F5 Distributed Cloud Services Overview

Westcon | Distributed Cloud Services

F5 Distributed Cloud Services

F5 Distributed Cloud Services are SaaS-based security, networking, and application management services that enable customers to deploy, secure, and operate their applications in a cloud-native environment wherever needed – data centre, multi-cloud, or the network or enterprise edge.

These services support a wide variety of use cases for the modern enterprise to connect and secure distributed applications across public/private cloud and edge infrastructure.

Key benefits

- **Cost-optimised:** A multi-tenant platform with no cloud provider integrations or third-party services, for a 70% cost saving
- **Operational simplicity:** Up to 12x reduction in time-to-market with an integrated, consistent set of SaaS-based services across any environment
- **Increased collaboration:** Self-service with separation of duties allows developers, DevOps, NetOps, and SecOps to openly collaborate
- **Improved app performance:** Applications and workloads can be deployed closer to users on the F5 Global Network
- **Integrated security:** Advanced AI/ML mitigates threats and enforces security policies across distributed environments
- **End-to-end observability:** A single portal shared by NetOps, SecOps, and DevOps for holistic view of app security and performance

Westcon | Distributed Cloud Services

F5 Distributed Cloud DDoS Mitigation

Deliver pre-emptive protection against L3–L7 DDoS attacks

What is it?

F5 Distributed Cloud DDoS Mitigation—a key offering in F5's SaaS-based Web Application and API Security (WAAP) solution—provides mitigation against a variety of Denial-of-Service (DoS) attacks across L3-L7. It does this through multiple layers of protection, from custom DoS rules and edge firewalls pre-screening traffic, to deep packet inspection with advanced scrubbing for enterprises, hosting, and service providers.

What does it do?

Delivers Distributed Denial of Service (DDoS) and advanced security services to protect against L3-L7 attacks on enterprises and hosting and service providers.

Key benefits

- Intelligent protection at scale
- Focus on your expertise
- Pre-emptive defence
- Business continuity
- Lower cost of ownership

Westcon | Distributed Cloud Services

F5 Distributed Cloud WAF

Cloud-based protection for your distributed web applications

What is it?

F5 Distributed Cloud WAF is a next-gen SaaS-based web application firewall that provides signature and behavioural-based threat detection to protect applications wherever they're deployed.

What does it do?

Connects, secures, and manages apps in the cloud, on-premises, edge or in the F5 Global Network. Protects web apps in any cloud, edge, and on-premises with a comprehensive WAF as a Service from F5 Distributed Cloud Services, leveraging F5's best-in-class Advanced Web Application Firewall.

Key benefits

- Easy-to-use, SaaS-enabled security
- Protect applications closer to the source
- Accelerate time to market
- Reduce time to resolution in responding to threats
- Gain end-to-end observability and policy enforcement

Westcon | Distributed Cloud Services

F5 Web Apps and APIs protection (WAAP)

Discover APIs and prevent data leakage

What is it?

Distributed Cloud API Security provides discovery and deep insights from use of AI/ML. Block API attacks in real time and eliminate vulnerabilities at their source. The SaaS-based portal enables users to manage and go deep for threat analytics, forensics, and troubleshooting of modern applications.

What does it do?

Automatically discover API endpoints that are connected to your applications and allow list and monitor for anomalous behaviour. API Protection guards application programming interfaces from threat actors that attempt to exploit them to facilitate a breach or other service outage. API protection performs similar functions as a WAF, however, traditional WAFs do not typically provide sufficient coverage for API protocols or data flows given their unique nature. This has left a lot of applications with serious coverage gaps if only a WAF has been deployed.

Key benefits

- Faster onboarding: Rapid deployment via SaaS with simple API discovery leading to operational savings
- Best-in-class performance: Points of Presence (PoPs) in API security deliver high speed, scale, and API protection
- Simplified management: Observing API security and networking metrics from a single, centralised user interface

Try the F5 Distributed Cloud Services Simulator

Westcon | Distributed Cloud Services

Bot Defense

Real-time detection and mitigation of malicious bot attacks

What is it?

Bot protection for APIs and web and mobile apps

What does it do?

Highly effective bot protection based on unparalleled analysis of devices and behavioural signals that unmasks automation. Gain the advantage of a network effect as the platform adapts to retooling attempts across thousands of the world's most highly trafficked apps.

Key benefits

- Protect your business
- Protect web and mobile apps, APIs and social assets
- Remove bad bots from the equation
- Stratify trust
- Delivery seamless customer experiences
- Enjoy fast, flexible deployment

Westcon | Distributed Cloud Services

Client-Side Defense

Security monitoring and mitigation in the browser

What is it?

Distributed Cloud Client-Side Defense is a monitoring and mitigation solution to protect customer credentials, financial details, and PII against Magecart, Formjacking, and other client-side supply chain attacks.

What does it do?

The Distributed Cloud Client-Side Defense JavaScript monitors your web pages for suspicious code, sending telemetry to the Distributed Cloud Client-Side Defense Analysis Service, which generates actionable alerts viewable in a dashboard with one-click mitigation. When you enable mitigation, the Client-Side Defense JavaScript will block network calls from the browser that attackers use to exfiltrate data.

Key benefits

- JavaScript behaviour monitoring
- Insightful alerts
- Data exfiltration mitigation
- Stop Magecart and formjacking attacks
- Prevention of PII harvesting
- Avoid session hijacking
- Protection against account takeover (ATO)

Sign up for a live demo

Westcon | Distributed Cloud Services

Aggregator Management

Enabling financial institutions to secure customer experiences

What is it?

The Distributed Cloud Aggregator Management platform includes an interactive dashboard to provide visibility into aggregator traffic and enforcement mechanisms to ensure that aggregators adhere to agreed usage policies. It also provides user cohort mapping between customers and verified aggregators. The platform incorporates intelligence from a globalized network of known aggregators from world's top FIs and enables adaptive mitigation that combines high-precision machine learning, powerful AI, and human intelligence.

What does it do?

Aggregators provide value-added services that improve the overall customer experience for financial institutions (FIs). However, aggregators can use valid credentials to scrape compliant data and can be used as a vector for account takeover. FIs need a way to manage aggregator traffic and mitigate risk.

Key benefits

- Increased visibility
- Attack protection
- Access policy enforcement

Contact your local account manager for more information.

Westcon | Distributed Cloud Services