FUTURUM.

CONFIDENTIAL COMPUTING:
The Future of Data Security and Digital Trust

Q42021

DANIEL NEWMAN
Principal Analyst + Founding Partner

SHELLY KRAMER
Lead Analyst + Founding Partner

FRED MCCLIMANS
Senior Analyst + Research Director

STEVEN DICKENS
Senior Analyst + VP of Sales

IN PARTNERSHIP WITH

IBM

Published: October 2021

OVERVIEW AND INTRODUCTION

In mid-2021, Futurum Research and IBM collaborated on a global study involving over 360 business, technology, and security professionals with a high level of influence and decision-making authority involving the planning, implementation, management, or oversight of their organization's data protection, data privacy, and/or data security systems and services.

We wanted to know how the need for more secure data protection has changed over the past few years, why protecting data in use is becoming important, and the potential of technical assurance approaches as a way to overcome the limitations of operational assurances in achieving complete data privacy and security.

The businesses and organizations these individuals represent are all actively implementing public, private, or hybrid cloud solutions in a range of industries including the banking, finance, insurance, government and public sector organizations, healthcare and pharmaceutical providers, and retail consumer packaged goods companies.

From our research, we have gained a solid understanding of the extent of cloud migration and the data security challenges organizations face during this migration, how organizations view the roles and importance of technical and operational assurance from their cloud providers, and how trust between enterprise organizations and their cloud providers can be more effectively established.

In this paper, we present the findings of our research, summarized as follows:

Key Insight: Security Models Have Been Disrupted

Data security professionals recognize that traditional data security models have been disrupted by recent global events, the acceleration of digital transformation agendas, and the migration of highly confidential, sensitive, or private data from on-premises deployments to the cloud.

- *77 percent of enterprises say their overall mindset regarding data privacy, protection, and risk has recently changed due to global events*

Key Insight: Data in Use is Data at Risk

With the migration of enterprise applications to the cloud, enterprises overwhelmingly acknowledge that data in use is increasingly at risk and must be protected. They also agree that the securing of data at rest or in transit is no longer enough to ensure complete protection.

- *94 percent of enterprises plan to invest in technologies that ensure data security for data in use*

Key Insight: Technical Assurance Enforces Operational Assurance

Operational Assurances by cloud providers that they will not access, read, or share customer data are not enough to protect confidential data in the cloud. The use of technical controls to provide Technical Assurance that a cloud provider cannot access customer data are required to enforce data security.

- *92 percent of enterprises agree that improving Technical Assurance would help simplify their compliance issues*

1. DATA DISRUPTED: Rethinking the Data Security Model

Every organization has data that they consider highly confidential, sensitive, or private in nature — data that contains Personally Identifiable Information (PII*) or simply must be secured for operational business reasons or for regulatory or compliance issues, such as in banking, financial, insurance, or healthcare industries.

48%

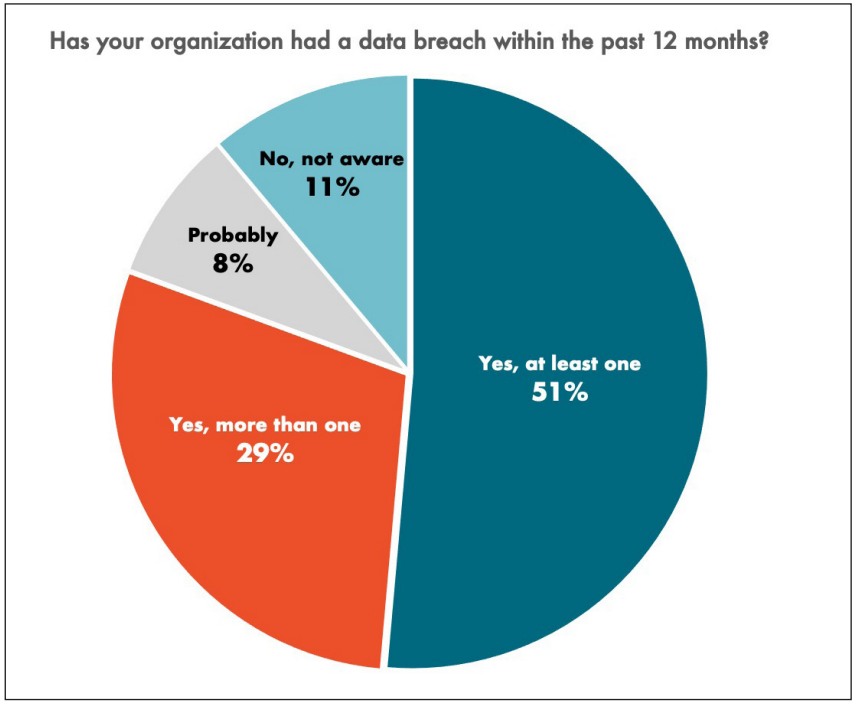
of enterprises say more than 50 percent of their overall data would be considered highly confidential, sensitive, or private in nature.

FUTURUM.

For purposes of this report, we define this to include the following, all of which are increasingly subject to government-led privacy policies:

- Consumer/Customer Data (to include PII)
- Operational Data (from devices/systems)
- Employee Data (to include PII)
- Corporate Sensitive Data (such as strategies, plans, financials, etc.)
- Partner or Supply Chain Data
- Any other type of data an organization would not want publicly disclosed

It's this data that business, technology, and security professionals must protect — a task that has become increasingly difficult due to recent global events.



**Personally Identifiable Information refers to any data that can be linked or connected to an individual or used to identify an individual, including but not limited to personal, employment, financial, or healthcare data.*

Enterprises are under attack and rethinking their approach to data security

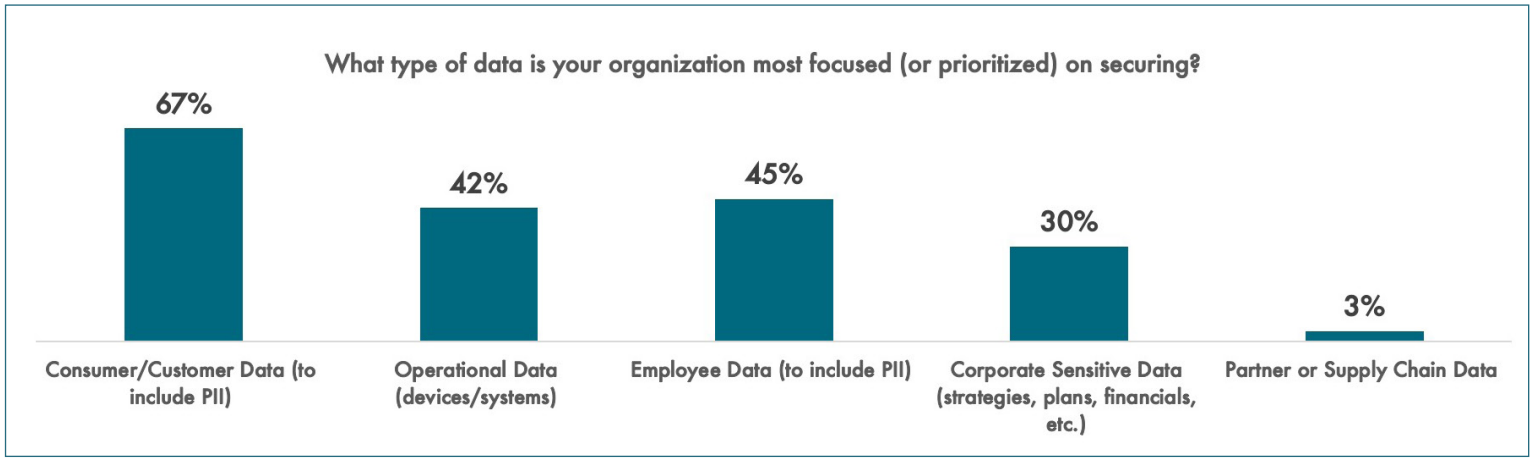
The past few years have been unprecedented in the level of change and disruption that has occurred, from trade and supply chain issues to the ongoing pandemic. Organizations have been forced to adjust and accelerate their digital transformation plans to accommodate; travel restrictions, remote employees, increasingly digital consumers, rapidly changing supply chain, distribution, and operational models.

- *77 percent of enterprises say their overall mindset regarding data privacy, data protection, cybersecurity, and risk management has changed as a result of recent global events*

Threat actors have taken advantage of this digital disruption, aggressively targeting both traditional threat vectors and new, emerging threat surfaces that take advantage of newly digital employees and security gaps that occur as a result of the accelerated deployment of digital technologies through enterprise organizations.

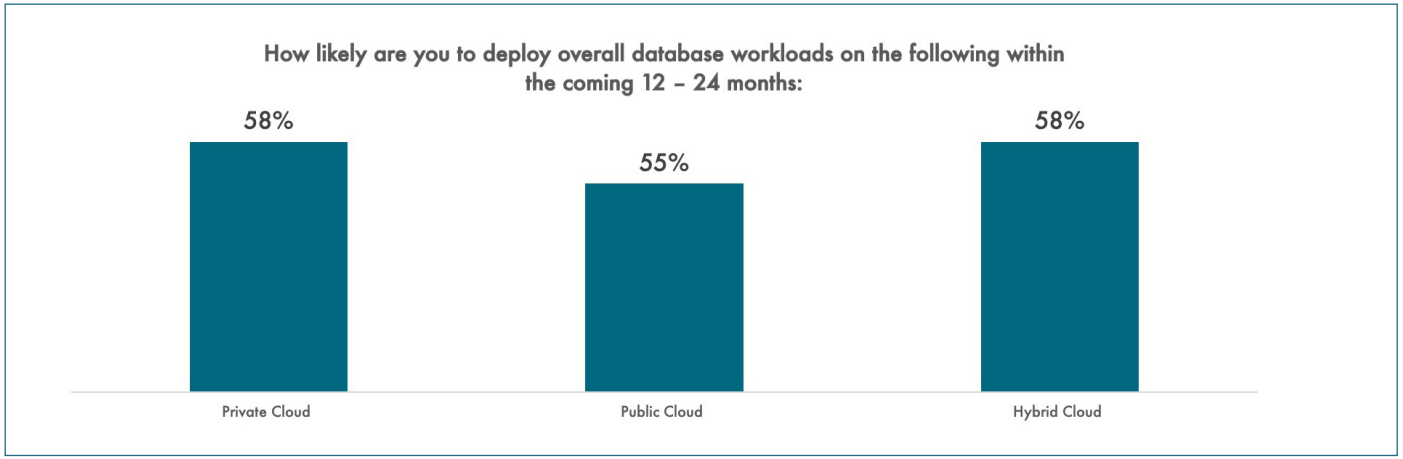
- *81 percent of enterprises say they've experienced a data breach within the past 12 months, with 29 percent experiencing multiple events*

As a result, 9 out of 10 organizations say they've been challenged to maintain a strong security posture to the point where they're rethinking their entire approach to data protection, data privacy, and security/risk management. What types of data are of most concern? Consumer and customer data, including PII, top the list.



Despite the disruption, data continues to move to the cloud.

The migration of data and applications to the cloud is common in many digital transformation and application modernization plans today. For most organizations that means movement from an on-premises private cloud (or data center model) into a hybrid cloud architecture spanning both public and private clouds.

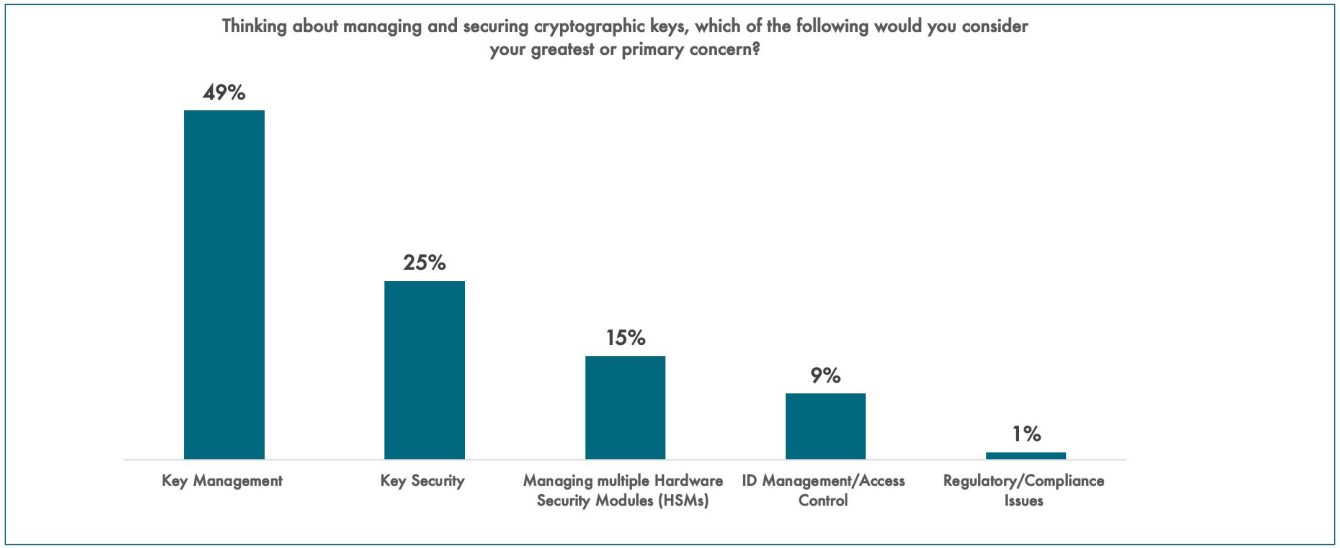


How much data has already been moved to the public cloud? 41 percent of enterprises say they've moved more than half of their overall database workload to the public cloud (this holds true based on both database instances and total data).

How much confidential data has been moved to the public cloud? 66 percent of enterprises say they've moved at least some confidential data to the public cloud. However, it's important to note that less than half of all corporate data is considered confidential by our survey respondents.

2. DATA IN USE: The Evolution of Data Security

As long as there has been a way to value data there has been a need to protect that data. In the beginning of the digital era most data was stored locally within an enterprise on a stand-alone server. Over time these servers were brought together to form the first data centers, but the basic concept of security remained the same: protect the data on the server, aka Data at Rest, through password-protected access and data encryption.

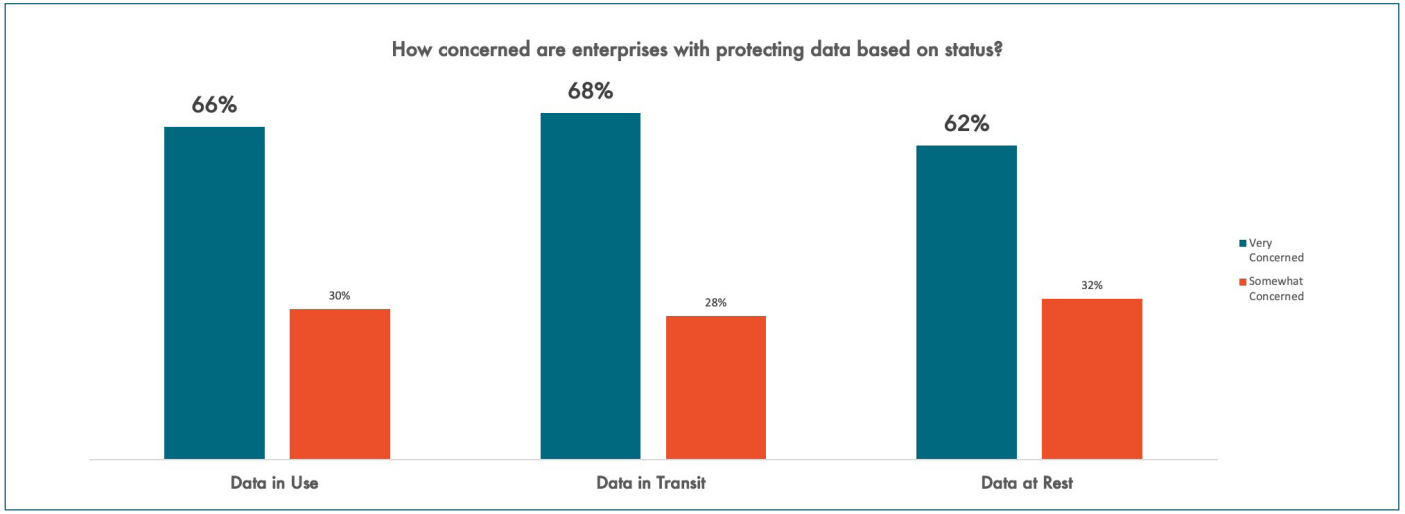


As enterprises began networking servers together across an extended enterprise, the threat evolved as threat actors began targeting (or intercepting) data on the network, aka Data in Transit, which enterprises countered by encrypting communication links.

Today, as organizations move not only their data to the cloud but their applications as well, we have a new threat emerging, one which targets the data while it is used by an application, aka Data in Use.

- *92 percent of enterprises agree that application hacks could potentially expose Data in Use (while data is unencrypted and being processed by an application)*

What's the risk? While existing data security technologies do an excellent job of encrypting Data at Rest (on a server or storage device) or Data in Transit (across a network), existing application and compute architectures require data to be unencrypted to be processed by an application. It's here, at the application level, that threat actors are able to access unencrypted customer data and keys to the encrypted Data at Rest and Data in Transit.



Enterprises have recognized this risk is as a significant threat – particularly for data and applications located in the public cloud.

- *64 percent of enterprises cite Data in Use as their greatest or primary concern*
- *88 percent of enterprises say they plan to invest in technologies or solutions to secure Data in Use within the coming 12 months*

While a majority of the enterprises we surveyed are planning to invest in securing Data in Use, protecting cloud-based applications and the data they process is a new capability not previously available that requires a new approach to architecting and ensuring data security within the applications and cloud compute systems. More importantly, until organizations invest in and implement new technologies their data is at risk.

3. DATA IN THE CLOUD: Building Provider Trust

The migration of data and applications to the public cloud carries with it a number of inherent risks, some of which are born by the enterprise and some of which fall cleanly into the providers domain. To understand these risks it's important to recognize that the ultimate control of any database or application resides with the owner of the system. Within the private cloud, that control resides with the enterprise. However, in the public cloud it's the cloud provider that controls the access to and security of an enterprise customer's data, and that's why it makes sense to encrypt as much data as possible within the cloud.

Even with the best of measures, insider threats from enterprise or cloud provider employees, who have the ability to access unencrypted data, are a very real concern. Similarly accidental misconfiguration of cloud provider assets (which is often cited in the accidental exposure of enterprise data) is another concerning threat.

- *95 percent of enterprises are very concerned about accidental misconfigurations leading to their data being exposed*

Cloud providers offer assurances

Access to data and applications residing in the cloud is ultimately controlled by the cloud provider, who has complete access to all customer assets. To mitigate this risk for customers, cloud providers rely on compliance to industry standards and best practices governing data access.

A cloud provider's certification of compliance or adherence to regulations and standards (such as ISO 27001) may provide a framework for best practices governing the security of data (Operational Assurance) it does not imply the use of technologies that prevent unauthorized access to data (Technical Assurance).

- *80 percent of enterprises agree that provider adherence to industry certifications alone is not enough to protect against security breaches or data theft*

Operational Assurance is about defining and enforcing operational controls (policies) to protect access to data and systems, and to meet security and compliance requirements. For example, in a shared responsibility model, cloud providers provide operational controls (assurances) that privileged access to data systems are monitored, and customers will be notified when operators access those systems.

However, cloud provider employees, can technically access those systems if they choose to do so and have the right credentials.

- *82 percent of enterprises would be very concerned if their cloud provider had the ability to access their data*

Cloud providers are in some circumstances legally obligated to turn over customer data (or to provide databases) if properly requested by government agencies, and there is global standard regarding any obligation by the cloud provider to notify its customers that data has accessed or shared without their knowledge.

- *Our research shows that an overwhelming 93 percent of enterprises would prefer their cloud providers were unable to access or share their data under any circumstance*

The role of Technical Assurance

Where Operational Assurance focuses on behavioral adherence to policies and procedure to not access data, Technical Assurance is about using technical controls (that complement operational controls) where technology is used to enforce data protection. For instance, leveraging hardware-based trusted execution environments (aka secure enclaves) to protect data access in memory or hardened systems that prevent cloud operators from having root-level access to the systems that host databases.

- *92 percent of enterprises believe improving technical assurance would help simplify their own compliance issues*

The net result is that Technical Assurance ensures that a cloud provider, or any other unauthorized party, cannot access or read your data. Just as encryption prevents unauthorized parties from reading Data at Rest or Data in Transit, Technical Assurance technologies can eliminate the risk of application data being exposed to a breach or third party.

- *94 percent of enterprises plan to invest in technology and processes that go beyond existing compliance standards to ensure data security for Data in Use (Technical Assurance)*

The value of employing Technical Assurance technologies goes beyond just locking down and protecting enterprise data and applications – it can provide a technical solution to ensure Operational Compliance as well as assist enterprise organizations in meeting their own regulatory or compliance requirements.

4. DATA SECURED: Why Confidential Computing?

As we've discussed in the prior sections, there is significant risk associated with (and interest in protecting) Data in Use, particularly as part of a Technical Assurance program within the public cloud. But how can these issues best be addressed by enterprises today? Confidential Computing is a key component of the answer, and essential for enterprises embracing a zero trust strategy, where no aspect of the enterprise, from users to servers to applications, is inherently considered a trusted or secure component.

In this section we'll review the different states of data and the challenges organizations have managing and securing data, especially Data in Use. We'll also touch on how Confidential Computing and Trusted Execution Environments can be woven into a larger application, cloud, modernization, and/or migration strategy.

The goal of Confidential Computing and the role of Trusted Execution Environments

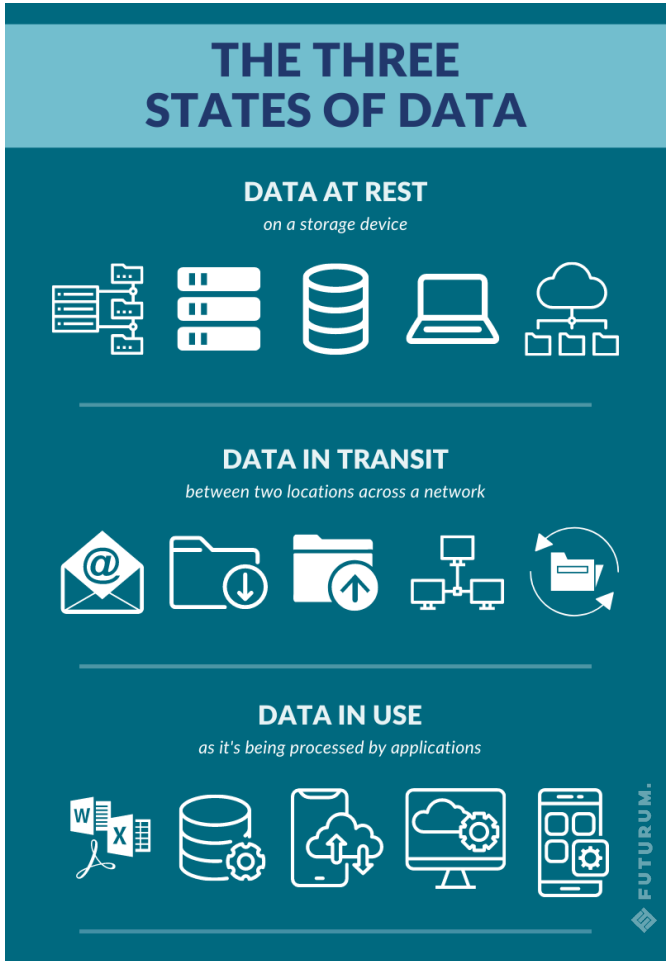
The goal of Confidential Computing is to reduce the ability for an insider (e.g. system administrator) within a public cloud provider's platform to access data and code such that this path is neither an economically nor logically viable attack during execution. This provides Technical Assurance that a provider cannot access customer data.

While it's relatively safe to say there's no such thing as absolute security, there is a way to integrate security more squarely into the architecture, and that's possible when users are able to work within Trusted Execution Environments (TEEs). TEEs are isolated environments for executing code which guarantees a higher level of security for trusted applications running on the device.

In contrast to Operational Assurances which focus on process integrity, a hardware-based TEE ensures that the execution of code (and the processing of data) is totally protected within this environment, thus offering a level of Technical Assurance, focused on hardware/software integrity.

The challenge with securing Data in Use

Enterprise data exists in one of three states:



Using data encryption to secure data on a server or data transiting a network is a routine process today. In contrast, securing data that's in use as it is being processed by applications is much more of a challenge.

Here's why: You can protect Data at Rest by encrypting it and you can protect Data in Transit by further encrypting the communications or network channel. But protecting Data in Use is a different challenge as traditionally you would need to unencrypt the data to use it. For example, it would be impossible to read your email if it's encrypted while you're trying to look at it — and therein lies the challenge. When you unencrypt data in order to use it, that data is in memory, which can be dumped, potentially providing threat actors access to unencrypted data. This issue is further complicated when the administrators of data repositories are no longer employees we trust — or perhaps they are no longer employees.

In addition, when the data resides on a public cloud service, there's the challenge of ensuring the container or virtual machine operators is operating in a trusted way. While our survey respondents told us they trusted their cloud provider partners, they also told us that they were not ok with those cloud providers having access to their data. The reality is that very often cloud providers have access and/or can share customer data as a result of their privileged access to their cloud infrastructure — and compliance to industry standards alone does not always equate to data security, especially the security of Data in Use. As mentioned earlier, our enterprise survey respondents shared that a whopping 64 percent perceive Data in Use as their organization's greatest threat, especially as it relates to data and applications located in the public cloud — with a solid 88 percent reporting an intent to invest in technology and/or solutions to secure Data in Use within the coming 12 months.

What is Confidential Computing and why it's a game-changer

Confidential Computing is a hardware-based approach that ensures the integrity and security of data by utilizing in-memory processing within a Trusted Execution Environment (and ensuring it is not exposed to external risks, exposure, or threats).

We believe Confidential Computing will be able to deliver significant business value include:

- Enabling true end-to-end security encryption
- Replacing policy and compliance-based approaches with technical solutions
- Protecting Data in Use and while being processed
- Providing a model where cloud customers can rest assured that they, and only they, have access to their data
- Enabling the development of technology deployment options that will provide protection against insider threats
- Providing for the simplified management of encryption of keys

It's not hyperbole when we say that Confidential Computing is a game-changer — we see this as the undisputable path forward for today's enterprise.

Hardware plays a crucial role in Confidential Computing

When we look at a full stack view, the overall security of the stack is only as strong as the layers below it. If any layer lower down the stack is compromised, every layer above it in the stack is inherently compromised. That's why we believe that hardware plays a crucial role in Confidential Computing.

When looking to implement the ultimate layer of security, IT leaders must focus on the lowest elements of the stack. In this case, that means a focus on the silicon components of the hardware. What we find exciting is that by focusing on security at the lowest layers of hardware, it is possible to remove the role of vendors in the following layers of the stack:

- Operating system
- Device driver
- Platform
- Peripheral vendors

We can then go even further into the realm of who administers and operates the systems, be they on-premises or in the cloud and remove them from the equation as well. In this case, we are specifically talking about service providers and their admins. This means we can remove these admins from the list of required trusted parties and, as a result, reduce exposure to potential compromise at any point in the system lifecycle.

To further emphasize the crucial role that hardware plays in providing Confidential Computing and on delivering the goal of decreasing the reliance on proprietary software for Confidential Computing environments, the Confidential Computing Consortium has excluded from its scope Trusted Execution Environments (TEEs) that have only software roots of trust and focused on hardware-based security guarantees for Confidential Computing environments.

We hope this background on Confidential Computing, as an adjunct to the data findings from our survey and our team's insights has been helpful. For a deeper dive on the rise of Confidential Computing, download our report: ***The Rise of Confidential Computing — Trust: The New Battlefield in the Age of Digital Transformation***.

NEXT STEPS: Conclusions and Recommendations

The digital world of today is one in which the security of any endpoint, application, or database cannot be guaranteed one hundred percent – we are in a world of zero trust and must act accordingly to secure enterprise assets. As we uncovered in our research:

- Organizations have significantly changed their approach to data privacy, security, and risk management as they have accelerated their digital transformation plans and cloud migration strategies.
- There is a strong need to build on existing measures for securing data at rest or in transit to now ensure security of data in use by enterprise applications, particularly in the public cloud.
- The offer of Operational Assurance by cloud providers, including adherence to process-focused standards and certifications saying they will not access customer data, is not sufficient to ensure privacy and unauthorized access to an organization's data.
- Technical Assurance, through the applications of technology that prevents unauthorized access to customer data, is essential in securing an organization's data in the public cloud.

We believe in the underlying concepts and value of Confidential Computing in a zero trust environment, including the application of Technical Assurance solutions to enforce compliance with process-oriented Operational Assurances by cloud providers regarding customer data in the cloud.

We offer the following recommendations for enterprises as they move forward and migrate their applications and data to the cloud:

Engage in dialogue with your cloud provider

Enterprise organizations are placing a significant level of trust in their cloud providers ability to secure their data, including 64 percent who are strongly confident in their provider's ability to comply with industry standards designed to product customer data. But cloud migrations are often incremental and may involve shadow data within a Line of Business that IT is unaware of and cannot properly secure. Futurum Research recommends that IT

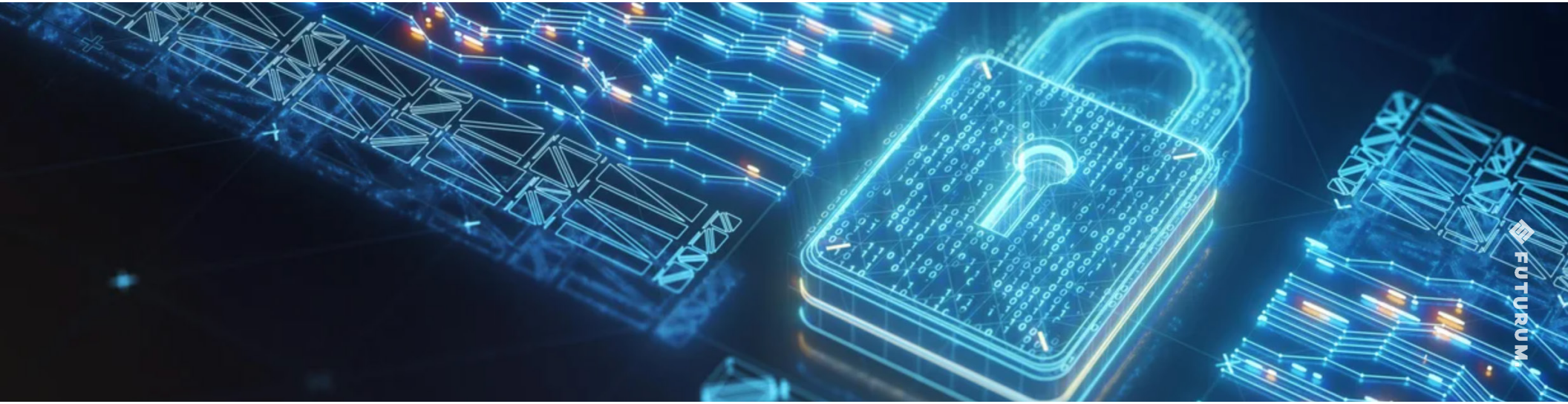
and Line of Business stakeholders actively engage with their cloud providers to ensure all data types and sensitivities are known to all parties and to understand not just a provider's operational controls, policies, procedures but the underlying technologies that are used to secure customer data. This conversation must go beyond compliance and certifications for Operational Assurance and address the underlying technologies needed to provide Technical Assurance.

Review data placement, controls, and the technology stack

It's not uncommon for the security requirements for database workloads to change or evolve over time, and we're pleased to see that 96 percent of enterprises say they're rethinking their approach to data protection, privacy, and security at least at some level. Futurum Research recommends that customers routinely and proactively assess key database workloads to understand the sensitivity of data current stored. We believe that the sensitivity of the data in the database must be matched by the level of security of the underlying cloud platform – the more sensitive the data the more security should be focused the tech stack that supports the data. Where this is not feasible, workloads should be migrated to more secure cloud services with the same provider or in extreme cases to other cloud providers if the level of service cannot be provisioned from the existing provider.

Protect data according to its need and plan accordingly

Organizations must understand the different types and levels of confidential data that exists within the extended enterprise ecosystem and plan data location and security provisioning accordingly. For mission critical, reputationally sensitive, or regulated data, organizations must prioritize for Technical Assurance, including during the provider selection process and particularly where Data in Use is involved. As a majority of enterprises say less than half of their overall data would be considered highly confidential, sensitive, or private in nature, we believe a multi-cloud approach, where the most sensitive data is located on the most secure cloud platforms, can be utilized to appropriately and cost effectively segment and secure data according to its need.



IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTORS:
Daniel Newman
Founding Partner + Principal Analyst, Futurum Research

Shelly Kramer
Founding Partner + Lead Analyst, Futurum Research

Fred McClimans
Research Director + Senior Analyst, Futurum Research

INQUIRIES: Contact us if you would like to discuss this report and Futurum Research will respond promptly.

CITATIONS: This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Futurum Research." Non-press and non-analysts must receive prior written permission by Futurum Research for any citations.

DISCLOSURES: This paper was commissioned by IBM. Futurum Research provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

ABOUT IBM
IBM is a leading cloud and cognitive solutions company. As the largest technology and consulting employer in the world, IBM is trusted by thousands of enterprises across 20 industries. IBM Cloud offers a faster, more secure journey to the cloud. IT teams can easily build and modernize apps with the latest cloud technology from any source using IBM Cloud. With Watson, the AI platform for business, we are building industry-based solutions to real-world problems.

ABOUT FUTURUM RESEARCH
Futurum is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets. Read our disclaimer statement here.

CONTACT INFORMATION

Futurum Research, LLC | futurumresearch.com | 817-480-3038 | info@futurumresearch.com | Twitter: @FuturumResearch