White Paper

Navigating a Multi-Cloud World with F5

Contents

The Transition to Cloud

Many enterprises have already embarked on their journey to the cloud. The promise, familiar by now to most observers, is that these organizations will realize many benefits: greater agility, better-aligned operational costs, on-demand scalability, and more focus on their core business. A world where digital transformation is an important strategic imperative demands these benefits and more.

What's happened recently, though, may be a little surprising to some. Many enterprises have actually deployed applications into a number of different clouds—public clouds, private clouds, and even various combinations. Those same businesses have also taken advantage of cloud-based SaaS offerings including Salesforce, Microsoft Office 365, and Oracle On Demand.

Reality looks starkly different than how the "cloud" appears in slideware or marketectures. The "cloud" isn't an amorphous single entity of shared compute, storage, and networking resources; rather, it is composed of a complex mix of providers, infrastructures, technologies, and environments that are often deployed in multiple global nodes.

This is multi-cloud.

A New Cloud Reality

As it turns out for many enterprises, multi-cloud is the new reality.

Some IT leaders and business owners may comfort themselves with the belief that multi-cloud is very advanced and far off in the decision-making horizon, or they hope to go "all-in" with a single preferred provider. Many may only have visibility into a limited number of app deployments or some test and development environments in one cloud provider, while others are already facing challenges that arise from multi-cloud adoption practices.

Nevertheless, to validate whether you are or may soon be a candidate for multi-cloud, you may want to ask yourself a few critical questions:

- Do you have applications that have varying performance requirements?
- Do you need to maintain supplier leverage with your infrastructure providers to hedge costs?
- Do you have different application development teams that procure cloud services?
- Are your users, employees, or business units geographically diverse?
- Are there applications that you know are migrating to a SaaS model, such as Office 365?

More than 85% of enterprise IT organizations will commit to multi-cloud architectures by 2018.

Source: IDC FutureScape: Worldwide Cloud 2017 Predictions, Doc #US41863916, Nov 2016

If you answered “yes” to any of these questions, you’re likely heading toward a multi-cloud world in the near future. And if you answered “yes” to more than one question, you are already multi-cloud.

Multi-cloud considerations become more prominent at higher levels in the IT organization. Many CIOs and enterprise architects, whose responsibilities span organizations and budgets, are more aware of the entire IT landscape that necessitates the use of multiple public and private clouds than any given application development team or specific IT function.

Multi-Cloud Challenges

Even in this rapidly evolving landscape, several factors are slowing cloud adoption and threatening to erode potential gains that IT organizations expect to achieve.

The first challenge is one that may not be identified until it happens: multi-cloud sprawl, where existing applications have been “lifted and shifted,” and “born-in-the-cloud” applications have been deployed in an unplanned and unmanaged manner. Different IT and DevOps teams, siloed by organizational structure or function, independently design and deploy their applications and select the cloud provider infrastructure services and technologies that best meet their individual needs. It should come as no surprise that siloed teams with varying needs result in architectures that are also siloed and varying.

In addition, many DevOps teams value both deployment agility and native cloud services to meet their short-term needs. Using native cloud services certainly seems like a simpler, faster, and more cost-efficient approach for small teams or narrowly focused projects. Across the entire enterprise and its IT organization, however, this lack of a disciplined methodology leads to the second challenge: the use of disparate cloud platforms, different architectures, varying application services, and multiple toolsets. This results in architectural complexity across the enterprise, and makes shifting applications from one environment to another much more difficult, not to mention more expensive.

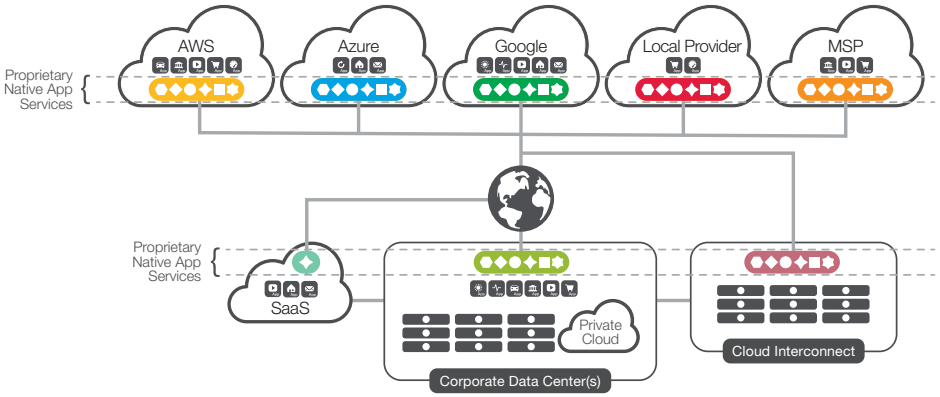

Figure 1: Every cloud architecture—how it operates, is managed, and its levels of visibility—is different.

Wasn't Cloud Supposed to Be Simple?

The result of application sprawl and architectural complexity is limited resiliency against architectural changes and inherited technical debt.

Native cloud services often are basic services that, while simple to use, are insufficient or immature for many enterprise applications. After having invested in understanding and then deploying these basic app services, issues may arise in production that are beyond the addressable capabilities they provide, cancelling out the benefit of the simpler initial deployment.

These native cloud services are also completely proprietary and cannot be used in other public or private cloud environments. As a result, this leads to IT staff—already short-skilled in cloud operations—having to learn, adapt, and maintain multiple rapidly evolving yet siloed cloud provider technologies to keep applications running effectively. Native cloud services vary broadly in capabilities, which can make applying the services effectively to applications more difficult individually or more fragmented collectively.

Because discrete security-oriented application services, such as WAF, identity and access control, and DDoS protection, are provided essentially as one-offs by cloud providers, IT organizations must cobble together a minimum bar for application security in different environments, from the apps already in private data centers to the newer apps deployed in public clouds. Trying to harmonize the different security services, apply policies in the context of services limitations, and maintain them over time as security policies that reflect current conditions change, is next to impossible. As a result, IT organizations invariably face significant compliance gaps and heightened security risks.

Simplify Your Cloud Life

There is a way to simplify and mitigate these adverse effects across public and private clouds. By using a common application services platform across cloud environments, you can reap many benefits.

First, extending an existing platform that is already used extensively in the private data center into new cloud environments can simplify deployments and reduce operational headaches, since IT teams are already familiar with the platform and its capabilities. This reduces staff training time and reduces the likelihood for deployment and operational mistakes due to managing multiple proprietary services. In addition, existing investments in customized application policies and deployment and configuration scripts can easily be reused, saving both time and money. In other words, rather than having to manage multiple solutions across many environments, you can use a single solution across all environments.

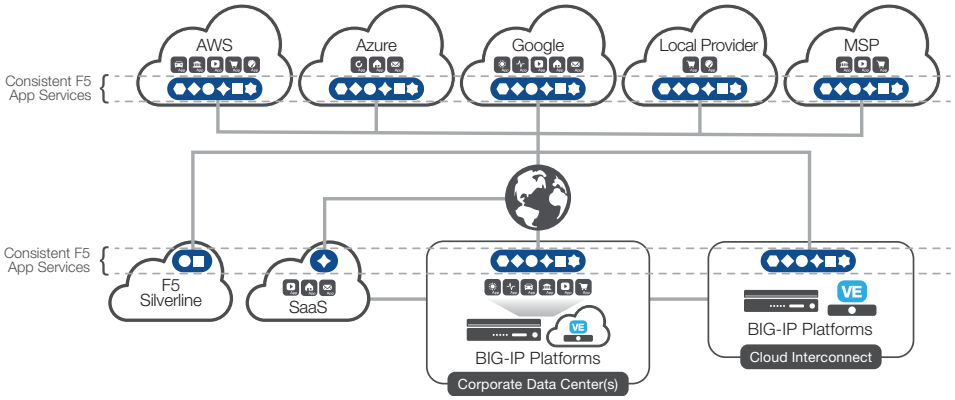

Figure 2: With F5, you can deploy any application anywhere with consistent application services and security, whether in the cloud, as a service, or on-premises.

Second, it may meet your initial needs to depend on basic native cloud services, but as application, scalability, and security requirements change, you can find yourself stuck in a technical cul-de-sac that requires a lot of work to get out of. With best-in-class application delivery and security services from a vendor that focuses solely on this space, you can gain the confidence to deploy into and across whatever cloud you need.

Third, another opportunity to simplify your cloud journey is to consolidate disparate application services you already use—and others you may already be considering—onto a single unified platform to support your applications more effectively. These application services may include load balancing, DNS services, WAF, identity and access federation, and DDoS mitigation. This strategy offers a roadmap to further reduce complexity as you reconsider your application architectures to reflect new cloud environments.

The end result of this simplification is faster cloud deployments, architectural flexibility as needs change, and effective, consistent security across all your application workloads environments.

Introducing New F5 Solutions to Enhance Multi-Cloud

F5 has long supported its customers deploying applications in private and public clouds. Building on that, F5 has recently introduced a number of new solutions that make operating in a multi-cloud world much easier.

For major public clouds, F5's core virtual ADC platform is available in several performance options, ranging from 25 Mbps to 5 Gbps in throughput capacity. F5 has an established presence in Amazon Web Services (AWS), Microsoft Azure, and other public clouds, and just recently announced availability in Google Cloud Platform. This breadth of availability—unequalled among application delivery vendors—ensures customers can use F5's best-of-class services wherever their cloud journey takes them. F5 also provides flexible licensing options, including a bring-your-own-license (BYOL) model, which enables license portability across public and private clouds, as well as a pay-as-you-go (PAYG) model, which allows you to align operational costs and usage more closely.

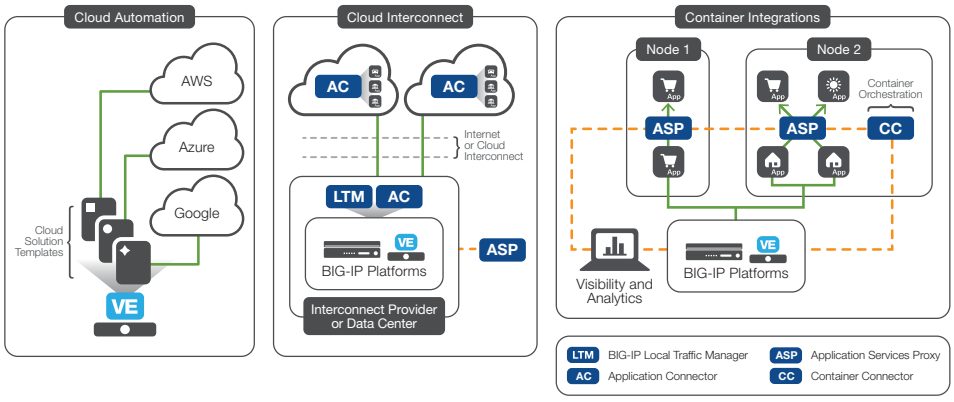

Figure 3: These new solutions extend F5 application services into multiple cloud environments.

F5 has also worked closely with public cloud providers to offer more integrated solutions that enable you to select and quickly deploy specific pre-built and pre-configured F5 services such as Autoscale WAF along with their applications directly from cloud provider marketplaces. For example, F5 now offers Autoscale WAF in AWS and Azure Marketplace and will soon offer additional services on other major public clouds.

The primary benefit of these integrated solutions is that F5 services can be deployed quickly and easily by DevOps and application developer teams, while IT operations can define and mandate consistent standards for application performance and security pre-deployment. They can also retain visibility and control post-deployment.

F5 has made further advances to ease application deployment in public clouds with the recent release of pre-packaged cloud solution templates built on the cloud-native toolsets of major cloud providers to automate and simplify cloud deployments. There are significant differences among public cloud environments; these templates enable you to mitigate this variability and streamline operations for common deployment scenarios. These solution templates are hosted on GitHub and supported directly by F5 support services.

To address the complexity of private cloud deployments, F5 created private cloud solution packages, which are pre-packaged, tested, and certified suites of F5 products and services, integrated with private cloud ecosystems like OpenStack, Red Hat OpenShift, VMware NSX, and Cisco ACI. These certified turnkey solutions from F5 enable you to deploy F5 within leading private cloud environments easily and simply.

Enterprises are beginning to use container technologies to enable IT agility and workload portability. F5 recently released new products that offer support for those container environments: the F5 Application Services Proxy (ASP) and F5 Container Connector. The F5 ASP is a containerized service mesh that can be deployed and managed in container environments, whether IT organizations leverage it themselves or make it available directly to their application development teams. In addition, F5 has released and open-sourced its Container Connector solution, which enables teams deploying apps in container environments to leverage existing F5 ADCs and F5 ASP for self-service use of robust application services through container management systems like Kubernetes, Red Hat OpenShift, Pivotal Cloud Foundry, and Mesos. Organizations that already use F5 and have support contracts will also be able to get support for Container Connector and ASP.

Finally, F5 also offers Application Connector, a solution targeted at the cloud interconnect footprint adjacent to most public cloud provider infrastructures. F5 Application Connector, an add-on to the BIG-IP platform, is a lightweight proxy instance for securely connecting public cloud apps to an organization's cloud interconnect provider or data center to enable application services insertion. F5 Application Connector can perform service discovery of AWS public cloud workloads and automatically provide them on the BIG-IP platform for easy and automated services insertion.

Enterprise IT executives expect 60% of workloads will run in the cloud by 2018.

Source: Voice of the Enterprise: Cloud Transformation survey of IT buyers, 451 Research, Sept 2016

Any public cloud apps can manually be added to F5 Application Connector, which provides a high-performance app services option for public cloud-hosted applications. This yields greater visibility and control across public clouds, and greater security through encryption key storage outside the cloud. It also produces lower attack surfaces for apps in the public cloud and consistent policies across environments.

Conclusion

The journey to multi-cloud has only just started. The nature of IT is that old systems and platforms often remain in place far longer than planned, and your cloud migrations will almost certainly follow that pattern. New deployments in and across public and private clouds will inevitably increase in the coming years—multi-cloud is the fast-approaching future. Forward-thinking IT leaders and enterprise architects must plan for this new world, or else risk reintroducing some of the complexity and support overhead that cloud was meant to remove. Standardizing tools, policies, and operations across a diverse estate of compute environments is a critical strategy for keeping things efficient, simple, and supportable.

ADDITIONAL RESOURCES

F5 GitHub Repository

Application Connector

Container Connector

Application Services Proxy

Multi-Cloud Solutions

BIG-IP Virtual Editions

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com