Solution Overview

Protect a New Generation of Apps and Critical Services with F5 Distributed Cloud API Security

Combine the power of data analytics and deep insights from machine learning to discover, monitor and mitigate threats to APIs that connect and power your AI-based workloads.

Key Benefits

Improve API Security
Pairs automatic global API discovery and OpenAPI spec import for positive security with in-line enforcement capabilities including WAF, layer 7 DoS, rate limiting, IP reputation, allow/deny listing, and more, for API endpoints.

Reduce Time Documenting APIs
Learn and generate OpenAPI spec (OAS) files to minimize manual tracking of all API endpoints.

Improve API Visibility
Easily identify all API endpoints mapped to applications and monitor for malicious activity and shadow APIs, observing global API metrics from a single, centralized user interface.

Strengthen API Access and Authentication
Augment API gateway functionality, delivering enhanced visibility, oversight and control over API authentication and access, while helping to identify gaps in API authentication, control access, and stop unauthorized attempts to exploit APIs.

Without proper management, continuous monitoring and security controls, APIs can pose a serious risk to organizations.

APIs power applications, and this includes emerging AI apps. As in other modern app architectures, APIs are a fundamental building block of AI app development.

They add to the complexity of new AI workloads in the form of plug-ins and third-party integrations that connect and power the increasingly distributed data sources and learning models that make up these emerging apps. As modern apps and AI have evolved, dependencies on APIs have increased—by enabling disparate systems to work collectively, APIs can speed up time-to-market for application development, increase agility of AI models, and enable organizations to deliver value faster.

The flipside is that the use of APIs has decentralized application structures. This makes securing them even tougher, which in turn makes them extremely attractive to attackers. API endpoints increase an application's attack surface area and introduce new risks and vulnerabilities that traditional app security tools struggle to mitigate. Without proper management, continuous monitoring, and security controls, APIs can pose a serious risk to organizations.

Attacks that target APIs, and vulnerabilities that exist within APIs deployed or integrated into modern apps including AI systems, are hard to mitigate and even harder to remediate. Scanning and testing APIs in a runtime environment help security teams uncover vulnerabilities in APIs before they're in production, where remediation is more costly and frustrating. Understanding how to secure APIs is a struggle for most operations and security teams.

Similarly, organizations frequently have outdated or undocumented APIs, as well as owned or third-party APIs that connect to distributed applications that have been abandoned or forgotten. These can introduce unknown security vulnerabilities.

Discover, Monitor, Control, and Mitigate

F5® Distributed Cloud API Security is a comprehensive solution to securely manage APIs across any data center or cloud using a simple, fast, and scalable architecture. It helps drive business velocity by enabling automated API deployments and management, while also protecting against API-specific threats. Distributed Cloud API Security, part of the F5 Distributed Cloud Web App and API Protection (WAAP) solution, delivers a broad approach to API security with a combination of management, monitoring, and enforcement functionality.

Distributed Cloud API Security allows organizations to easily and effectively discover unknown APIs, as well as monitor and secure APIs with continuous learning, inspection, and schema enforcement capabilities. With the service in place, organizations can quickly discover, learn, and map an app's API endpoints and communication paths, including unknown/shadow or old, outdated APIs. This delivers a complete view into all the connections within an app's ecosystem.

Key Features

Automatic API Discovery

Detect APIs and determine normal behavior as APIs are used, and monitor usage, methods, sensitive data and detect outliers including rogue and shadow APIs, with the generation of OpenAPI spec (OAS).

Import API Schema

Automatically deliver a positive security model with existing OpenAPI spec (OAS), to enforce desired API behavior through valid endpoint, parameter, method, authentication, and payload details.

Rich API Monitoring and Visualization

Identify the most used and attacked API endpoints, usage patterns, correlate good and bad actor activity, plus sensitive data, including PII, to optimize and tune protection policies for APIs.

Sensitive Data Detection and Masking

Provides visibility into endpoint details, including the detection and flagging of PII that is being exposed, with capabilities to mask sensitive data or block end points distributing sensitive data.

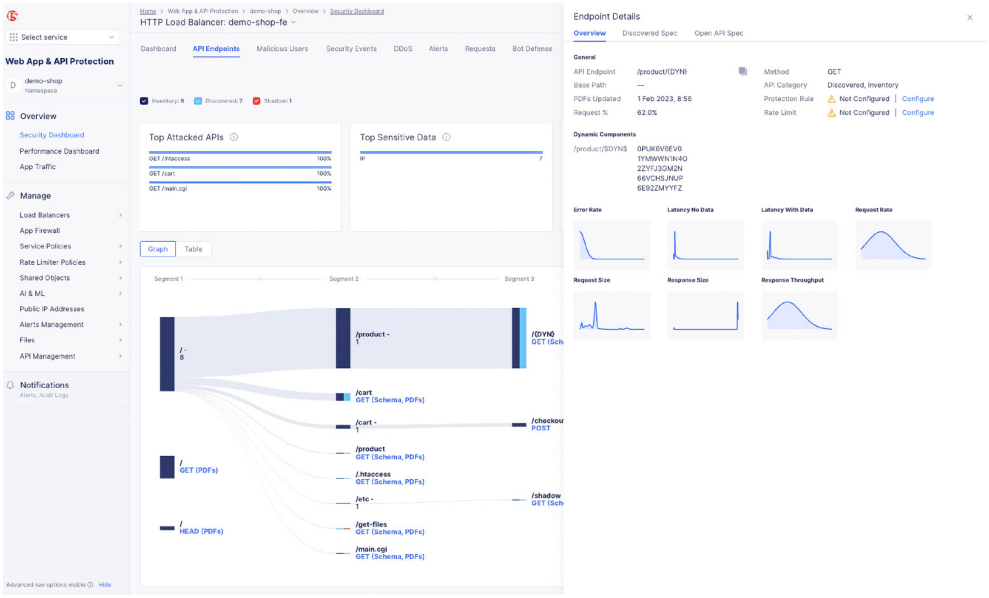

Figure 1: Learned API schema with ability to drill down into usage baselines and view any PII information at the individual API level.

The service delivers advanced machine learning (ML) functionality that continuously tracks and monitors API endpoints, allowing organizations to easily baseline API behavior, validate authentication status, including access and visualization of API usage over time, streamlining the identification of communication patterns and the correlation of normal behaviors with anomalies. This ability helps organizations identify and act on suspicious activity as APIs evolve, including the identification of sensitive data and personal identifiable information (PII), being sent within API communications.

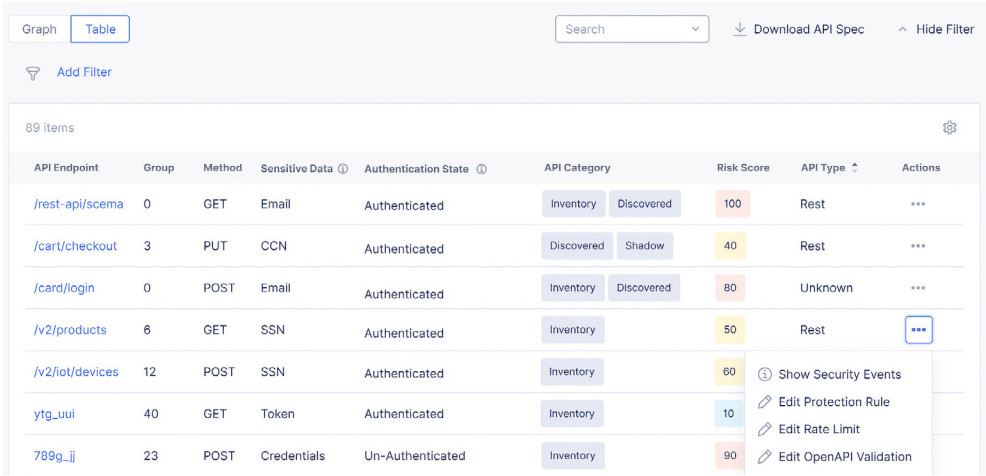

Figure 2: API Authentication Discovery and Validation–discover and view authentication status, details and risk score of all APIs, including the ability to create protection or blocking rules.

Key Features (Continued)

App and API Security Enforcement Engine
Combines in-line app and API security capabilities with WAF, including granular L7 policy engine delivering rate limiting, IP reputation, Allow/Deny, and L7 DoS functionality, to control and block API endpoints.

Authentication Discovery and Risk Scoring
Identifies and baselines the authentication state of all APIs within an environment, allowing for automatic discovery with views into authentication status, details, and the risk score of APIs.

Distributed Cloud API Security uniquely pairs speedy global API discovery and learning with the in-line enforcement capabilities of WAAP. Organizations can benefit from a robust set of enforcement functionality to maintain security of their apps and API endpoints. This includes implementation of a positive security model via imported OpenAPI spec files for specific endpoints, methods, and payloads of known, documented APIs. Paired with in-line protection capabilities to block unknown or unwanted endpoints, limit connections or communication, the service can identify and stop the exfiltration of PII or other potentially sensitive data. It combines WAF signatures and granular layer 7 policy enforcement with rate limiting, IP reputation, allow/deny list, and layer 7 DoS functionality, to accurately filter out malicious traffic, prevent attempts to attack, or exploit APIs.

These advanced API security controls and complimentary WAAP functionality are all delivered via F5's scalable, SaaS-based Distributed Cloud platform. Distributed Cloud WAAP provides comprehensive app and API security that enables organizations to reduce tool sprawl and overall architectural complexity. This solution simplifies the deployment and management of all critical app and API security controls necessary to protect an app's entire ecosystem in one unified console, with centralized visibility and management. This allows DevOps and SecOps teams to quickly identify suspected API abuse as anomalies are detected, as well as create policies to stop misuse, thus better protecting API endpoints and the apps that they support.

Conclusion

Deliver AI Applications and Learning Models with Performant, Effective, and Scalable Application and API Security

Distributed Cloud API Security, as part of Distributed Cloud WAAP, helps organizations drive business velocity by enabling extensive, modern application and API deployments with the necessary management and protection against API-specific threats.

The landscape of AI is perpetually evolving, and environments housing AI applications and models also undergo frequent changes. Distributed data sources must exhibit flexibility and adaptability, with APIs facilitating seamless integration of new data streams and accommodating modifications to AI models as innovation progresses.

However, the convergence of distributed data sources must not compromise security. AI systems are susceptible to a spectrum of targeted, sophisticated attacks orchestrated by malicious actors aiming to exploit vulnerabilities in applications and APIs to gain unauthorized access to sensitive data. As AI-driven enterprises rely on comprehensive datasets, fortifications against these threats are essential to maintaining data integrity and safeguarding intellectual property.

The next generation of AI-powered apps is increasingly modular, complex, and distributed, ultimately requiring security services that can do more. Distributed Cloud API Security, part of the Distributed Cloud WAAP solution package, delivers the cybersecurity efficacy and ease of use that today's application architectures require. This SaaS-based solution is a better way to secure modern applications and APIs—with unparalleled performance and availability at scale—offering consistent operations, security, and end-to-end observability.

With this solution, organizations benefit from comprehensive app and API security to more effectively secure and manage APIs. This, in turn, drives business velocity by enabling extensive modern, AI-powered app and API deployments that include necessary management tools and built-in protection against API-specific threats. Organizations can seamlessly augment existing API management and gateway functionality, pairing rich API discovery and positive security capabilities with critical enforcement tools in one global, SaaS-delivered solution.

This innovative and accessible solution helps reduce app and API security gaps and enables consistent coverage across an organization's entire app portfolio, regardless of where those apps and APIs are deployed, including on premises, across clouds, or at an organization's edge. With Distributed Cloud API Security as part of Distributed Cloud WAAP, organizations can simplify their path to effective security while fostering the innovation that their business—and their customers—demand.

Explore more and request a free trial at f5.com/cloud/products/api-security.