ESG SHOWCASE

The Value of Distributed Cloud Services

Date: February 2022 **Author:** Bob Laliberte, Principal Analyst; and Mark Bowker, Senior Analyst

ABSTRACT: Modern, cloud-native applications are being distributed across multiple public cloud environments. Unfortunately, the traditional network, security, and application services are not able to keep up. These services need to be cloud-based and distributed with applications to ensure performance, protection, and visibility. F5 has built a distributed cloud services platform to enable organizations to accelerate the adoption of fully integrated network, security, and application services to support distributed cloud environments.

Applications are Becoming Distributed

Organizations are rapidly adopting distributed applications for many reasons, from taking advantage of unique native cloud services, for resiliency (not relying on a single cloud provider), and to push services closer to the edge for better customer experiences. This concept is enabled by modern application architectures, the introduction of 5G technology, public cloud services (consisting of both infrastructure and applications), colocation facilities, and of course on-premises data center and edge locations. Essentially, distributed applications require a digital ecosystem of cloud services, developer-ready infrastructure, and legacy IT that provides consistent operations (see Figure 1).

Figure 1. Distributed Application Ecosystem
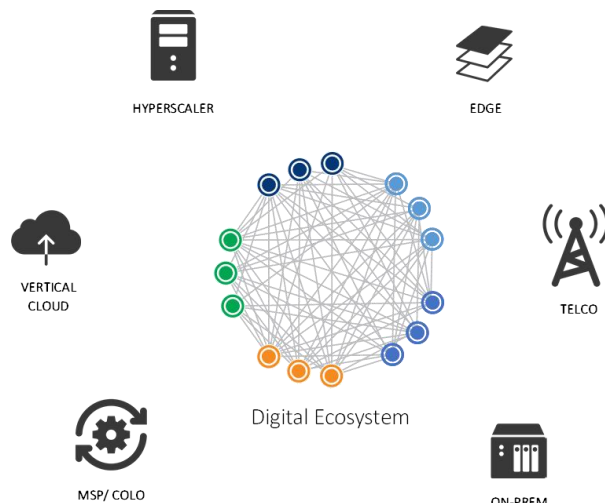
Source: ESG, a division of TechTarget, Inc.

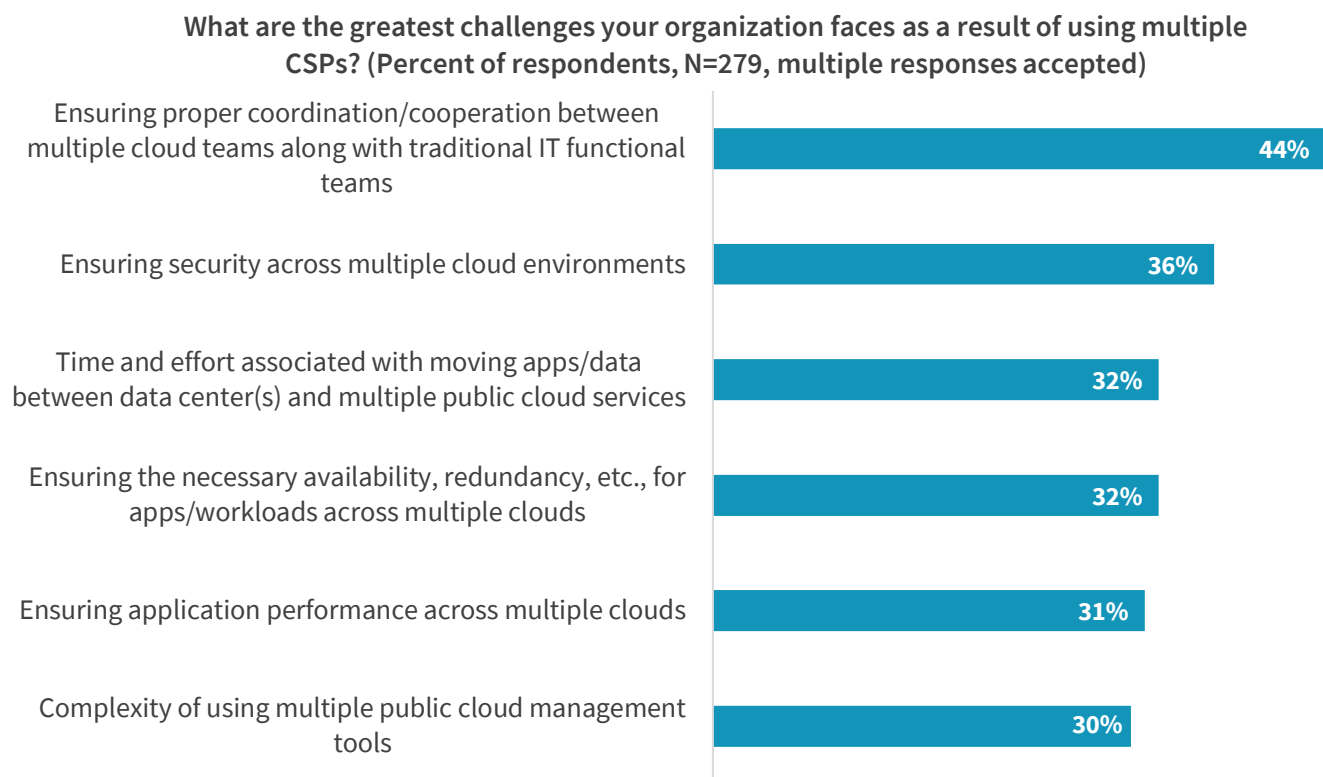## Challenges with Distributed Applications Environments

Distributed application environments create a new set of challenges for organizations. These applications are being deployed across multiple public cloud locations and according to ESG research, nearly nine out of ten (86%) of organizations report using two or more public cloud providers. As a result, these modern application environments are

more complex. ESG research highlights some of the top challenges when leveraging multiple public cloud service providers (see Figure 2). The top challenges include coordinating between multiple cloud teams and traditional IT teams (44%), ensuring security across multiple clouds (36%), ensuring availability for apps and workloads (32%), delivering application performance (31%), and the complexity associated with using multiple cloud management tools (30%).[1]

Figure 2. Top Six Challenges Using Multiple Public Clouds

What are the greatest challenges your organization faces as a result of using multiple CSPs? (Percent of respondents, N=279, multiple responses accepted)

Ensuring proper coordination/cooperation between multiple cloud teams along with traditional IT functional teams	44%
Ensuring security across multiple cloud environments	36%
Time and effort associated with moving apps/data between data center(s) and multiple public cloud services	32%
Ensuring the necessary availability, redundancy, etc., for apps/workloads across multiple clouds	32%
Ensuring application performance across multiple clouds	31%
Complexity of using multiple public cloud management tools	30%

Source: ESG, a division of TechTarget, Inc.

It is not surprising that security is one of the top challenges, as organizations can no longer rely on "castle and moat" perimeter-based security architectures to protect highly distributed and dynamic applications and workloads. While that model worked when all the applications were housed in a one or two data centers, it is not a viable option moving forward.

Visibility is another significant challenge, especially when trying to coordinate and collaborate across multiple different teams. DevOps, NetOps, SecOps, and cloud architects all need visibility to this distributed environment. Typically, each of these teams have individual tools with limited views—which has the potential to create conflicts or, worse, performance-impacting events. Disparate products from different vendors also mean organizations have to invest more in training but still have to perform manual correlation of events between the tools, which requires additional time and is error-prone. Without granular, end-to-end visibility down to the container level, ensuring compliance and consistency across the entire environment becomes very difficult.

Trying to deliver these services from a centralized location can also create latency issues. Organizations attempting to leverage existing network, security, and application services located in data center or primary cloud provider locations will find that latency issues impede progress when the applications are located across multiple public clouds or at the network or enterprise edge. Often, the reason for deploying applications there is to satisfy a need for real-time or near real-time

---

[1] Source: ESG Research Report, *Application Infrastructure Modernization Trends across Distributed Cloud Environments*, to be published.

analysis, and any latency incurred accessing centralized services will impact application performance and, ultimately, the user or customer experience.

As a result of these challenges, business agility, operational efficiency and customer experience can be impacted. Yet, according to ESG research, respondents reported that their organization's most important objectives for their digital transformation initiatives included becoming more operationally efficient and delivering an enhanced and differentiated customer experience.[2]

Organizations embracing distributed application environments need to ensure that key application services are distributed as well. This means that security, network, and application platforms need to be located close to applications. Wherever there are new workloads being deployed, there needs to be a consistent cloud-native environment and end-to-end visibility and control. Enter distributed cloud services.

Distributed Cloud Services Provide Value

As applications continue to be distributed, now is the time for organizations to distribute services to accompany the applications. These services should include:

- Security: DDoS, API sec, WAF, bot defense.

- Networking: Multi-cloud routing, load balancing/app delivery.

- Application: Kubernetes, identity/key management and other platform services.

Key attributes of a distributed cloud service to ensure operational efficiency and differentiated customer experience include:

- Visibility across distributed environments: Organizations should strive to deploy the same solution across all geographically dispersed locations and different app environments to ensure end-to-end visibility. This enables organizations to leverage a single pane of glass and minimizes training and troubleshooting time.

- Agility and operational efficiency: Organizations require cloud-native SaaS-based services to ensure they can be deployed quickly where and when they are needed, without the need to deploy and maintain hardware or virtual appliances.

- Common policy enforcement: Centralized control and distributed enforcement are key to managing large highly distributed environments. Being a cloud solution means that policies and control can be administered and automated from anywhere. The ability to quickly define policies and roll them out to all locations ensures consistency, even when new applications are turned up or a new site is deployed.

- Better cross-team collaboration: Leveraging a common management solution as a single source of truth, users can take advantage of role-based access to get the requisite data and control when needed. This ensures the ability to accelerate troubleshooting, reduce total cost of ownership, and optimize performance, which yields higher customer satisfaction.

---

[2] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021.

The F5 Distributed Cloud Services Platform

To enable organizations to take advantage of distributed cloud services, F5 has built a platform specifically designed to secure and deliver modern cloud-native applications, as well as legacy workloads. F5 Distributed Cloud Services (Figure 3) delivers:

- 100% SaaS-based security, networking, and edge compute capabilities. These include security solutions such as Bot Defense, Advanced Web Application Firewalls (WAF), Denial of Service protection, and API security. For multi-cloud networking, there is routing, load balancing, and firewall. For edge computing, it supports automated deployment and hosting of Kubernetes workloads and provides platform services like key and identity management. Utilizing curated signature, client, and threat intelligence and employing AI/ML ensures the highest efficacy without additional administrative overhead.

- Integrates multiple services for simplified deployment/management and lower cost of ownership. The ability to manage multiple different services under a single pane of glass provides operational efficiency and accelerates deployments.

- End-to-end visibility across distributed apps. Comprehensive visibility enables organizations to effectively manage these complex environments, ensuring compliance and optimized performance.

- Centralized control and distributed policy enforcement. Operations teams have confidence that network, security, and application policies are enforced in all locations, consistently. This also ensures that all new applications and sites deployed will have consistent policies as well.

- Support collaboration. The integration of network, security, and application services into a single platform will help integrate operations teams by removing barriers and providing them with a single shared source of information and control for distributed cloud environments. Network and security teams can create the guard rails (policies) that enable DevOps to deploy with the confidence that the applications are fully supported and policy-consistent.

Leveraging F5 Distributed Cloud Services can increase an organization's application and business agility, as new applications can be deployed quickly and easily with the appropriate services to ensure security, performance, and visibility.

Figure 3. F5 Distributed Cloud Platform
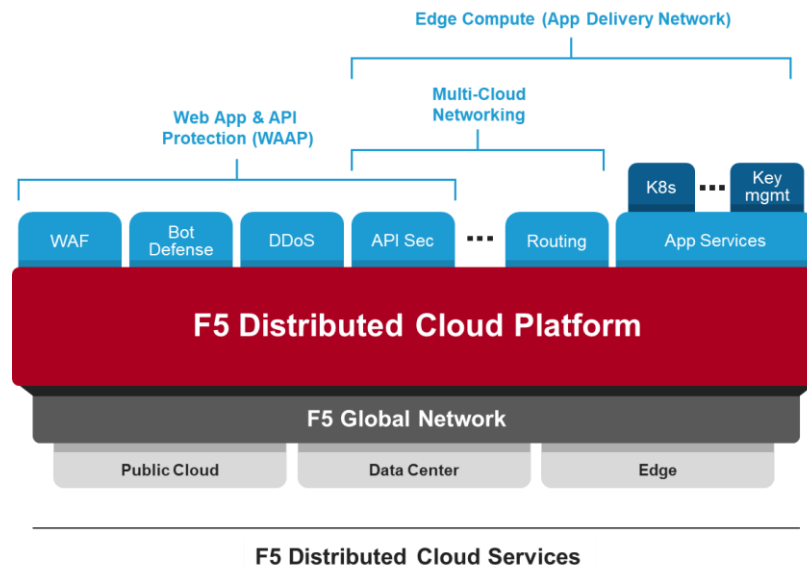
Source: F5

The Bigger Truth

Organizations are rapidly adopting distributed application environments with modern, cloud-native applications being deployed across multiple data centers, multiple public clouds, and edge locations. However, legacy, appliance-based services will not be able to support these highly dynamic and dispersed applications. A new approach is required.

It is imperative that the network, security, and application services are distributed as well in order to ensure the requisite levels of performance, protection, and availability. To deliver these services in an operationally efficient manner, an integrated approach is required. This would entail a centralized, and preferably cloud-based, control plane that would ensure consistent services and policies are deployed and enforced at the distributed locations, ensuring optimized performance, protection, and visibility.

To enable organizations to accelerate the adoption of cloud-based services, F5 has built a distributed cloud platform that delivers integrated cloud-native network, security, and application services in a 100% SaaS-based platform. Organizations that are deploying applications in a distributed environment need to understand how the F5 Distributed Cloud Platform can deliver improved business agility, operational efficiencies, and enhanced customer experiences.