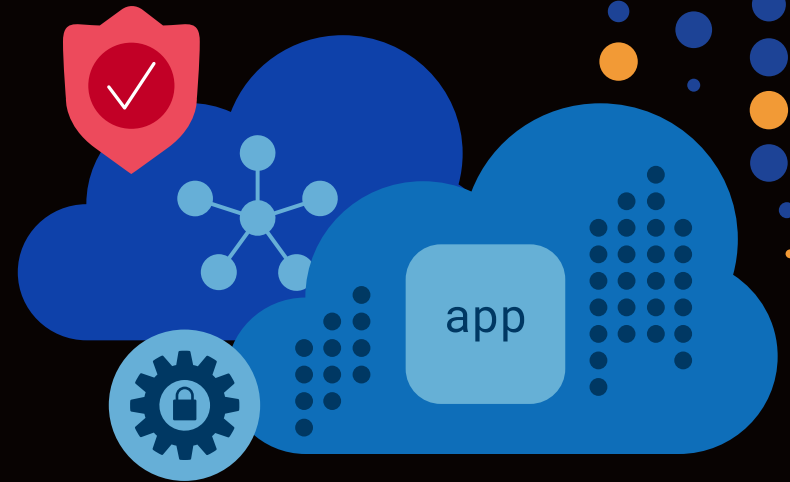


Modernize Your Apps with F5 and Google Cloud

Application innovation and security for the hybrid and multicloud world.



Google Cloud

Contents

3	Hybrid Cloud Challenges: The Need for Secure App Innovation
4	Drive App Modernization Efforts
5	Develop Apps Securely
6	Accelerate Container Adoption for DevOps
7	Manage and Scale APIs
8	Seamlessly Connect Apps and Services
9	Prevent Bot, Fraud, and DDoS Attacks
10	Modernize Your Apps with F5 and Google Cloud

Hybrid Cloud Challenges: The Need for Secure App Innovation

Businesses large and small have embraced hybrid cloud and multicloud strategies to accelerate modernization journeys and satisfy the unique needs of apps, users, and data. These strategies have also empowered organizations to modernize at their own pace. Need to achieve new speed, scale, and innovation? Quickly migrate applications to the cloud to drive availability and performance. Managing strict compliance, infrastructure, and regulatory standards? Maintain select services on-premises to meet stringent organizational requirements.

While this flexibility of choice increases the velocity of development and deployment cycles, it introduces new risks. With hybrid cloud and multicloud environments here to stay, organizations must overcome a new wave of challenges to ensure application security and performance—without compromising modernization efforts.



Advanced Cyberattacks

Sophisticated threats are targeting apps in new ways.



Application Sprawl

IT architectures have become too complex to properly secure and manage.



Inadequate Tools

Existing solutions and processes cannot keep pace with growing security risks.

#1

Cybersecurity risks are the #1 priority for executives.¹

85%

of businesses must manage and secure apps across a variety of hosting environments.²

21%

Only 21% of today's organizations have a mature cyber practice.³

Drive App Modernization Efforts

In the hybrid and multicloud world, successful transformation requires the ability to securely run applications where you want, without sacrifice. This means going beyond just app delivery to connect and protect services distributed across multiple heterogeneous environments.

With Google Cloud and F5, businesses can accelerate and secure their apps across the entire modernization lifecycle. Organizations can now develop and deploy services where they see fit, enforce consistent security policies, and uniformly safeguard apps running across cloud, on-premises, virtualized, and containerized environments.

The Top Focus Areas for App Modernization⁴

1 Achieving a competitive advantage

2 Extending new benefits to users

3 Driving security-centric development

Keep your apps fast, available, secure, and connected—anywhere you need them.

Together, F5 and Google Cloud make app modernization a reality with standardized security for new and legacy apps.

Google Cloud

Google Cloud provides the foundation for developing and managing modern apps. This allows for multi-tier and distributed architectures over cloud- or container-native services.



F5's industry-leading solutions offer a rich portfolio of automation, security, performance, and insights for consistent protection of apps anywhere.

Develop Apps Securely

As cyberattacks escalate, safeguarding apps is paramount to preserving modernization efforts and ensuring the integrity of digital ecosystems. This includes across clouds, in the data center, and at the edge. F5 and Google Cloud empower businesses to create, manage, and protect applications and users from advanced and sophisticated threats, no matter the workload. This negates the need to manage multiple toolsets across environments, creating simplicity for security and ops teams while boosting the performance of apps running on Google Cloud. It also enhances secure software development lifecycles. Now, businesses can build security into applications from the start or extend protections to existing services with ease.

31%

of apps are deployed to production with misconfigurations, vulnerabilities, and other security issues.⁵



Google Cloud

Develop and run apps anywhere using cloud-native technologies.



Web Application Firewall (WAF) from F5

Safeguard digital services—from the core to the cloud to the edge.



Deploy, secure, and operate applications in Google Cloud and other clouds from a single portal.



Centralize management for consistent security policy creation and distribution across apps and APIs.



Protect against prevalent cyberattacks such as OWASP Top 10 threats and zero-day exploits.



Unify access policy management to ensure secure access to apps and data.









Enable identity and location-aware validation for multi-layered and zero trust infrastructure security.

Accelerate Container Adoption for DevOps

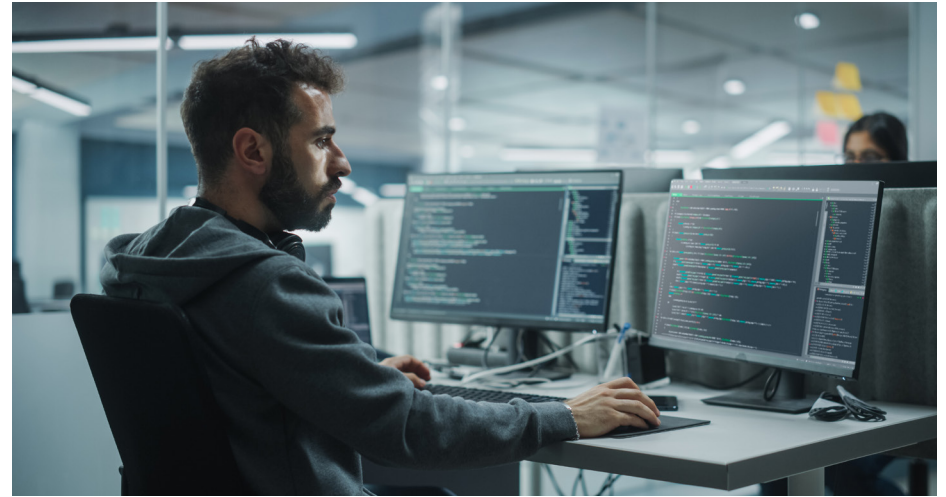
Businesses are turning to containers to modernize their applications due to their portable and agile nature. While containers enable DevOps teams to improve resource utilization and streamline their deployment efforts, they can be highly dynamic and difficult to manage—requiring new strategies to secure containerized apps. In fact, nearly 70% of businesses have delayed or slowed container deployment due to security concerns.⁶

Google Cloud and F5 simplify container adoption for a secure and easier path to application development. Google Kubernetes Engine (GKE) removes the complexities of managing Kubernetes clusters by providing a fully managed service for automated provisioning, scaling, and maintenance of the underlying containerized infrastructure. This means developers can focus on building and deploying modern applications without worrying about the operational overhead of managing the Kubernetes environments themselves. DevOps and SecOps teams can also consolidate configurations with F5's centralized policy management to maintain security and compliance as applications transition to and run on container-based architectures.

Simplify container adoption with Google Kubernetes Engine (GKE)		Enhance security for containerized apps with F5
 Automated Orchestration	 Auto Scaling	Seamlessly connect F5® BIG-IP® to GKE and automatically inherit rules setup by SecOps.
 Resource Allocation	 Service Discovery	Control ingress traffic and load balance across containers.
 Load Balancing	 Configuration Management	Integrate and automate security into the CI/CD pipeline to improve effectiveness earlier in dev cycles.
		Ensure secure application experiences for GKE, virtualized, and serverless apps.

Manage and Scale APIs

APIs play a pivotal role in driving app modernization by facilitating seamless integration and interoperability between systems and services. They enable developers to build modular, scalable, and agile applications by abstracting away underlying complexities and providing standardized interfaces for accessing data and functionality. While this allows development teams to rapidly innovate and adapt to changing business requirements, securing growing API connections can be challenging. With Google Cloud and F5, businesses get proven solutions to implement, manage, and scale APIs effectively across new and legacy applications and environments.



Drive application innovation on Google Cloud.



Google Cloud Endpoints

Simplify API creation, deployment, and management to build innovative, scalable, and secure applications hosted on Google Cloud.



Apigee API Management

Accelerate application design and development with an API-first approach. Govern, analyze, and get visibility into all your APIs across hybrid and multicloud environments.

Secure APIs everywhere with F5.

Web Application and API Protection (WAAP)

Eliminate silos and standardize API protection broadly across cloud and edge environments.



Discover and protect all APIs—in Google Cloud and beyond.



Secure exposed or unmanaged interfaces from threats.



Enforce consistent configurations and security policies.

Seamlessly Connect Apps and Services

An immediate challenge for network teams navigating hybrid environments is how to maintain connectivity to and between environments and clouds. F5 empowers businesses to overcome this hurdle by reliably connecting Google Cloud-centric apps to other services and environments—at scale. F5's secure multicloud networking unifies and securely links workloads, infrastructure, and instances rapidly across clouds, regions, and providers—without sacrificing performance or control. This means businesses can maintain optimal performance, reliability, and observability of digital services in dispersed hybrid cloud and multicloud landscapes.

Multicloud networking with F5



Deliver a globally unified, scalable, and secure infrastructure.



Reliably connect Google Cloud and GKE services to other apps and clouds from a single console.



Minimize the risk of distributed infrastructure and deploy standardized security across environments.

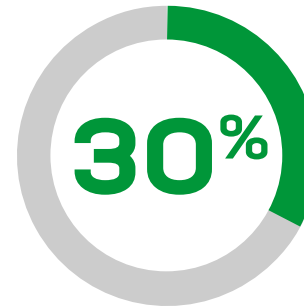


Reduce vendor sprawl and build applications how you see fit.



Prevent Bot, Fraud, and DDoS Attacks

Automated cyberattacks continue to evade security measures and threaten modern apps. By emulating human-like behaviors to blend in, threat actors employ malicious bots to bypass traditional perimeter defenses and commit fraud, degrade customer experiences, and interrupt critical business operations. F5 and Google Cloud provide proven security that mitigates automated threats and adapts faster than criminals retool. Easily deploy F5® Distributed Cloud Bot Defense on Google Cloud to ensure legitimate user access to apps, thwart fraudulent activity, mitigate bots and denial-of-service attacks, and deliver extraordinary digital experiences users expect.



30% of all internet traffic is bad bots.⁷

Distributed Cloud Bot Defense on Google Cloud



Identify malicious bots from legitimate traffic with near-zero false positives.



Safeguard against fraud attempts, including credential stuffing, scraping, and account takeover.



Prevent volumetric L3–4 distributed denial-of-service (DDoS) attacks and targeted attacks on networks.



Protect applications against cross-site scripting (XSS), SQL injection, and layer 7 DDoS attacks.



Stop reverse-engineering with tamper-resistant code obfuscation to stay ahead of attacker retooling.



Employ reCAPTCHA and native Google Cloud capabilities for volume-focused defenses.

Modernize Your Apps with F5 and Google Cloud

F5 and Google Cloud provide the connectivity, security, and performance needed for the hybrid and multicloud era. No matter where your apps run, you get centralized management, consistent policies, and zero trust networking to simplify and accelerate app modernization efforts.

Ensure your apps and APIs are always:



Connected



Available



Secure

Learn more about F5 and Google Cloud at f5.com/gcp.

The F5 and Google Cloud Partnership

- **6+ years** of collaboration
- **Over 50 listings** in the Google Cloud Marketplace
- **Joint expertise** across security, networking, and industries

Sources:

¹ PwC, [2024 Global Digital Trust Insights](#), Sep 2023

² F5, [2024 State of Application Strategy Report](#), 2024

³ Deloitte, [2023 Global Future of Cyber Survey](#), 2023

⁴ Insight, [The Path to Digital Transformation: Where Leaders Stand](#), Feb 2023

⁵ TechTarget, [Security Continues to Lag Behind Cloud App Dev Cycles](#), Nov 2023

⁶ Red Hat, [State of Kubernetes Security Report](#), Apr 2023

⁷ Barracuda, [Threat Spotlight: How Bad Bot Traffic is Changing](#), Oct 2023

ABOUT F5

BRINGING A BETTER DIGITAL WORLD TO LIFE

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere—on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats.

For more information, go to f5.com. (NASDAQ: FFIV).

Learn more about F5 and Google Cloud at f5.com/gcp

