EBOOK

aptum

CLOUD IMPACT

STUDY

2022

www.aptum.com

SOLVING THE DATA SECURITY EQUATION

INTRODUCTION

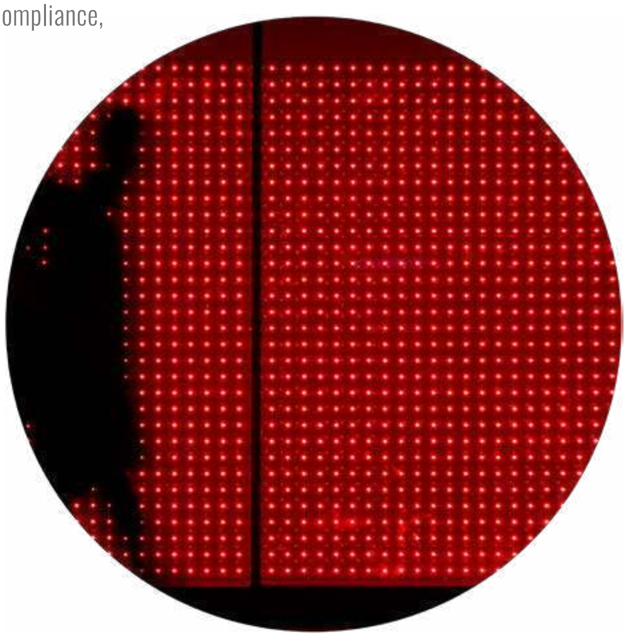
Over the last few years, companies have moved to the cloud seeking security and resilience. They recognized that its distributed infrastructure held the promise of better data protection and robust availability.

But the pandemic caused many companies to rush to the cloud without considering the full security implications of that migration. Now, having realized this issue, many are re-architecting their solutions with security in mind.

The result is a disconnect between the cloud's promise of secure, reliable operations and what cloud users are actually experiencing. While cloud has clearly been instrumental in improving security, organizations still have blind spots.

The first part of Aptum's Cloud Impact Study 2022 revealed that some organizations have, or are considering, moving data back to traditional infrastructures.

In this second part of the Cloud Impact Study 2022, we drew once again on our detailed survey of 400 senior IT professionals to learn more about this issue, and to understand how organizations are working to improve security, compliance, and data governance.



THE CLOUD ATTRACTION: SECURITY AND RESILIENCE

One message came through loud and clear in our research: companies are convinced of the value of the cloud. In fact, 91% of our respondents consider cloud computing to be essential for data management.

Yet effective data management can be expensive, and cost has been a perennial draw for customers since the advent of cloud computing. Switching from a CapEx to an OpEx pricing structure that incorporates security as part of the offering, organizations can more easily regulate costs. Companies eager to cut costs and improve efficiency have gone all in on the cloud. Fifty percent (50%) of our respondents cited efficiency as the top motivator for cloud investments.

The drivers for cloud computing have evolved beyond financial considerations though. Increased security is the second most popular business driver for organizations investing in cloud computing, with 48% of respondents citing it as a key factor in their investment.

The historic rise in cybercrime has already put companies on high alert. More recently, we have seen even more urgent threats relating to cyber-attacks from nation states. The UK, US, Canadian, and Australian governments have all warned of attacks on critical infrastructure from state-sponsored cyber groups. Consequently, organizations are seeking shelter in the cloud.

Resilience is also a key driver of cloud computing investments for 40% of companies. They understand that cloud service providers can offer more robust, reliable infrastructures than they will generally find in their own server room.

This focus on resilience also showed up in attitudes toward disaster recovery. More than a third (37%) of respondents to our survey said that improved backup and disaster recovery inspired their migration to a cloud environment.

Security and backup are critical functions for responsible stewardship of data, which often includes sensitive customer information. With this in mind, data governance was a priority in the choice of cloud for many companies. At 54%, over half believe that cloud transformation has had a positive impact on data governance.

> “The allure of the cloud has always been about resiliency, security, and cost. Paying for what you use has typically been a draw for organizations that have traditionally shelled out huge amounts on servers and other hardware due to the unpredictability of their consumption.”
>
> – Richard Hotchkin
> Director, Cloud Platform Product Manager
> Aptum

54%

BELIEVE CLOUD TRANSFORMATION HAS HAD A POSITIVE IMPACT ON DATA GOVERNANCE

50%

CITE EFFICIENCY AS THE TOP MOTIVATOR FOR CLOUD INVESTMENTS

THE GAP BETWEEN EXPECTATION AND REALITY

> “Businesses use different environments for different purposes. A platform for application development and another as a production site, for example. That’s where you achieve the benefits of a hybrid cloud environment.
>
> But moving workloads between the two environments puts data at risk. So in a hybrid work environment, organizations need to consider securing point A and point B, as well as the movement of data between them.”
>
> – Marvin Sharp, Vice President,
> Product and Strategy
> Aptum

HYBRID CLOUD INFRASTRUCTURES CREATE UNEXPECTED COMPLEXITY

A deeper look at the data reveals some shortcomings in the way organizations are approaching cloud security and resilience, and how they have hampered the results organizations have seen.

What’s causing the disconnect between expectation and reality? One problem facing companies is that ‘the cloud’ is an anachronism. There isn’t just one cloud solution anymore; there is a disparate set of services, spanning multiple providers and on-premises environments with diverse and disconnected infrastructures. These hybrid and multi-cloud infrastructures are now commonplace, with 44% of companies using multi-cloud environments, and 42% using hybrid cloud.

This move to hybrid and multi-cloud environments has made disaster recovery more complex than people initially imagined. Many companies that envisioned a single backup site are finding themselves spreading data across multiple providers.

This diversity has its upsides in terms of data resiliency because companies no longer need to rely on a single provider. The challenge is in its complexity. Deciding what data to back up, and how often, has always been a challenge for organizations, but now they must factor in distinct locations too.

Organizations must consider issues such as cost, recovery time objectives (RTOs), and data sovereignty when backing up into the cloud. This all increases the management burden and creates concern over the speed and scope of data restoration in the event of a disaster.

This complexity also affects an organization’s ability to manage data privacy in cloud environments. Entrusting data to a third party is unnerving enough for some companies, but dispersing it across multiple cloud providers makes IT teams extra anxious. It’s no wonder that 44% of our respondents cited data privacy and security as top challenges in their cloud transformation projects.

NOT JUST ‘THE CLOUD’ ANYMORE

44%
USE MULTI-CLOUD

42%
USE HYBRID CLOUD

> "Disaster recovery is traditionally thought of as being in one environment – usually very secure public or private cloud facilities. Various experiences of downtime during the pandemic confirmed the importance of a coherent disaster recovery strategy. But as hybrid environments become more widespread, disaster recovery becomes more complex, and it's likely to become more dispersed as a result."
>
> – Marvin Sharp, Vice President,
> Product and Strategy
> Aptum

CLOUD COMPLEXITY IMPACTS ON SECURITY

As companies find themselves taking on more cloud services to serve different use cases, the complexities increase. They also cause other concerns and barriers that affect business outcomes in several areas:

Access

Deciding and enforcing who has access to hybrid and multi-cloud environments is one consideration. As the number of providers and user profiles grow, access controls become more complex. Yet secure, well-managed access is a table-stakes measure in cloud computing. According to our research, 90% of respondents said controlling and governing access to cloud environments is a challenge to cloud security and governance.

Visibility

You can't manage what you can't see, and many cloud computing customers cannot see all their operational data. We found that 88% of respondents cite full visibility into all cloud environments as a challenge to security, compliance, and governance. Fragmented hybrid and multi-cloud environments exacerbate this problem.

Transfer

Another challenge for hybrid and multi-cloud customers is transfer of data. While customers might trust each of their cloud service providers, they will need to move data between them, or between their own premises and the cloud. Cloud-based backup and disaster recovery at the very least demands this. Transferring this data between different infrastructures is a potential weak spot for security, and a headache for customers.

48%

INVEST IN CLOUD
FOR INCREASED SECURITY

> "Organizations must view cloud as another piece of an expanding estate that is becoming ever more complicated. They may have traditional on-premises infrastructure services; others in a data center; a private cloud with Aptum or another provider; and they are likely to have environments in a hyperscaler like Azure or AWS. It is more complicated than ever before.
>
> Security is an issue because as organizations add more environments, they inherit the security problems that come with each of them, as well as the resiliency, cost, and data governance implications."
>
> – Richard Hotchkin
> Director, Cloud Platform Product Manager
> Aptum

Detection and response

Lack of visibility into infrastructure and operations data also makes it difficult to spot and respond to security threats. Nine in ten respondents said they lack a clear mechanism to detect and respond to security threats across all cloud environments.

Compliance

The above problems all risk putting companies in violation of regulations such as GDPR and California's Consumer Privacy Act (CCPA). Rules are growing increasingly strict, and regulators are empowered to impose stronger penalties. It is no wonder that 90% of respondents consider it a challenge to meet compliance needs.

Service Level Agreements

The effect of distributed cloud infrastructures on reliability also creates practical problems for cloud users. Almost nine in ten told us it is challenging to provide internal service level agreements (SLAs) to the business when running services in the cloud.

STRATEGY IS KEY TO CLOUD TRANSFORMATION

These challenges stem from something that came up in the first part of Aptum's Cloud Impact Study 2022: a lack of strategic thinking when tackling cloud transformation. Only 20% of organizations had a holistic cloud computing strategy. The other 80% have a fragmented approach to cloud transformation that lacks the necessary big-picture thinking.

80% LACK A CLEAR CLOUD STRATEGY

This has affected security in cloud transformations, which demands strategic thinking because it touches every part of a company's technical and business operations. The importance increases as cloud implementations become more complex. The strength of your security is only as strong as the weakest link, and a complex hybrid cloud environment has many moving parts.

> "The cloud is maturing, and customers' expectations are maturing along with it as they learn about the possibilities it offers for digital transformation. Nevertheless, we still see companies rushing enthusiastically into migration projects without stopping to understand all the implications of their actions. When it comes to game-changing projects, planning is key."
>
> – Marvin Sharp, Vice President,
> Product and Strategy
> Aptum

COMPREHENSIVE CLOUD STRATEGY DELIVERS SECURITY RESULTS

You can create space for a strategic approach by assessing your cloud readiness before and throughout the migration. Consider the types of data you store in the cloud, or need to, along with who is using the data more frequently, and for what purpose. Understand your assets, the processes that protect them, and how these can be mapped to a hybrid or multi-cloud environment.

After considering your readiness for the cloud and your desired business outcomes, you can create an ideal architecture for your cloud solution. It should cover every consideration from the application layer through to core infrastructure.

This architecture should also span multiple domains extending beyond individual cloud service providers, and infrastructure should be included in your cross-provider strategy. It is crucial to craft data communication, visibility, and control frameworks that encompass your entire hybrid and multi-cloud strategy.

Eliminate any disconnect between the cloud's promise of secure, reliable operations and what might be experienced by including security as part of a comprehensive cloud strategy. Seeking expert advice from a technology-neutral third-party provider that specializes in unifying hybrid environments will help develop your strategy and implementation plan and ensure a clear path to success.

TO LEARN MORE ABOUT HOW OUR SERVICES CAN HELP YOUR ORGANIZATION, PLEASE VISIT:

info@aptum.com
www.aptum.com