Hybrid Multicloud Application Security
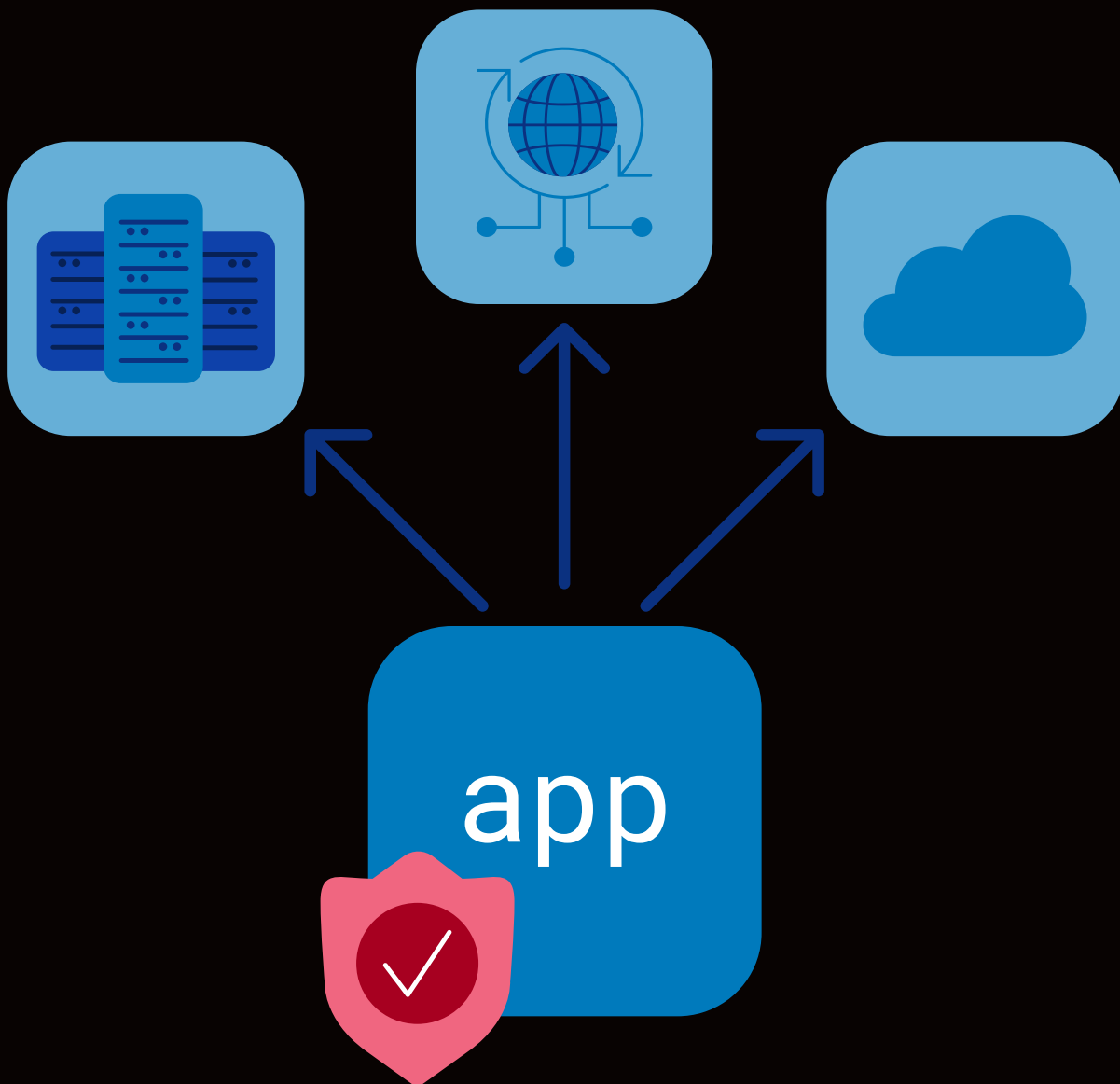
Enforce powerful and consistent security for every application in the cloud, on-premises, or at the edge.

f5

Key Benefits

Assure consistency in security policies for all your apps
Ensure your apps and APIs are safeguarded with uniform security policies no matter where they are deployed—in the data center, public cloud, or remote edge sites.

Upgrade the security close to your apps
Enhance your security and compliance by extending the Distributed Cloud Platform into your clouds and environments, providing localized delivery of app security services.

Increase SecOps productivity
Improve your SecOps team's efficiency by providing end-to-end visibility of threats and identified vulnerabilities for all apps deployed across public clouds and in on-premises data centers.

Lower TCO and operational costs
Reduce total cost of ownership (TCO) by consolidating disparate cloud security solutions onto a single security stack, eliminating the need to replicate multiple policies and infrastructures.

Improve the developer experience and lower time to market
Optimize the developer experience by integrating into existing CI/CD workflows and DevOps tools, enabling automated security workload deployments and validation to be part of your normal processes.

Figure 1: A distributed security architecture to protect applications in hybrid and multicloud environments.

# Protect Modern and Legacy Apps Wherever They Are Deployed

Modern enterprises count on hybrid multicloud networks that often result in complex environments that hinder consistent security enforcement. But protecting all applications against threats is crucial. F5 offers scalable solutions to secure your apps, wherever they are deployed, through a unified control panel.

With application workloads spread across diverse environments and architectures, modern apps are more complex and modular than traditional monolithic ones. This complicates their security management.

Organizations need security solutions that do not impede app evolution, sabotage the user experience, or worsen performance. The challenge lies in balancing robust security with the flexibility and performance required by modern, distributed applications.

Streamline App Security with Distributed Cloud App Connect

F5® Distributed Cloud App Connect serves as a simple proxy that can be bound to apps wherever they are deployed. Inline security can then be administered to these apps by enabling any of the Distributed Cloud Web App and API Protection (WAAP) services in the console.
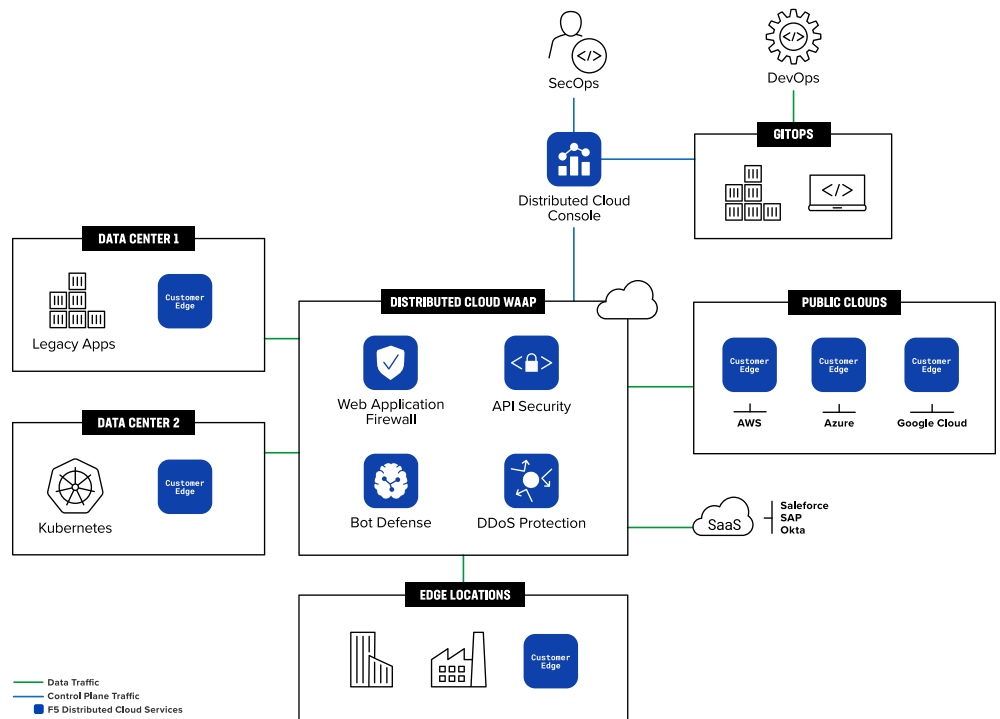
Key Features

Comprehensive application security

Deploy a secure lightweight proxy Defend every app and API with always-on, AI-powered threat detection, API protection, web app firewalls, DDoS mitigation, and effective bot management.

Consistent security everywhere

Apply uniform security policies for modern and legacy apps deployed in distributed environments. Manage your system via a single, centralized control plane.

Flexible delivery options for every app

Protect public, private, and local apps and APIs with security that can be delivered locally in your environment for internal apps, or simply enforced via the SaaS console.

Complete end-to-end observability

Gain visibility and insights into all your apps and APIs, regardless of where they are deployed, in one centralized console.

Pre-built security policies can be applied to specific applications, regardless of whether they are deployed in the cloud or on-premises. This significantly reduces dependencies on public cloud providers or having to replicate policies across disparate tooling.

Applications that are subject to increased data compliance requirements can also be protected by delivering these services locally from lightweight software extensions deployed in a container, on a virtual machine, or via an F5 appliance.

Conclusion

The F5 Distributed Cloud Platform is a specialized offering geared to meet the stringent security requirements for any type of application, whether deployed in the cloud or on-premises in the data center, branch, or remote edge. With extensibility for locally delivered app security, the F5 platform can clear many of the hurdles you would normally encounter with traditional SaaS-based services where strict data residency requirements can render those services unusable.

Discover how F5 products and solutions can help you achieve your desired outcomes. Contact F5.