
Isolation of workloads	58%	62%	54%	45%	61%	40%	63%	65%	61%	67%	46%	54%
Performance enhancement	27%	35%	29%	34%	22%	45%	30%	29%	22%	16%	29%	28%
Better code integrity	22%	25%	23%	35%	16%	25%	12%	20%	28%	12%	41%	21%
Easier programmability	17%	25%	20%	18%	12%	12%	22%	17%	18%	18%	6%	18%
Unspoofability/recoverability	11%	11%	9%	15%	10%	11%	15%	12%	7%	12%	7%	12%
Ability to build a chain of trust	9%	9%	9%	12%	8%	11%	10%	5%	7%	14%	4%	11%
Other benefit (write in)	0%	1%	1%	0%	0%	0%	0%	0%	0%	0%	3%	0%
No perceived benefits expected	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
What are the key challenges or risks that you see in adopting confidential computing?												
Validating attestation chains of trust	85%	81%	79%	82%	88%	89%	80%	86%	89%	85%	86%	79%
Niche technology with limited proof points	78%	75%	72%	84%	78%	83%	91%	83%	70%	86%	56%	72%
Lack of skilled personnel	75%	63%	70%	75%	80%	62%	80%	75%	75%	73%	79%	76%
Inconsistent approaches from public cloud providers causing vendor lock-in	68%	64%	69%	74%	67%	66%	82%	77%	52%	80%	44%	71%
Lack of standardization	62%	51%	62%	67%	64%	43%	79%	66%	44%	61%	81%	61%
Compute performance deterioration	21%	27%	22%	21%	19%	18%	24%	25%	21%	26%	13%	20%
Implementing source code targeted to a specific confidential computing archit	20%	33%	18%	20%	16%	40%	15%	17%	24%	16%	10%	19%
Using key life-cycle management	16%	27%	20%	16%	12%	23%	18%	11%	14%	19%	14%	15%
Validation of third-party component evaluation	14%	17%	16%	17%	11%	17%	11%	11%	16%	20%	7%	13%
Instantiating and enforcing policy controls around enclave deployment	14%	13%	13%	19%	12%	22%	17%	6%	12%	18%	7%	12%
Other challenge (please explain)	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%

Source: IDC, 2025

FIGURE 5C

Survey Results in Total and by Industry and Country

	Industry					Country						
	Total	Fin Serv	Healthcare	Gov	Other	Canada	China	France	Germany	India	United Kingdom	United States
Unweighted base	600	100	100	100	300	65	100	65	100	100	70	100
Which privacy-enhancing technologies (besides confidential computing) is your organization currently using or considering to help manage and control sensitive data? Are you using ...												
Differential privacy techniques	62%	70%	77%	60%	53%	63%	58%	54%	56%	72%	73%	63%
AWS Nitro Enclaves	62%	74%	70%	61%	53%	60%	63%	55%	63%	72%	61%	59%
Secure multiparty computation	49%	58%	68%	50%	35%	44%	53%	46%	47%	41%	49%	61%
Federated learning	48%	77%	67%	8%	45%	47%	51%	43%	44%	48%	53%	52%
Zero-knowledge proofs	40%	80%	75%	18%	13%	42%	38%	41%	33%	36%	44%	48%
Fully homomorphic encryption	33%	65%	6%	58%	17%	35%	31%	39%	24%	33%	36%	33%
Now we want to consider a number of security and privacy issues related to the handling of sensitive data. Whether you have resolved this issue or not, please tell me how important managing the issue is to the organization. Is it a top priority, a critical priority, a priority, a lower priority, or not a priority. (% indicating "top priority")												
Security of workloads from outside attackers	68%	89%	83%	87%	41%	75%	59%	64%	69%	64%	81%	71%
Protection of personally identifiable information (PII)	63%	64%	66%	76%	53%	75%	71%	75%	71%	41%	51%	59%
Compliance with relevant data privacy regulation	60%	77%	75%	82%	33%	70%	53%	60%	63%	56%	56%	68%
Maintaining privacy of workloads from public cloud providers	55%	68%	69%	81%	28%	72%	52%	65%	63%	60%	37%	41%
Workload integrity verification	51%	66%	61%	67%	30%	58%	49%	58%	58%	43%	42%	53%
Adherence to data sovereignty requirements	46%	68%	70%	75%	8%	51%	34%	55%	51%	41%	49%	50%
Improved security via workload compartmentalization and containment	45%	67%	20%	71%	32%	57%	40%	62%	47%	41%	44%	31%
Analysis of multiple sensitive data sets in a single workload	41%	61%	78%	26%	20%	36%	41%	45%	45%	35%	37%	48%
Security and compliance of data sets used for AI model training	36%	64%	61%	23%	15%	43%	29%	24%	41%	25%	41%	48%
Assurance of integrity of digital supply chains	33%	49%	16%	17%	41%	34%	29%	24%	36%	40%	36%	29%
Security of public cloud workloads from malicious cloud tenants	32%	63%	19%	22%	28%	42%	19%	45%	29%	30%	37%	31%
Unlocking sensitive data sets safely for wider analytic use	30%	61%	57%	8%	12%	36%	26%	25%	38%	15%	44%	31%
DORA compliance	22%	44%	5%	40%	10%	38%	7%	38%	37%	9%	22%	15%
General security of AI systems	12%	17%	12%	9%	11%	9%	9%	2%	12%	4%	25%	23%
Personal key management for users	11%	19%	5%	15%	7%	9%	5%	9%	8%	9%	17%	20%
RAG security and confidentiality in AI analysis	8%	9%	7%	7%	8%	8%	8%	5%	10%	5%	7%	11%

Source: IDC, 2025

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com