Article

F5 Is Shifting Left to Protect APIs

INSERT PARTNER LOGO

Size to be visually equal to F5 logo.
Align to left edge & center vertically.

APIs are the hidden central nervous system of our modern digital lives.

Application programming interfaces (APIs) are the hidden central nervous system of our modern digital lives. All day every day, APIs power the apps we use to purchase our first coffee from a favorite shop, badge into the door at the office, grab a rideshare to get lunch with a colleague, check the weather, and finally sit down at the end of a long day to stream a beloved TV show. Nearly every organization that we interact with each day relies on APIs to drive their digital business, whether they think of it that way or not.

The rise of API-first software development and delivery has changed the world for the better, in countless ways. But there's a problem—when your applications and architectures change, so does your attack surface. Traditional security measures like WAF, DDoS, and bot protection remain essential, but they fall short in fully safeguarding these APIs. They were built for the attack surfaces of the day, unable to predict the future attack surface and changes brought about by the rapid adoption of APIs in the last few years.

As a global leader in application and API security, F5 technology sits in the data path of nearly half of the world's applications, providing a unique line of sight into the attacks on modern web and mobile applications. Our analysis shows that today over 90% of web-based cyberattacks target API endpoints, attempting to exploit newer, less understood vulnerabilities, often exposed by APIs not actively monitored by security teams.

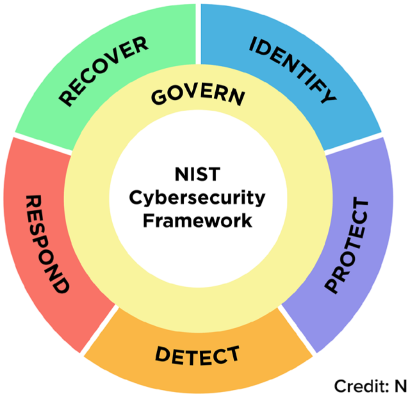
As attacks and attack surfaces change, your defense must adapt as well. The industry's current focus on generative AI is also spurring rapid growth in the volume of apps and APIs to support artificial intelligence and machine learning (AI/ML) models, adding further complexity. Modern businesses need a dynamic defense strategy, focusing on discovering and mitigating risks **before** they escalate into expensive, embarrassing, and often preventable breaches.

The pace of these rapid changes has made securing critical APIs a significant challenge for organizations of all types. Already-stretched teams of developers and defenders often do not even know how many APIs their companies use, where they are, and the compliance and other risks associated with the critical data and business processes these interfaces support.

Credit: N. Hanacek/NIST

Simply put, you can't protect what you can't see, and it's impossible to effectively manage the risk of an attack surface you do not understand.

While technology is always changing, the API security phenomenon underscores the bedrock principles of cybersecurity. There's a reason major control frameworks like NIST almost always start with "Identify" first. Simply put, you can't protect what you can't see, and it's impossible to effectively manage the risk of an attack surface you do not understand.



Credit: N. Hanacek, NIST

API blind spots have become a fundamental problem, and far too many organizations are flying blind today when it comes to their APIs. Gartner and other industry analysts have been predicting since at least 2019 that APIs would become the #1 attack vector, and our data supports that assertion, with no sign of slowing.

The cybersecurity industry has responded, so far mostly with point solutions geared toward one aspect of API development or another. Such products offer diverse but limited capabilities, like API discovery to find APIs known to be in use, or scanning and testing tools to help find vulnerabilities and attempt to close these gaps.

But the future of API security is not a set of point solutions you must cobble together and try to integrate yourself. Enter F5 Distributed Cloud Services.

To build the future of your company, you must equip your company for the future.

The industry leaders in distributed computing and application security at F5 saw this essential emphasis on APIs coming, and 5 years ago started building a game-changing suite of capabilities brought to market as F5 Distributed Cloud Services.

Today's AI-powered apps rely on a distributed arrangement of data sources, models, and services across on-premises, cloud, and edge deployments, joined together by a rapidly increasing number of APIs. To help customers navigate these intertwined challenges and opportunities, we are happy to announce that F5 is bringing advanced API code testing and telemetry analysis to F5 Distributed Cloud Services, creating the industry's most comprehensive and AI-ready API security solution. The addition of capabilities recently acquired from API security innovator Wib enables vulnerability detection and observability in application development processes, identifying risks and implementing policies before APIs enter production.

Much like the future of API security, the F5 Distributed Cloud Platform is built for the future of all enterprise computing, sharing these essential attributes:

- Multicloud
- API-first
- Powered by AI

Making the best even better

F5 has already offered robust API discovery and protection in the F5 Distributed Cloud suite of web app and API protection (WAAP) services. The platform automatically creates and validates robust schemas for APIs, illuminates API risks with actionable insights, leverages AI/ML to mitigate complex API attacks, and more. With Distributed Cloud WAAP, along with NGINX App Protect and BIG-IP Advanced WAF, F5 gives customers the unique ability to secure any app and any API, anywhere.

And now F5 is shifting left, to address the full API lifecycle.

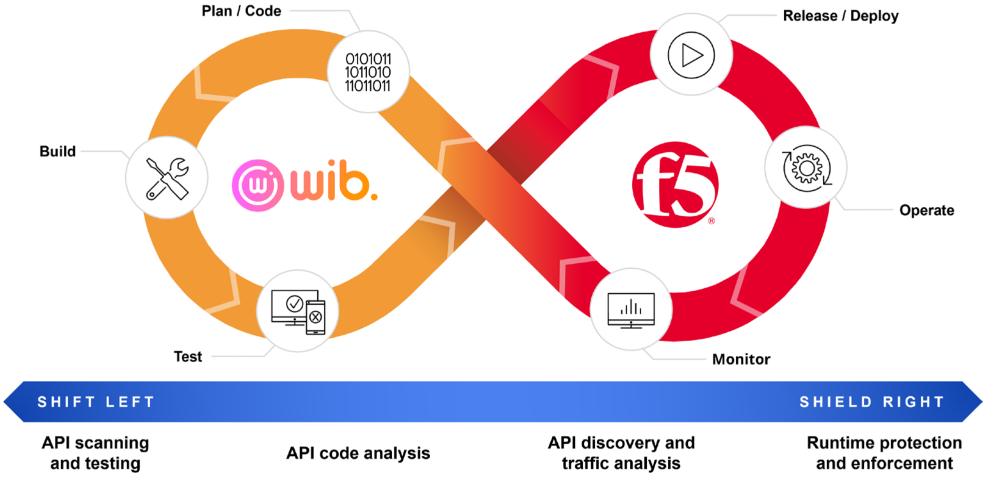


Figure 2: The combination of the Wib platform with F5 Distributed Cloud API Security provides the industry's most comprehensive API security solution.

With Distributed Cloud WAAP, along with NGINX App Protect and BIG-IP Advanced WAF, F5 gives customers the unique ability to secure any app and any API, anywhere.

To achieve this, we are augmenting the current API discovery and protection capabilities with:

- **API code analysis** to discover API endpoints and assess their risks before they are deployed in production.
- **API testing** to probe for vulnerabilities and to validate suspected threats detected in code and traffic analysis.
- **API compliance analysis** to ensure proper API security posture aligned with the customer's regulatory requirements.
- **API threat surface assessment** to monitor an organization's public assets for the emergence of new APIs and for those which are outside of security governance.
- **API security fusion engine** to create a seamlessly integrated solution where every threat, vulnerability, or insight is validated across all information sources.

Join us in securing your apps and APIs with the world's first holistic app and API security solution, with true visibility and security from code to cloud. Run anywhere, secure everywhere—only with F5.

For more information, visit [www.partnername.com] or contact [emailname@partnername.com] to schedule a demo.