Protecting Your Web Apps and APIs Across Distributed Environments

Secure your web applications and APIs deployed across multi-cloud and on-prem infrastructure with a comprehensive, easy-to-use SaaS security solution.

KEY BENEFITS

Get comprehensive, easy-to-use SaaS security
Protect your web apps and APIs in any cloud and on premises with a single SaaS security solution.

Deploy anywhere with a purpose-built solution for distributed applications and multi-cloud environments
The F5 Distributed Cloud Platform is built from the ground up to deliver advanced, accessible security for modern, highly modular, distributed applications.

Empower SecOps to do more, faster with end-to-end observability and policy enforcement
Improve the efficiency of your SecOps teams by providing visibility and unified security policies that are portable across clouds and premises.

Lower TCO through integrated services, SaaS form factor, and flexible deployments
Reduce overall total cost of ownership by collating disparate cloud security solutions onto a single cloud security stack that eliminates the need to maintain separate policies and infrastructure.

Enhance developer experience and speed time to service
Optimize the developer experience by easily plugging into existing CI/CD workflows and DevOps tools—allowing for automated security workload deployments and validation as part of your normal processes.

Extend Application and API Security Across Multi-Cloud and Edge Environments

In today's application-centric world, app security is business continuity.

Securing your apps means protecting your business, customers, and revenue streams. That's why no one hoping to operate or facilitate commerce online can afford to neglect security. Threats to your apps are universal, while application security technology and expertise has traditionally been difficult to acquire, implement, and maintain. This has become even more challenging as development models and application architectures have evolved to include multi-cloud deployments, API proliferation, auto-scaling, and serverless implementations.

Modern microservices are increasingly being built using distributed app architectures to accommodate growing application usage and deliver improved performance. As users' availability and performance expectations change, organizations are choosing to run lightweight applications at branch and satellite locations to speed up data access and processing of critical telemetry on premises or at the edge as opposed to long hauling back to an originating cloud. But it can be challenging for businesses to provide consistent and effective security for these distributed application instances.

NetOps and SecOps have been unable to keep up with the rapid pace of change, and DevOps teams see them—and their security toolkits—as impediments to the innovation the business demands. Plus, the growth in modern microservices-based applications and APIs has only expanded application attack surfaces and traditional solutions are unable to provide consistent coverage. SecOps teams have been forced to leverage and maintain disparate, legacy security solutions and as a result, their efforts net fewer returns than they would otherwise.

The results of all these challenges are higher TCO and a reduction in security efficacy in combatting evolving attacks. Stretched resources and ineffective tooling often mean SecOps responses when attacks occur are conducted manually—placing an even greater burden on their already-constrained resources.

Organizations that neglect security do so at the risk to the business itself. However, there's a way to simplify the complexity and make things difficult for cybercriminals: investment in a security-focused infrastructure that can adapt, scale, and leverage machine learning and global threat intelligence can mean the difference between frustration and efficacy in protecting the web apps and APIs that drive your business.

KEY FEATURES

Full-featured security solutions wherever your apps are
Automate security provisioning for applications and workloads wherever they are deployed—at the network edge, in a public cloud or on-prem—via the centralized control plane, including self-healing and progressive rollout with health monitoring.

Strong protection that scales to meet your needs
Robust and adaptive security services such as an advanced web app firewall, DDoS mitigation, bot detection, and API security can be layered according to the needs of your organization—or the needs of individual apps.

Centralized observability: network + apps + security
Get unified visibility from application to infrastructure across heterogeneous edge and cloud deployments, including granular status of application deployments, infrastructure health, security, availability, and performance.

Purpose-built global network
F5 offers a high-performance global network with PoPs across 23+ metro markets—optimized for app-to-app connectivity, global app delivery and security.

Identity and secrets management
Manage identity lifecycle for each application instance via automatic certificate rotation, delivering uniform identity services for applications across different multi-cloud and/or edge environments.

Secure Centrally, Operate Globally–with Ease

F5 protects and secures your modern apps with unparalleled performance and global scale. Our SaaS-based security services are backed by decades of experience and innovation protecting applications of all sizes and functions for organizations around the world.

These services leverage machine learning and globally sourced threat intelligence to protect against the ever-evolving threats that can potentially target applications. A layered and modular approach to security means you can acquire and implement only the controls you need, saving costs and boosting overall efficacy.

And with the F5 Distributed Cloud Platform, you can now deploy and run modern containerized apps with cloud-native management, consistent security, and end-to-end observability—from the data center to the cloud and the edge. Critical apps become increasingly available to a global audience with a common set of policies and services—deployed efficiently and within minutes.

SOLUTION COMPONENTS

The F5 Distributed Cloud Web Application and API Protection (WAAP) solution operates across the F5 global network, providing SaaS-based application and infrastructure protection that delivers robust and effective app and API security on a broad scale.

- **Web Application Firewall (WAF):** Protects web-based applications from a myriad of threats by acting as an intermediate proxy and inspecting application requests and responses to block and mitigate a broad spectrum of risks stemming from the OWASP Top 10, persistent and coordinated threat campaigns, bots, layer 7 DoS, and more.
- **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.
- **Bot Defense:** Manages and deflects malicious automation and brokers legitimate machine-to-machine communication to defend against business logic risks, such as web fraud, intellectual property theft, credential stuffing and account takeover, industrial espionage, denial of service, and more.
- **DDoS Mitigation:** Provides network-level shielding of volumetric denial-of-service attacks by filtering spoofed and malformed traffic, request floods, and other forms of abuse that attempt to overload your services and take them offline or disrupt them in a way that would result in a loss of customer confidence and access to services.

SECURING YOUR APPS MEANS PROTECTING YOUR BUSINESS, CUSTOMERS, AND REVENUE STREAMS.

- **Client-Side Defense:** Delivers protection against Magecart, formjacking, skimming, and other client-side security vulnerabilities. JavaScript monitors web pages for suspicious scripts and collects telemetry, which generates actionable alerts with one-click mitigation.
- **App Infrastructure Protection:** Helps organizations protect their modern apps and the cloud-native infrastructure they run on. Provides high-efficacy intrusion detection for cloud-native workloads, combining telemetry collection with rules and machine learning to detect risks, vulnerabilities, and anomalies in real time across the entire app infrastructure stack.

You can seamlessly add any (or all) of these protections to any application regardless of where it is deployed—and then implement and evolve protections as needed to combat common threats like injection, cross-site-scripting, software vulnerabilities, and more.

In addition, F5 Distributed Cloud WAAP delivers operational insight and performance data for your globally distributed applications from a central location to boost overall efficacy, streamline support, and improve business intelligence metrics that help you grow and sustain your customers.

F5's centrally managed SaaS platform offers other adjacent benefits as well, such as enabling easier audits, providing policy adherence for applications at scale, and ensuring that policies are appropriate for the risks and threats that applications face.

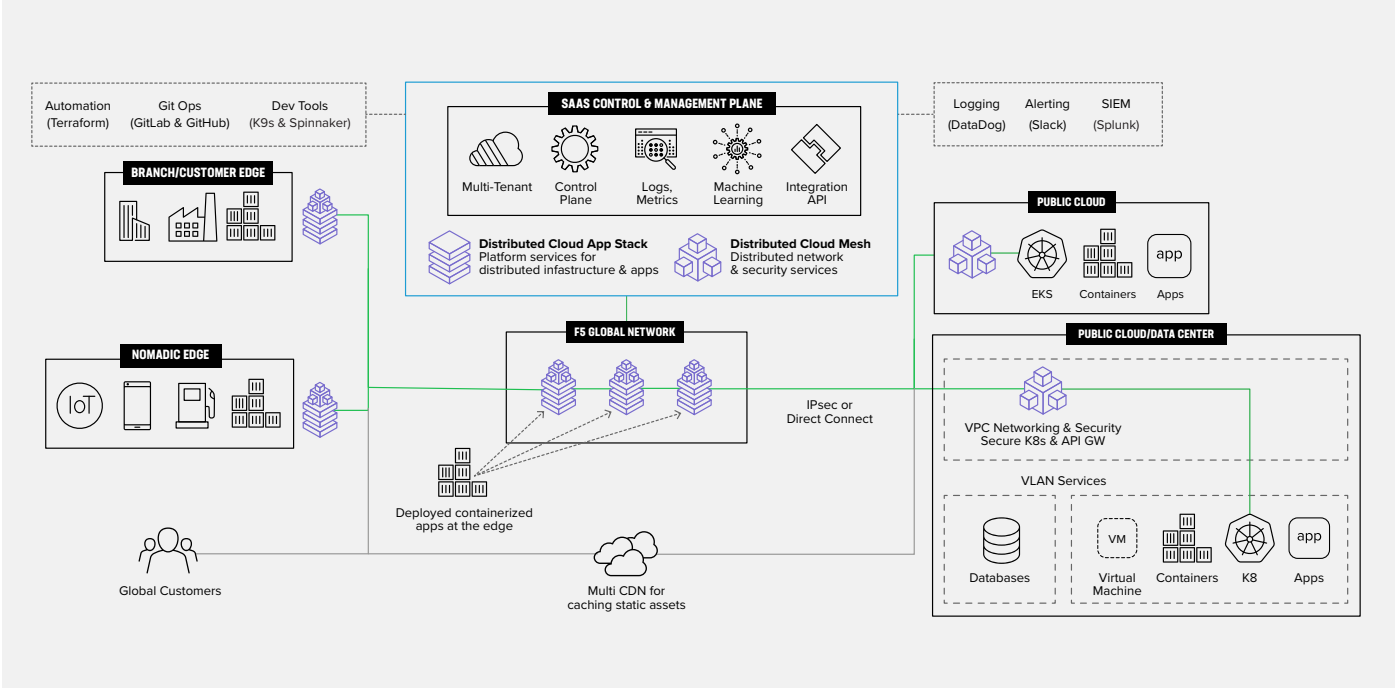

Figure 1: The F5 Distributed Cloud Platform

THE F5 DISTRIBUTED CLOUD WEB APPLICATION AND API PROTECTION SOLUTION OPERATES ACROSS THE F5 GLOBAL NETWORK, PROVIDING SAAS-BASED APPLICATION AND INFRASTRUCTURE PROTECTION THAT DELIVERS ROBUST AND EFFECTIVE APP AND API SECURITY ON A BROAD SCALE.

Deliver Superior Digital Experiences with Performant, Effective, and Scalable Security

Apps are the lifeblood of your business, a fact that cybercriminals understand all too well. Modern threats call for scalable and adaptive security solutions. As applications become increasingly modular and distributed, they require secure services that can be deployed wherever they are deployed while being managed via a centralized SaaS infrastructure.

The F5 Distributed Cloud Platform delivers the security efficacy and ease of use that today's application architectures require. It's a better way to deliver modern application services with unparalleled performance and availability at scale. You can deploy and run containers and microservices applications anywhere customers demand—from data centers or colocation sites to cloud partners and out to the edge—offering consistent operations, security, and end-to-end observability.

Reap the benefits of "write-once, run anywhere" security policies for consistent and repeatable results, global coverage, and enforcement. Our API-driven approach to application protection enables improved collaboration between network, security operations, and developers, while our cloud-agnostic application deployment and management infrastructure provides cross-cloud operations, performance, analytics, and threat visibility wherever your apps are deployed.

This innovative and accessible platform can help you reduce application protection coverage gaps and get consistent coverage across your application portfolio. With F5 Distributed Cloud WAAP, you can simplify your path to effective security while fostering the innovation your business and your customers demand.

Next Steps

To learn more, visit f5.com/waap.