F5 Open Banking Solutions

Enterprises need to maintain and evolve their traditional APIs, while simultaneously developing new ones using modern architectures. F5 has a broad range of products and services that can help.

KEY BENEFITS

API-Centric Security
API Gateway security alone is largely inadequate for exposed APIs. We offer API security efficacy that API gateways simply can't deliver.

Modern API Architectures
Modern API delivery designs are innovative and fluid. We offer adaptive API gateway and security solutions that support virtually any deployment model.

Integrated API Delivery Solutions
We're a leading vendor for API management, high-performance API gateways, and advanced high-efficacy security controls.

DevOps / AppDev Friendly
Drive business velocity by enabling automation of API deployments, management, and approved security controls.

In a world where virtual experiences are becoming increasingly more important, open banking brings opportunities to serve customers in more innovative and intuitive ways. These innovative interactions with banking and financial services institutions are quickly becoming a digital experience expectation, with examples including personal finance management or mobile point-of-sale apps.

Regulatory intervention around open banking standards, which vary by international region, complicate the initiative. A common thread requires banks to create mechanisms—most commonly APIs—to provide data quickly, securely, and reliably to third-party providers with the consent of their customers.

Additionally, open banking faces performance and security challenges by typically generating massive volumes of API calls—a concern highlighted in a recent survey.[1] When asked the "four most important factors to consider before integration with an API," security (71.0%) and performance (70.9%) rated near the top.

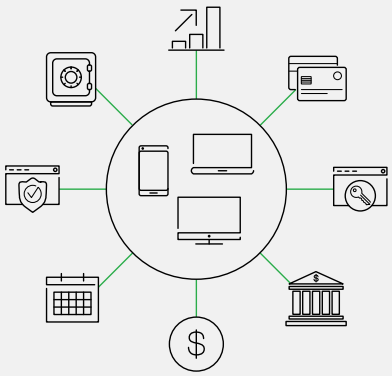

Figure 1: Regardless of how many APIs connect to your open banking platform, F5 has your API performance and security covered.

Secure and High-Performing APIs Are Critical in Open Banking

THE MOST FREQUENT PROBLEM IS A COMPLETE LACK OF AUTHENTICATION IN FRONT OF API ENDPOINTS, FOLLOWED BY BROKEN AUTHENTICATION AND BROKEN AUTHORIZATION.

APIs are a strategic necessity to give your business the agility and speed needed to succeed in today's open banking initiatives. We can help with comprehensive solutions to securely manage APIs across any data center or cloud platform using simple, fast, and scalable architecture. This accelerates business velocity by enabling automation of API deployments and management, while also protecting against API-specific threats. F5 leads the way in delivering API management, high-performance API gateways, and advanced security controls all in one solution, which reduces tool sprawl and architectural complexity. That's why the top 15 US commercial banks employ F5 solutions.

With our solutions, you can achieve previously impossible speeds through real-time APIs. Take the case of Capital One's developer portal. F5 technology has enabled the company to scale applications to 12 billion operations per day, with peaks of 2 million operations per second at latencies of just 10-30 milliseconds.

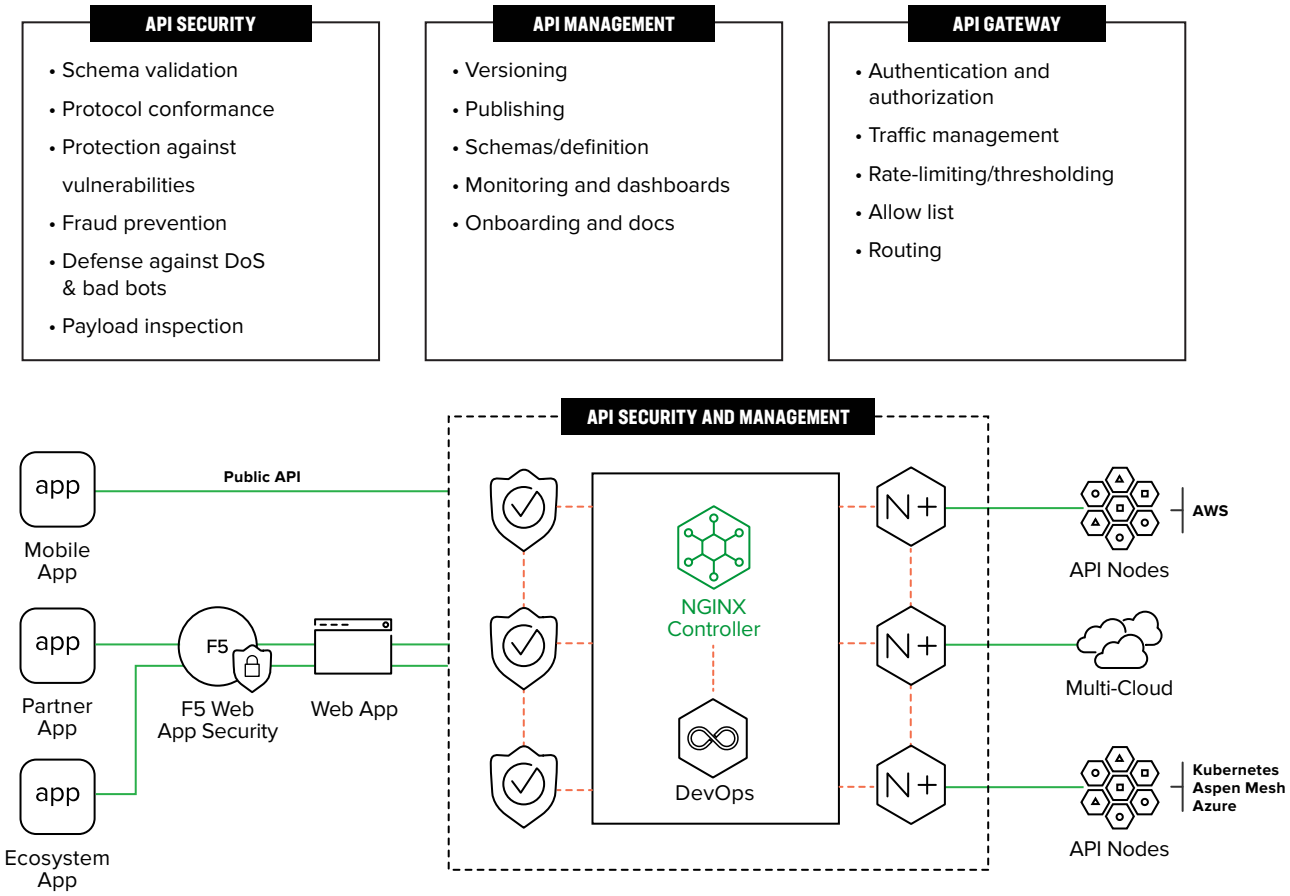

Figure 2: F5-powered API security and management

Open banking not only refers to customer-facing innovations, but also business process innovations.

For example, a large financial firm offers six pre-built APIs for popular treasury management solutions (TMS) and enterprise resource planning (ERP) software. The APIs allow clients to initiate U.S. real-time payments, retrieve balances, manage bank accounts, and track payments directly with their system.

How Do You Properly Secure APIs?

Research conducted by F5 Labs shows that APIs are highly susceptible to cyber attacks. The most frequent problem is a complete lack of authentication in front of API endpoints, followed by broken authentication and broken authorization.

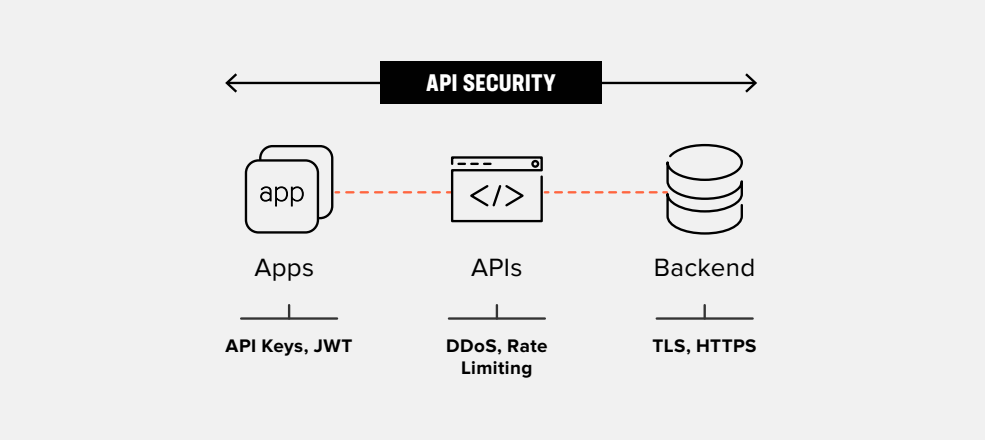

Figure 3: Traditional security teams no longer own a single point of control to enforce security across API development and management processes, exposing potential security vulnerabilities.

Inconsistent Controls in Modern API Environments Impact Open Banking Security

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 most API incidents during the last two years were related to a low level of security maturity, which is often caused by tool sprawl.

Different development teams working on multiple applications often have disparate tool sets. That means traditional security teams may not own a centralized point of control to enforce security. This requires a standard set of tools to embed the right controls into the API development and management processes, like the ones highlighted in the following chart.

Set of Tools Required	What it Does	What F5 Offers
Web Application Firewall (WAF)	A WAF recognizes illegitimate requests, designed not to exercise the API's intended functionality but to exploit vulnerabilities—allowing attackers to steal information or execute malicious code.	Provides solutions that are optimized for CI/CD and DevOps workflows, and support XML, JSON, text, and HTML request and response payloads. Its advanced API protection profiles protect against attacks with parsing and structure enforcement, attack signatures, method enforcement, and path enforcement.
Bot Protection	HTTP APIs can be subject to bot and other forms of malicious or unwanted automation-based traffic.	Includes solutions that provide visibility, throttling, and mitigation options to protect HTTP-based APIs from bots and other forms of automated attacks that generate online fraud and application abuse.
API Management	Among other functions, API management solutions provide interfaces for defining security policies which the API gateway then applies as it processes API calls.	The API Management Module includes important protections like implicit Uniform Resource Identifiers (URIs) that allow listing based on the API specification, as well as programmable rate limiting, multiple rate-limiting policies, and throttling.
API Gateway	An API gateway like NGINX Plus provides authentication and authorization, traffic management, rate limiting/thresholding, allow list, and routing.	Provides solutions to complement or replace existing API gateways.
SSL/TLS Encryption	All public API traffic should be encrypted. If possible, use ephemeral keys for added security. If your API gateway cannot handle the cryptographic workload due to performance or price, consider offloading the workload to a dedicated system.	Maximizes infrastructure investments, efficiencies, and security with dynamic, policy-based decryption, encryption, and traffic steering through multiple inspection

To complement and extend the security of the above solutions, organizations can leverage the power of industry and security experts. F5 Silverline Managed Security Services protects your infrastructure against volumetric, DNS, and higher-level denial of service attacks.

A Performance-Driven Approach to Open Banking

Other than security, nothing is more important to open banking applications than user experience. If increased API volumes related to growing open banking ecosystems lead to a poor, high-latency transaction between a critical point of interaction, like submitting loan requests, then your open banking initiatives will likely be unsuccessful. Milliseconds matter to your business and F5 has a broad range of products and services that can help.

Driving the performance point further, a leading US-based financial services corporation recently deployed the API Management Module for NGINX Controller. The incumbent API management solution added 500 milliseconds (ms) of latency to every one of their API calls. To avoid adverse impact to revenue as it transitions to open banking, the customer needed a solution that processed API calls with latencies under 70ms. The customer deployed the NGINX Controller API Management Module and now their API processing time is consistently below 10ms—exceeding their performance requirements by 85%.

Improved API Performance With F5

API management is the key to open banking performance and our approach to API management is different from traditional solutions. Unlike those solutions, the NGINX Plus API gateway (data plane) does not require constant connectivity to NGINX Controller (control plane), so API runtime traffic is isolated from management traffic. NGINX Controller eliminates the need for local databases or additional components that may introduce needless complexity, latency, and points of failure for NGINX Plus API gateways.

This approach maximizes performance by reducing the average response time to serve an API call and minimizes the footprint and complexity of the gateway. Decoupling the data plane from the control plane gives you the flexibility to deploy as many or as few API gateway instances as your application architecture requires. NGINX Controller gives you the freedom to choose the right deployment for both internal and external API needs with a lightweight, simple, and high-performance solution that fully leverages the power of the NGINX Plus data plane.

Conclusion

Banking and financial services organizations that do not invest properly in open banking will be out-maneuvered by competition and lose significant market share, as well as being much more vulnerable to increasingly complex cyber attacks. Securing APIs and ensuring high API performance and availability, while navigating compliance requirements, are critical components to open banking success.

F5's open banking solutions can effectively deliver, manage, and secure APIs and the infrastructure used to host them, regardless of architecture preferences. DevOps publishing integration and API performance visibility also protect against bots, and both common and advanced API exploits. Ultimately, these solutions promote application portability and ensure the agility necessary to support the business. You're never locked into the constraints of any single environment, whether it's cloud-hosted or on-premises infrastructure. Open banking solutions scale into the future and support secure and scalable API service for all your financial requirements.

To learn more, explore F5 open banking solutions or contact your F5 representative.

[1] 2020 State of the API Report, Postman, found at https://www.postman.com/state-of-api/#key-findings