CHECKLIST

Top Three Considerations To Build, Deploy, and Run Your Application Journey

As organizations pursue their digital acceleration initiatives, successfully executing upon 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. Yet, organizations are all at different stages of their application journey toward 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. To help organizations wade through the murky waters of securing their application journeys, here are things to consider to help guide the development of a strategic roadmap.

Where In the Application Journey Are You?

For many organizations, their application journey involves a continuous life cycle composed of three stages: build, deploy, and run. Start with identifying which stage your organization is in the journey, or what is most critical to secure first.

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. Security at this stage needs to be integrated as a foundational part of development methodologies.

- Adopt DevSecOps solutions for continuous application testing to ensure built-in security best practices from the start.
- Leverage container security and workload protection alongside cloud security posture management to protect deployed workloads. Choose solutions that provide both visibility and protection capabilities.

Deploy: As applications get deployed to the cloud, organizations need to consider the security of the cloud environments 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, but the onus of securing the applications and virtualized cloud instances they run on is left to the customer. Where applications live should not impact experiences delivered to customers and end-users.

- Choose a network firewall solution that is deployable in the cloud and on-premises, both in physical and virtual form factors. This provides for consistent policies no matter where the applications need to be deployed, which ultimately reduces operational complexities that often happen in multi-cloud and hybrid cloud deployments.
- Ideally, the networking solution should provide secure multi-cloud software-defined wide-area network (SD-WAN) connectivity and can orchestrate between all cloud and hybrid cloud instances to help deliver the best application experiences possible.

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.

- To protect running applications, deploy a web application firewall (WAF). Choose a WAF solution that offers advanced artificial intelligence/machine learning (AI/ML) capabilities to help automatically discover and protect APIs, and includes advanced protection against bots.
- Consider adding application scale-up and load-balancing solutions to ensure the best application experiences can be delivered. Ideally, these solutions can act as security accelerators that offload secure sockets layer (SSL) and security processing of application traffic for even better application performance.

Top Three Considerations To Build, Deploy, and Run

☑ Can the solutions be deployed on any cloud or virtualized data center?

Over 76% of organizations deploy two or more clouds.[1] Ensure the solutions you are choosing to protect your application journey can deploy wherever you need your applications deployed. Effective cloud security should free your organizations to deploy where needed and know they can be secured rather than have the choice of security options dictate where you can deploy your applications. Or worse yet, don't get stuck in a situation where your organization chooses to deploy without any form of security at all.

Solutions that provide a broad range of deployment flexibility and deep levels of integration with major cloud platforms will help organizations future-proof their application journey investments, allowing organizations to readily adapt and expand their cloud security strategy as their needs evolve. Ideally, the solutions should leverage and be integrated with the latest technologies and capabilities available from major cloud platforms like AWS, Azure, and Google Cloud for seamless security and deployments on these platforms.

☑ Can the solutions work as part of a cybersecurity mesh platform?

As more application and cloud edges appear, organizations are faced with greater complexity and visibility blind spots. To address this, a cybersecurity mesh platform is critical. It empowers organizations with centralized management and visibility, consistent policies, and automated response and operations. Additionally, this helps address cybersecurity skills and resource gaps that many organizations face. For best results, choose solutions that integrate well with a cybersecurity mesh platform.

☑ Can the solutions support flexible cloud consumption models?

The decision to pursue application journeys in the cloud is not just about technology; it is also a financial one. Ensure that the security solutions you are considering offer a range of consumption models to fit the needs of your organization. Licensing options should include term-based (BYOL) and pay-as-you-go (PAYG) at minimum. For even more flexibility, consider solutions that also offer enterprise agreements that give organizations the option of scaling as needed without being encumbered with additional purchasing.

Fortinet Cloud Security Secures any Application Journey on any Cloud

Fortinet helps customers secure the digital acceleration of their application journeys into, within, and across clouds. We do this by offering Cloud Security solutions that are natively integrated across major cloud platforms and technologies alongside the ability to extend the Fortinet Security Fabric across all hybrid and multi-clouds. Together these offer customers reduced operational complexity, greater visibility, and robust security effectiveness as a result of delivered capabilities that include consistent policies across all hybrid and multi-clouds, centralized management, deep visibility across applications and workloads, and FortiGuard delivered protection and intelligence to protect all stages of the application life cycle from build to deploy to run.

Fortinet Cloud Security also supports a wide range of deployment and consumption models. Our solutions are deployable directly from cloud marketplaces, as physical and virtual appliances, and as SaaS-based options. Additionally, our solutions are consumable as BYOL, PAYG, and as part of a flexible enterprise agreement program called Flex-VM.

[1] "2021 Cloud Security Report," Cybersecurity Insiders and Bitglass, 2021.

FORTINET

www.fortinet.com

1474254-0-0-EN