POINT OF VIEW

A Practical Approach to Cloud Security

Executive Summary

Organizations are accelerating digital business initiatives to help them survive and grow in response to the global pandemic experience and ongoing sophisticated threats. This environment creates challenges and opportunities for CIOs and CISOs as they are expected to create new value for customers and accelerate their digital investments while keeping their networks secure.

Digital acceleration has led organizations to drive toward delivering faster and better application experiences via cloud and cloud-native applications and to bring applications and data closer to users and devices through edge computing. However, the pandemic has also forced organizations to migrate to the cloud faster than planned, resulting in increased operational complexity, visibility gaps, explosion of cloud platforms and tools, and "accidental multi-clouds."

To securely reach their digital acceleration goals while maintaining momentum, organizations need to consider adopting a cloud strategy that is centered around a cybersecurity mesh platform approach.

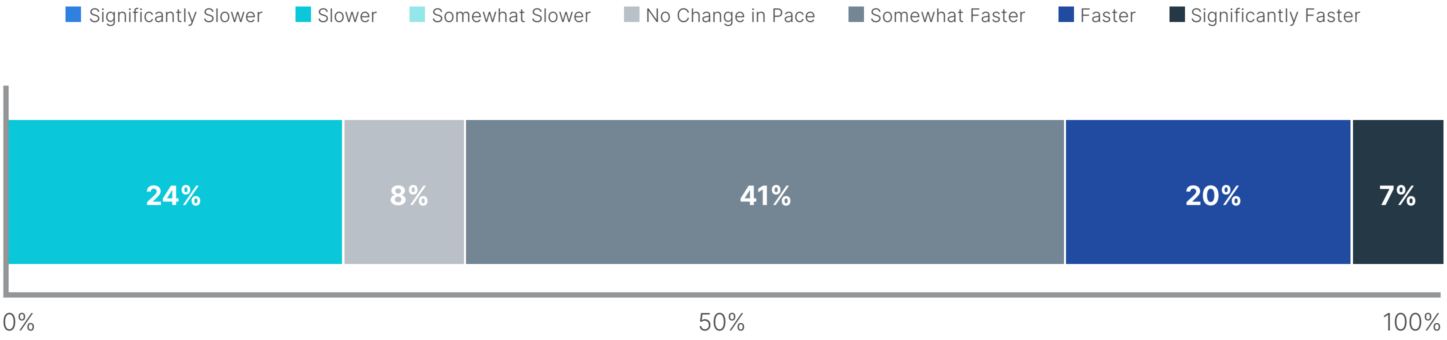
In a recent Gartner® survey, 68%[1] of boards have responded to post-COVID-19 with digital business acceleration to improve operations excellence through digital business by investing into modern technologies to deliver superior user experience. Steady progress isn't enough anymore, and boards have CIOs focused on acceleration.

Digital Acceleration: All Roads Lead to Cloud

In the push toward digital acceleration, cloud adoption and the migration of applications into the cloud are key success factors for many. This journey, however, is also personal for many organizations.

Organizations are all at different stages of their application journey to the cloud; many are still unsure where their application journey will take them. At the same time, those making application journeys into the cloud are faced with security and operational challenges as they increase the number of cloud and application edges.

Increased Digital Acceleration Post-COVID-19



n = 60; Education Industry Respondents, excluding "Unsure/NA"

Source: 2021 Gartner Innovation in Crisis Survey

753775_C

Gartner, "Advancing Digital Innovation in Education in Response to a Crisis", Saher Mahmood, Robert Yanckello. September 16, 2021

Cloud Challenges and Trends

Despite the pathway to the cloud being varied, the top challenges organizations face are the same. At some point, every organization will come across the following in varying degrees:

Multiple application and cloud edges

- Organizations are migrating applications toward a "cloud-native" approach that promises faster application delivery and outcomes. However, the reality is that not all applications are suitable for transitioning to the cloud in full, and not all applications are suitable to be deployed on all clouds. With the explosion of application and cloud edges across differing cloud platforms, organizations struggle with maintaining full visibility and consistent security policies across all points of their deployment.

Forced acceleration to the cloud

- External drivers such as the COVID-19 pandemic or dynamic business drivers such as board mandates or response to intense competition force organizations to undergo unplanned rushed acceleration to the cloud. Examples of these unplanned decisions include "accidental multi-clouds" and lack of security policy and process consistencies across clouds. The consequence is increased risk due to exposure to misconfigurations, operational complexity, loss of visibility, and inconsistent policies—all of which are further exasperated by resource and skills gaps.

Customer experiences should not be impacted by where applications live

- Organizations pursue the cloud to deliver better application experiences to their users and customers. The choices, whether intentional or unintentional, in where applications live or what technologies are used in their delivery should not matter or impact customers or users.

Edge compute

- To further improve customer experiences of cloud-enabled applications and reduce costs of delivering those experiences, some organizations have started to pursue edge compute architectures. Edge compute moves applications and data closer to users and devices. However, the cost of doing so is increased deployment, operational and security complexity, and even greater loss of visibility. Now organizations need to worry about regional and local clouds on top of hybrid and multi-clouds that they are already overwhelmed by.

A Practical Approach to Cloud Security

Fundamentally, these deployment challenges come down to that it is all about the application journey itself. The emergence of cloud edges, edge compute, the need for hybrid and multi-cloud, etc., all come down to the need to deliver application experiences faster with the best performance possible.

For many organizations, their application journey involves a continuous lifecycle composed of three stages: build, deploy, and run.

- **Build:** As part of moving faster, organizations are moving toward a continuous and rapid development methodology in the cloud, often referred to as the continuous integration/continuous deployment (CI/CD) pipeline.
- **Deploy:** As applications get deployed to the cloud, organizations need to consider security of the cloud environments of where the applications live. This is often part of what cloud providers consider to be the "shared responsibility" model, whereby the provider ensures the physical security and integrity of the cloud infrastructure itself. Still, the onus of securing the applications and virtualized cloud instances they run on are left to the customer. Again, where applications live should not impact experiences delivered to customers and end-users.
- **Run:** Applications and application programming interfaces (APIs) themselves require protecting against threats. Additionally, application performance through security acceleration and automated application scale-up and load-balancing are also important.

Organizations should first ask where they might be in their application journey. Are they driving toward accelerating delivering new cloud-native applications? Or are they at a point where they are focused on putting already built applications into production and in need to secure the cloud or virtualized data center environment as well as securing the running applications and APIs themselves? Doing so makes the problem of securing the cloud much simpler to solve as organizations can prioritize their investment and deployment plans.

Next, organizations should ask themselves where in the cloud do they need to deploy and ensure that the security solution is well integrated and seamless for that environment. If deploying on AWS, Azure, or Google Cloud, does the solution offer integration into the cloud technologies or marketplaces of the respective clouds? Oftentimes, applications might be in need to work across multiple clouds and hybrid clouds. Does the security solution allow for this scenario and work seamlessly across the deployment points with consistent policies? This matters as it not only reduces complexity but also solves for one of the major threat vectors of the cloud—namely, misconfigurations.

To further reduce complexity and increase security effectiveness, organizations pursuing application journeys in the cloud need to leverage a cybersecurity mesh platform approach. A cybersecurity mesh platform empowers organizations to benefit from centralized visibility and management, and automation across all solution points, and allows them to leverage intelligence sharing for the fastest response to threats. Ultimately, this reduces complexities, solves for cloud cybersecurity skills and resource gaps, and increases overall security effectiveness. As such, organizations should look for solutions that integrate and support a broad, integrated, and automated cybersecurity mesh platform.

And finally, when speaking to customers, we often find that the application journey through the cloud is constantly evolving. Many are still unsure what the move-forward strategies will be. As a result, organizations should also consider how flexible the cloud security solutions they adopt can be, and if these solutions will allow them to secure any application journey on any cloud.

Conclusion

As organizations pursue their digital acceleration initiatives, successfully securing and executing on their application journey plans is a critical element of the initiative. The application journey they take is directly tied to how well they can compete and succeed in today's business landscape. While organizations aim to move their applications toward cloud-native, the reality is that there will be critical applications that will need to be maintained on-premises for legacy or compliance or for business-driven considerations that create cloud and application edges that span across hybrid and multi-clouds, varying cloud platform providers, virtual data centers, and edge compute instances. Ultimately, this creates complexity, overhead, and security challenges that work against the spirit of digital acceleration.

> **"By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%."[2]**

To succeed in securing and achieving digital acceleration without compromise, organizations need to adopt flexible, well-integrated security solutions across build, deploy, and run stages of their application journeys, which are supported by a broad, integrated, and automated cybersecurity mesh platform. Not only will this allow organizations the ability to secure any application journey on any cloud, but it will also empower them with the freedom and flexibility to evolve as needed, building upon today's investment for tomorrow's journey.

[1] Gartner, "Advancing Digital Innovation in Education in Response to a Crisis", Saher Mahmood, Robert Yanckello. September 16, 2021

[2] Gartner, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. 18 October 2021.

FORTINET®

www.fortinet.com

March 24, 2022 3:40 PM

1519764-0-0-EN