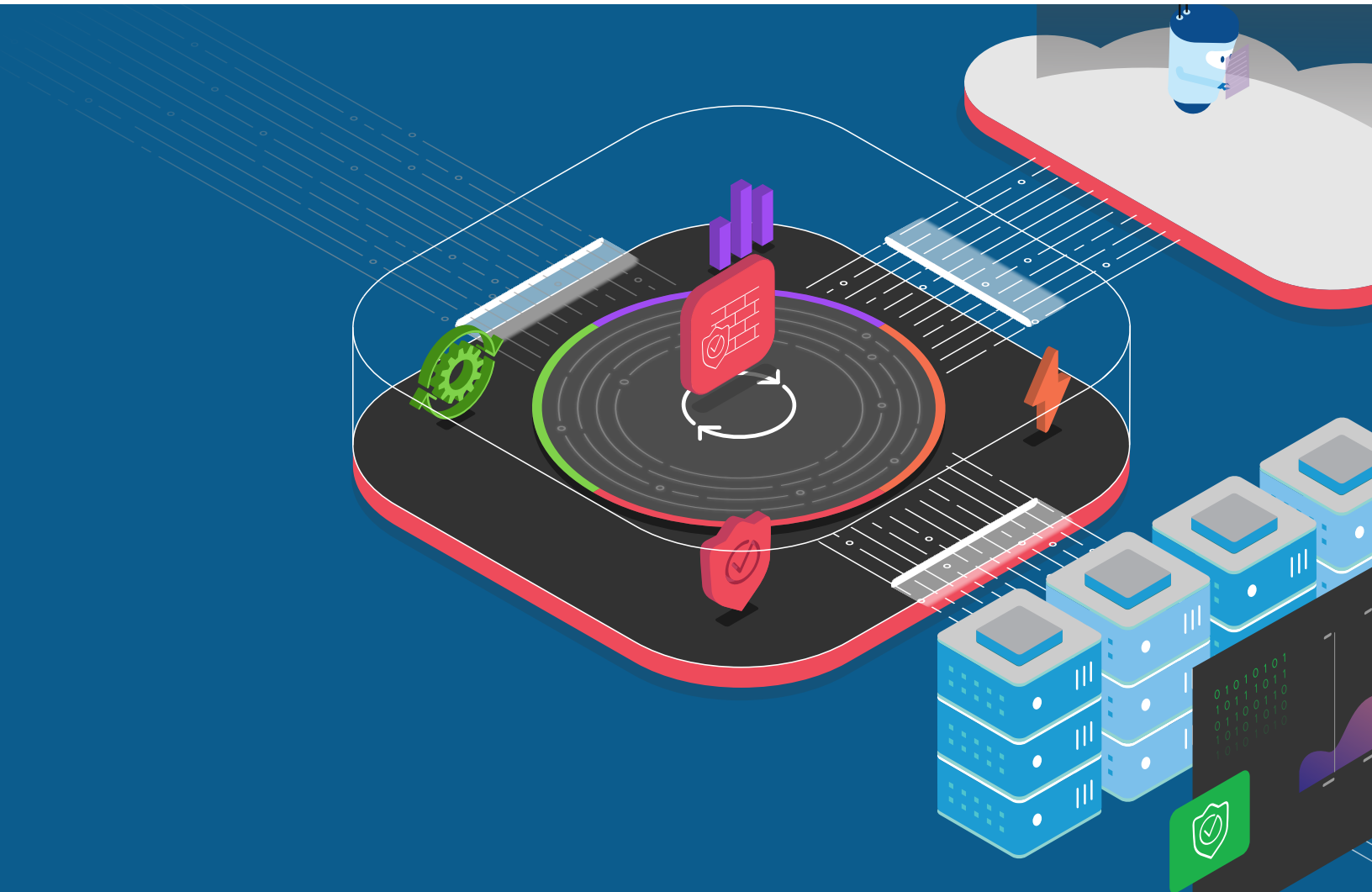
SOLUTION OVERVIEW

Manage and Secure Your APIs

Multi-cloud API management, security, and flexible authentication.



KEY BENEFITS

API-Centric Security
Provides protection against common and advanced API-specific vulnerabilities that API gateways can't deliver

Modern API Architectures
Seamless integration into virtually any deployment design or architecture: edge proxy, Kubernetes, Ingress gateways, serverless, and more

Integrated API Delivery Solutions
Improved operational efficiency with integrated security and gateway

DevOps/AppDev Friendly
Provides security as agile as your DevOps teams, speeding up time to market at a reduced cost

APIs are a fundamental building block of modern application development. By enabling disparate systems to work collectively, APIs can speed up time to market for application development and deliver improved user experiences. The flipside is that the use of APIs has decentralized the structure of applications. This makes securing them even tougher, which in turn makes them extremely attractive to attackers. Without proper management and security controls, APIs can pose a serious risk to organizations.

F5 has a comprehensive solution to securely manage APIs across any data center or cloud using a simple, fast, and scalable architecture. This helps drive business velocity by enabling automation of API deployments and management, while also protecting against API-specific threats. F5 is the only company that can deliver API management, high-performance API gateways, and advanced security controls all in one solution, which reduces tool sprawl and architectural complexity.

Understanding the Challenges and Potential Risks of APIs

Application development moves swiftly, and innovation is continually changing the face of our interactions. With such speed, security is often left behind. Sometimes security is not included into the design of the APIs themselves, or it is forgotten, misconfigured, or lacking security controls against common attacks. Since APIs are designed for machine-to-machine data exchange, many APIs represent a direct route to sensitive data. This means that most API endpoints need at least the same degree of risk control as web applications, but potentially they require even more because there is no human/browser involved in the exchange.

MOST API GATEWAYS LACK ADEQUATE SECURITY CONTROLS

API gateways are typically designed for managing both the publishing of APIs to the Internet and performance, but security is usually not a core competency. This explains why API security failures have been the cause for some of the highest-profile API data breaches.[1] Unfortunately, it is still common for development teams to assume that no malicious human is ever going to communicate with or attack API endpoints. The result is that they don't properly implement authentication and authorization, which are the most common threats according to OWASP's API Security Top 10.[2]

APIS ARE POTENTIALLY SUSCEPTIBLE TO MANY OF THE SAME KINDS OF ATTACKS AS WEB APPLICATIONS.

KEY FEATURES

API Definition and Publication—Define APIs Using an Intuitive Interface

- Define base path and backend services
- Route APIs to appropriate backend services
- Manage versioning of APIs
- Import APIs that follow OpenAPI standards
- Publish APIs to one or more environments, such as production or staging
- Configure API gateways
- Configure security policies
- Deploy and run on containers

Rate Limiting—Mitigate DDoS Attacks and Protect Your Applications by Setting Rate Limits

- Specify the maximum request rate for each client, consumer, or resource
- Protect API endpoints and ensure SLAs for API consumers
- Define multiple rate-limiting policies

Authentication and Authorization

- Validate JSON Web Tokens (JWTs)
- Create and manage API keys for consumers
- Import API keys from external systems
- Share with API consumers
- Apply policies to groups of API clients

APIs are also potentially susceptible to many of the same kinds of attacks that affect web applications. None of the following attacks are new, but all of them can easily be used against APIs.

- Injection and Cross-site scripting (XSS) are common web app attacks that apply to APIs, but others such as requests for invalid data types can also lead to unauthorized access to data.
- Distributed denial-of-service (DDoS) API endpoints are among the growing list of DDoS targets that can make an application unavailable to intended users, or machines in the case of APIs.
- Credential stuffing and other automated attacks can potentially lead to fraudulent activity.

INCONSISTENT CONTROLS IN MODERN API ENVIRONMENTS

Applications have moved toward an increasingly distributed and decentralized model, with APIs as the connection point. The most recent F5 Labs research shows that the number of API security incidents is growing every year, and that the most frequent causes of API incidents in the last two years are related to a low level of security maturity, which is often caused by tool sprawl.

Different development teams working on different applications often have disparate tool sets. That can result in the traditional security team no longer owning a single point of control to enforce security. This necessitates a standard set of tools to embed the right controls into the API development and management processes.

Solution

Enterprises need to maintain and evolve their traditional APIs, while simultaneously developing new ones using modern architectures. These can be delivered with on-premises servers, from the cloud, or in hybrid environments. APIs are difficult to categorize as they are used in delivering a variety of user experiences, each one potentially requiring a different set of security and compliance controls. The flexibility of the combined F5 and NGINX solution can address multiple different use cases or architectural patterns.

KEY FEATURES (CONT.)

Real-Time Monitoring and Alerting—Get Critical Insights Into API Performance

- Graphs of key metrics such as latency and response duration
- Gateway-specific metrics such as requests per second, active connections, and bandwidth usage
- Alerts on more than 100 metrics such as CPU usage, 4xx/5xx errors, and health check failures, based on predefined thresholds
- Easy integration with any monitoring tool of your choice using REST API

Dashboards—Monitor and Troubleshoot API Gateways Quickly

- An overview dashboard that aggregates metrics across API gateways
- An application health score that measures successful requests and timely responses
- Customizable dashboards to monitor metrics specific to your environment

THE MOST RECENT F5 LABS RESEARCH SHOWS THAT THE NUMBER OF API SECURITY INCIDENTS IS GROWING EVERY YEAR.

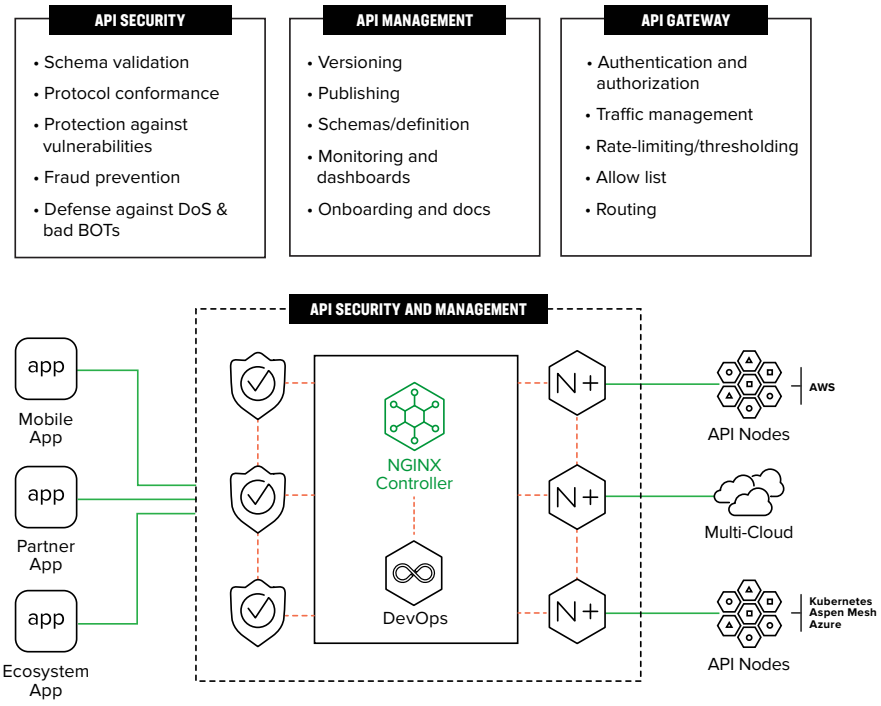


Figure 1: F5 is the only vendor that can deliver API management, high-performance API gateways, and advanced security controls all in one solution

Common API Delivery Patterns

In all of the patterns outlined below, NGINX Controller is used for API management functions such as publishing the APIs, setting up authentication and authorization, and using the gateway functionality to form the data path. Security controls are addressed based on the security requirements of the data and API delivery platform.

1. APIs for highly regulated business

Business APIs that involve the exchange of sensitive or regulated information may require additional security controls to be in compliance with local regulations or industry mandates. Some examples are apps that deliver protected health information or sensitive financial information. Deep payload inspection at scale, and custom web application firewall (WAF) rules become important mechanisms for protecting this type of API. Using the advanced features of F5's WAF is recommended for providing security in this scenario.

THE FLEXIBILITY OF THE COMBINED F5 AND NGINX SOLUTION CAN ACCOMMODATE MULTIPLE USER EXPERIENCES, EACH ONE POTENTIALLY REQUIRING A DIFFERENT SET OF SECURITY AND COMPLIANCE CONTROLS.

2. Multi-cloud distributed API

Mobile app users who are dispersed around the world need to get a response from the API backend with low latency. This requires that the API endpoints be delivered from multiple geographies to optimize response time. F5's cloud-based global DNS load balancing service is used to connect API clients to the endpoints closest to them. In this case, using F5's WAF in the cloud offers baseline security, and the software-based WAF deployed closer to the API workload can be used for granular security controls. Learn more about best practices.

3. API workload in Kubernetes

F5 service mesh technology helps API delivery teams deal with the challenges of visibility and security when API endpoints are deployed in a Kubernetes environment. F5's NGINX Controller can control WAF functionality, offering seamless north-south connectivity for API calls. F5 service mesh is used to provide east-west visibility and mTLS-based security for workloads. The Kubernetes cluster can be on premises or deployed in any of the major cloud provider infrastructures including Google's GKE, Amazon's EKS/Fargate, and Microsoft's AKS. Learn more about implementing this pattern.

4. APIs as Lambda functions

Both F5's SaaS-based or software-based WAF deployed in AWS Fargate can be used to inject protection in front of Lambda-based API endpoints.

Conclusion

F5's solutions can effectively deliver, manage, and secure APIs as well as the infrastructure used to host them, regardless of your architecture. They provide strong protection against bots and common and advanced API exploits, as well as DevOps integration for publishing and providing visibility into API performance. Ultimately, these solutions support the goal of application portability. This ensures the agility necessary to support the business by not locking you into constraints of any single environment whether it's cloud-hosted or on-premises infrastructure. These solutions can also scale into the future as they can support portability from one architecture to another.

To learn more, contact your F5 representative, or visit F5.

[1] Highest-profile API data breaches, found at https://owasp.org/www-project-api-security/

[2] OWASP's API Security Top 10, found at https://nordicapis.com/5-major-modern-api-data-breaches-and-what-we-can-learn-from-them/