CHECKLIST

Top 3 Considerations for Simplifying Code-to-Cloud Security

Executive Summary

As organizations continue to pursue digital acceleration, successfully executing their application journey plans is a critical success factor. Applications can now live anywhere from the data center to hybrid and multi-clouds to edge compute instances. Given this, those making application journeys into the cloud face even more security and operational challenges than before. To help organizations wade through the murky waters of securing application journeys of today and tomorrow, here are key things to consider to help guide the development of a strategic roadmap.

☑ Is the solution part of a consolidated platform that enables organizations to see and protect their applications?

As more applications and cloud edges appear, organizations face greater complexity and visibility blinds spots. A broad, integrated, and automated cybersecurity platform is critical to address this. A platform empowers organizations with centralized management and visibility, consistent policies, and automated response and operations. Choose a vendor that offers visibility and protection to simplify cloud and security operations while increasing the speed of response to address risks and threats in your hybrid and multi-cloud environments.

☑ Can the solutions be deployed anywhere applications live, be it cloud, data center, or edge compute?

Ensure the solutions you choose to protect your application journey can be deployed wherever your applications need to live. Look for security solutions available across various form factors: appliances, virtual machines (VMs), hosted, and cloud-native. This will also enable your organization to benefit from consistent security, as the same policies can be applied everywhere.

At minimum, consider deploying the following to achieve a broad coverage of use cases to both solve today's needs and build the foundation for those in the future:

- **Securing data center, cloud, and edge compute networks** with a network firewall solution offers the same capabilities with consistent policies, whether deployed in the cloud or on-premises at physical and virtual data centers or private clouds.
- **Secure web applications and APIs** with a web application firewall (WAF) that offers advanced artificial intelligence (AI) and machine learning (ML) capabilities to help automatically discover and protect APIs and includes advanced protection against bots.
- **Secure clouds natively** with a cloud-native application protection platform (CNAPP) to manage risk, gain visibility, and reduce friction across all cloud environments. As applications can live across hybrid and multi-cloud, choose a solution that offers agentless and agent-based approaches to gain deep visibility and context across your full environment so you can completely understand your cloud. Ensure that the solution provides prioritized and actionable insights to reduce complexity and speed response, lowers alert volumes, and leverages advanced AI/ML capabilities to help detect threats and risks faster.
- **Secure workloads** with cloud-native protection. Deploy cloud workload protection, part of a CNAPP solution, to protect your workloads. For even better security, leverage deploying an agent within the workload if the CNAPP solution offers an agent-based approach capability to get deep visibility, especially for critical workloads.

☑ 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 your organization's needs: term-based (BYOL), pay-as-you-go (PAYG), and enterprise agreements that give organizations the flexibility to scale as needed.

Even more important is that many organizations take on committed use and spend agreements with cloud providers to make their cloud costs predictable. Oftentimes, this is based on forecasted consumption, and many organizations find themselves behind on their spend commitments, resulting in a penalty owed to the cloud service provider. As such, organizations need to adopt a solution that enables them to gain credit against their committed spend—even better, if the solution they choose allows them to shift these committed dollars into preserved credit that can be used in future years, so they are not forced to make hurried decisions to meet deadlines versus true need.

Fortinet Secures Any Application Journey on Any Cloud

Delivering a consistent, secured, and optimized experience for organizations to build, deploy, and run cloud applications across all data centers, clouds, and hybrid and edge-compute deployments, Fortinet empowers organizations to achieve their digital acceleration goals for today and tomorrow. We do this by offering cloud security solutions that are natively integrated across major cloud platforms and technologies, deployable directly from cloud marketplaces, as physical and virtual appliances, as SaaS-based and as cloud-native options, and provide the ability to extend the Fortinet Security Fabric across anywhere applications live. Fortinet Cloud Security Solutions deliver 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. By offering a comprehensive, integrated code-to-cloud security platform that empowers organizations to see and protect their application journeys, Fortinet can help customers reduce operational complexity and gain greater visibility and robust security across their infrastructure.

March 21, 2025 10:20 PM / MKTG-1175-0-0-EN