SOLUTION GUIDE

DEPLOYING CONSISTENT APPLICATION SERVICES IN MULTI-CLOUD ENVIRONMENTS

Innovation and speed to market have become critical to success for many organizations. With F5, you don't need to trade security or performance for rapid delivery.

Most organizations prioritize cloud flexibility—and let application teams choose the best environment for each application—over the organizational benefits of common environments, processes, and tools. This leads to 9/10 of organizations supporting multiple clouds, selecting best-of-breed capabilities from each platform.

As applications proliferate, it becomes more challenging to implement consistent cross-cloud security, regulatory compliance, and application performance policies—and organizations rightly have concerns about long-term operability. In fact, as the size of the application portfolio grows, so does the threat landscape with bad actors targeting apparently inconsequential applications that tend to be poorly protected but offer a pathway into corporate data and other systems.

The key for IT is to strike the right balance between freedom and flexibility for application development teams, while enabling the easy and consistent inheritance of corporate security, compliance, performance, and operability requirements. That means standardizing on core application services across cloud environments—without slowing down CI/CD deployment velocity.

BALANCING SPEED AND SECURITY

Create common security and performance policies across your application portfolio to decrease risk and improve customer experiences.

As new threats emerge, working from a common set of policies allows you to mitigate them far more easily. Security is complex, and while developers should follow secure code practices, they are not security experts—and they really shouldn't be. Instead, they should focus on areas of high exposure and allows IT to address the rest with external controls that protect against both known and unknown threats.

STANDARDIZING ON APP SERVICES THAT IMPROVE PERFORMANCE CAN HELP ENSURE GOOD CUSTOMER EXPERIENCE.

Standardizing on application services that improve application performance can also help ensure good customer experience across applications. User patience with poor response times continues to decline, and developers vary in their ability to code highly performing applications. High turnover may also leave organizations with different developer skill sets. Organizations can compensate for these deficiencies by offering a standard set of performance optimization services for all apps.

THE ARCHITECTURAL COMPONENTS

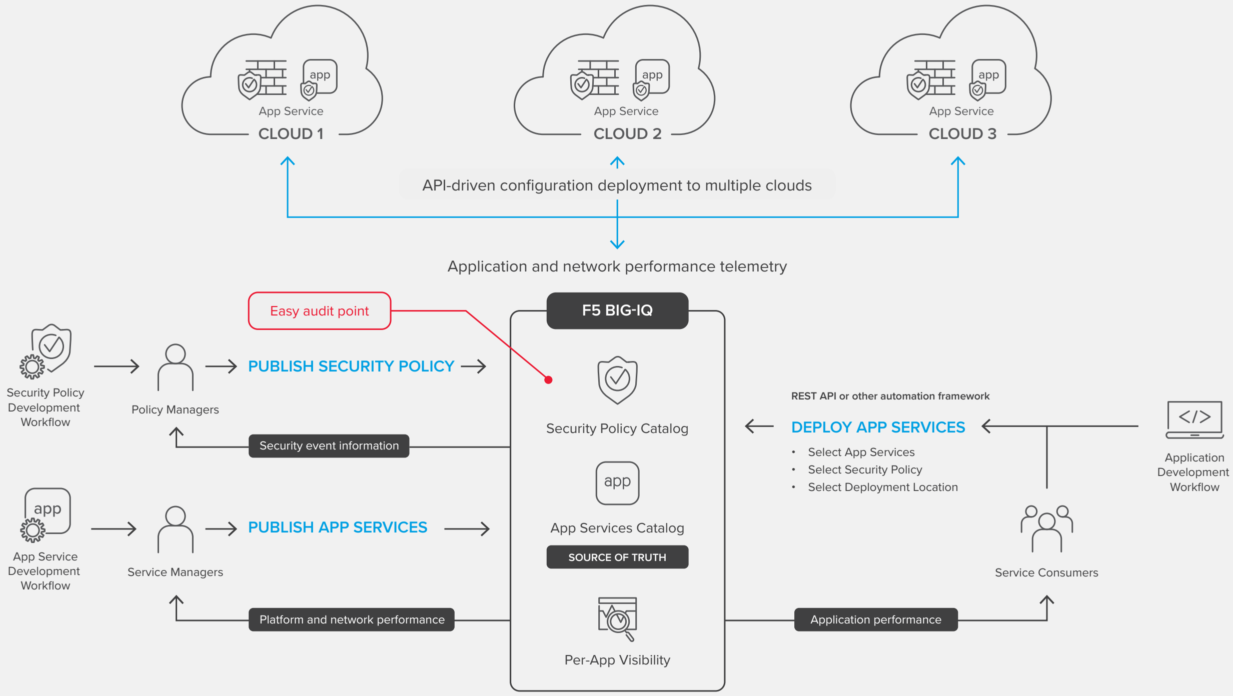
To deliver consistent and powerful multi-cloud application services, organizations can leverage a few F5 components.

F5 BIG-IP® Virtual Editions bring the power, protection, and unparalleled flexibility of the market-leading Application Delivery Controller to a range of private and public clouds. Offering full traffic control, inspection, and telemetry, BIG-IP VEs give your virtualized applications the protection and optimization they need to deliver reliable performance, while defending them from an increasing set of threats and unwanted bot activity.

BIG-IQ PROVIDES A SERVICE CATALOG OF APPLICATION DELIVERY AND SECURITY SERVICES THAT ARE MAINTAINED BY EXPERTS BUT CAN BE EASILY CONSUMED BY APPLICATION TEAMS ON DEMAND.

The F5 BIG-IQ® Centralized Management platform can manage many hundreds of virtual and physical BIG-IP platforms across multiple public and private cloud environments—as well as BIG-IPs deployed in on-premises data centers—all from a single pane of glass. As well as performing more traditional platform monitoring and management, BIG-IQ provides a service catalog of application delivery and security services that are maintained by experts but can be easily consumed by application teams on demand. In addition, BIG-IQ offers device, network, security, and application-level visibility and insights with personalized, role-based per-app dashboards. Finally, BIG-IQ can manage pools of recoverable, reusable licenses—allowing you to flex capacity across multiple clouds as needed.

Consistent policy defends and manages traffic in all cloud locations



GETTING FROM HERE TO THERE

Like all IT initiatives, getting to a great end result involves the three Ps: people, processes, and products.

The reality of delivering secure and fast but quickly evolving applications in the cloud is that security, operations, and development need to collaborate and communicate efficiently to deliver consistent services across a multi-cloud environment. These interactions are, of course, facilitated by the right processes and technology, but people are key to success.

ASSEMBLE YOUR TEAM

NetOps

The network operations team, which is typically led by the network administrator/keeper of the keys, is responsible for network infrastructure. In cloud environments, simple services like load balancing might be the domain of application owners; however, the networking team's expertise in managing application traffic at scale and providing high-quality application performance and security services are as vital in the cloud as they are in the data center.

SECURITY TEAMS HAVE THE RESPONSIBILITY OF PROTECTING YOUR APPS, YOUR CUSTOMERS, AND YOUR DATA FROM AN INCREASING RANGE OF THREATS.

SecOps

Security teams have the responsibility of protecting your apps, your customers, and your data from an increasing range of threats. While app teams have a huge role to play, the security team—together with their networking counterparts—and the application security services they provide are the first (and often the last) line of defense against a horde of bots and bad actors that would exploit vulnerabilities to harm your business.

Dev/DevOps

These are the consumers of the NetOps- and SecOps-created application performance and security services. Whether the cloud has helped create the modern CI/CD deployment model of application development, or the methodology changes have helped create the cloud might be a subject of debate. Wherever you land on that question, it's clear that CI/CD and other DevOps methodologies are here to stay—and the rest of the infrastructure needs to snap in to this application development and deployment methodology, across all the locations in use.

Getting these three teams working together, with the right processes and technology, will allow you to deploy your applications at the speed your business requires—and withthe performance and protection you need.

CREATE PROCESSES

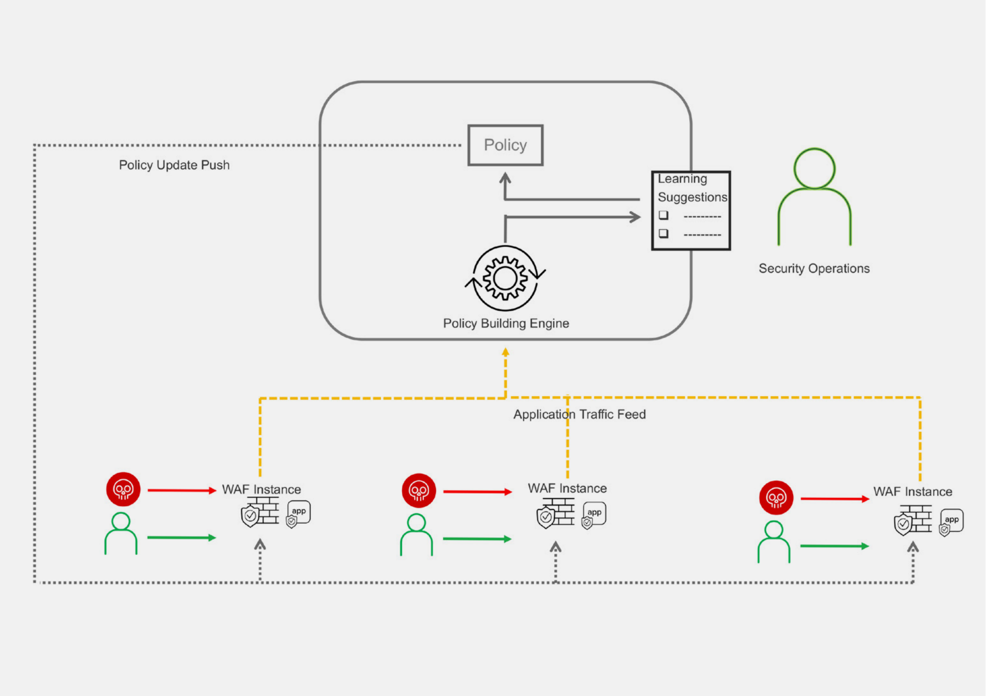
Build a security policy library

Supplying the same baseline security policies for web applications in multiple clouds gives you the assurance that your applications are protected from the most common exploits, no matter where they are deployed. It also simplifies auditing and remediation when a small number of policies are stored centrally and deployed consistently.

THE INDUSTRY-LEADING F5 ADVANCED WAF TECHNOLOGY MAKES IT EASY TO TEST, DEVELOP, AND REFINE A SECURITY POLICY THAT CAN THEN BE DISTRIBUTED TO MULTIPLE ENFORCEMENT POINTS IN DIFFERENT CLOUDS.

A web application firewall policy is generally developed by a security team with expertise in the organization's application types and the threat surface area they expose. The industry-leading F5 Advanced Web Application Firewall (WAF) technology makes it easy to test, develop, and refine a security policy that can then be distributed to multiple enforcement points in different clouds.

As an example, you can create a baseline policy in a development and test environment, then export it to the BIG-IQ management platform where it can be referenced by an application template (which defines the application delivery and security services for an application) and deployed with the rest of the configuration—across multiple clouds. Even better, the policy can then use the learning capability of all devices it's deployed on and combine the data to improve the policy, which can then be pushed back out to the BIG-IP images running in the clouds. The result: an intelligent, highly scalable, and constantly evolving security policy that spans your entire application development and deployment environment.



Harness machine learning to deploy an intelligent, scalable, and dynamic security policy.

Build an application services library

Security polices attach to larger application delivery policies, which set up things like SSL cipher suites, TCP optimizations, and application health checking. NetOps can assemble a catalog of services that combine security policies, application delivery policies, and logging configurations, and then expose them to internal consumers based on role or app type they manage. One team might work on external-facing web apps that require strong TLS encryption, whereas other teams might be working on IoT solutions that require different security and performance settings. Assigning the appropriate catalog services each time increases stability and reduces the chance of error.

APPLICATION TEMPLATES CAN BE CREATED MANUALLY OR CLONED FROM EXISTING CONFIGURATIONS.

Application templates can be created manually or cloned from existing configurations. Templates can even be stored in source code management systems and deployed by API. F5 continues to innovate within application services with our new Application Services 3 (AS3) templates that offer a programmatic, automated, declarative model for configuration of BIG-IP devices and app services. Building application service templates allows operational teams to add best practices into a central repository that can be deployed wherever your applications are.

Stand up some infrastructure

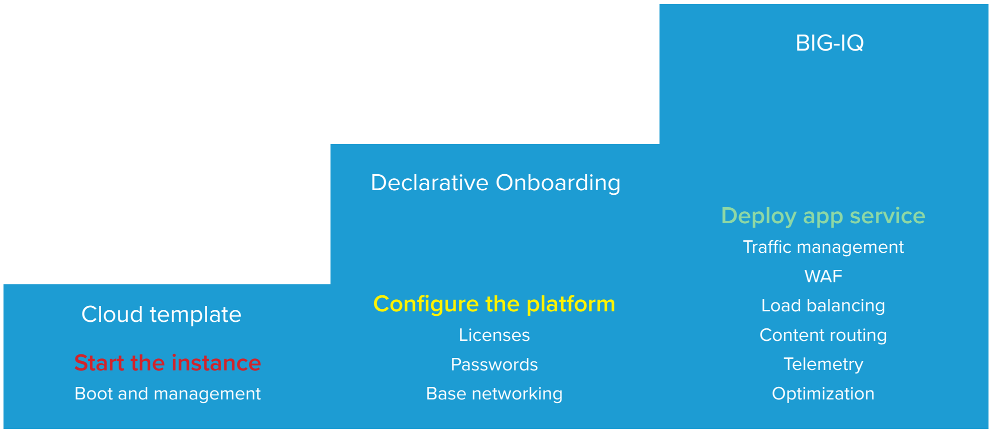
A multi-cloud world needs a multi-footprint solution. The BIG-IP platform can be deployed as software in the public or private cloud, or as hardware in private cloud environments, like a corporate data center. The software image and functionality of a BIG-IP VE is equivalent to its hardware variant—and the app services templates can be used to deploy onto any platform. The best part is that your entire F5 portfolio can be managed from one console regardless of where your BIG-IP devices and the applications they serve are deployed—in public clouds, private clouds, or on bare metal.

THE BIG-IP PLATFORM CAN BE DEPLOYED AS SOFTWARE IN THE PUBLIC OR PRIVATE CLOUD, OR AS HARDWARE IN PRIVATE CLOUD ENVIRONMENTS.

If you need a dedicated per-app architecture, then BIG-IP Cloud Edition offers a right-sized platform designed to give every app its own individual BIG-IP instance, combined with centralized management, deep application-centric analytics for easy troubleshooting, intelligent autoscaling, and flexible consumption models.

Of course, you might need to deploy and onboard new instances dynamically—so there are cloud templates for all major clouds that enable API-driven platform deployment, and a reusable, declarative onboarding system to perform the initial configuration.

Boost speed by automating platform deployment, initial configuration, and app services deployment.



Connect to the cloud

Even if your apps run over the public internet, we recommend a VPN for managing traffic. If you have BIG-IP device on premises, you can stand up an IPsec VPN to most cloud providers from the BIG-IP—and then route management traffic over it to your cloud deployments, so you won't even need a separate VPN solution.

Decide how you want to consume

F5 APPLICATION SERVICES ARE AVAILABLE IN UTILITY, PERPETUAL, SUBSCRIPTION, AND ENTERPRISE LICENSE AGREEMENTS.

Cloud platforms offer a range of consumption models for their services, from flexible pay-as-you-go to enterprise agreements that cover multiple products. It's important that your multi-cloud components mirror these options. F5 application services are available in utility, perpetual, subscription, and enterprise license agreements, offering a commercial model to suit your business needs.

Expose the services to your consumers

Now that you've built it, they will come. But only if you give people the access they need, in the way they want. For some teams, that might still mean a slick GUI, but for many (looking at you, DevOps teams), an API is the right way to expose your service catalog—so application delivery and security services can be created programmatically and linked to a larger workflow or orchestration effort. All the consumer needs to specify is the service they want, the deployment location, and some application specific information, and the service will be deployed in the cloud of their choice—self-service and request ticket-free.

Monitor the deployed applications

Knowing that your applications are delivering a great experience to your customers while you're blocking bots and bad actors can help to overcome some of the concerns (legitimate or imagined) of a multi-cloud application environment. BIG-IQ delivers the right insights to the right people, helping them optimize their applications. By configuring rich telemetry feeds from the BIG-IP instances, then aggregating and displaying the data in an interactive drill-down GUI, BIG-IQ gives each team the information they need to do their jobs better.

NetOps

NetOps teams get information on network and platform performance, as well as key application insights, which enables them to become more valuable to their organizations.

BIG-IQ DELIVERS THE RIGHT INSIGHTS TO THE RIGHT PEOPLE, HELPING THEM OPTIMIZE THEIR APPLICATIONS.

SecOps

Security teams can author and maintain tight control of security policies, monitor the rate of attack and attack vectors, and glean other key insights that help them keep applications and the infrastructure they run on safe from malicious actors and insider errors alike.

Dev/DevOps

Application teams can monitor the apps they are responsible for in any virtualized environment—and get critical metrics like latency, round trip times, and page load times. These insights help them flag issues early, identify root causes accurately and quickly, and collaborate with SecOps and NetOps more effectively.

CONCLUSION

Multi-cloud is here to stay. If you want to maximize the benefits and minimize the risks, then putting together the people, processes, and technology to deliver consistent, high-quality application performance and security services in all your private and public cloud locations is a smart move. Partnering with F5 to do it is an even smarter one.