Data sheet

F5 Distributed Cloud Services Packages

What's Inside

Application security and delivery for the hybrid multicloud enterprise

F5® Distributed Cloud Services is available in two distinct packages: Essentials and Enterprise. Both provide an array of application security and delivery capabilities that modern enterprises need for their applications.

Essentials is best suited for organizations that need a cloud-based solution to securely deliver public facing web applications and properties.

The Enterprise package is built for customers with increased security and compliance needs, protecting critical applications across hybrid environments. It offers AI-enabled risk scoring and strong defenses against malware and client-side attacks.

Key benefits

Essentials

- **Fast, simple entry into secure application delivery**
  Provides foundational load balancing, WAF, API protection, and CDN to get modern applications online quickly with built in security.
- **Integrated protection without added complexity**
  Combines delivery, security, and core platform services in a single SaaS offering, reducing reliance on point solutions.
- **Designed to grow with you**
  Serves as a predictable starting point that supports add ons like API discovery, Bot Defense or Routed DDoS as requirements evolve.

Enterprise

- **Advanced security for mission critical applications**
  Delivers deeper threat protection and traffic controls for applications with higher risk, scale, or business impact.
- **Greater scale, flexibility, and operational control**
  Supports more demanding workloads with expanded platform usage, enhanced policies, and richer observability.
- **Ideal foundation for advanced services and add ons**
  Optimized for customers deploying advanced protections such as API discovery, Bot Defense (Web, Mobile, Advanced) and Routed DDoS.

PACKAGE COMPARISON

Service	Description	Essentials	Enterprise
Web App Firewall			
Web App Firewall	Protects web applications from common attacks (e.g., OWASP Top 10) using L7 inspection and enforcement policies.	●	●
Service Policies	Apply traffic governance rules (allow/deny, routing actions, security checks) to control how requests are handled.	●	●
Rate Limiting	Limits request volume by client/app attributes to prevent abuse and protect backend capacity.	●	●
Threat Campaigns	Provides curated, continuously updated protections for active/exploited vulnerabilities and attack waves.	●	●
L7 DDoS	Detects and mitigates high-volume or application-layer DDoS attacks targeting HTTP(S) services.	●	●
Threat Mesh	Shares and correlates threat signals across protected apps/sites to improve detection and coordinated enforcement.	●	●
Fast ACLs	Enforces high-performance allow/deny lists (e.g., IP/CIDR) at the edge to quickly block unwanted traffic.	●	●
Malicious User Detection and Mitigation	Utilizes user behavior analysis and heuristics to create dynamic, holistic profiles of clients interacting with your application. Real-time risk levels evolve as behaviors accumulate, enabling adaptive responses by scoring behavior over time across multiple signals to effectively identify and mitigate malicious activity.	●	●

Web App Firewall			
Malware Protection	Safeguards web applications and APIs from malicious file uploads by scanning and blocking harmful content during the upload process.	●	●
AI-enabled Risk Scoring	Combines signatures, attack indicators, and machine learning to assign dynamic risk levels (High, Medium, Low) for every request. This reduces manual policy tuning, accelerates safe enforcement, minimizes false positives, and enhances detection of advanced threats, enabling confident risk-based blocking across distributed environments.	●	●
Bot Protection			
Signature-based Bot Detection	Identifies and blocks known bad bots using signatures, reputation, and behavioral indicators.	●	●
Protects against OWASP automated threats.	Prevent attackers' use of OWASP Automated Threat attack vectors.	Add-on	Add-on
Advanced bot protection	Uses rich signal collection and behavioral analysis to detect and mitigate automated threats, including sophisticated, low-and-slow bot attacks that evade signature-based defenses.	Add-on	Add-on
Credential stuffing and account takeover mitigation	Prevent automated bots from entering stolen credentials on login pages, which can lead to account takeover and fraud.	Add-on	Add-on
Prevent web scraping	Prevent automated bots and web crawlers from extracting content or data from your site, and from using your data for competitive pricing or AI training without your permission.	Add-on	Add-on
Device fingerprinting	Uniquely identify and track a web user or a mobile application. The device's fingerprint is retained as the user interacts with the application over time.	Add-on	Add-on
API Security			
API protection rules	Applies API-focused security controls (e.g., method/path enforcement and attack detection) to API traffic.	●	●
API rate limiting	Throttles API calls per key/client/endpoint to protect APIs from spikes and abusive usage.	●	●
JWT validation	Validates JWTs (signature/claims) to authenticate and authorize requests before they reach the API.	●	●
API schema upload	Imports an API specification (e.g., OpenAPI) to drive validation, discovery, and policy enforcement.	●	●
API endpoint and groups management	Organizes and manages API endpoints into logical groups for consistent policy and reporting.	●	●

API Security			
Enterprise API Discovery	Continuously discovers and inventories APIs across your environment from traffic and configuration signals to expose unknown or unmanaged endpoints.	Add-on	●
API Schema Validation	Validates API requests/responses against an uploaded schema (e.g., OpenAPI) to enforce allowed methods, paths, parameters, and payload formats.	●	●
Sensitive Data Detection	Detects exposure of sensitive data (e.g., PII, secrets, tokens) in API payloads/logs and flags or enforces controls to reduce leakage.	●	●
Compliance Reporting	Produces audit-ready reports mapping security controls and activity to common compliance requirements and evidence needs.	●	●
API Threat Surface Detection	Identifies publicly exposed, vulnerable, or misconfigured API endpoints to reduce attack surface and prioritize remediation.	●	●
Code-based API Discovery	Discovers APIs by analyzing application code/repositories to find routes, parameters, and dependencies beyond what's seen in runtime traffic.	Add-on	●
API Testing	Exercises APIs with automated tests to validate behavior and uncover security issues such as auth gaps, injection, and schema violations.	●	●
Client-Side Defense			
Client-Side Defense	Detects and mitigates malicious JavaScript, formjacking, and supply-chain script abuse running in the browser on your application pages.	●	●
DNS & GSLB			
Standard DNS Zones	Hosts and serves authoritative DNS records with standard management and resolution capabilities.	●	●
Secure DNS Zones	Adds DNS security controls (e.g., access control and anti-abuse protections) to authoritative DNS zones.	●	●
Application Delivery			
Content Caching	Caches content at edge locations to reduce origin load and improve latency for repeat requests.	●	●
Support for Customer Edge nodes	Extends the data plane to customer environments to enforce policies and route traffic close to private apps.	●	●
TCP and UDP protocol support	Load balances and proxies non-HTTP services over TCP/UDP in addition to HTTP(S).	●	●
Network segmentation	Granular network isolation and micro segmentation to secure network segments on premises and across public cloud networks.	●	●

Application Delivery			
End-to-end-encryption	Native Transport Layer Security (TLS) encryption for all data transit across networks.	●	●
Rich traffic insights	Get more granular insights into application traffic with time-series anomaly detection, top talkers, and flow analysis diagrams.	●	●
Platform			
AI Assistant	Provides guided help to create, troubleshoot, and optimize configurations using natural language.	●	●
Audit & request log observability	Captures admin/audit actions and request logs to support troubleshooting, forensics, and compliance.	●	●
Global Log Receiver	Streams logs to an external destination/SIEM for centralized retention and analysis.	●	●
Metrics	30 days	●	●
Request logs	Seven days	●	●
Audit logs	30 days	●	●
Alert & notification policy rules	Defines conditions and routing for operational/security alerts and notifications.	●	●
Fast ACLs on Regional Edge	Applies fast allow/deny filtering specifically at regional edge sites for low-latency enforcement.	●	●
Reports	Generates summarized views of traffic, security activity, and operational posture over time.	●	●
Dashboards	Provides real-time and historical visualizations of key traffic, performance, and security metrics.	●	●
Synthetic Monitoring	Easily monitor your critical applications and systems from regions around the world. Quickly correlate performance and availability issues to a specific region or location. Leverage built-in TLS reports to quantify risk of certificate expiry, assess the use of vulnerable protocols and ciphers, and determine overall TLS score for your monitored endpoints. Receive relevant alerts before your customers start calling in and clearly identify if they were impacted during the last change window or outage. Includes 500 thousand executions.	●	●
Service policies	Enables micro-segmentation and supports advanced security at the application layer with development of allow/deny lists, Geo IP filtering, and custom rule creation to act on incoming requests, including match and request constraint criteria based on a variety of attributes and parameters such as TLS fingerprint, geo/country, IP prefix, HTTP method, path, headers, and more.	●	●

Platform			
CORS policy	Cross-Origin Resource Sharing (CORS) is useful in any situation where the browser, by default, disallows cross-origin requests, but you have a specific need to enable them. CORS policy is a mechanism that uses additional HTTP headers to inform a browser to allow a web application running at one origin (domain) to have permission to access selected resources from a server at a different origin.	●	●
Trusted client IP headers	Identification of real client IP addresses for monitoring, logging, and defining allow/deny policies. When this feature is enabled, security events and request logs will show this real client IP address as the source IP.	●	●
Mutual TLS	Support for both TLS and Mutual Transport Layer Security (mTLS) for authentication with policy-based authorization on the load balancer. Proxy provides the capability to enforce end-to-end security of application traffic. Mutual TLS supports the ability to send client certificate details to origin servers in x-forwarded-client-cert request headers.	●	●
Administration	Unlimited number of users Single Sign-On Role-based Access Control	●	●
Support			
24/7/365 support	Support is provided in various methods including console ticketing, email, and phone support.	●	●
Uptime SLA	99.99%	●	●
Security logs	30 days	●	●
Response SLA	One hour	●	●
Onboarding	Customer Success Team and access to training.	●	●
Entitlements			
Tenant VIP	A VIP (virtual IP) is the front-end listener address (IP/hostname and port) that clients connect to, which then routes traffic through the F5 Distributed Cloud Services load balancer to the configured origins.	1	1
Public/Distributed Load Balancer	A public load balancer distributes external user requests across servers or data centers located in multiple geographic regions to optimize performance, reduce latency, and ensure availability. Public = Public VIP + Public Origin Distributed = Public/Private VIP + Private Origin across different sites	1	4
App Rules	An Application Rule is any configuration on a load balancer that matches traffic parameters and takes any application delivery action.	100	1000

Entitlements			
Synthetic Monitoring Executions	An execution is one instance of one monitor endpoint operating from one region. If you have one HTTP monitor operating in three regions every five minutes, you have three executions occurring every five minutes.	500k	500k
CDN Data Transfer	CDN Data Transfer is the volume of data passing from the CDN to an end user over the F5 Global Network per month. CDN Data Transfer is aggregated across regions, so you can adjust the distribution of traffic.	5 TB	15 TB
Standard/Secure DNS Zones	A DNS zone is a distinct division of a domain namespace that is managed by an entity such as an organization. Customers can exercise granular control on components such as name servers which hold the DNS records for the domain namespace represented by the zone.	5	10
DNS Load Balancers (GSLBs)	DNS Load Balancers are globally distributed load balancers (GSLB) which distribute user requests across servers or data centers located in multiple geographic regions to optimize performance, reduce latency, and ensure availability.	5	10
Web App Scanning Applications	An application is a deployed instance hosted on a web server, available through a defined entry URL. Different URLs are counted as different applications.	3	3
DDoS Mitigation Rules	DDoS rules are automated policies that detect and mitigate distributed traffic floods. These rules include Fast ACLs, which are high-performance allow/deny IP and request-filter lists enforced at the network/edge to quickly block unwanted traffic.	100	100
Requests	Requests are any single inbound transaction evaluated by a given security capability, and it is counted once as it traverses through the configured Application Delivery and Security services.	30M	30M
Logs	Logs, metrics, alerts, and events are automatically generated, and are used for troubleshooting. Each request directly translates into a line of logs.	1M	50M
Public Application Non-HTTP Traffic	Public Application Traffic addresses throughput of non-HTTP applications. Any non-HTTP application protocols (including TCP, UDP, MQTT, and QUIC) are metered by maximum throughput.	Add-on	20 Mbps
Customer Edge Nodes	Customer Edge nodes extend Distributed Cloud Services into customer environments, enabling local service deployment and hybrid multi cloud security (Optional WAF add-on available).	Add-on	3 Medium Nodes
Data Transfer	Data transfer is the volume of data passing from a Customer Edge node to a Regional Edge node on the F5 Global Network per month.	Add-on	1 TB

Entitlements			
Client-side Defense Transactions	Client-Side Defense transactions refer to distinct page views of an Authorized Website with Client-Side Defense JavaScript. This number is generally lower than the total page views on those pages.	Not included	1M
Malware Protection Transactions	Malware Protection protects web apps and APIs, from malicious file uploads by scanning files in real-time. Each scan is a single transaction.	Not included	1M

More Information

Contact F5 to learn how Distributed Cloud Services can help

DC 04.2026 | DS-4438248588