Confidential Computing, Part 2: Critical Success Factors

IDC ANALYZE THE FUTURE

With growing adoption of public cloud and hosted services, accompanied by fast-growing ecosystems of technology and software providers, organizations face an increased chance that their data can be compromised. Trusting third-party providers can be financially and reputationally risky – even damaging, at times – for organizations if they become the target of successful cyberattacks and data breaches.

Achieving greater profitability with a heightened sense of trust in today's digital environment means delivering business agility that is not only efficient but also effective in addressing data concerns, such as risk, security, privacy, and compliance. IDC's recent survey data identifies the top two drivers for organizational trust initiatives – improving risk management processes and securing private data. Data security is critical to success, particularly for enterprises in highly regulated industries.

In our first Confidential Computing installment, we discussed the technology and its promise to address security and privacy issues in public clouds (see ***Confidential Computing, Part 1: Extending the Circle of Trust to Public Clouds***).

The reality, however, is that Confidential Computing is still in an early adoption phase – offerings remain fragmented and characterized by inconsistent approaches that limit the potential for multi-cloud implementations. To date, most Confidential Computing platforms or services are typically targeted at limited use cases, such as fraud detection in the financial world. The Confidential Computing Consortium – Microsoft and Google are members but, notably, Amazon is not – is trying to drive standardization of this technology.

Confidential Computing: Key Considerations

When evaluating Confidential Computing, end-users should define efficiency and quality metrics that will ultimately drive successful implementation:

Efficiency Metrics:

- **Adaptability** – How easily can the technology emulate real-world workloads?
- **Cost** – What is the appropriate balance between risk assessment and cost-effectiveness?

Quality Metrics:

- **Technical Assurances** – Are public cloud providers providing demonstrable assurances to address customer requirements for security, privacy, and compliance?
- **Trusted Ecosystems** – Can you work with partners to create a hardened supply chain that provides the underlying infrastructure and software?

"Specific to healthcare, the challenge will be funding it, because most of the research is funded through grants. So, it requires a level of sophistication by the researcher to document, describe the benefits, the use cases themselves, the reasons why they're using these solutions. Again, typically that's why we collaborate directly with AWS, with Microsoft, because we need some of that (technical) interaction with them to ultimately get the grant funding."

- CIO/CISO of a healthcare university and hospital

In addition, IDC urges end-users to understand and embrace the following key consideration when evaluating and adopting Confidential Computing:

Data Authority & Ownership – Regardless of where data resides (on-premises or in the cloud), customers are responsible. In addition to reputational damage, data breaches have significant financial impacts.

Data Privacy – Public cloud providers store exabyte-scale data of thousands of enterprise customers, exposing them to severe reputational damage for willingly or inadvertently disclosing sensitive data

Confidential Computing in Public Cloud: Adoption Viewpoints

IDC's Adoption Scenario Viewpoints	**Adoption**	IDC's Future of Trust survey data reveals that the top two drivers for organizational trust are improving risk management processes and securing private data.
	User Profile	Highly regulated industries, such as Finance and Healthcare, that need to protect intellectual property and sensitive data while collaborating with partners and using public cloud.
What it Means for Business Executives	**Use Case**	Procesing petabyte+ scale datasets in secure, isolated, and collaborative environments that will drive brand, reputation, and profitability as outcomes of trust.
	Metrics	Reduced number of sensitive data leak/breaches and reduced privacy related complaints and fines from customers and regulators.
	Customer Impact	Customers will realize greater agility in leveraging extensive datasets with trusted outcomes.

Source: IDC, Confidential Computing in Public Cloud: Extending the Circle of Trust, April, 2021

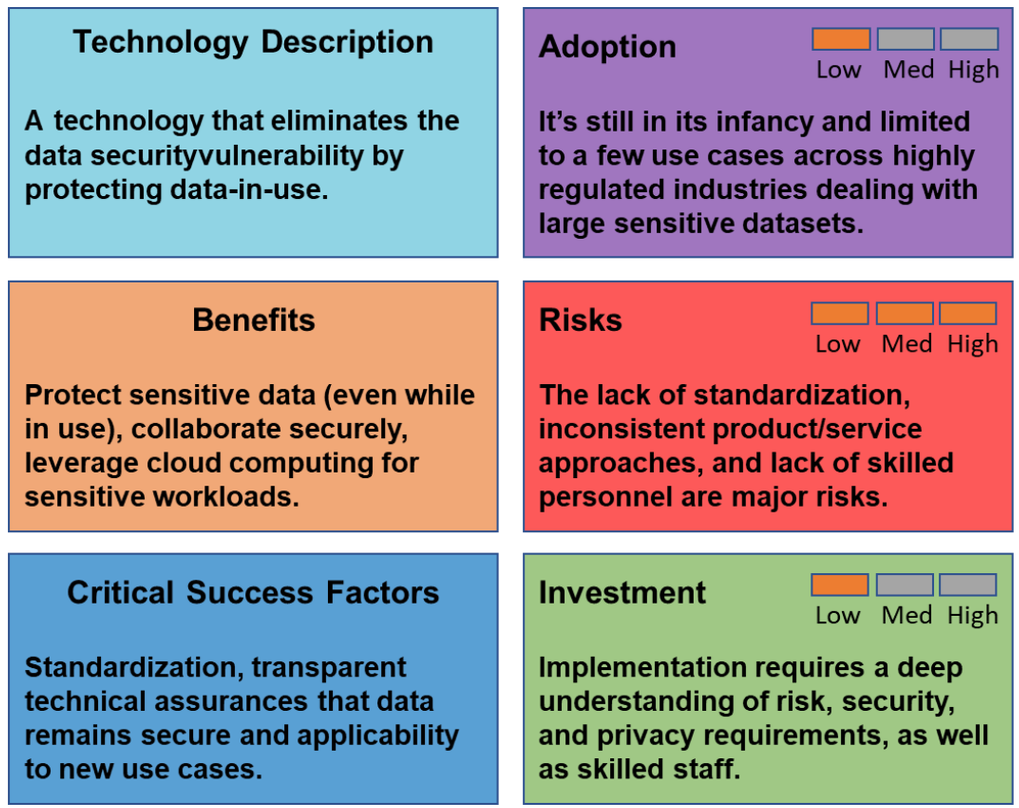
As enterprises move on-premises workloads to hybrid/multi-cloud environments, they will need to rely on third-party assurances for data authority and ownership while addressing interoperability concerns. Several public cloud providers offer operational assurances that they will not share customer data with third parties. However, customer data can still be subject to potential disclosure if subpoenas are issued to public cloud providers.

Lack of standardization remains a critical issue. Confidential Computing offerings are fragmented. Inconsistent approaches often lead to de facto vendor lock-in, which benefits neither customers nor suppliers. The Confidential Computing Consortium is trying to address this issue, but still lacks participation from key players – notably Amazon

With the increased sophistication of side-channel attacks, a strongly vetted ecosystem is imperative. Trusted – and limited – ecosystems are critical to maintaining technical assurances for data security and privacy. And, as with all technology solutions, organizations will need to identify – and optimize – the required financial investment. They will need to find the right balance between risk exposure and cost.

In addition, several in-depth interviews with customers who have deployed or are deploying Confidential Computing has revealed that the acquisition and retention of skilled talent are important success criteria. If the appropriate talent is not readily available in-house, enterprises can partner with service providers that can offer support.

Confidential Computing in Public Cloud: Snapshot



Source: IDC, Confidential Computing in Public Cloud: Extending the Circle of Trust, April, 2021

Ultimately, business leaders must reconcile two incontrovertible facts:

1. Data security is not optional – it's a core element in a robust trust program.
2. It is impossible to eliminate all risks.

As enterprises, including those in highly regulated industries, leverage large datasets across various deployment locations – including public clouds – to drive positive business outcomes, Confidential Computing platforms can help address significant data security and privacy issues.

To learn more about Confidential Computing and how it addresses Future of Trust data security and privacy requirements, download our first eBook installment, ***Confidential Computing, Part 1: Extending the Circle of Trust to Public Clouds***.

To learn more about IDC's Future of Trust research, visit idc.com/FoX or read:

eBook: ***Cloud Computing, Part 1: Extending the Circle of Trust to Public Clouds***

IDC Techbrief: ***Confidential Computing: Extend the Circle of Trust with Confidential Computing in Public Cloud, April, 2021***