EBOOK

aptum

# CLOUD IMPACT STUDY

www.aptum.com

# THE SECURITY AND COMPLIANCE BARRICADE

"More organizations are adopting 'cloud-first' strategies and shifting core business processes to public cloud systems and services every day. Although the public cloud comes with great financial and technical benefits, like any other infrastructure, it also has its share of security challenges," said Dan Webb, VP of Partner Sales and Alliances, Alert Logic. "With increases in cloud incidents related to vulnerability scanning, web application attacks, and brute force attacks, organizations must understand the types of threats potentially targeting their cloud deployments and reduce the attack surface. By combining cloud native security technologies with cloud infrastructure security experts, organizations will successfully find vulnerabilities in their IT environments before their adversaries do."

– Dan Webb, VP of Partner Sales and Alliances, Alert Logic

## INTRODUCTION

**The Security and Compliance Barricade** is the second report in a four-part series, evaluating the findings of Aptum's Global Cloud Impact Study. Aptum's inaugural annual study canvassed opinions from 400 senior IT decision-makers across the UK, the US, and Canada.

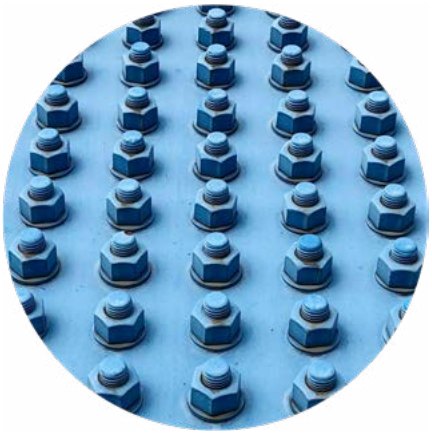
The first report reveals the business drivers behind cloud adoption and the obstacles impacting organizations undergoing cloud transformation. Building on these initial findings, our second report takes a deep dive into the common security, compliance, and governance challenges affecting organizations as they digitally transform.

## EXECUTIVE SUMMARY

As a result of the global pandemic, Gartner predicts IT spending will decline by 8 percent this year, dropping from $3.7T in 2019 to $3.4T. Despite this, enterprises' spending on cloud computing continues to grow, defying the pandemic-driven economic downturn with the analyst firm predicting worldwide public cloud revenue will grow 6.8 percent in 2020.

As organizations increasingly move workloads and applications to the cloud; they are also investing in cloud security. Gartner further predicts that cloud security revenues will see a 33 percent year-on-year growth during 2020 – the only area of security enjoying double-digit growth this year.

Part 2 of Aptum's survey reveals the importance of security as a significant driver for cloud transformation but also highlights how security and data protection concerns present a challenge that acts as the primary barrier to cloud transformation. This report explores how cloud computing can bolster the overall security of an organization, but as deployments become more complicated, so too does data governance and security.



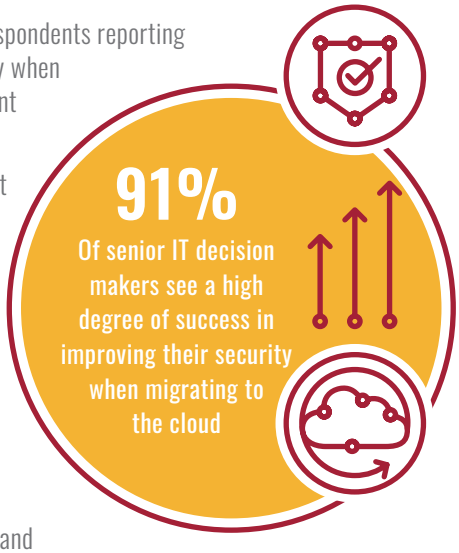
"Cloud security standards have drastically matured over the last five to ten years to surpass on-premise alternatives. On-prem security is usually infrastructure-based, where it is down to IT staff who may not possess specialist skills to manage and configure security policies in automated way. On the other hand, cloud security frameworks have become more sophisticated, and the data-centric approach that cloud providers encourage has entrenched a higher standard of security in cloud environments, to the extent that those security policies and frameworks are now largely fully automated leveraging infrastructure as code."

– Craig Tavares, Global Head of Cloud, Aptum

## SECURITY DRIVES CLOUD ADOPTION

There's no doubt that security and data governance are significant drivers for cloud adoption. Over recent years the same message has been promoted: user data is safer in cloud infrastructures than in on-premises environments.

This claim has merit with 91 percent of Aptum's respondents reporting a high degree of success in improving their security when migrating to the cloud, and an impressive 42 percent claiming to see complete success.

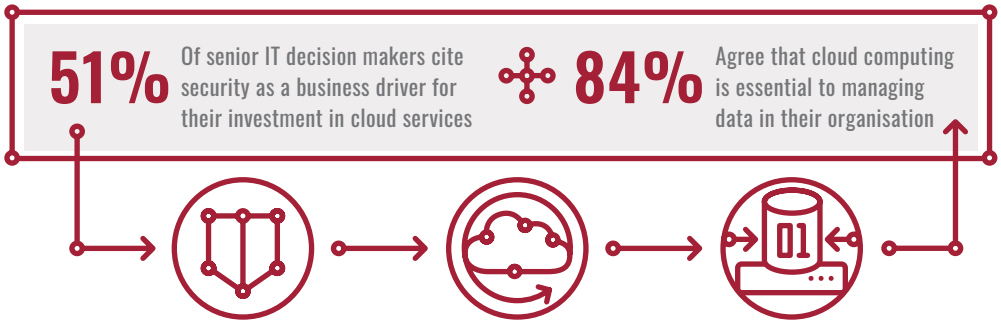



The range of cloud-based solutions used over recent years, and during the pandemic, has enabled organizations to achieve a stronger standard of security. Cloud productivity applications, for instance, can keep sensitive files from being copied to unauthorized computers in combination with endpoint protection strategies on remote devices. For companies with employees working from home on their personal computers during the pandemic, this kind of data protection is essential.

Cloud service providers also offer valuable identity and authentication based tools to handle logical security functions such as access rights, either as part of a software as a service (SaaS) productivity solution or via virtual desktop services. With 84 percent of respondents agreeing that cloud computing is essential to managing data in their organizations, cloud access security and control solutions help manage what personnel have access to that data.

The standard level of physical security organizations can achieve with cloud computing is significantly higher than on-prem alternatives. This is especially important for companies with fewer dedicated IT resources that may not have the knowledge or equipment to protect data held in a server room on their premises. Restricting access to authorized personnel is a demanding process involving a mature approach to physical security. Not all organizations have the benefit of, or resources to support, sophisticated physical security like multi-factor authentication or buildings designed to protect sensitive assets.

Additional necessary security measures such as perimeter security, server hardening, advanced detection and response are part of a cloud managed service provider's core business. Combined with the above, it is clear to see why over half of all survey respondents (51 percent) list security as a business driver for their investment in cloud services.



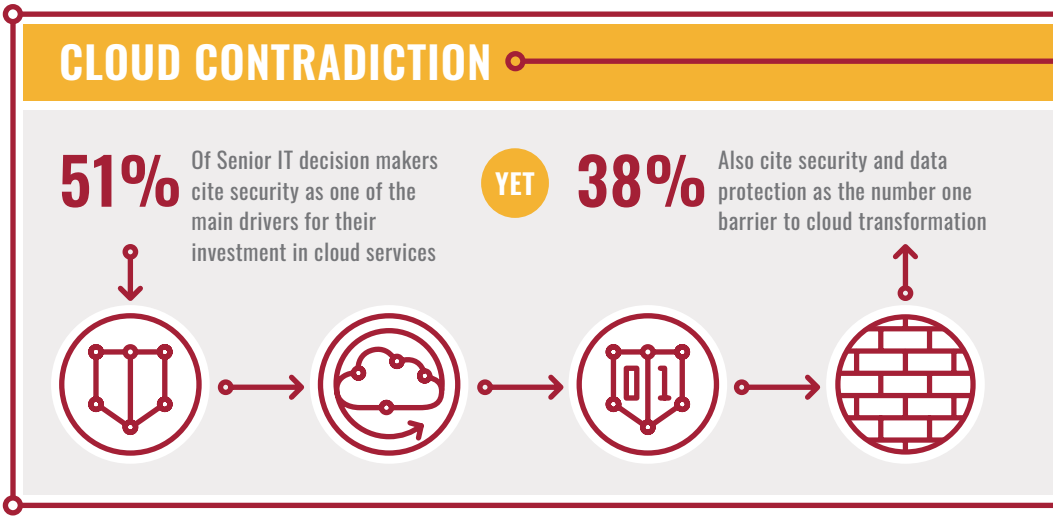
## SECURITY ALSO HOLDS IT BACK

While security may drive organizations to the cloud, it is also the most significant source of speed bumps along the way. Over one third (38 percent) of respondents cite security and data protection as the number one barrier to cloud transformation. The sentiment around cloud security seems contradictory. So, what's going on?

Cloud transformation is a gradual process rather than a binary one. Organizations rarely move everything to a cloud environment all at once. Part one of Aptum's Cloud Impact Study, Bridging the Cloud Gap, found that respondents are planning to take a hybridized approach to their cloud set up within the next 16-24 months:

- 59 percent plan to reduce on-premises workloads
- 59 percent plan to increase public cloud deployments
- 66 percent plan to increase private cloud deployments

The move towards a hybrid approach to cloud leaves organizations with disparate systems scattered across traditional and private cloud environments on a company's premises, hosted private cloud alternatives, and multi-tenant public cloud instances. Many organizations will use multiple cloud providers to suit varying business needs. For IT teams ill-prepared to manage this array of new ecosystems, that creates more problems than it solves.



## THE BIGGEST PROBLEM IS COHESION

Despite 84 percent of respondents agreeing that cloud computing is crucial to managing data in their organization, this seems to be the largest stumbling block. Having created complex infrastructures, organizations are encountering difficulty in monitoring and uniformly managing them.

**85%**

Of respondents cite a lack of a clear mechanism to detect and respond to threats across all cloud environments as a barrier to security, governance and compliance.

**82%**

Of respondents cite access management to multiple cloud environments as a barrier to security, governance and compliance.

**81%**

Of respondents cite a lack of visibility into all cloud environments through a single portal as a barrier to security, governance, and compliance.

This lack of visibility makes a hybrid cloud environment challenging to manage. It can be a challenge to manage and have visibility into a cloud that abstracts data and applications away from the hardware. A multi-cloud environment only exacerbates this problem.

Without this capability, organizations cannot easily handle security events across private and public cloud installations. As cybercriminals move to faster, more frequent attacks, security becomes a growing problem for hybrid and multi-cloud users.

In addition to this, if organizations don't have full visibility into their hybrid and multi-cloud infrastructure, then it creates a challenge for them to meet their regulatory or compliance requirements. Eighty percent of respondents' state their ability to meet requirements of compliance audits efficiently across their cloud environments as a main challenge.

This is where one of the cloud's most significant benefits becomes one of its biggest challenges. By design, cloud infrastructures are flexible and empower their users. The ability to spin services up and down has helped many businesses adapt over the last six months. Still, if one of those resources has been misconfigured with sensitive information and left unmanaged, security and compliance can be very difficult to achieve for IT staff.

"A Hybrid environment, increases the overall surface area of attack. As the variety of platforms increases, so too do the number of systems, applications and endpoints that need to be secured. The switch to remote working has further complicated these issues, as Bring Your Own Device (BYOD) policies have increased endpoints, creating more avenues for attack. Managed detection and response (MDR) solutions give enterprises the tools to manage the risks and threats across all platforms, including private clouds, public clouds and bare-metal environments. Organizations can also reduce the burden on their internal resources by outsourcing the management and detection of vulnerabilities, threats and intrusions to security specialists."

– Craig Tavares, Global Head of Cloud, Aptum

## A STRATEGIC APPROACH

Businesses are hoping for more secure operations as they venture to the cloud. For the most part, they are successful, but complexity stops many of them from fulfilling all their security and data governance goals. How can they solve their complexity problems to unlock the full security benefits of a cloud environment?

The answer lies in a strategic approach to security as part of a cloud transformation initiative. Security should be a priority at all stages of the cloud transformation process, from initial concept through design, implementation, and ongoing operation.

Visibility has always been a vital part of the security equation. In on-premise environments the entire infrastructure operates within a single trust domain under the administrator's control. When that infrastructure atomizes, spreading across multiple environments, controlled by different service providers, visibility becomes harder to obtain but is equally important.

Holistic security practices should also focus on individual applications and data. Who can access them, and with what privileges? Where are those privileges stored, and how? Beyond that, it encompasses workloads, in which multiple applications interact together to produce the desired outcome, possibly across different cloud provider environments or in a hybrid on-premises and cloud environment. What are those applications exposing via cloud-based APIs? How secure are the connections between them?

These considerations have implications for hybrid architecture design. They affect which applications migrate to the cloud and how. They also inform which security services move to the cloud. Many security tools that work well in an on-premise environment won't work in the cloud, but service providers offer alternatives.

"Historically, security has been a significant issue for cloud users. However, most companies now understand the security benefits of cloud computing, and the opportunities it offers in terms of securing a remote workforce, especially during the pandemic. Yet, a common challenge among businesses, including our customers, is the ability of internal teams to architect a cloud solution that embeds strategic security principles from design. One should design a cloud infrastructure using secured landing-zones and leverage industry best practices, like the Centre for Internet Security benchmarks, Cloud Adoption Framework and Well-architected Framework."

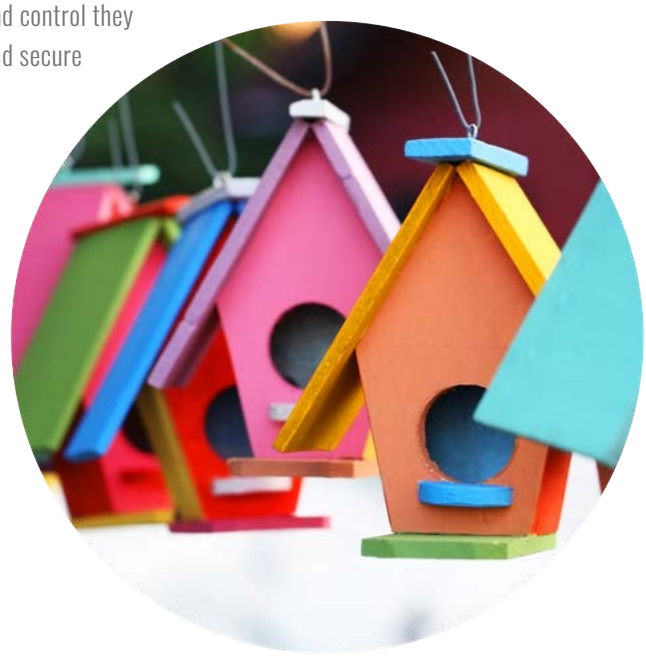
– Craig Tavares, Global Head of Cloud, Aptum

## CONCLUSION

With so many moving parts, it's no wonder that organizations feel out of their depth when tackling their cloud security issues. Over a quarter (26 percent) of respondents cite a lack of expertise as a barrier to cloud transformation. Many of the cybersecurity issues affecting cloud transformation projects are 'unknown unknowns'. For many who start down this road without the necessary in-house expertise, the problems only become apparent after a project has hit critical milestones.

Organizations should take a strategic approach to cloud security from the beginning of a project. Working with a seasoned third-party service provider can help them to understand all the issues during the design phase so they can build on solid foundations.

By taking a holistic approach to cloud architectures, with security principles embedded in the design, businesses can mitigate and minimize risks to create an environment safer than any on-premises or legacy alternatives. Organizations can then create a hybrid cloud infrastructure that gives them the visibility and control they need to achieve a successful and secure cloud transformation.



**Demographics:** Aptum commissioned research company Vanson Bourne to survey 400 executives in the US, Canada and UK. They spanned business unit heads (58 percent), business leaders (22 percent), and departmental managers (21 percent). across industries including IT, financial services, professional services, manufacturing, retail, and the public sector. Business sizes ranged from 500 employees upwards.

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

info@aptum.com
www.aptum.com