SOLUTION OVERVIEW

How to Continuously Discover, Monitor, and Protect APIs

Detection and in-line enforcement are essential components of F5 Distributed Cloud API Security, enhancing control over API behavior, mitigating malicious or unwanted activity (including automated threats), and preventing the exposure of sensitive data.

Detect vulnerabilities and implement critical protections across APIs, the services they enable, and the systems and data they access

In today's digital landscape, APIs are the backbone of modern applications, enabling integration and data exchange between services. As organizations increasingly rely on APIs to enhance functionality and deliver innovative solutions, the risk associated with unprotected APIs has grown exponentially. Cybercriminals actively target these endpoints, which enable critical business functions and act as gateways into organizations, exploiting vulnerabilities to access sensitive data, disrupt services, abuse business logic to commit fraud, and execute attacks—including denial-of-service (DoS), injection, and other threats.

To safeguard digital assets and maintain customer trust, organizations must prioritize API protection. Implementing robust security measures for APIs not only mitigates risk over a growing threat surface but also ensures compliance in regulated industries. API security promotes resiliency across an organization's digital services, its infrastructure, and the customer experience.

An API security solution must include discovery, vulnerability detection, monitoring, and real-time mitigation against bots and other threats. In-line enforcement is critical. It is not reasonable to expect organizations to stall development and immediately fix every vulnerability in API code, or to halt the flow of code releases until the code is perfected. This is where in-line API detection and protection capabilities come into play.

In-line Enforcement to Control, Monitor, and Protect API Endpoints

A robust API security stack relies on multiple layers of enforcement and control mechanisms to ensure comprehensive protection. The OWASP API Security Top 10 highlights a broad spectrum of threats, including the distinct vulnerabilities and security risks that APIs encounter. This includes attacks that attempt to leak or exfiltrate data, or that consume or abuse resources (such as DoS attacks)—as well as standard injection attempts, gaps in access and authentication, and security misconfiguration. These exploits and the unique properties of APIs require specialized detection and protection, as they expose critical endpoints that are prime targets for automated attacks and malicious actors--increasing the risk of unauthorized access to critical systems and sensitive data. Complex authentication and authorization mechanisms can further heighten security risks if not properly enforced and consistently monitored. Additionally, APIs often handle dynamic business logic and integrate with third-party services, necessitating additional security measures to defend against a diverse range of threats and exploits unique to APIs.

Key Benefits

Reduce exposure of API vulnerabilities
In-line enforcement and control —including positive security capabilities—to respond to attacks and other API exploits in real time, minimizing potential damage from threats across the OWASP API Security Top 10.

Stop unauthorized access and limit data loss
Gain deeper insight into API usage and the exposure of sensitive data—including personally identifiable information (PII)—with capabilities to mask, restrict, or block APIs from exposing critical data.

Monitor API endpoints and improve visibility
Continuously monitor API endpoints from a centralized console, detecting anomalous and malicious activity to enhance response strategies, optimize controls, and strengthen API protection policies.

Easily apply consistent protection and policy management
Manage API security from a single point with a common set of control mechanisms—simplifying policy implementation and ensuring consistent protection across all APIs.

Cybercriminals actively target these endpoints, which enable critical business functions and act as gateways into organizations, exploiting vulnerabilities to access sensitive data, disrupt services, and abuse business logic.

Key Features

Ensure comprehensive runtime protection
Combines in-line app and API security capabilities with a web application firewall (WAF) and bot defense protections, leveraging rich client-side signals and machine learning (ML) to ensure maximum efficacy and near-zero false positives.

Protect sensitive data
Masks sensitive data exposed through API requests—including API protection rules—by limiting data transmission or fully blocking API endpoints that expose any form of data.

Enforce positive API security
Automatically delivers a positive security model using learned, automatically generated, or existing OpenAPI Specification (OAS) files to enforce desired API behavior through valid endpoint, parameter, method, authentication, and payload details.

Perform behavioral analysis and anomaly detection
Leverages ML-based analysis to identify the most frequently used and attacked API endpoints, assess usage patterns—including behavioral anomalies—and identify exposed sensitive data.

Implement real-time threat detection and risk scoring
Pinpoints the most frequently targeted APIs and high-risk endpoints by identifying authentication status, sensitive data exposure, and behavioral anomalies—utilizing continuous traffic inspection, threat monitoring, and vulnerability identification.

With F5® Distributed Cloud API Security, organizations have access to a robust set of enforcement functionalities aimed at maintaining the security of their API endpoints. Distributed Cloud API Security combines global API discovery with in-line detection and the enforcement capabilities of web app and API protection (WAAP). APIs are susceptible to the same types of injection attacks as the applications they support, including injection flaws like SQL and command injections. This is why traditional web application firewall (WAF) functionality still plays a significant role in the protection of modern apps and the APIs that drive them. F5 Distributed Cloud Services features F5's core WAF, equipped with a robust attack-signature engine containing over 8,500 signatures for CVEs (common vulnerabilities and exposures), along with known vulnerabilities and techniques identified by F5 Labs—forming a strong baseline for API protection against recognized threats.

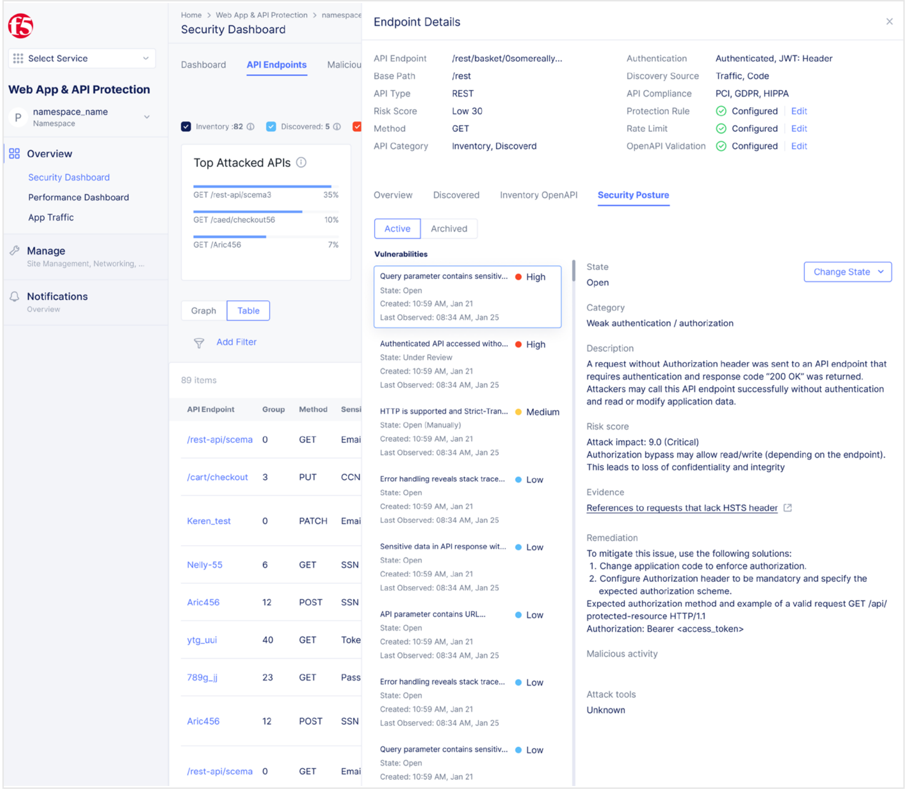
Like any network or compute resource, APIs are susceptible to abuse and DoS attacks. F5 Distributed Cloud Services provides layer 7 DoS protection and rate-limiting capabilities to maintain service availability for web applications and APIs. Organizations can precisely control API endpoint connectivity and the rate of requests, identifying, monitoring, and blocking specific clients and connections entirely or applying customized thresholds. This granular control of API connections and requests can be enforced at the individual API level or across an entire domain.

Mitigating bots and automated traffic is a vital component of any comprehensive API security strategy. With Distributed Cloud Services, organizations gain access to F5 Distributed Cloud Bot Defense which offers robust protection against automated threats. Adversaries use bots to directly exploit three of the top ten OWASP API Security vulnerabilities: broken authentication, unrestricted resource consumption, and unrestricted access to sensitive business flows. The other seven items on the top ten list—which include vulnerabilities such as security misconfiguration, poor inventory management, and broken authorization—are indirectly related to bots: attackers rely on bots to effectively discover and rapidly exploit these vulnerabilities. Many API endpoints—for login, checkout, credit card validation, and reservations, for example—are particularly vulnerable to bots.

In addition, Distributed Cloud Services delivers advanced machine learning (ML) and behavioral analysis to continuously track and monitor API endpoints. This capability enables organizations to baseline API behavior, validate authentication status and visualization of API usage over time—streamlining the detection of communication patterns and the correlation of normal behaviors with anomalies. As APIs evolve, this approach helps organizations identify and act on suspicious activity, including the exposure of sensitive data and personal identifiable information (PII) within API communications.

Sensitive data is often unknowingly or inadvertently exposed or transmitted within APIs, making it essential to identify web app and API endpoints—where potential PII and other sensitive data may be at risk—so that the data can be protected and potential breaches can be prevented. Distributed Cloud API Security enables organizations to gain control over their API landscape, offering visibility into sensitive data that may be exposed through their web apps and APIs.

Organizations can easily configure sensitive data policies to discover, tag, and report on critical data being exposed within their APIs. This includes basic policies to identify common PII data (including credit card numbers, physical and email addresses, and phone numbers), specific compliance frameworks that can be applied with hundreds of predefined data types relevant to more than 20 critical compliance frameworks (e.g., PCI-DSS, HIPAA, GDPR, SOC2, etc.), and even custom sensitive data unique to specific organizations. The service can automatically discover and document an organization's APIs directly from code repositories and analysis of traffic, providing detailed visibility into each endpoint for every individual API.



☑ Inventory :82 ☑ Discovered: 5

Top Attacked APIs

GET /rest-api/scema3	35%
GET /caed/checkout56	10%
GET /Aric456	7%

89 items

API Endpoint	Group	Method	Sensi
/rest-api/scema	0	GET	Emai
/cart/checkout	3	PUT	CCN
Keren_test	0	PATCH	Emai
Nelly-55	6	GET	SSN
Aric456	12	POST	SSN
ytg_uui	40	GET	Toke
789g_jj	23	GET	Pass
Aric456	12	POST	SSN
/rest-api/scema	0	GET	Emai

API Endpoint	/rest/basket/0somereally...	Authentication	Authenticated, JWT: Header
Base Path	/rest	Discovery Source	Traffic, Code
API Type	REST	API Compliance	PCI, GDPR, HIPPA
Risk Score	Low 30	Protection Rule	Configured | Edit
Method	GET	Rate Limit	Configured | Edit
API Category	Inventory, Discoverd	OpenAPI Validation	Configured | Edit

Vulnerabilities

Query parameter contains sensitiv... ● High
State: Open
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

Authenticated API accessed witho... ● High
State: Under Review
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

HTTP is supported and Strict-Tran... ● Medium
State: Open (Manually)
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

Error handling reveals stack trace... ● Low
State: Open
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

Sensitive data in API response wit... ● Low
State: Open
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

API parameter contains URL... ● Low
State: Open
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

Error handling reveals stack trace... ● Low
State: Open
Created: 10:59 AM, Jan 21
Last Observed: 08:34 AM, Jan 25

Query parameter contains sensitiv... ● Low
State: Open
Created: 10:59 AM, Jan 21

State
Open

Category
Weak authentication / authorization

Description
A request without Authorization header was sent to an API endpoint that requires authentication and response code "200 OK" was returned. Attackers may call this API endpoint successfully without authentication and read or modify application data.

Risk score
Attack impact: 9.0 (Critical)
Authorization bypass may allow read/write (depending on the endpoint). This leads to loss of confidentiality and integrity

Evidence
References to requests that lack HSTS header

Remediation
To mitigate this issue, use the following solutions:
1. Change application code to enforce authorization.
2. Configure Authorization header to be mandatory and specify the expected authorization scheme.
Expected authorization method and example of a valid request GET /api/protected-resource HTTP/1.1
Authorization: Bearer <access_token>

Malicious activity

Attack tools
Unknown

Endpoint details are provided on a per API basis–delivering critical insights into vulnerabilities, ranked by severity. Plus, these critical insights include description, evidence, and remediation guidance. Swiftly take action with new API protection rules to limit or block APIs and data, or to control API behavior.

Distributed Cloud API Security also features a custom sensitive data detector, enabling users to define and search for uncommon or unique patterns which may indicate other sensitive data types within API requests and responses. This functionality can be used to search for unique, organizational-specific data that needs to be detected and protected, continuously monitoring API traffic to identify inadvertent leaks or suspicious activity.

F5 Distributed Cloud API Security provides multiple layers of protection for APIs, enabling organizations to quickly detect and act when vulnerabilities, suspected attacks, or abuses are identified–including automated threats that target exposed APIs.

On top of this detection capability, Distributed Cloud Services offer a variety of ways—including sensitive data masking and leakage detection capabilities—to help organizations protect sensitive data identified within APIs. This allows organizations to establish API data protection policies, defining how data is handled within API responses to limit, block, or mask. Policies that control exposure and masking of data within APIs can easily be applied to specific API endpoints, a group of endpoints, specific paths, or an entire domain, ensuring that even if an attacker gains access to a given API's traffic, the sensitive data remains secure and incomprehensible. In addition to masking capabilities, the service includes continuous monitoring of all APIs, with analysis of all transmitted data to help detect and report inadvertent leaks or suspicious activity within API responses.

When it comes to handling access and authorization threats, Distributed Cloud API Security augments API gateway functionality by providing enhanced visibility, oversight, and control over API behavior, authentication, and access. This helps organizations identify authentication gaps, enforce access control, and block unauthorized attempts to reach APIs, back-end systems, and sensitive data. The service learns, models, and maps all app and API endpoints via continuous discovery—including authentication status. Through direct code analysis and traffic-based discovery, it can also learn about and document authentication types and API endpoint details. By leveraging OAS files—whether learned or uploaded—it enforces authentication requirements and blocks unauthenticated traffic at the edge, reducing reliance on API gateways and servers for request handling.

The service also includes JSON Web Token (JWT) validation functionality, which allows organizations to upload authentication keys and validate JWT sign-in requests at the edge. This capability eliminates the need for organizations to store session states on the server or retrieve user information from a database or cache. By enabling immediate validation, it removes the need to query the origin for verification, enhancing API scalability and delivering a faster user experience.

Organizations can also leverage Distributed Cloud API Security to enforce proper API behavior based on valid schema definitions, using automatically generated or imported OAS files. The service validates input and output data against documented API characteristics—including data type, length constraints, permitted characters, and valid value ranges—to ensure compliance. By continuously monitoring API traffic, it enables automatic validation, blocking, or implementation of protection rules—allowing granular access control to individual API endpoints, API groups, or base paths defined in a specification file.

F5's scalable, SaaS-based Distributed Cloud platform delivers advanced API protection capabilities alongside complementary WAAP functionality. Distributed Cloud API Security provides multiple layers of protection for APIs, enabling organizations to swiftly detect and respond to vulnerabilities, suspected attacks, and abuses. This solution simplifies the deployment and management of essential API security controls, safeguarding an application's entire ecosystem—including the increasing number of APIs—within a unified console that offers centralized visibility and management.

Conclusion

As organizations adopt modern applications powered by APIs, they expose more endpoints—heightening their susceptibility to cyber threats and underscoring the need for robust API protection. APIs serve as critical conduits for data exchange, service enablement, and transaction execution, making them prime targets for cybercriminals. As organizations increasingly rely on APIs to enhance functionality and streamline operations, the risks associated with unprotected APIs have surged. Vulnerabilities can lead to unauthorized access, data breaches, and service disruptions, ultimately compromising sensitive information and damaging customer trust. Due to the complexity of authentication mechanisms and the dynamic nature of APIs, traditional security measures often prove insufficient, necessitating specialized protections.

This is exactly what Distributed Cloud API Security offers: the platform and tools organizations need to implement robust API protection to mitigate these risks and foster resilience within their modern digital infrastructure and ecosystem. By prioritizing API protection, businesses can better defend against evolving threats, ensure the integrity of their services and data, and maintain compliance with industry regulations without impacting the pace of innovation—securely unlocking the full potential of their new, modern apps in a rapidly evolving digital ecosystem.

By prioritizing API protection, businesses can better defend against evolving threats, ensure the integrity of their services and data, and maintain compliance with industry regulations without impacting the pace of innovation.

See it in action

Try the interactive demo or check out the website.

Interactive Demo ›

Website ›