Solution Overview

How to Continuously Monitor, Control, and Protect APIs

Detection and in-line enforcement are critical elements of F5® Distributed Cloud API Security, improving the ability to control API behavior, limit undesirable or malicious activity, and block sensitive data from being exposed.

Key Benefits

Reduce Exposure of API Vulnerabilities to Limit Attacks and Exploits
Respond to attacks and other API exploits as they occur with positive security capabilities including in-line enforcement and control, minimizing potential damage from threats across the OWASP API Top 10.

Stop Unauthorized Access and Limit Data Loss
Better understand and monitor API usage and sensitive data being exposed by APIs, including personally identifiable information (PII), with capabilities to mask, limit, or block APIs from exposing critical data.

Monitor and Improve API Visibility
Continuously monitor API endpoints in a single, centralized console, including detection of anomalous or malicious activity, to inform response and optimize controls and protection policies for APIs.

Get Consistent Protection and Policy Management
Manage API security from a single, centralized point with a common set of control mechanisms, simplifying policy implementation and ensuring consistent protection across all APIs.

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 seamless 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 are actively targeting these endpoints as facilitators of critical business functions and pathways into organizations—exploiting vulnerabilities to access sensitive data, disrupt services, exploit business logic to commit fraud, or launch other attacks, including Denial of Service (DoS), injection, and more.

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 can be critical to ensuring compliance in regulated industries. It can be critical to promoting resiliency within an organization's digital services and infrastructure and maintaining customer experience.

Discovery is one thing, and a crucial component of an organization's overall API security, but organizations need to be able to detect vulnerabilities and threats, plus act. It's crucial for them to have control over these endpoints and client interactions, as well as be able to implement protective policies across their APIs. The only way to do that is with in-line enforcement. It's not reasonable to expect organizations to stall development and fix every vulnerability in API code immediately or stop the flow of code releases until the code is perfect. This is where in-line API detection and protection capabilities come into play.

Cybercriminals are actively targeting API endpoints as facilitators of critical business functions and pathways into organizations–exploiting vulnerabilities to access sensitive data, disrupt services, and exploit business logic.

Key Features

Comprehensive Runtime Protection
Combines in-line app and API security capabilities with a web application firewall (WAF), including a granular L7 policy engine delivering rate limiting, IP reputation, allow/deny, and L7 DoS functionality to protect, control, and block API endpoints.

Sensitive Data Protection
Masks any data that is identified as being exposed within API requests, including API protection rules to limit data transmission or block API endpoints exposing data altogether.

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

Behavioral Analysis and Anomaly Detection
Uses AI and ML-based analysis to identify the most used and attacked API endpoints, usage patterns including behavioral anomalies, plus any sensitive data.

Real-Time Threat Detection and Risk Scoring
Identifies the most attacked APIs and endpoints with the highest risk, including issues in authentication status, sensitive data exposure, and behavioral anomalies, through continuous traffic inspection, attack monitoring, and vulnerability identification.

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

Critical to any API security stack are multiple layers of enforcement and control mechanisms for APIs, delivering in-line detection and protection. The OWASP API Top 10 highlights the variety of threats, including some of the unique vulnerabilities and threats that APIs face. This includes attacks attempting to leak or exfiltrate data, consume or abuse resources (such as DoS attacks), standard injection attempts, gaps in access and authentication, and security misconfiguration. These exploits and the unique properties of APIs require specialized detection and protection because they expose critical endpoints that can be targeted by automated attacks and malicious users, increasing the risk of unauthorized access to critical systems and sensitive data. They also have complex authentication and authorization mechanisms that can create vulnerabilities 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 ensure defense against the variety of unique threats and exploits APIs face.

Distributed Cloud API Security uniquely pairs speedy global API discovery with in-line detection and the enforcement capabilities of web app and API protection (WAAP). Organizations can benefit from a robust set of enforcement functionality to maintain security of their API endpoints. Traditional web application firewall (WAF) functionality still plays a huge role in the protection of modern apps and the APIs that drive them. APIs are susceptible to the same types of injection attacks as the applications they support, including injection flaws like SQL, NoSQL, command injections, and more, attempting to execute unintended commands or access data. F5® Distributed Cloud Services includes F5's core WAF with its robust attack-signature engine containing over 8,500 signatures for CVEs, plus known vulnerabilities and techniques identified by F5 Labs, forming the baseline of protecting an organization's APIs from known vulnerabilities.

Like with any network or compute resource, APIs are also susceptible to abuse and DoS attacks, and Distributed Cloud Services has the layer 7 DoS capabilities and rate limiting functionality to ensure service availability of web apps and APIs. Organizations can granularly control API endpoint connectivity and the rate of requests. They can identify, monitor, and block specific clients and connections all together or set particular quotas or thresholds, and discrete methods to be rate limited. This granular control of API connections and requests can be done for individual APIs or an entire domain.

On top of this granular rate limiting functionality, the service delivers advanced machine learning (ML) and behavioral analysis that continuously tracks and monitors API endpoints, allowing organizations to easily baseline API behavior and 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 personally identifiable information (PII) being sent within API communications.

Often data is sent or exposed within APIs unknowingly or inadvertently. That's why being able to identify web app and API endpoints where potential PII and other sensitive data are being transferred or exposed is critical, so it can be protected and breaches prevented. Distributed Cloud API Security helps organizations get a handle on their API landscape and provides a view into sensitive data being exposed via 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 (such as 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 over 20 critical compliance frameworks (such as PCI-DSS, HIPAA, GDPR, or SOC2), and even custom sensitive data patterns unique to an organization. The service can automatically discover and document an organization's APIs directly from code repositories or traffic analysis with the ability to view all endpoint details for each individual API. This includes the detection and flagging of PII that is being exposed and tagging of the relevant compliance framework(s).

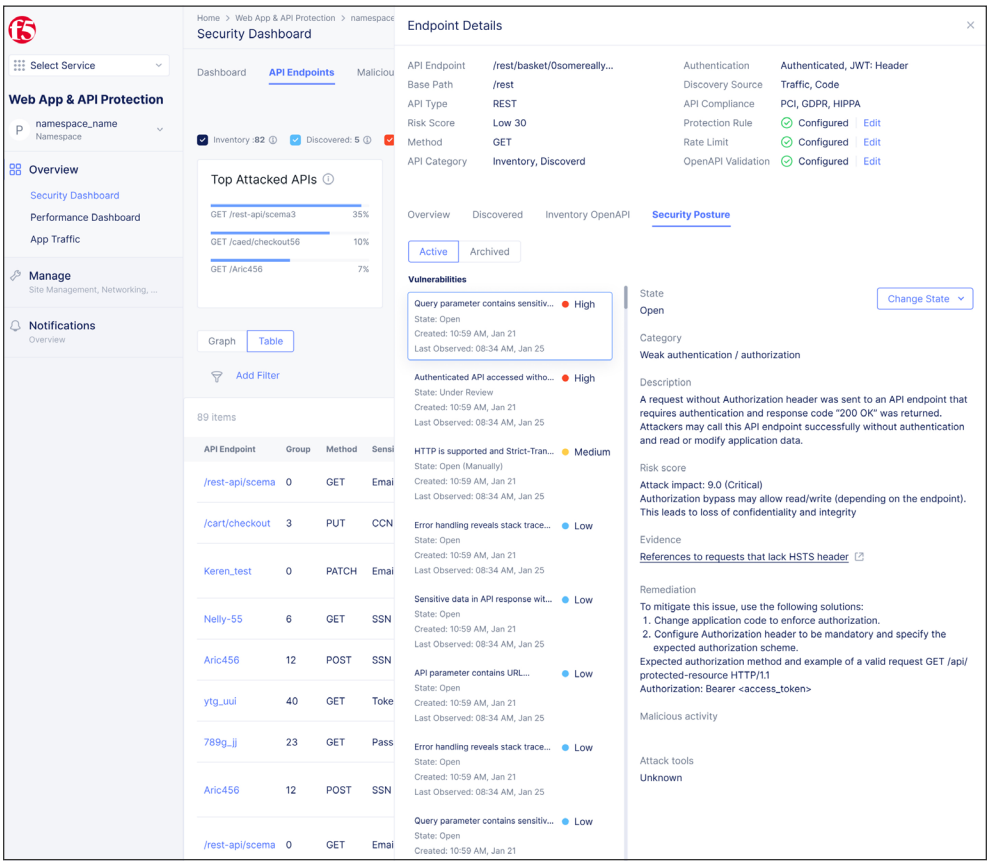

Figure 1: Endpoint details are provided on a per API basis, delivering critical insights into vulnerabilities ranked by severity, plus critical insights including description, evidence, and remediation guidance. Swiftly take action with new API protection rules when necessary to limit or block APIs and data or control API behavior.

Distributed Cloud API Security provides multiple layers of protection for APIs that enable organizations to quickly detect and act when vulnerabilities, suspected attacks, or abuse are identified.

Distributed Cloud API Security also includes a custom sensitive data detector functionality, allowing users to specify and search for less common or unique patterns which may be indicators of other sensitive data types in API requests and responses. This can be used to search for any unique organizational specific data that needs to be detected and protected, including active monitoring of all API traffic to spot any inadvertent leaks or suspicious activities.

On top of this detection capability, Distributed Cloud Services offer a variety of ways to help organizations protect sensitive data that is identified within APIs, including sensitive data masking and leakage detection capabilities. This allows organizations to establish API data protection policies, defining how data is handled within API responses to limit, block, or mask. These policies controlling 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. On top of the masking capabilities, the service also includes continuous monitoring of all APIs with analysis of all transmitted data to help detect and report on any inadvertent leaks or suspicious activity of data within API responses.

When it comes to handling access and authorization threats, Distributed Cloud API Security has several capabilities that augment API gateway functionality, delivering enhanced visibility, oversight, and control over API behavior, authentication, and access. This helps organizations identify gaps in API authentication, control access, and stop unauthorized access attempts to APIs, back-end systems, and data. The service learns, models, and maps all app and API endpoints, including the status and type of authentication present, via continuous discovery. The service can learn and document authentication types along with other API endpoint details based on direct code analysis and traffic-based discovery. Allowing organizations to better understand and easily associate authentication information with individual API endpoints for examination, and in support of a positive security model to maintain appropriate authentication of their APIs or for the development of critical API protection rules to limit or control API behavior and access. With OpenAPI Specification (OAS) files, either learned or uploaded, the authentication information that is part of OpenAPI spec details can be automatically enforced, and unauthenticated traffic can be stopped at the edge, removing the need for origin API gateways and servers to handle these requests.

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. With this capability, organizations don't have to store session states on the server and load user information from a database or cache. This immediate validation negates the need to go back to the origin for verification and increases the scalability of APIs—providing an overall faster client-server experience.

By prioritizing API protection, businesses can better defend against evolving threats, ensuring the integrity of their services and sensitive data.

From an API protection standpoint, organizations can also leverage Distributed Cloud API Security to enforce proper API behavior based on valid API definitions through automatically generated or imported OAS files, using documented API characteristics to validate input and output data from API endpoints like data type, minimum or maximum length, permitted characters, or valid values ranges. The service will check API traffic for compliance, allowing organizations to automatically validate API traffic and block or implement protection rules, further limiting or controlling access to individual API endpoints, API groups, or base paths defined in a spec file. This includes the enforcement of undefined parameters, allowing users to specify whether to block or allow requests containing parameters not explicitly defined in an OAS file.

These advanced API protection capabilities and complementary WAAP functionality are all delivered via F5's scalable, SaaS-based Distributed Cloud platform. Distributed Cloud API Security provides multiple layers of protection for APIs that enable organizations to quickly detect and act when vulnerabilities, suspected attacks or abuse are identified. This solution simplifies the deployment and management of the critical API security controls necessary to protect an app's entire ecosystem, including an increasing number of APIs, in one unified console with centralized visibility and management.

Conclusion

As organizations increasingly leverage modern applications with APIs, they are exposing more endpoints that can leave them susceptible to a host of threats, making API protection paramount. For most organizations, APIs serve as essential conduits for data exchange, enabling services, and executing transactions, 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. Given the complex authentication mechanisms and the dynamic nature of APIs, traditional security measures often fall short, necessitating specialized protections.

And this is exactly what is available with F5 Distributed Cloud API Security, giving organizations the platform and tools to implement robust API protection to mitigate these risks and foster resilience within an organization's 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 any relevant industry regulations without impacting the pace of innovation—securely unlocking the full potential of their new, modern apps and an evolving digital ecosystem.

Try the interactive demo or check out the website.