DELPHIX

Your Guide to Developing a Multi-Cloud Data Strategy

Dive into key data challenges IT teams must overcome when mapping a multi-cloud strategy.

The multi-cloud dream

Organizations today are adopting cloud-based applications, platforms, and services to achieve greater elasticity and faster delivery times in today's app-driven world.

In fact, a recent Gartner survey found that 81 percent of enterprises are working with two or more public cloud providers.

As the name suggests, adopting a multi-cloud strategy means using multiple cloud services from different providers, with workloads spread out across cloud environments. While most businesses require rapid and flexible access to computing, storage, and networking resources, not all enterprises are pursuing multi-cloud for the same reasons. Intentions may be motivated by regulatory concerns, as a hedging strategy to avoid unwanted vendor lock-in, or build an optimal business solution by leveraging the best-of-breed services.

Of course, not every team, business function, or application workload will have similar requirements in regards to performance, privacy, security, or geographic reach for its cloud environments. Whatever the impetus, companies must build a culture that puts data front and center in a world where every company is becoming a data company. This leads us to our main points: understanding key data challenges and getting your data ready for multi-cloud environments.

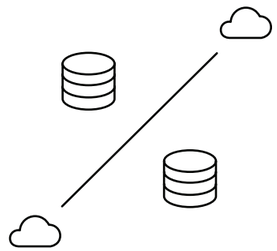
Let the data drive your multi-cloud strategy

While the promise of driving greater operational efficiency, productivity, agility, flexibility, and profitability are luring more organizations to adopt the cloud, IT leaders must first consider addressing data-related challenges in order to successfully build and manage their multi-cloud strategy.

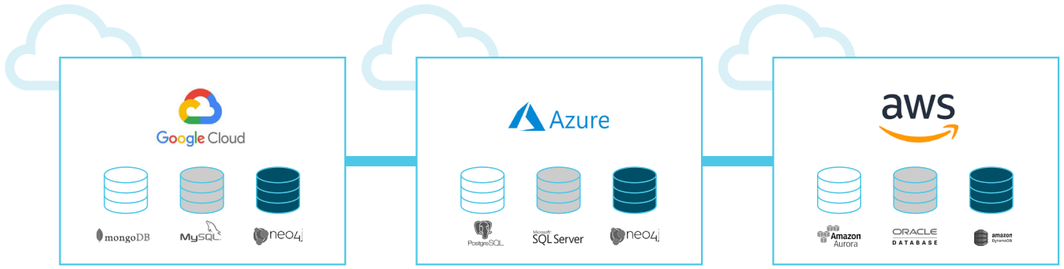
Supercharge your multi-cloud strategy by overcoming these 5 data challenges.

1. Heterogeneous Data Sources
2. Slow, Manual Migration Processes
3. Slow Data Provisioning For Testing
4. Visibility
5. Securing Data In The Cloud

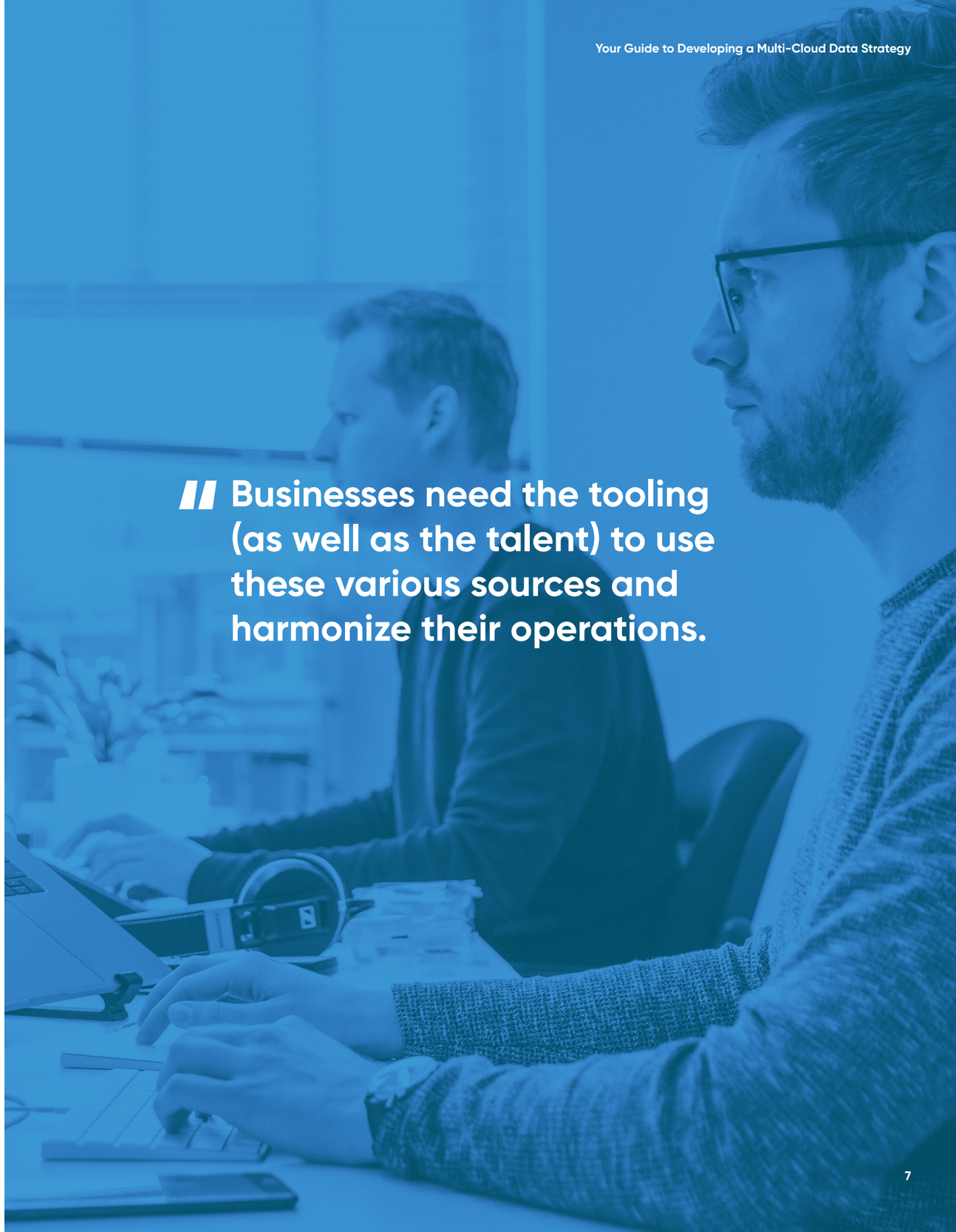
1



Heterogeneous Data Sources

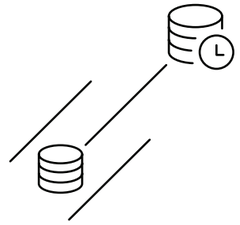


Multi-cloud architectures often encompass a distributed set of applications or services that run on a diverse set of underlying data sources including RDMS, NoSQL, or PaaS offerings that are native to specific clouds. Businesses need the tooling (as well as the talent) to use these various sources and harmonize their operations.



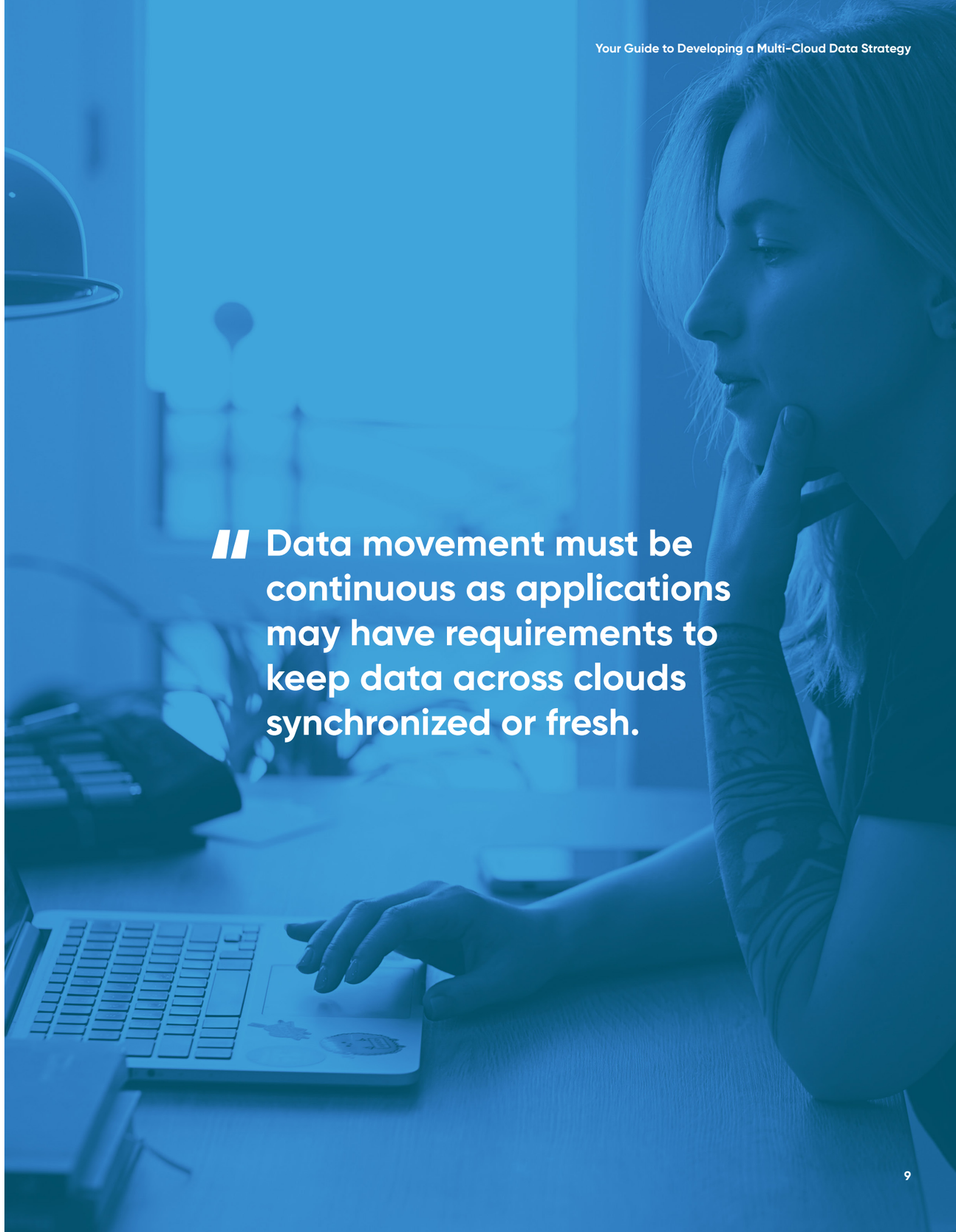
> Businesses need the tooling (as well as the talent) to use these various sources and harmonize their operations.

2

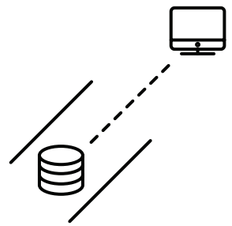


Slow, Manual Migration Processes

Securely migrating large volumes of data to cloud providers can take weeks—and sometimes even involve the shipment of a physical appliance. Moreover, data movement across clouds is not a one-time migration. It must be continuous as applications may have requirements to keep data across clouds synchronized or fresh.



3



Slow, Data Provisioning For Testing

Many multi-cloud scenarios create requirements for rapid, iterative testing that drive demand for test data availability. For instance, when migrating application workloads from one cloud to another, IT teams need new data environments for validation and cutover rehearsal. Or if QA is testing composite applications with components/services that are distributed across multiple clouds, he or she will need data environments (potentially derived from multiple data sources) for integration testing.

67%

Enterprises require 4+ individuals to deliver a data environment

78%

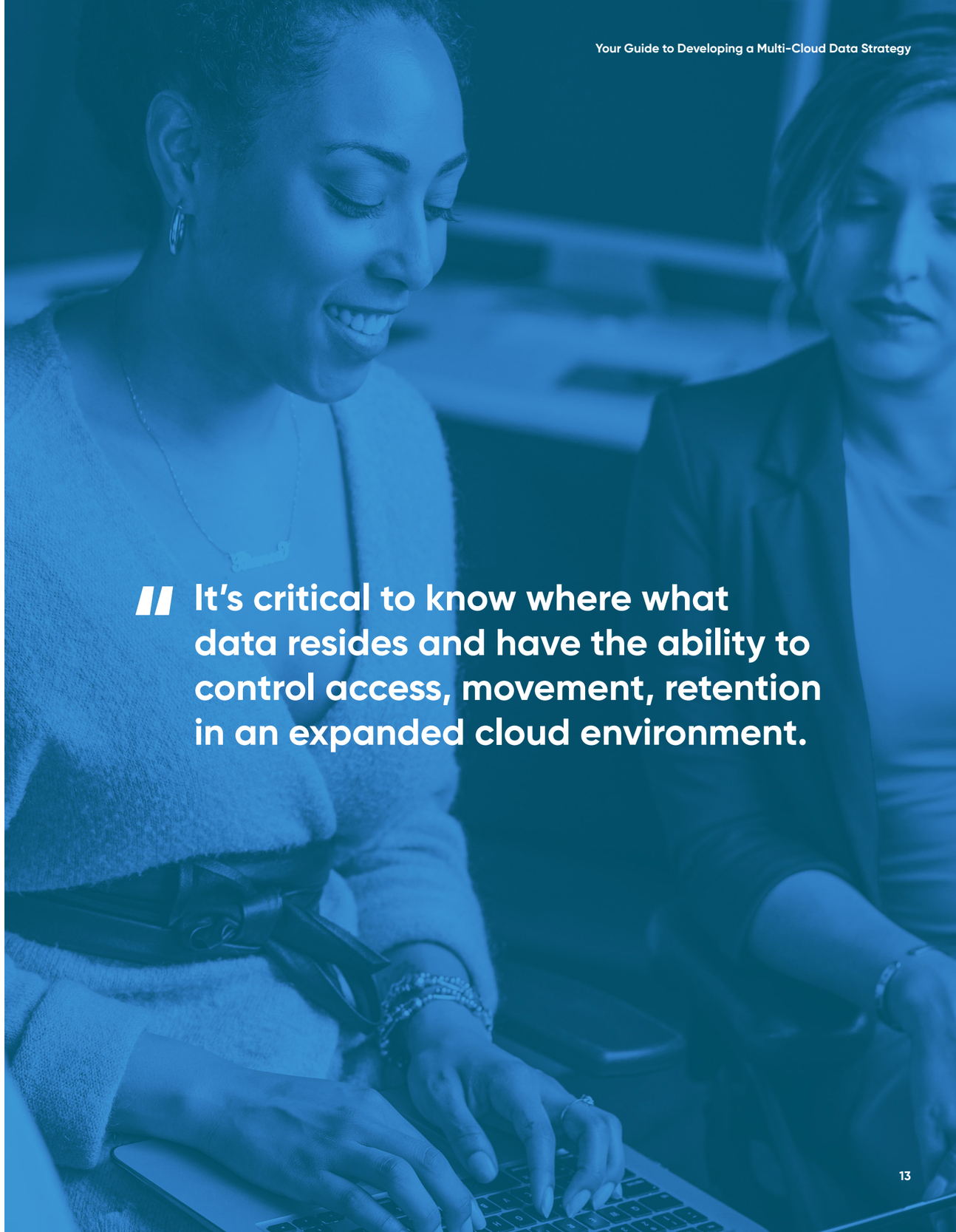
Enterprises take 4+ days to deliver a data environment

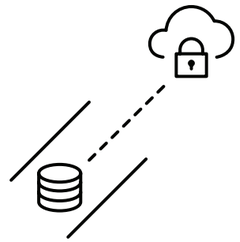
*451 Research: DataOps Survey

4

Visibility

Teams need visibility into data environments across clouds from a single point that establishes who has access to what data in the cloud. It's critical to know where what data resides and have the ability to control access, movement, retention in an expanded cloud environment. Hence, the processes and tools for understanding and controlling data environments must be standardized in a way that works across multiple clouds.





Securing Data In The Cloud

Gartner predicts at least 95 percent of cloud security failures will be the customer's fault. The surface area of risk for sensitive data potentially increases with multi-cloud, and the number of people with access to data may increase as well. Teams need an approach for finding and securing confidential information — to mitigate the risk of breach and stay compliant with privacy regulations, such as the GDPR and CCPA.

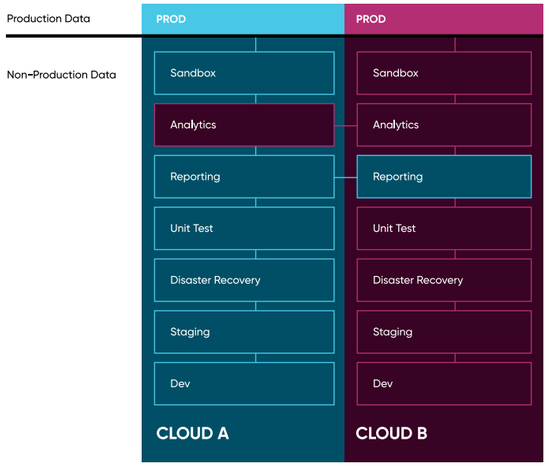
> The surface area of risk for sensitive data potentially increases with multi-cloud, and the number of people with access to data may increase as well.

Getting a grip on data security and compliance in the cloud

Eighty-four percent of organizations say traditional security solutions don't work in cloud environments, according to Crowd Research Partners.

What many organizations fail to realize is non-production environments for development, testing, reporting, and analytics represent most of the surface area of risk. Nearly 47 percent of organizations in the U.S. and Europe already use the cloud for application development and testing, according to a survey by Luth Research and Vanson Bourne. Developers need real data that provides realistic cases for thorough and complete testing. Copying and cloning sensitive information to more and more non-prod environments presents an increased surface area of risk for exposure.

This idea extends to (and is perhaps even magnified or complicated by) multi-cloud architectures in which non-production data proliferates across multiple clouds because data is distributed across a number of locations instead of one—making it that much harder to secure sensitive information.



> Eighty-four percent of organizations say traditional security solutions don't work in cloud environments, according to Crowd Research Partners.

While encryption is recognized as a common and familiar method to safeguard sensitive data, it's not an effective technique when it comes to protecting sensitive information flowing out of downstream environments for development, testing, reporting, and analytics.

Companies need to address this challenge by combining modern security practices, like data masking, with the ability to move data quickly across the organization.

Data masking replaces real data with fictitious but realistic data that is valuable to testers, developers, and data scientists, whereas encrypted data may not be usable or valuable to those same teams.

When data is masked, it has "no value" to a hacker and a compromise is typically a non-event because the masked data is not real. Moreover, masking brings non-production environments that hold most of an enterprises' sensitive data into compliance with privacy laws such as GDPR and CCPA.

Unmasked

Last Name	Phone
Lee	415-230-1283
Rogers	510-512-5123
Lee	317-512-4489
Jacobson	650-965-1117
Sanchez	310-634-8145

Masked

Last Name	Phone
Jones	905-263-7354
Frank	847-512-5472
Jones	415-612-8452
Williamson	312-623-3833
Jones	708-512-5647

Designing a data roadmap for multi-cloud with DataOps

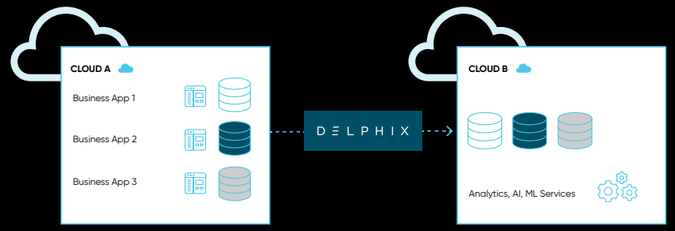
Global business leaders are waking up to the paradox of having to ensure secure data flow in a highly regulated world. Failure to comply with privacy standards can mean millions - if not billions - of dollars in fines, and failure to innovate can mean bankruptcy.

In order to overcome the data challenges in a multi-cloud environment, industry leaders are looking to DataOps as a platform-based approach to grapple with the increasing tension of having to innovate quickly while complying with data privacy regulations. Central to DataOps is the alignment of people, process, and technology that enables the rapid, automated, and secure management of data.

Your DataOps platform should hold these 6 key characteristics in order to eliminate any friction throughout the data lifecycle.

1 Cross-cloud data movement

Allowing teams to move data from one cloud to another at speed while keeping data across clouds synchronized.



2 Fast data environment provisioning within clouds

Accelerating integration testing of distributed, multi-cloud applications as well as be a source of validation for the workloads that are migrated.

3 API-driven automation

Eliminating manual processes and facilitate the integration the integration into DevOps toolchains.

4 Governance across clouds

Understanding where your sensitive data resides and specifying who has access to what data in the cloud through visibility from a single point into data environments across clouds.

5 Protect sensitive data

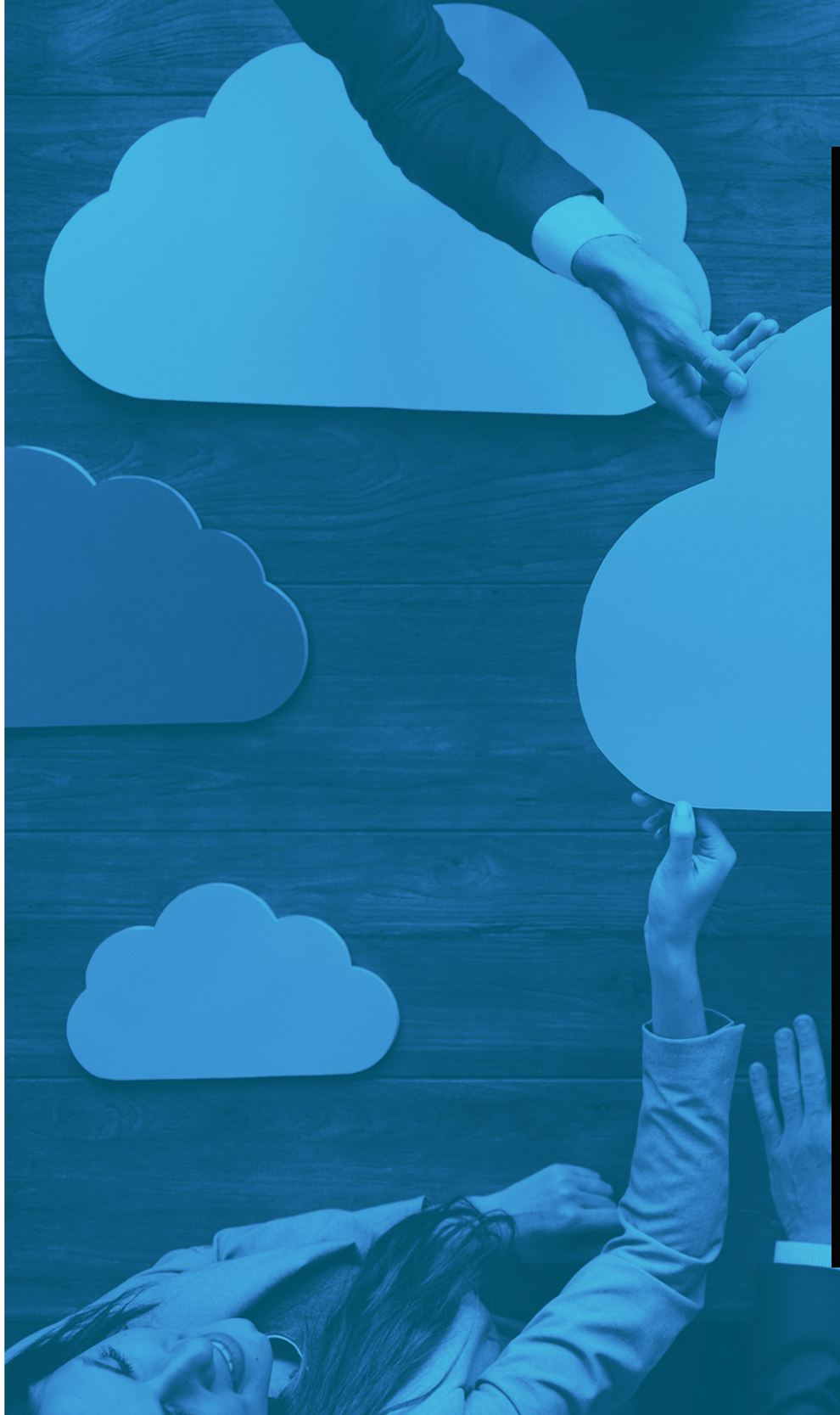
Consistently masking data across clouds in lower tier environments.

6 Works across heterogeneous environments and data sources

Enabling rapid development and delivery of applications by empowering teams to work with data from a diverse set of data sources and securely deliver data to every stakeholder at the speed and scale required by the business.

Putting your data on cloud 9

In a multi-cloud world, addressing the data layer is more important than ever. Data can no longer exist within isolated silos distributed across multiple clouds and locations, and that's exactly what DataOps is devoted to.



Adopting a DataOps platform can help enterprise teams achieve a state of connectedness in which:

1. **Data moves fluidly and securely from anywhere, to anywhere;**
2. **Data is governed in a consistent, holistic manner;**
3. **Businesses can see and control data through a single data platform.**

At the end of the day, companies are only able to innovate when they can unlock the data they need, so companies need to combine the right tools to enable rapid data transformation. When an organization is able to solve their data challenges, it can count on more opportunity to monetize the data, build better experiences for customers, and take their products and services faster to market.

About Delphix

Delphix's mission is to empower businesses to accelerate innovation through data. In a world where every company is becoming a data company, the Delphix Dynamic Data Platform gives teams self-service access to secure, personal data environments to fuel application development, analytics, and AI while also minimizing data risk.

The Delphix Dynamic Data platform serves as the foundation for DataOps across hundreds of the world's leading enterprises. By increasing secure data flow to the business, leading companies across industries have unlocked significant outcomes trapped in their development and IT investments.

DELTA DENTAL®

Migrates and provisions terabytes of secure data to AWS in hours instead of weeks.

StubHub

30% increase in year-over-year sales by enabling superior mobile user experience.

BECU

Masks hundreds of millions of rows of data across thousands of database columns.

eharmony

Enables development and QA teams to create and refresh on-demand, masked data environments based on live production data.

 | delphix.com | info@delphix.com | +1.650.494.1645

Q320-000025

DELPHIX