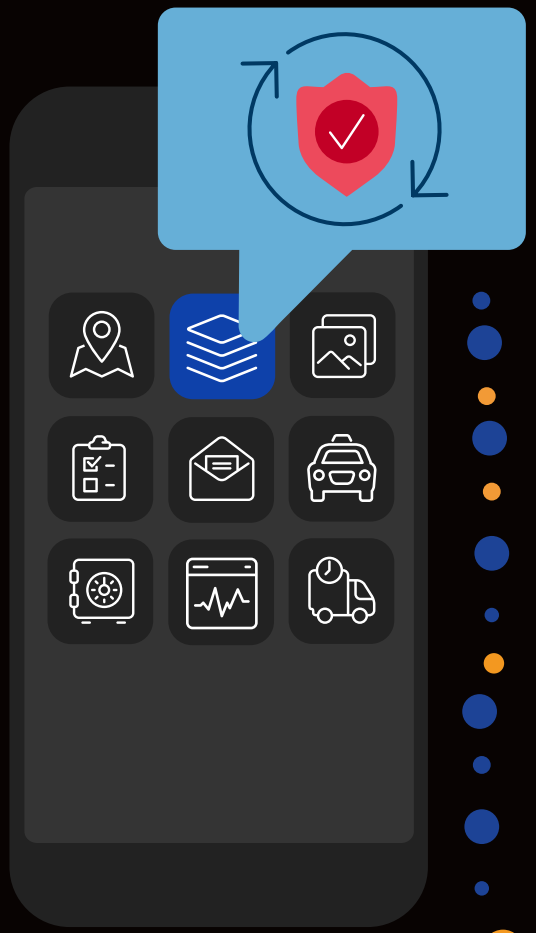
Protect and Manage APIs with F5 and Google Cloud

Learn how to defend every API in your environment—even the ones you don't know about.



f5 | Google Cloud

Contents

An Explosion of APIs and Attacks

APIs are at the core of modern applications, making it easier to integrate services, connect data, or make updates. As organizations continue to modernize their app portfolios, the number of APIs in use is projected to exceed one billion by 2031.[1]

That's a lot of APIs to keep track of—and more importantly, to secure.

Unfortunately, attackers have realized that APIs are often an easier target than applications. Security teams may be more focused on vulnerabilities in applications than in APIs, and often APIs are built by different teams or even different companies than those building the apps.

Back in 2019, Gartner predicted that APIs would become the top attack vector,[2] and subsequent breaches proved their point. Between late 2022 and early 2023, the number of attacks targeting APIs increased by 400%.[3]

API security is still a relatively new discipline. OWASP published its first top 10 for APIs five years ago, which has helped spur adoption of API security solutions. Regulations are also now paying attention to API security, such as requirements included in PCI DSS.[4]

As the number of apps and APIs continues to explode in support of AI and machine learning, API security and governance must keep pace.

90% **of web-based cyberattacks target API endpoints, per F5 analysis.[4]**

API Protection Challenges

Protecting your APIs might not seem like it should be that difficult. Deploy a web application firewall (WAF) and you're good. While WAFs do help, they're not enough for two key reasons.

Shadow APIs

Not all of the hundreds of millions of APIs in the world are managed. In fact, Gartner predicts that by 2025, less than 50 percent of enterprise APIs will be managed, as explosive growth outpaces API management capabilities.[5]

When these unmanaged, shadow APIs are exposed to the Internet, they become a prime target for attackers. It's hard to protect an API you don't know is in your environment.

Zombie APIs are a related problem—both unknown and no longer in use, these APIs are more likely to be vulnerable due to not being updated or maintained.

Bots

You might not consider bots to be a major security threat for APIs, but take a look at some of the OWASP API Security Top 10 threats for 2023:

Unrestricted Resource Consumption

This is a denial-of-service (DoS) attack waiting to happen and is ideal for a bot to exploit.

Broken Authentication

An API can permit credential stuffing or brute force attacks, both of which are frequently performed by bots.

Unrestricted Access to Sensitive Business Flows

Bots can abuse this access to buy and resell inventory, spam systems, or reserve all open time slots, blocking legitimate users.

To overcome these challenges, you need a way to discover and manage APIs in your environment as well as provide comprehensive security that goes beyond WAF.

Building a Protection Framework

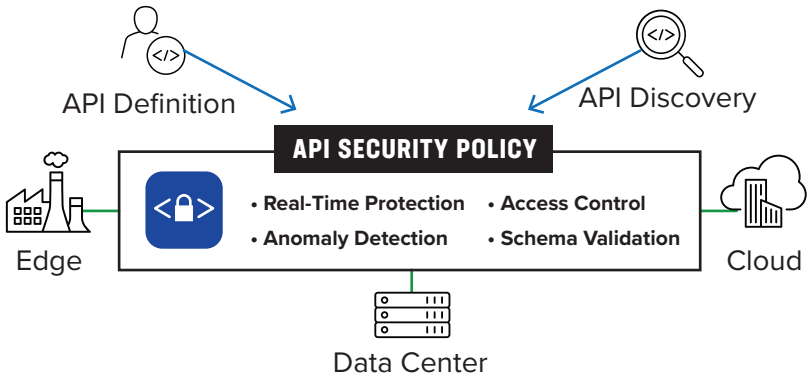
Retailers have adopted APIs in droves to accelerate new innovations and drastically improve the speed and scale of their applications. From in-app search engines and product catalogs to inventory management and fulfillment operations, APIs have become a mainstay in modern eCommerce applications and play a critical role in underlying functions and app-to-app communications. Yet as API use increases, so do risk profiles. A top target for cyber exploits, unmanaged, ungoverned, or exposed APIs provide a direct pathway for bad actors to compromise businesses and their consumers.

Amazon API Gateway secures businesses with fine-grained and certificate-based authorization for AWS-hosted applications, while F5® Distributed Cloud API Security extends protections in AWS and other environments—keeping critical retail operations and services resilient from attack.

Manage and Secure APIs Anywhere

F5 and Google Cloud work together to secure your apps and the APIs that connect them. Apigee API management from Google Cloud lets you create APIs and deploy them in a hybrid or multicloud environment. F5® Distributed Cloud Services provide API discovery and security anywhere your apps run—on Google Cloud, at the edge, on premises, or in other public clouds.

With consistency across your distributed environment, you can implement more effective governance and security for APIs.



Governance

Secure APIs start with effective governance, but many organizations struggle with this due to the potential for delivery slowdowns. Forrester suggests a federated approach to governance is more likely to be successful than centralized governance because it can offer greater flexibility using guardrails for policies, performance, and acceptable risk.[6]

Management

A single system to create, publish, and manage your API connections across environments can help with both governance and security. You can share documentation and coding constructs to reduce development times and better track which APIs are in use.

Discovery

Securing APIs requires knowing what you have in order to protect them. You need a way to catalog APIs as new apps are deployed. While a management system can help, discovering rogue APIs in your environment is still necessary for security and governance.

Security

Now that you have the tools and processes to identify APIs in your environment, you can properly protect them with multi-layered security that spans the range of human-driven and automated attacks.

Discover and Manage APIs

Apigee is a cloud-native API management platform from Google Cloud that can be used to build, manage, and secure APIs in your hybrid or multicloud environment. It offers high performance API proxies to create a consistent, reliable interface for your backend services. Apigee supports REST, gRPC, SOAP, and GraphQL, providing the flexibility to implement any API architectural style.

Add further API discovery and security features to Google Cloud with F5. Integrate F5® Distributed Cloud API Security with your CI/CD pipeline to capture API changes without disrupting the development process. Upload an existing API schema to enforce appropriate API behavior and automatically generate policies based on app-to-app and API-to-API patterns.

Detect and map all APIs across your applications and environments, including forgotten and shadow APIs, for a complete view into your ecosystem. The discovery features built into F5 can identify which endpoints, methods, and payloads are valid, letting you save time on configuring and deploying APIs while improving security and governance.

Visualization tools also help you identify usage patterns of APIs to correlate good and bad actor activity. By minimizing manual tracking and configuration, you can simplify API management.

Not all API security products are created equally. Products that understand API context dynamically discover and visualize API dependencies, score risk factors, provide runtime protection, and work effectively in a distributed cloud environment provide the most value.

- Datos Insights[7]

Multi-Layered API Security

API attacks can take many forms, requiring broad defenses. F5 solutions work with services like Google Cloud Armor to provide advanced security backed by AI and machine learning. Unified policies and single pane-of-glass management eliminate complexity and duplicated effort.

API Security Is a Key Part of Web App and API Protection (WAAP)

According to Gartner, by 2026, 40% of organizations will select a WAAP provider on the basis of its advanced API protection and web application security features, up from less than 15% in 2022.[8]

F5's multi-layered security for APIs includes:

F5 Distributed Cloud API Security

controls connections and monitors for anomalous behavior in addition to automated API endpoint discovery.

Machine leaning monitors all traffic to maintain API baselines, enabling it to predict and block suspicious activity.

F5 Distributed Cloud Bot Defense

uses human experts and machine learning to detect malicious bot traffic while admitting legitimate users and helpful bots.

Distributed Cloud Bot Defense blocks the automated tools attackers use to find weaknesses in your APIs, including those covered in the OWASP API Security Top 10.

F5 Distributed Cloud DDoS Mitigation

protects against L3-L7 attacks in every environment, including Google Cloud, to reduce operational costs and slowdowns.

F5's 99.99% uptime SLA protects not just your apps but also your APIs against DDoS attacks that can disrupt your business operations.

F5 Distributed Cloud WAF

protects apps and APIs across Google Cloud, private data centers, on-premises, and edge clouds with unified management and consistent policies.

The advanced behavior engine deciphers intent using AI and machine learning to improve accuracy alongside robust signature-based protection.

These solutions are part of F5® Distributed Cloud Web App and API Protection (WAAP), which lets you bring multi-layered security to Google Cloud and anywhere else your apps and APIs run. Manage security policies and track threats from the unified F5® Distributed Cloud Console to keep your apps and APIs fast, secure, and available without complexity.

Protect APIs with F5 and Google Cloud

F5 and Google Cloud provide the tools you need for secure and high-performing apps and APIs. No matter where your apps run, you get a simplified path to digital transformation that includes centralized management, consistent policies, and zero trust networking. Multi-layered API security paired with discovery and management from F5 and Google Cloud accelerate your multicloud journey so you can reach your goals faster.

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] F5, Continuous API Sprawl, Nov 2021

[2] Gartner, API Security: What You Need to Do to Protect Your APIs, Aug 2019

[3] Infosecurity Magazine, Attacks Targeting APIs Increased By 400% in Last Six Months, Mar 2023

[4] F5, F5 Is Shifting Left to Protect APIs, Feb 2024

[5] Gartner, Predicts 2022: APIs Demand Improved Security and Management, Dec 2021

[6] Forrester, The Eight Components Of API Security, Sep 2023

[7] Datos Insights, API Security Solution Evaluation Guide, Dec 2023

[8] Gartner, Market Guide for Cloud Web Application and API Protection, Nov 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