# F5 Distributed Cloud Mesh

## Connect, Secure, and Deliver Applications Across Clouds and Edge Sites

F5® Distributed Cloud Mesh connects, secures, and delivers applications deployed across multiple clouds and edge sites. Distributed Cloud Mesh's unique, distributed, proxy-based and zero-trust architecture significantly improves security by providing application access without network entry across clusters and sites. Using F5's global network backbone, it delivers deterministic, reliable, and secure connectivity across multiple clouds, edge sites, and to and from the Internet.

Distributed Cloud Mesh is a SaaS-based service that minimizes the complexity of managing and operating multiple services deployed within a single cloud, across multiple cloud or edge sites. Customers don't have to worry about managing the lifecycle of the infrastructure or services that run on it.

Since policy and configuration are centralized, changes are reflected across the system's entire deployment. All logging and metrics are also centrally available for observability with API-based integrations to external tools such as Datadog or Splunk. Ultimately, Distributed Cloud Mesh's ability to simplify operations and provide dynamic and scalable connectivity sets it apart from the competition.

Reduce the operational costs of connectivity and security services across a fleet of edge or cloud sites with SaaS-based provisioning, policy, security, observability, and lifecycle management. And you get highly scalable, on-demand, secure connectivity across many sites with a purpose-built control plane and high-performance data plane for providing L3-L7+ network services.

# Key Benefits of Distributed Cloud Mesh

## SECURE END-TO-END GLOBAL INFRASTRUCTURE

Improve the performance and security of distributed infrastructure with a high-performance private backbone, optional PrivateLink to premises, densely interconnected network, and security services that offload applications at the edge.

## LEVERAGE BEST-OF-BREED CLOUD SERVICES

Deploy applications across multiple clouds and operate, manage, and automate key services, such as AWS Transit Gateway, via a cloud-agnostic, distributed application management platform.
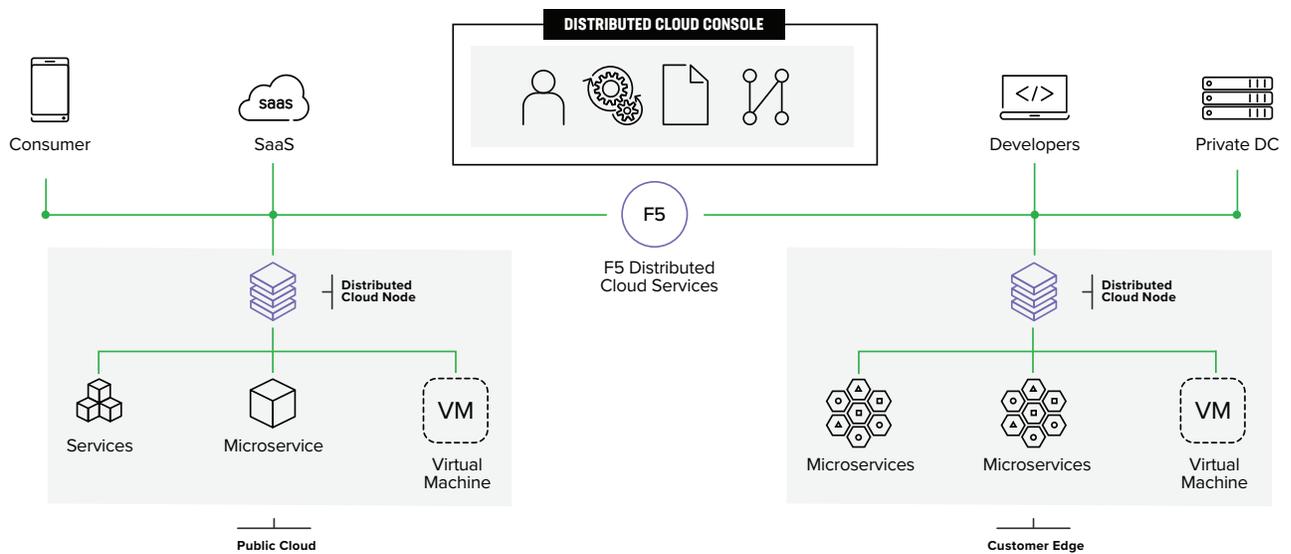


**Figure 1:** Cloud-native stack for managing distributed workloads

## WIDESPREAD USES ACROSS CLOUDS, NETWORKS, AND EDGE SITES

### Multi-cloud

- Multi-cloud application management
- App and network services consolidation
- Cloud and SaaS acceleration
- Secure, multi-cluster Kubernetes gateway and mesh

- AWS Transit Gateway connectivity across multiple clouds
- Private backbone as a service

### Network security cloud

- Secure cloud DMZ
- DDoS mitigation

- Automatic app layer security
- Global distributed load balancing

## VERTICALS

F5 Distributed Cloud Services helps enterprises across numerous industry verticals distribute cloud-native applications spanning multiple public and private clouds and edge sites—without having to rebuild their software infrastructure.

E-commerce

Healthcare

Finance

Manufacturing
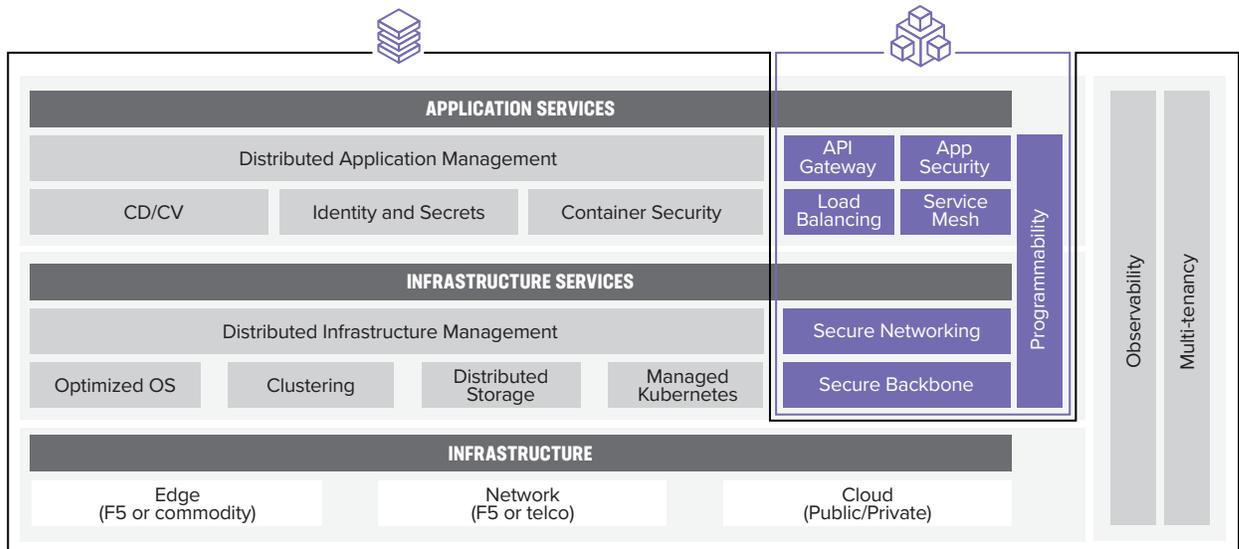
High-tech

Retail

Telecommunications

Automotive

Gaming

Energy

# Distributed Cloud Mesh Features

Improve the performance and security of distributed infrastructure with a high-performance private backbone, optional PrivateLink to premises, densely interconnected network, and security services that offload applications at the edge.



**Figure 2:** A complete range of networking and security services to connect and secure applications

## APPLICATION SERVICES

### Load balancing

Improve the performance and security of distributed infrastructure with a high-performance private backbone, optional PrivateLink to premises, densely interconnected network, and security services that offload applications at the edge.

- Global load balancing (GSLB, Anycast)
- HTTPs (TLS/mTLS) and TCP proxy
- Dynamic reverse proxy and HTTP connect
- Service discovery and health checks
- Traffic management
- Service policy and application micro-segmentation

### Service mesh

SaaS-based multi-mesh platform, including a centrally managed distributed proxy, service discovery, and security for modern and legacy applications.

- Multi-cluster secure and auto tunnels
- Service discovery and health checks
- Traffic management
- Identity authority for AuthN/AuthZ
- Globally distributed load balancing
- Service policy and advanced security

### API gateway

High-performance, extendable, and distributed API gateway for hybrid applications regardless of location.

- Authentication
- API routing and load balancing
- Traffic management and policy

- Transformation and markup
- Programmable, pluggable architecture
- Observability and monitoring

### Application security

Easily enable identity-driven security policies and enforcement using algorithmic techniques and machine learning.

- NG-WAF and anomaly detection
- Application-level DDoS
- API endpoint detection and markup
- API security and rate-limiting

- Managed PKI identity infrastructure for APIs, apps, and networking
- Vulnerability detection and mitigation
- Programmable service and identity policies

### Programmability

Data plane programmability through Javascript v8 and customizable policies to address the evolving needs of applications, business policy, and regulatory compliance.

- Custom data plane extensions
- Data transformations, customized load balancing, HTTP snooping, custom HTTP headers, direct response, terminate/serve requests, etc.

- Programmable policy framework matching on custom tags, labels, and headers
- Programmable DDoS and security protection

## INFRASTRUCTURE SERVICES

### Secure backbone

Global network cloud infrastructure and private backbone with interconnected PoPs and dense peering for high-performance connectivity with integrated security.

- Multi-terabit global backbone
- Advanced traffic engineering for granular SLAs
- Network and application security including DDoS, filtering, and anomaly detection

- Physical or tunneled connection to Distributed Cloud Mesh
- Private connectivity across backbone

### Secure networking

Industry-proven network stack for highly scalable connectivity and security across public clouds, private clouds, and the edge.

- Fully integrated network firewall
- Forward proxy
- Routing and SD-WAN

- VPN (IPsec and SSL)
- AWS Transit Gateway support

### Private link to cloud and SaaS services

Safely connect from and between on-premises environments, and from the edge to the cloud, to exchange data and services for applications without exposing them to the Internet.

- Direct connection to F5 global backbone to bypass the Internet
- Optimized routing to accelerate traffic delivery

- Private end-to-end connectivity from your premises to major public clouds and SaaS

### Observability

Insights across heterogeneous cloud environments, networks, and application layers to provide a full view of application and infrastructure performance, security, and health.

- Global visibility of network and application performance
- Logs and metrics, alerting, and auditability

- Service-level connectivity metrics and tracing
- Custom dashboards
- Integration APIs for third parties

### Multi-tenancy

Run third-party and/or multiple business lines' applications while providing complete isolation of compute, network, and storage resources. Provides the ability to run heterogeneous workloads (containers, VMs) across different namespaces within a tenant.

- Virtual private compute, storage, and networking per namespace
- Multiple VPNs per namespace

- Multi-tenancy across shared application and security services

## About F5 Distributed Cloud Services

F5 Distributed Cloud Services operate as a SaaS-based service to provide application management, infrastructure, and secure connectivity services across distributed customer sites in public cloud, private cloud, or edge sites.

For more information on Distributed Cloud Mesh and App Stack, visit f5.com.
Interested in talking to an F5 Distributed Cloud Services sales specialist?
Contact sales@f5.com today.