F5 Distributed Cloud API Security

Combine the power of data analytics and deep insights from AI and machine learning to discover, detect and protect your APIs. Distributed Cloud API Security Identifies and blocks API attacks, eliminates vulnerabilities and prevents sensitive data leakage via APIs.

f5

Improve API Security
Pairs complete automatic API discovery, testing and positive security with in-line enforcement capabilities to control and protect APIs.

Limit Data Loss
Better understand and monitor sensitive data being exposed by APIs and implement critical data exposure rules.

Improve API Visibility
Easily identify all API endpoints mapped to applications and monitor for malicious activity.

Strengthen API Access and Authentication
Augments API gateway functionality, delivering enhanced visibility, oversight and control while helping to identify gaps in API authentication and access.

Limit Exposure of API Vulnerabilities in Production
Begin discovery, testing and monitoring of APIs earlier, improving visibility and understanding of vulnerabilities before release into production.

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

Without proper governance, consistent documentation, monitoring and protections, APIs can expose organizations to serious risk.

APIs power apps, but without proper attention, they can expose organizations to significant risks. APIs are a fundamental building block of modern application development, powering apps that impact lives. As modern applications have evolved, dependencies on APIs have increased. That's because 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 application structures which are changing frequently. Organizations are dealing with more teams developing APIs across an increasing number of different environments. Leaving them with a complex, constantly changing threat surface with more new and changing APIs. And many organizations with blindspots, gaps in visibility and control over outdated or undocumented APIs that have been missed or have never been tracked. This makes securing them even tougher, and in turn makes APIs extremely attractive to attackers.

Overall, 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 governance, consistent documentation, monitoring and specialized security controls, APIs can pose a serious risk to organizations.

Discover, Detect, and Protect APIs

F5® Distributed Cloud API Security delivers a comprehensive approach to protecting API's throughout their full-lifecycle from build and test through to release, operate and monitor. It enables organizations to maintain business velocity with modern, API enabled app deployments while seamlessly 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 governance, monitoring, detection, and enforcement functionality.

Distributed Cloud API Security allows organizations to easily and effectively discover all their APIs, as well as monitor and secure APIs. With the service in place, organizations can quickly discover, learn, test and automatically document an app's API endpoints and communication paths combining code-base discovery with continuous traffic analysis and automated client-side web crawling. This delivers a complete view into all the connections within an app's ecosystem including unknown (shadow), unused (zombie) or old, outdated APIs.

Key Features

Automatic API Discovery and Documentation

Detect and document all APIs directly from code repositories, with traffic based analysis and client-side web crawling including automatic generation of OpenAPI spec (OAS) files.

API Testing

Proactive API testing feature that runs targeted tests on API endpoints discovered by the platform. All APIs in inventory can be run through critical tests to uncover vulnerabilities across a wide range of OWASP API Top 10 threats.

Import API Schema

Automatically deliver a positive security model with learned, automatically generated and existing OpenAPI spec (OAS) files, 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 Protection

Discover, tag and report on data being exposed including common PII, data types relevant to critical compliance frameworks (e.g. PCI-DSS, HIPAA, GDPR etc.) and custom patterns — with capabilities to limit, mask or block APIs exposing the data.
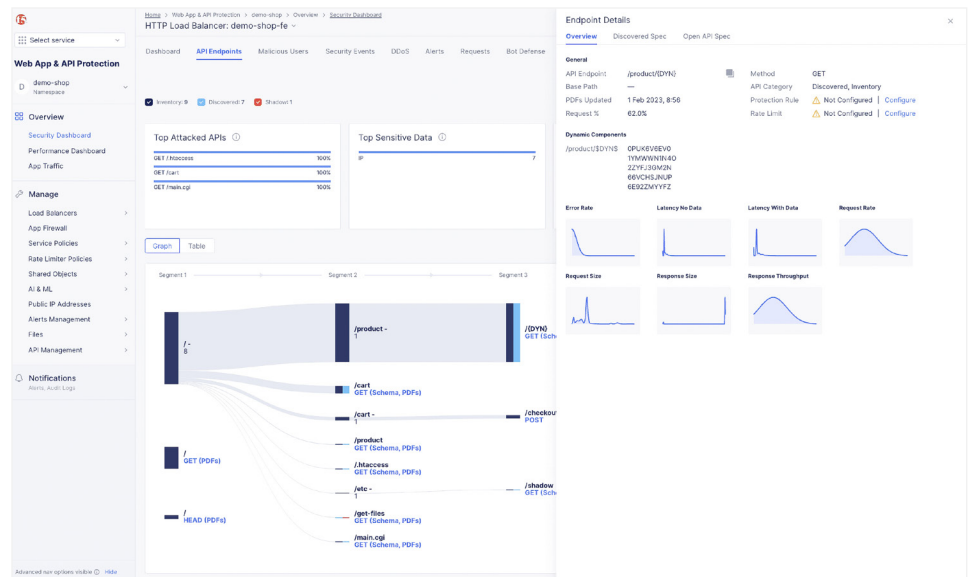
Figure 1: Learned API schema with ability to drill down into usage baselines and view any PII information at the individual API level.

The service includes multiple mechanisms to detect vulnerabilities and anomalies in APIs and API behavior that can be indicators of an attack or compromise. Starting with API testing, organizations can test all discovered APIs for vulnerabilities with automated testing capabilities against the OWASP API Top 10, to identify vulnerabilities in pre-production (e.g. testing or staging) environments and continuously across the entire API lifecycle. On top of this testing functionality, the service includes an advanced machine learning (ML) engine that continuously tracks and monitors API endpoints overtime. This allows 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. These critical tools provide important detection capabilities, helping organizations identify and act on suspicious activity and weaknesses including unauthorized access, authentication flaws, sensitive data exposure and misconfiguration—all as their API ecosystem evolves.

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.

AI Powered Assistant
Leverages the power of natural language queries to streamline analysis of and access to API security events, with context and actionable recommendations.

API Endpoint	Group	Method	Authentication State	API Category		Discovery Source	Risk Score	API Compliance	Actions
/rest-api/scema	0	GET	Authenticated	Inventory		Code, Traffic	80	PCI	...
/cart/checkout	3	PUT	Authenticated	Inventory		Code, Traffic	40	PCI, GDPR, HIPPA...	...
Keren_test	0	PATCH	Un-Authenticated	Discovered	Inventory	Code, Traffic	80	PCI	...
Nelly-55	6	GET	Authenticated	Discovered	Inventory	Traffic	50	GDPR	...
Aric456	12	POST	Authenticated	Discovered	Shadow	Traffic	60	GDPR	...
ytg_uui	40	GET	Authenticated	Discovered	Shadow	API Crawling	34	GDPR	...
789g_jj	23	GET	Un-Authenticated	Discovered	Inventory	Code	100	PCI, GDPR, HIPPA...	...
Aric456	12	POST	Un-Authenticated	Discovered	Inventory	API Crawling	20	HIPPA	...
/rest-api/scema	0	GET	Unknown	Discovered	Inventory	Traffic	0	HIPPA	...

Figure 2: View and understand details for every API, including authentication details, sensitive data and compliance status, category and risk score including the ability to create protection and blocking rules.

Distributed Cloud API Security uniquely pairs speedy global API discovery, testing and detection 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 for an organizations APIs via imported or automatically generated OpenAPI spec files from discovery, paired with in-line protection capabilities to automatically block unknown or unwanted endpoints, limit connections or communication. The service can also identify and stop the exfiltration of PII or other potentially sensitive data via APIs. 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. It enables organizations to identify vulnerabilities and suspected API abuse at all stages of the development lifecycle, including before release into production via code analysis and testing, plus continuous monitoring, anomaly detection and API protection rules. All of this helps them limit the exposure of vulnerabilities and thwart potential threats with ease, better protecting their API endpoints and the apps they support.

Conclusion

Deliver Modern Digital Experiences with Performant, Effective, and Scalable API Security

Applications and the APIs that power them are the lifeblood of most businesses today. Modern applications call for scalable and adaptive security solutions. As applications become increasingly modular, complex, and distributed, they require security services that can do more. Distributed Cloud API Security, delivers the cybersecurity efficacy and ease of use that today's application architectures require. It's 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 across the entire API lifecycle.

With this solution, organizations benefit from comprehensive app and API security to more effectively secure and manage APIs, helping drive business velocity by enabling extensive modern app and API deployments with the necessary oversight and protection against API-specific threats. Organizations can seamlessly augment existing API management and gateway functionality, pairing complete API discovery, detection 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 across on-premises, across clouds, or at an organization's edge. With Distributed Cloud API Security, organizations can simplify their path to effective API security while fostering the innovation their business and customers demand.

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