FORTINET

Securing the Application Journey

Table of Contents

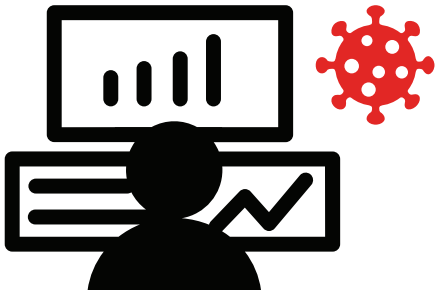
Executive Summary

Well ahead of plans, the COVID-19 pandemic has forced organizations to significantly advance their digital acceleration initiatives into cloud—in some cases, maybe even unplanned. Additionally, many organizations underwent forced acceleration to cloud due to external factors such as competitive pressures. This has resulted in "accidental multi-clouds," comprising public and private clouds, wrought with complexity and likely security ineffectiveness and weaknesses. In fact, according to the 2021 Cloud Security Report, the majority of organizations have a hybrid or multi-cloud deployment, and 76% utilize two or more cloud providers. This, in turn, has resulted in an explosion of cloud and application edges—all of which become part of the greater threat landscape.

The quick move to cloud is further exasperated by cybersecurity skills and resource gaps, particularly those related to cloud and cloud security. The accidental multi-cloud environment has amplified security risks from operational complexity, misconfigurations, and loss of visibility into the network.

Ultimately, the journey to cloud is all about the application journey in itself. Evaluating where an organization is in its application journey across its build, run, and deploy stages can help to effectively adjust the strategy and investments to better realize and secure digital acceleration outcomes while reducing complexity. More importantly, this allows organizations to course-correct as needed and lay the foundation to effectively scale as their digital acceleration initiatives and business goals evolve.

A well-designed cloud strategy should allow organizations to secure any application on any cloud with a significant level of security effectiveness with the least amount of complexity.



Did you know? COVID-19 forced organizations to accelerate their digital transformation plans ahead by as many as six years?[1]

Introduction

Successfully executing their application journey plans is a critical element of any organization in pursuit of their digital acceleration initiatives. The application journey they take is directly tied to how well they can compete and succeed in today's business landscape. Yet, organizations often find themselves stuck at a crossroads, unsure how to progress—some are not even sure where to begin. Lack of visibility, control, and staff expertise are the top barriers to faster cloud adoption.[2]

Despite organizations aiming to move their applications toward being cloud-native, the reality is that there will be critical applications that will need to continue to be maintained on-premises for reasons of legacy or compliance, etc. This situation gives rise to hybrid clouds, which in turn causes operational complexity and security ineffectiveness arising from resulting cloud security misconfigurations, insecure interfaces and APIs, the probability of sensitive data exfiltration and unauthorized access.

To overcome these challenges, organizations need to right-size their approach to cloud and their application journeys to get to cloud by adopting solutions that can secure all stages of the application lifecycle from building applications, deploying them in the cloud or data center, and protecting running applications in production no matter where the application gets deployed. Additionally, being in a world of hybrid and multi-clouds, organizations should strive for solutions that integrate with a broad, integrated, and automated cybersecurity mesh platform to reduce operational complexity and increase security effectiveness.

Understanding the Application Journey

Organizations looking to optimize their cloud journey should focus on the application journey itself as, ultimately, the application journey is the key driver in most cloud transformation efforts. Once the application journey is clear, the approach to deploying applications in the cloud, multi-cloud, or hybrid cloud becomes much easier to strategize and implement.

In its simplest form, the application journey is composed of three key phases: Build, Deploy, and Run.

- **Build:** In this stage, organizations are looking to gain greater efficiency and greater speed at delivery application experiences. They do this by migrating toward building cloud-native applications and leveraging the wide breadth of cloud technologies, such as microservices architecture and rapid, iterative development and deployment processes.
- **Deploy:** Once applications are built, they are then deployed into various cloud, hybrid cloud, and/or virtualized data center platforms. This includes cases where legacy on-premises applications are migrated to the cloud as a "lift and shift."
- **Run:** Naturally, the point of all the effort that goes into developing and maintaining applications is to put them into production. At this stage, organizations have deployed their applications into the cloud or virtual data center, running them, and providing access for customers or even other applications to interact with them. For many organizations, the quality of the application experience being delivered is also important, in which case these organizations might also desire the ability to improve scalability and reduce latency.


Build
Deploy
Run
Application Journey

Build Securely

In today's modern cloud-centered and cloud-enabled world, building applications is a blended practice of development, quality engineering, and IT operations along with a set of rapid development philosophies and practices. Collectively, this modern approach is known as development operations, or DevOps. The goal of DevOps is to take an integrated approach to speed the development and delivery of applications in an iterative manner to both deliver applications experiences quicker and to ensure that what is delivered meets the demands of the customer and the market. Typically, this involves a fair degree of automation, people, tools, and processes to come together. The collective end-to-end iterative process is also known as the continuous integration/continuous deployment pipeline (CI/CD).

Surprisingly, in many organizations implementing DevOps practices, security is an afterthought. The consequence is that applications are built and deployed without being fully secure or don't include any security at all, leaving organizations and their customers and users at risk of potential compromises. As a result, organizations leveraging or intending to leverage DevOps should consider adopting security as a foundational core of their development culture. Those that do not only implement a security mindset as a core philosophy into their DevOps practices but also adopt security-oriented processes and tools, which are known collectively as development security operations (DevSecOps).

For organizations leveraging DevOps and/or DevSecOps, they should consider these following best-practice guidelines in identifying security solutions to help better secure their applications through the development process:

- Detect threats during development stages
- Ensure images and registries are vulnerability free
- Minimize vulnerabilities propagation in the pipeline
- Build images using security best practices
- Continuous scanning for new and evolving vulnerabilities
- Minimize alert fatigue

Security solutions that should be considered at this phase are:

- **Application security testing tools** that can be integrated into development processes to automatically scan and test applications across several security tools to provide insights into security flaws and vulnerabilities that may exist. These vulnerabilities and flaws might not be present in the underlying code itself but might be in the resources and microservices being leveraged in the development of the application.
- **Cloud security posture management (CSPM) solutions** provide insights into deployment containers and workloads in the cloud. This is critical to safeguarding not only the containers and workloads but also the underlying data. The insight and visibility provided allow organizations to understand and proactively manage their risks and exposures. Additionally, CSPM tools also aid organizations in achieving compliance requirements.
- **Cloud workload protection (CWP)** allows organizations to secure the workloads and containers themselves, protecting them from exposures and active compromises.

BUILD

Secure Development/ Deployment Cycle

- Detect threats during development stages
- Ensure images and registries are free from vulnerabilities
- Minimize propagation of vulnerabilities in pipeline
- Build images using security best practices
- Continuous scanning for new and evolving vulnerabilities
- Alert fatigue

Deploy Securely

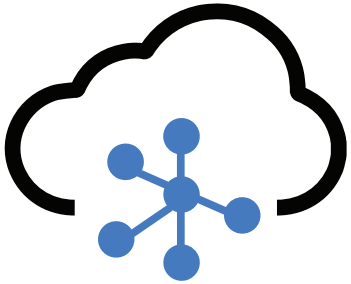
As organizations migrate their applications to cloud either via “lift-and-shift” by moving preexisting on-premises applications or directly deploying CI/CD pipelined delivered cloud-native applications into the cloud, it is critical for them to secure the cloud environment itself.

Critical capabilities to securing both the cloud and virtual data center networks include:

- Microsegmentation
- East-west traffic
- Visibility into anomalous traffic
- Secure network connectivity across clouds

Organizations should look for cloud networking security solutions that deliver virtual firewall, segmentation, and SD-WAN for multi-cloud capabilities to satisfy these requirements.

Organizations should invest in distributed denial-of-service (DDoS) protection for an added layer of protection. This prevents attackers from overwhelming the network or service to the point that it cannot deliver or respond. Often, many cloud delivery services offer some degree of this capability. For organizations that leverage a hybrid cloud approach, DDoS is a critical, must-have protection solution for their physical and virtual data centers.



DEPLOY

Secure Network Layer

- Virtual Firewall
- Segmentation
- SD-WAN for Multi-cloud
- DDoS Protection

Run Securely

Despite all efforts to ensure applications are free from risks during the development and deployment phases, the reality is that running applications have their fair share of threats. Many applications either publicly expose APIs or leverage third-party APIs. In turn, these APIs can expose organizations to significant risks and compromises. APIs often grant access to users, other applications, and devices to resources with the organization. Successful compromise of the application and its underlying APIs might result in consequences such as the leakage of sensitive data and financial and reputational loss.

To protect web applications and related APIs, organizations need to deploy web application firewalls (WAFs), also known as web application and API protection (WAAP), that provide protection against known and unknown threats, including those identified in OWASP's Top 10 list; bot mitigation; and advanced artificial intelligence (AI) and machine learning (ML) to automate identifying and protecting APIs.

Additionally, as web applications often involve personally identifiable information (PII) and financial transactions, an ideal WAF/WAAP solution should also be able to help organizations meet compliance requirements.

Organizations should also consider adding application delivery controllers (ADCs) to their deployment, in addition to WAF/WAAP solutions, to help secure and scale application experiences. An ideal ADC solution should act as a security accelerator that offloads functions such as SSL offloading and security pre-filtering for best application performance and security effectiveness. The ADC solution should also be able to provide critical application-experience feedback into its SD-WAN operations to optimize application performance.

RUN

Secure Web/Data Access Layer

- Application and API Security

Simplifying Cloud Operations

To further reduce complexity and increase security effectiveness, organizations on their application journeys into the cloud need to leverage a cybersecurity mesh platform approach.

A cybersecurity mesh platform offers centralized visibility and management, automation across all solution points, and leverages intelligence sharing for the fastest responses 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 ensure that the chosen solutions to secure across build, deploy, and run stages:

- Work seamlessly with a cybersecurity mesh platform
- Integrate across a broad ecosystem of cloud platforms and technologies
- Can be deployed across a range of form factors for maximum flexibility, from appliances to virtual machines to hosted offerings

Additionally, an important consideration is what type of consumption model an organization requires. This is often an overlooked aspect of cloud transformation for many organizations. However, how solutions are licensed and consumed can impact the financial and operating model and, ultimately, the success of the cloud transformation itself.

Is the organization looking at more predictable fixed-cost structures, or does it want to migrate deployments from on-premises into the cloud with an existing license and a bring-your-own-license (BYOL) approach? Or, is there a desire to take a flexible utility-based pricing model approach that can be particularly beneficial to organizations focusing on driving DevOps forward? In this case, a pay-as-you-go (PAYG) approach might be the best option. For cloud-first/digital-first organizations, there might be a desire to only consume cloud solutions via a self-service cloud marketplace approach. For some organizations that are still uncertain about how they will go about scaling their application journey and subsequent rollout of that journey across clouds, hybrid clouds, and virtual data centers, then the right answer might be to adopt a flexible enterprise agreement approach.

Because cloud and the application journey is and will continue to be a fluid conversation as organizations' needs and business environments evolve, organizations should prioritize choosing security solutions that can be deployed anywhere on any cloud to secure any application, and that also offer the greatest range of consumption model options.

Successfully Securing Any Application Journey on Any Cloud

Regardless of where organizations are in their application journeys, they should take pause to reevaluate where they are, how far they have come, and if they have implemented the right cloud security solutions to meet the needs of each application lifecycle stage across their build, deploy, and run. This pause to assess their journey will help them to adjust their cloud strategy, priorities, and investments to help them best achieve their digital acceleration goals.

Organizations should then choose solutions that can enable them to bring forth their application journey on any cloud, multi-cloud, hybrid cloud, or virtual data center–centric deployment as their business demands. An optimal cloud security solution set should allow them to deploy and secure their application journey on any cloud seamlessly through both tight integrations with major cloud platforms (like AWS, Azure, and Google Cloud) and a cybersecurity mesh platform such as the Fortinet Security Fabric. Additionally, organizations should consider future-proofing their investments by considering solutions that offer the greatest flexibility in consumption and deployment models and scale.

For organizations looking to improve and expand their security effectiveness while reducing complexity, Fortinet Cloud Security solutions offer a broad portfolio that covers all application lifecycle stages with tight integrations with a broad ecosystem of cloud and third-party platforms and technologies and the Fortinet Security Fabric. This empowers organizations to securely deploy on any cloud or virtual data center with consistent policies, centralized management and visibility, and security automation and orchestration. Additionally, Fortinet Cloud Security solutions come in all of the form factors and consumption models that organizations need to successfully meet their digital acceleration initiatives and goals today and tomorrow.

[1] "COVID-19 Digital Engagement Report," Twilio, accessed March 7, 2022.

[2] "2021 Cloud Security Report," (ISC)², 2021.

FORTINET®

www.fortinet.com

March 8, 2022 10:33 AM

1510417-0-0-EN