SOLUTION GUIDE

PROTECT AND OPTIMIZE CONTAINERIZED APPS

Agile platforms need agile protection.

Container platforms such as Kubernetes and RedHat OpenShift combine with agile development methodologies to speed up application development and deployment. By allowing developers to break applications up into smaller components (also known as microservices), containers can help reduce dependencies, allow component-level scaling, and encourage rapid release lifecycles.

However, containerized apps can still be exposed to application-layer vulnerabilities, denial-of-service attacks, and the impacts of client-side network latency. This means they still need app delivery and security services such as web application firewalls, TCP optimization, and protocol gateways.

But a traditional solution with a static configuration changed only by an IT operator conflicts with the agile container paradigm where new microservice containers might be created dynamically for just a few minutes to service a spike in demand or roll out an upgrade by simply replacing old containers with new ones. How do you ensure that your app services deployments keep up with your rapid release cycles in containerized environments?

F5 CONTAINER INGRESS SERVICES COMBINE POWER AND INTEGRATION

INTEGRATE F5 CONTAINER INGRESS SERVICE TO PROVIDE ROBUST PROTECTION THROUGH AUTOMATED RESPONSES TO CONTAINER EVENTS.

You need powerful application security and optimization services integrated with the container platform management plane.

Integrating F5 Container Ingress Services enables your native app services to automatically respond in real time to container events (such as the creation of a new container, or a whole new service)—without an application developer or container platform manager needing a lot of domain-specific knowledge.

You can provide robust protection and advanced traffic management for container applications by combining the market-leading F5® BIG-IP® application delivery platform, an extended container network fabric, and a management container that integrates into the container management plane.

THE ARCHITECTURAL COMPONENTS

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

BIG-IP HELPS SECURE APPLICATIONS, DIRECT INCOMING REQUESTS, AND OPTIMIZE CLIENT CONNECTIONS.

BIG-IP Platform

The BIG-IP platform is a powerful application proxy available as a software appliance for a wide range of public and private clouds—plus dedicated hardware options for on-premises deployments that require the largest scale in the smallest compute footprint. Whether deployed as hardware or software, BIG-IP provides a range of functionality to secure applications, direct incoming requests, and optimize client connections. With full visibility and control of all traffic—including decryption and re-encryption capabilities—the BIG-IP system can keep your applications protected and optimized at scale.

Although this robust set of capabilities might imply complexity, the platform supports a powerful templating system that allows security and operations experts to create standardized templates, which can be implemented by application teams with a few simple inputs and no advanced security or traffic management expertise.

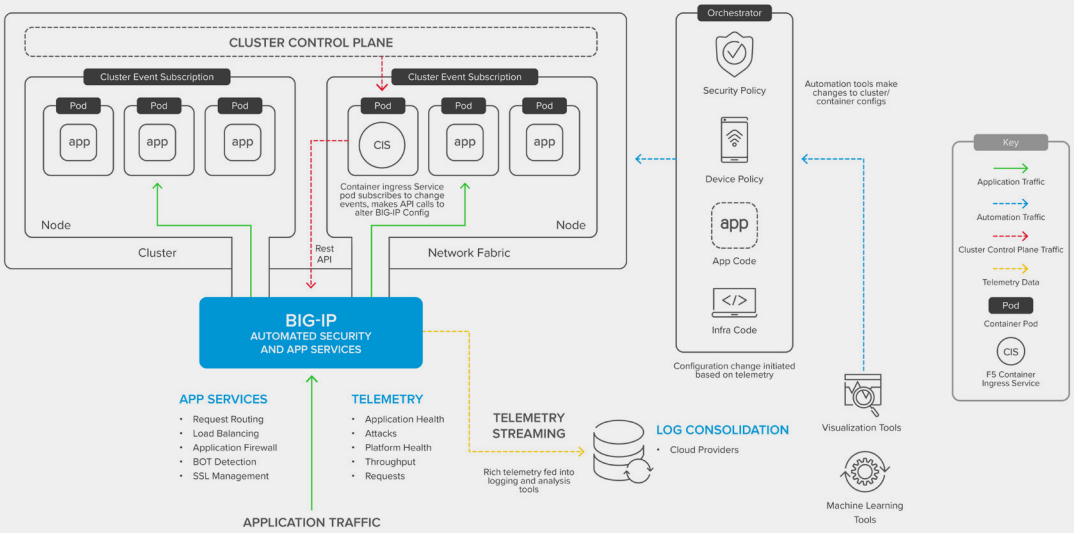
Of course, you also have to be able to get application traffic in and out of your container environment—so VXLAN support is essential to extend a cluster fabric into a gateway device such as a BIG-IP. Both hardware and software BIG-IP platforms offer full VXLAN integration (as well as a number of other network overlays).

Container Connectors

The power and network integration of a BIG-IP needs to be deployed and updated in coordination with container events. To do this, F5 provides a free container integration solution—the Container Ingress Services (CIS) component, which runs as a container and subscribes to cluster management events. CIS combines event awareness with native container platform tools like config maps and annotations to configure Ingress services via the BIG-IP REST API.

Telemetry and instrumentation of your container apps is essential to their continuous improvement. As the BIG-IP platform has deep insight into application traffic, it's an obvious point to stream stats and event data into the collection and visualization tool of your choice.

Combine event awareness with native platform tools



PARTNERS

F5 works closely with its technology partners to help you optimize your apps in containerized environments.

Container Ingress Services

Container Ingress Services are available for the following container management platforms:

- Kubernetes
- OpenShift
- Cloud Foundry
- Mesos Marathon

Virtual Environments

The BIG-IP platform can run in the following virtual environments:

Public:

- AWS
- Microsoft Azure
- Google Cloud Platform
- Alibaba Cloud

Private:

- VMware (ESX, ESXi, vCloud Director)
- Microsoft HyperV
- Linux KVM, Xen Project, OpenStack

CONCLUSION

No matter where they run, applications can benefit from the performance and security services that F5 offers. With Container Ingress Services, applications running in dynamic container platforms can get the services they need configured on demand by tools native to the container management system—with no need for specific BIG-IP knowledge from application owners.

RESOURCES

Read more about BIG-IP application services.

Learn how to optimize traffic management and load balancing for containerized environments in this F5 white paper.