F5 Distributed Cloud Web Application Firewall

Managed Service

Whether protecting applications on-premises or in the cloud, F5 Distributed Cloud Web Application Firewall (WAF) managed service delivers market leading Application Security while augmenting your in-house resources and decreasing operational expenses with a service that is deployed and maintained by F5 security experts.

KEY BENEFITS

OWASP Application Security
Protect your applications against application-layer attacks and adapt each policy.to current threat landscape.

Ease of Deployment
Speed up time to protection by onboarding applications with support from F5 Security experts.

SaaS Delivered, Globally Available, Minimal Business Impact
Leverage the F5 global network and security experts to maintain continuous application security and availability.

Low Cost of Entry and Ownership
F5 Distributed Cloud Services - SaaS and managed services allow customers to obtain the solution they need at a competitive price point to maximize their total cost of ownership.

Staff Augmentation, WAF Experts On-Call, Knowledge Aggregation
Internal customer teams can work collaboratively with F5 Security experts who are available 24x7 and have the latest vulnerability information available from internal F5 Security Incident Response teams (F5 SIRT).

High Availability, Dedicated Proxies, Traffic Steering, Health Monitoring
The F5 global network offers a 99.99% uptime SLA, dedicated load balancers, traffic shaping, continuous back-end health and availability monitoring.

DDoS Mitigation Included
Managed WAF services include DDoS protection.

F5 Distributed Cloud Web Application Firewall (WAF) is a SaaS delivered managed service that detects and mitigates general, automated and application-specific security threats. The managed WAF service protects organizations' internet facing web applications and data, and enforces compliance with industry security standards, such as PCI DSS. The service is supported 24/7 by highly specialized, F5 application security experts. The managed WAF service is delivered via our global network with 23 Regional Edges (RE) in 22 metro markets. The current list of REs and availability is located at F5 Distributed Cloud Status.

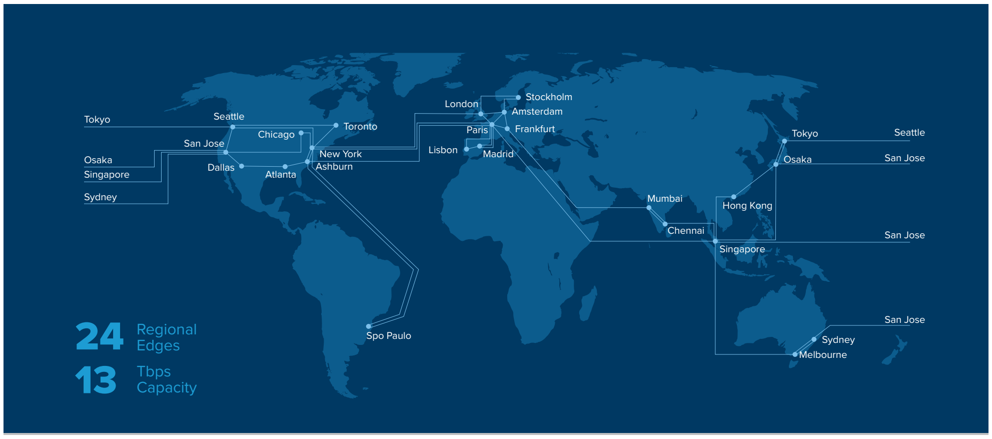


Figure 1: F5 Distributed Cloud Global Network with DDoS mitigation and protection capabilities

Managed Web Application Firewall

Managed security and performance policies across your application portfolio to decrease the risk of data breaches and improve customer experiences

A Web Application Firewall (WAF) policy is a set of rules (or "blocking modules") that will identify traffic to be blocked or permitted to reach an application's origin. F5 application security experts will work with customers to create and tune specific WAF security policies deployed to protect one or many applications. The managed WAF service will mitigate the risk of network layer attacks such as Denial of Service (DoS) as well as application attacks such as SQL Injections, Cross Site Scripting, Cross Site Request Forgery, malicious bot traffic and other threats specifically aimed at the customer's application.

F5 PROVIDES A SERVICE CATALOG OF APPLICATION DELIVERY AND SECURITY SERVICES THAT ARE MAINTAINED BY EXPERTS BUT CAN BE EASILY MODIFIED BY WORKING WITH SECURITY EXPERTS IN THE OPERATIONS TEAM.

The F5 Distributed Cloud WAF managed service will use a combination of techniques and sources to determine if traffic is malicious. Attack Signature Sets maintained by F5 Threat Labs and F5 security engineers block known threats, as well as defining and enforcing custom rules based on HTTP Headers, packet payloads or and other request parameters specific to each customer.

Below is a sample list of our extensive library of functions available for configuration:

- IP Deny/Allow Lists
- Fast Access Control Lists (ACLs)
- User Behavior Analysis (WAF Events/Login Failures/L7 Policy Deny)
- WAF Policy Management
- Service Policies
- IP Reputation
- Threat Campaigns

F5 security experts will collaborate with customers to determine which functions will be configured and provisioned for each application. The managed WAF service provides mitigation for attacks by virtually patching customer applications without the need for application source code changes or patches, while additionally providing visibility into both legitimate and malicious traffic.

Managed WAF Service Components

Customers depend on F5 Distributed Cloud Services to provide complete security management for the application perimeter and to continue evolving client trust

Subscriptions

F5 Distributed Cloud WAF managed services are consumed as a one, two or three year subscriptions, and there are two primary components calculated to determine the total subscription cost; number of **Load Balancers** deployed, and **category of managed service** customer would like to obtain **(Standard or Enhanced)**.

DDoS Protection

The F5 Distributed Cloud platform provides comprehensive protection against DDoS attacks -including automatic mitigation of volumetric attacks and capabilities to defend against layer 3-4 protocol attacks and attacks specifically targeting apps at layer 7. The F5 Distributed Cloud WAF managed service includes DDoS protection for an **unlimited number of attacks**.

F5 DISTRIBUTED CLOUD MANAGED SERVICES.

Standard Services
Provides customers assistance with onboarding and post-deployment support via incident request with 15 min response.

Enhanced Services
Enhanced visibility into security risks, cyber-attacks and remediation activities, prioritized and personalized consultative technical engineering support for expeditious triage and configuration updates.

Provides improved security and compliance posture to reduce overall operational risk factors.

Customer teams may obtain custom reporting to ensure data is correlated appropriately and leads to actionable remediation to prevent WAF threats and improve identification and fast blocking of potential WAF vulnerabilities during policy evolution. Data can also be provided to Law Enforcement for further legal action.

Roles and Responsibilities

F5 Distributed Cloud WAF managed security service includes F5 security experts to build and maintain WAF Policies. Customers may provide initial input on the application and web server technologies to assist security experts in policy creation and maintenance. Customers will need to perform routing configuration changes to direct traffic to the F5 Distributed Cloud Services platform on the F5 Network (Authoritative DNS Record Change Management).

Customer Service Onboarding

The F5 services team will schedule an initial onboarding call with the customer to review application setup, policy deployment (covering SSL certificate upload), transition from "monitoring to blocking", and the customer application and infrastructure architecture for the creation of a WAF policy. The F5 security operations team may coordinate an optional call when a customer initiates traffic routing to the Distributed Cloud platform.

The initial onboarding call is an opportunity for the customer to:

- Review steps for successful deployment
- Obtain an overview of the F5 Distributed Cloud console
- Understand best practices for role based access control and management
- Defining and provisioning applications to be protected
- Deploying and securing SSL assets and defining security profiles
- Perform a review of the WAF technical questionnaire review
- Discuss managed service details related to the operation of the WAF
- Explain policy elements and capabilities for protection
- Collaborate to define desired policy features
- Agree on actionable items for learning and blocking phases (WAF best practices)

Deployment

Successful implementations are the result of a strong relationship between customers and the F5 services and operations teams. Both teams will guide customers through the process so that the experience is seamless and maximizes protection capabilities. Policy protection typically follows the steps outlined below.

- The F5 services team creates the WAF policy and waits to attach the policy to the application based on the application information provided by the customer.
- Customer creates application configuration either in the console or via API.
- Customer deploys the application to the Distributed Cloud platform via the console or API.
- The services team will finalize the application configuration and ensure everything is working correctly.

KEY FEATURES

Robust attack-signature engine
The Distributed Cloud WAF signature engine contains more than 7,000 signatures for CVEs, plus known vulnerabilities and techniques identified by F5 Labs.

Threat Campaigns
Delivers protection against sophisticated, multi-vector attack campaigns via fully vetted attack campaign signatures developed by F5 threat researchers.

Advanced Behavior Engine
Client interactions are analyzed on how a client compares to others—the number of WAF rules hit, forbidden access attempts, login failures, error rates, and more.

Powerful Service Policy Engine
Enables micro segmentation and support for advanced security at the application layer with development of allow/deny lists and customer rule creation based on a variety of parameters to act on incoming requests.

IP Reputation Service
Easily allow or deny IP addresses based on threat categories or threat score backed by F5's database of known malicious IP addresses.

Reporting and Analytics
With a 360-degree view of performance and security posture for all apps including granular status of application deployments, health, performance and detailed real-time information on violations, attack activity, sources, paths and more.

Customers may schedule an optional conference call with the F5 services team as part of initial onboarding to review configuration and commit routing changes to the Distributed Cloud platform.

WAF Policy Learning and Building

WAF security policies will be created by the F5 services team as follows:

- using a baseline security template that is pre-configured for known vulnerabilities related to the particular application framework to be protected
- and/or output related to a third-party WAF vulnerability assessment or scan output
- and/or an existing policy from other vendors.

Policy deployment and tuning tasks may include some or all the following vulnerability mitigations and may be implemented upon an agreed order by the F5 services team and customer.

Configure Allowed HTTP methods
Configure Allowed HTTP Response Codes
Configure Disallow File Types
Configure Attack Signatures
Configure relevant attack signature based on customer's requirement
Tailor architecture-based attack signatures to match customer's environment
Configure Explicit Entities
URLs
Parameters
Configure Session and Logins
(Verify with the customer if they want the module on and inform the customer before enabling)
Configure Logon pages
Enable Login Page based Session Awareness
Configure Headers
Cookie enforcement
Redirection Domains
Enable additional WAF policy features as agreed upon during the Onboarding Call
Configure Block Response Page

The F5 services team will attach the policy to the load balancer and initiate the learning phase. F5 engineers will work collaboratively with the customer to tune the policy. Once a policy is deployed, the customer and the operations team may collaborate to perform violation reviews and on-going tuning. F5 security experts will advise on best practices for unique customer scenarios.

For any issues that arise from mitigation, policy tuning, violation identification through log data, false positives or negatives, construction and tuning of additional policies, the customer has the option to contact and work with the F5 operations team using email or phone communications. The team may also identify issues that require tuning or changes to parameters in the system. The operations team will initiate contact with a customer via a service request to ask for participation as required.

WAF Violation Blocking and Enforcement

Once the policy tuning has been completed in the monitoring phase, the F5 services team will setup a call to transition the policy to blocking mode. Customers may also elect to move the policy into or out of blocking mode at any time. Most customers will elect to perform a one phase or aggressive deployment. However, customers who require additional tuning in the policies may choose a phased implementation that entails several steps to ensure a gradual and disciplined approach to policy development.

During this call customers will be able to:

- Understand the development methodology used during the policy lifecycle
- Work on a process with the operations team to remediate violations and attack types
- Collaborate in joint reviews of the application security best practices, as required
- Review "mission-critical" sections of the web application
- Review system defaults, customized features and protection settings
- Determine whether policy will be deployed in a phased or aggressive methodology
- Establish a tentative maintenance window to start policy enforcement

Policies may continue to be tuned until the customer or the operations team determines that no further tuning may be required for the initial deployment.

The F5 operations team will keep the customer updated via tracking incidents for each phase of deployment and any changes in the state of the policy. Customers can also have visibility into any action taken on the policy by reviewing audit reports. Customers are encouraged to schedule a maintenance window with the operations team in order to:

Enable Blocking Mode
Monitor for False Negatives and Positives - Adjust policy as required

Policy Maintenance

F5 conducts on-going policy maintenance for all customers.

The F5 operations team will notify the customer of any new observations via a support/escalation incident request. Customers can also notify the operations team directly to request assistance with policy tuning. The F5 operations team will investigate issues and determine the best course of action.

HELPFUL LINKS AND VIDEOS

The web links will provide a basic understanding of the Recommended Practices for WAF applications and also a video review of several of the features available in the F5 Distributed Cloud Services.

F5 Distributed Cloud Web Application Firewall

Configure Multi-Cloud Environments with F5 Distributed Cloud Simulator

Layer 7 Connectivity with F5 Distributed Cloud

Attack Signature Maintenance/Emerging Threats

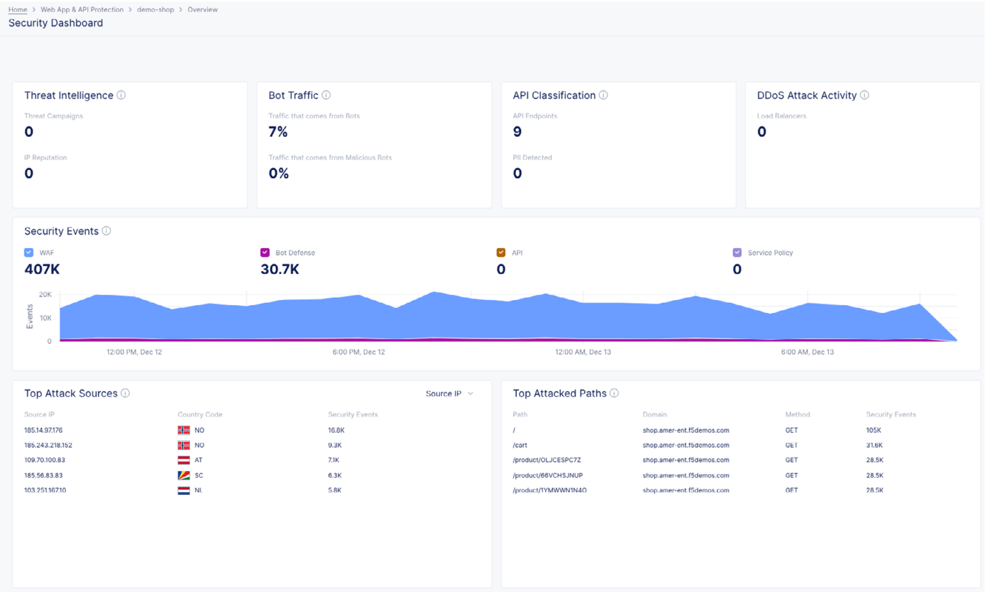
Application protection provided by the F5 Distributed Cloud is delivered through a combination of toolsets. These tools utilize and leverage application attack pattern signatures, Bot identification signatures, L7 (application layer) Denial of Service (DoS) patterns, and more. The F5 operations team continually updates signatures across the platform without customer intervention. Customers also have the option to collaborate with the F5 operations team to tune policies. This managed service provides continuous protection offering customers assurance that their applications are always protected and available.

New threats are constantly being discovered and policies must be updated rapidly to protect against new and emerging vulnerabilities. The F5 operations and engineering teams work with the F5 Security Incident Response Team (F5 SIRT) to develop and implement a protection framework for these types of instances. They can be deployed as a new service policy, by adding additional countermeasures into the policy, or other mitigation techniques within the F5 Distributed Cloud platform.

Visibility

The F5 Distributed Cloud WAF managed service includes access to a service management console to allow customers the ability to modify and update configurations. It also offers in-depth operational visibility via enhanced network and security reporting.

The console provides detailed real-time information on WAF Violations (Security Events), Threat Campaigns, DDoS Attack Activity, Top Attack Sources, Attack Paths and more. Console users and administrators can create custom dashboards that showcase relevant info based on user persona/role.



Home > Web App & API Protection > demo-shop > Overview

Security Dashboard

Threat Intelligence ⓘ

Threat Campaigns
0

IP Reputation
0

Bot Traffic ⓘ

Traffic that comes from Bots
7%

Traffic that comes from Malicious Bots
0%

API Classification ⓘ

API Endpoints
9

PII Detected
0

DDoS Attack Activity ⓘ

Load Balancers
0

Security Events ⓘ

☑ WAF 407K

☑ Bot Defense 30.7K

☑ API 0

☑ Service Policy 0

Top Attack Sources ⓘ

Source IP	Country Code	Security Events
185.14.97.176	NO	16.8K
185.243.218.152	NO	9.3K
109.70.100.83	AT	7.1K
185.56.83.83	SC	6.3K
103.251.167.10	NL	5.8K

Top Attacked Paths ⓘ

Path	Domain	Method	Security Events
/	shop.amer-ent.f5demos.com	GET	105K
/cart	shop.amer-ent.f5demos.com	GET	31.6K
/product/OLJCESPC7Z	shop.amer-ent.f5demos.com	GET	28.5K
/product/66VCHSJNUP	shop.amer-ent.f5demos.com	GET	28.5K
/product/1YMWWN1N4O	shop.amer-ent.f5demos.com	GET	28.5K

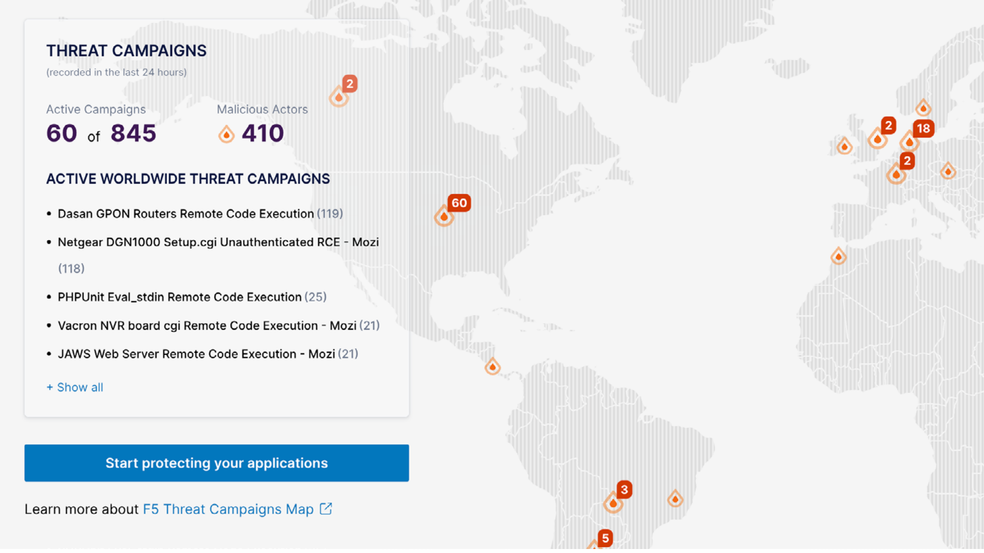
Figure 2: F5 Distributed Cloud Management Console

Automation

The F5 Distributed Cloud Services RESTful API is available for customers to programmatically complete tasks such as: creating new load balancers, updating denylist IP addresses, configuring SSL attributes and more. To obtain more information about the API select this link.

Threat Campaigns

Threat campaign signatures are based on current “in-the-wild” attacks that exploit the latest vulnerabilities and/or new ways to exploit old vulnerabilities. Threat campaign signatures contain contextual information about the nature and purpose of the attack. F5 Distributed Cloud allows you to work with the F5 operations team to manage threat campaigns and apply them selectively to protect your most valued applications.



THREAT CAMPAIGNS

(recorded in the last 24 hours)

Active Campaigns

60 of 845

Malicious Actors

410

ACTIVE WORLDWIDE THREAT CAMPAIGNS

- Dasan GPON Routers Remote Code Execution (119)
- Netgear DGN1000 Setup.cgi Unauthenticated RCE - Mozi (118)
- PHPUnit Eval_stdin Remote Code Execution (25)
- Vacron NVR board cgi Remote Code Execution - Mozi (21)
- JAWS Web Server Remote Code Execution - Mozi (21)

+ Show all

Learn more about F5 Threat Campaigns Map

Figure 3: Threat Campaign Landscape and Current Threats

System Logs Integration

Customers can securely send WAF Violation data in real-time to their internet facing Log collection systems for further investigation. The F5 Distributed Cloud platform Logging API enables customers to have a unified view of all their security events whether their apps are in the cloud, on-prem, or both.

System Status

Real-time status information of F5 Distributed Cloud Service operations is available by selecting this link. F5 provides at least fifteen calendar days’ notice to customers for routine maintenance work. However, F5 reserves the right to perform emergency maintenance at any time. Emergency maintenance notices are made available to customers before any maintenance work is performed. Service Delivery Responsibilities.

WEB APPLICATION FIREWALL SERVICE TIERS

The following table, indicates which managed services are provided by F5 as part of the subscription for each specific service tier. The list represents the most commonly requested tasks. Customers may request additional services that may not be included in this list by contacting their F5 Account team.

To obtain additional information about the service components, navigate to the **Service Footnotes** on the next page.

Table 1: WAF Managed Service Tiers

SERVICE	STANDARD	ENHANCED
LB Setup, Configuration and Troubleshooting	✓	✓
WAF Policy Assessment and Tuning	✓	✓
L7 DoS Configuration and Tuning	✓	✓
IP Reputation, Threat Campaign Configuration	✓	✓
TLS Cert Upload and Renewal	✓	✓
Autocert Configuration using LetsEncrypt	✓	✓
Troubleshooting TLS Handshake Issues	✓	✓
Troubleshooting Routing and Latency Issues	✓	✓
Standard Service Policy Configuration	✓	✓
WAF Allowlist/Denylist Configuration	✓	✓
Assist with DNS Authoritative Record Changes	✓	✓
User Management on Console	✓	✓
API Token Generation	✓	✓
SSO Configuration	✓	✓
Remote Logging Configuration	✓	✓
Escalation Management	✓	✓
Customer Success Manager	✓	
Named Technical Account Manager		✓
RCA Reporting		✓
Project Management		✓
Assisted Service Policy Creation		✓
Business Reviews	BI-ANNUALLY	QUARTERLY
Solution Designing		✓
Security Policy Reviews		✓
Product Training		✓
Technical Consultation		✓

Conclusion

A WAF is a foundational element of any strong security posture. The F5 Distributed Cloud WAF managed service will provide protection and defense against malicious actors and allow organizations to control and monitor the flow of traffic prior to arrival at the origin servers. Customers will realize immediate security gains when rapidly deploying policies to inspect traffic and block malicious requests that could negatively affect business operations.

To learn more, contact your F5 representative, or send us an inquiry at F5 Sales

Services Footnotes

Troubleshooting TLS Handshake Issues

The F5 team will not only upload and configure certificates, but will also assist in troubleshooting TLS connectivity issues throughout the customer lifecycle.

Troubleshooting Routing and Latency Issues

The F5 team will assist customers is setting up all necessary app endpoints and connections, and will work with the customers to troubleshoot any routing challenges or latency issues throughout the customer lifecycle.

Assist with DNS Authoritative Record Changes

The service requires customers delegate their domain to the F5 Distributed Cloud platform, which enables the platform to manage the domain and be the authoritative domain name server for a customer's domain(s). This requires an update to the domain records. If a customer is using the F5 Distributed Cloud DNS service, this domain record change will be performed by F5. Customers using a 3rd party DNS provider(s) will need to make the change themselves and F5 resources can be there to walk them through the process if necessary.

User Management on Console

The F5 team will set up admin accounts for access and visibility into the F5 Distributed Cloud console. Additional users can be easily added by customers admins directly in the console or admins can submit a support request to have additional users added by the operations team.

API Token Generation

If customers want to automate or integrate elements of their service and reporting using the platform API they will need a token to access the API. The F5 team can generate the token on a customers behalf if necessary.

SSO Configuration

F5 as part of onboarding will perform SSO integration with F5 Distributed Cloud Services. This can be done for several different SSO platforms including Azure AD, Okta, and Google.

Remote Logging

F5 onboarding teams will perform the setup of a global log receiver, enabling tenant logs to be sent to any number of external log collection systems, including Amazon S3, Datadog, Splunk, AWS CloudWatch.

Technical Account Manager (TAM)

Assigned F5 Technical Account Manager (TAM) works directly with customers as their trusted advisor, helping with project management of on-boarding and on-going change management, scheduling of product training (as needed), and conducting quarterly business reviews.
The TAM will serve as a customer's primary point of contact with F5 throughout their service lifecycle.

Escalation management

Provided by assigned F5 Technical Account Managers (TAMs) on a customer's behalf, for critical issues or requests from the customer when resolution is not available via standard support channels and process based on service SLAs.

Root Cause Analysis (RCA)

Led by Technical Account Manager (TAM), RCA will be done with all P1 incidents, and the report will include a summary of the incident timeline, time to solve/mitigate, root cause, lessons learned and remediation actions taken to prevent its occurrence in future.

Project Management

Provided by assigned F5 Technical Account Manager (TAM) as part of the enhanced Distributed Cloud WAF managed service tier, and includes coordination of initial customer on-boarding and service configuration, on-going change management, development of best practices and processes around reporting, efficiency and efficacy of app security posture etc.

Business and Roadmap Reviews

Quarterly meeting with assigned F5 Technical Account Managers (TAM) to review service metrics, including SLAs, support cases, service posture and entitlement details, plus notable changes to the service.

Security Policy Reviews

With the ever evolving threat landscape it is paramount that Security Policies are continuously reviewed and updated to deal with new threats. The assigned F5 security experts will proactively conducts security policy reviews and notify customers of any new recommendations.

Product Training

Individualized technical training on F5 Distributed Cloud Services. It is scheduled by an assigned F5 Technical Account Manager (TAM) and trainings are conducted by Distributed Cloud Services security experts. In addition, these experts are available to provide hands-on training on any new Distributed Cloud Services features and update customers on the product roadmap and enhancements as they are released.

Technical consulting

F5 Security experts will be available for ad-hoc or as needed technical review of existing Distributed Cloud Services configurations and recommend steps to improve the security posture. Each consulting session will span up to one hour and will involve one FQDN.