WHITE PAPER

F5 Distributed Cloud WAAP with Comprehensive API Security

Combine the power of data analytics and deep insights from AI and machine learning to discover, monitor, and mitigate threats to your APIs. Block API attacks, eliminate vulnerabilities, and prevent sensitive data leakage via API endpoints.

KEY BENEFITS

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

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

Improve API Visibility
Observing global API metrics from a single, centralized user interface for easy identification of all API endpoints and streamlined monitoring for anomalous or malicious activity, including zombie and shadow APIs.

Strengthen API Access and Authentication
Augment API gateway functionality, delivering enhanced visibility, oversight and control over API authentication and access. Identify gaps in API authentication, control access, and stop unauthorized attempts to exploit APIs and the back-end systems and data.

Modern applications are challenging the traditional security paradigm. APIs represent a new and expanding technological lever for organizations' competitive advantages, driving speed to market for new digital capabilities. This represents a key growth driver. However, APIs represent an expanding attack surface, with new entry points to disrupt services and gain access to data, including Personal Identifiable Information (PII).

The pervasiveness of APIs and the unique role they can play in the security or vulnerability of any application, and thus an entire organization, can't be overstated. In an analysis of breaches[1] in recent years, F5 Labs noticed that in most API-related incidents, the breach method is technically very simple, impacting public-facing, poorly-secured API endpoints.

Security, when it comes to APIs, is easier said than done. With the wave of application security event data being generated for a growing number of applications, and with API endpoints being monitored by most organizations these days, it can feel like an impossible task to stay on top of everything. And as the pervasiveness of modern, microservices-based application development continues, so will the number of APIs. Thus, the application threat surface will continue to get more difficult for organizations to deal with.

Why Are APIs Vulnerable?

There are many reasons why API security is difficult. First, consider the sheer scope and complexity of modern application environments and APIs deployed across highly distributed multi-cloud and hybrid architectures. This is all compounded by the speed at which apps and APIs are being developed. New connections and services are being introduced, including updates to existing APIs, through rapid CI/CD development cycles.

APIs are developed with common transport protocols REST, GraphQL, and more, which can contain flaws, creating vulnerabilities that can be exploited just like the applications they serve. It's likely most enterprises don't know all the APIs running in or connected to their environments. API visibility is a blind spot for many organizations. When speed and innovation are the goals, rigor in API documentation and tracking is often not the focus for developers.

Moreover, organizations with acquisition and integration activity, where IT environments and applications have been inherited, are dealing with situations where there are unknown applications, and APIs that are not well documented. This can create a large security blind spot. APIs are fast, lightweight, and reliable, often enabling critical communications and transfer of data between applications or clients. They have the potential to expose sensitive data, so they have become a desired target. This ever-growing, complex threat surface provides a struggle for legacy security technology and operations teams, pushing more of them to the brink of what is possible to try to secure and keep up with.

[1] F5 Labs, Post-Breach Analysis: Sophistication and Visibility, https://www.f5.com/labs/articles/threat-intelligence/post-breach-analysis-sophistication-and-visibility

What Core API Security Capabilities Do Organizations Need to Implement?

IN THE F5 2022 STATE OF APPLICATION STRATEGY REPORT, 68% OF RESPONDENTS RANKED AUTHENTICATION AND AUTHORIZATION AS THE MOST VALUABLE COMPONENTS OF API SECURITY—FOLLOWED NOT FAR BEHIND BY BEHAVIORAL ANALYSIS AND ANOMALY DETECTION TO MONITOR APIS IN PRODUCTION (RUNTIME).

API gateways traditionally handled elements of API security for most organizations. This included versioning and publishing, schema validation, monitoring, connectivity and routing, access, authentication, and rate-limiting. However, this is simply the first step and bare minimum when it comes to API security. Organizations need to treat API security more comprehensively, just as they do their core web applications. There are core elements of API security that organizations should be prioritizing when it comes to their application security stack. This includes technology and services that can provide rich **API visibility and discovery**. Relying on securely developed and well-documented APIs with schema enforcement functionality (Positive Security) is critical, but only part of the equation. Organizations need capabilities to constantly learn and map APIs that aren't documented, across all communication paths of an application. Discovery technology allows organizations to map their entire API landscape, exposing unknown or shadow APIs, abandoned or zombie APIs that can be blocked, as well as any unknown "good" APIs that should be considered for governance, providing greater oversight.

Knowing an API exists and having access control capabilities are two critical pieces to the API security puzzle. In the F5® 2022 State of Application Strategy Report, 68% of respondents ranked authentication and authorization as the most valuable components of API security. Not far behind was behavioral **analysis and anomaly detection** to monitor APIs in production (runtime), identifying and alerting on abnormal behavior and potential abuse, since there are ways to bypass authentication and authorization. Being able to track API behavior over time should include API request analysis and time series anomaly detection to build baseline behavioral attributes that can be used to identify anomalies in API request rates, errors, latency, throughput, and more. With this functionality, an alerting element is critical to raise issues when unexpected spikes or drops occur, unique traffic patterns are present, or abnormal API requests are detected.

Rounding out a modern API security stack requires an **in-line application and API security enforcement engine**. This most likely includes a WAF with multiple layers of application security functionality, such as granular application layer 7 policy enforcement with rate limiting, IP reputation, allow/deny list functionality, and layer 7 DoS. All this gives organizations the capabilities to further investigate and act on malicious endpoints, users, and other activity. This functionality allows operations teams to quickly and easily identify suspected API abuse as anomalies are detected. The teams can then create policies to stop any misuse, while better protecting APIs and app endpoints over time, as they evolve and as behavior changes.

F5® Distributed Cloud Web Application and API Protection (WAAP) delivers a comprehensive approach to API security with a combination of management and enforcement functionality. The service allows organizations to more easily and effectively **monitor** all API endpoints and application paths, **discover and track** unknown or shadow APIs, and **secure** with continuous inspection and schema enforcement. Let's explore how.

Attacks Attempting to Leak or Exfiltrate Data via APIs

APIs are often implemented in a default or generic way without considering implications to the data they are intended to collect or connect to and the individual sensitivity of different data. Sometimes, data is sent unknowingly or inadvertently. That's why being able to identify web app and API endpoints, where potential personal identifiable information (PII) is being transferred, is critical, so data can be protected and breaches prevented. Distributed Cloud WAAP can help organizations with both critical elements.

Within the advanced artificial intelligence (AI) and machine learning (ML) engine, the service can discover and map all APIs for a given application endpoint, with the ability to view endpoint details. This includes the detection and flagging of PII that is being exposed. Organizations can quickly and easily identify any critical PII that is being shared for any API, so remediation can be put in place.

When sensitive data is identified, users can leverage Dataguard functionality. This prevents HTTP/HTTPS responses from exposing sensitive information such as credit cards and social security numbers by masking the data. When enabled, Dataguard will mask the data using a string of asterisks (*). Masking can easily be applied to specific API paths or an entire domain, rendering any potentially sensitive data being exposed via an API useless and providing time for teams to patch or update the schema for the exposed API to protect the information moving forward.

Distributed Cloud WAAP also includes custom regex detector functionality to search for and detect other, less common patterns which may be indicators of PII in API requests and responses. This can be used to search for other potential PII such as names, addresses, phone numbers, or unique social security numbers from different countries. This is useful for organizations trying to identify and address all instances of sensitive data being stored or transmitted in an insecure manner via APIs.

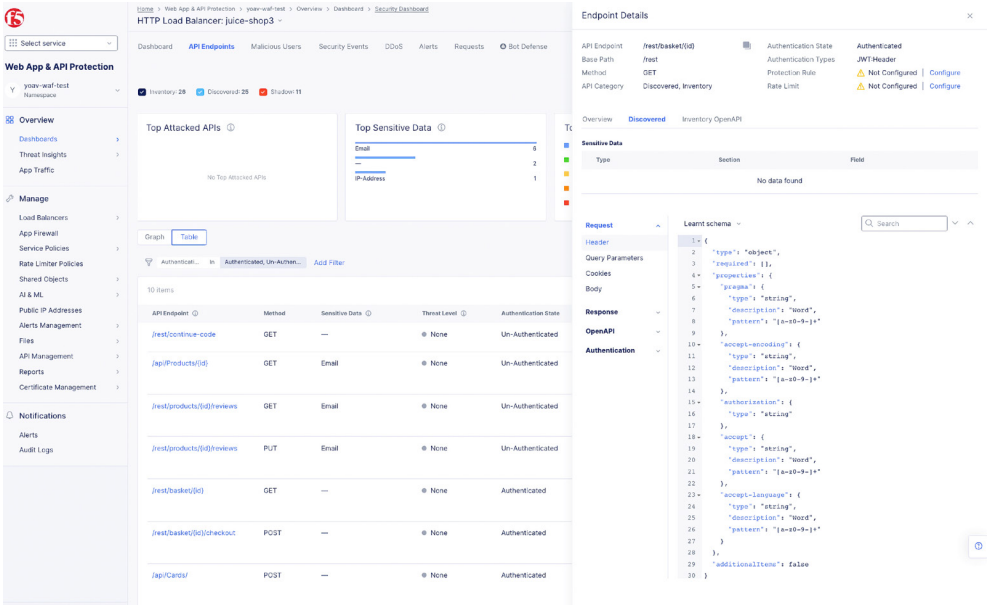

Figure 1: Learned API schema with ability to drill down into usage baselines and view any PII information at the individual API level.

Resource/DoS Attacks and Abuse of APIs

Like with any network or compute resource, APIs are susceptible to abuse and denial of service (DoS) attacks. APIs respond to client requests with responses which require CPU, memory, RAM, and more, with resource consumption being dependent on logical processing of inbound requests or the amount of data returned. Without rate limiting or other layer 7 DoS protections in place, this leaves web apps and APIs vulnerable to a single user or group flooding an API endpoint with too many concurrent requests. Such activity can slow down the service, leave an API unresponsive and, in many cases, lead to a denial of service of an endpoint.

It's critical that organizations implement or deploy technology that can provide rate limiting and other DoS mitigation functionality at layer 7 for web apps and APIs. Distributed Cloud WAAP 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 thresholds (number of requests allowed) with a duration (over a set period of time), and discrete HTTP 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, Distributed Cloud WAAP delivers robust layer 7 DoS attack detection and mitigation for web applications and APIs using a combination of techniques that includes alerts and blocking from traditional signature-based WAF functionality as well as anomaly detection and alerts from AI/ML. Machine learning happens in the centralized control plane, using metrics and log data collected from an organization's endpoints.

The visibility generated by this continuous analysis and baselining of web app and API behavior provides practitioners and organizations with the insights and alerting on anomalies, which can be used to generate layer 7 protection policies. There are a variety of remediation actions that can easily be put into place. These include rate limiting or deny listing based on IP address, region/country, ASN or TLS fingerprint, plus more advanced rules defining specific match criteria guiding app and API interactions with clients, including HTTP method, path, query parameters, headers, cookies, and more.

Combined, the rate limiting and layer 7 DoS functionality, along with behavioral AI/ML capabilities, of Distributed Cloud WAAP delivers a rich set of capabilities to keep web app and API endpoints free from abuse, running smoothly, and available to process requests.

Injection Attempts and Other App and API Vulnerabilities

Traditional WAF functionality still plays a huge role in the protection of modern applications 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.

Distributed Cloud WAAP includes a robust attack-signature engine containing nearly 8,000 signatures for CVEs, plus known vulnerabilities and techniques identified by F5 Labs. The service also includes threat campaign functionality which delivers protection against sophisticated, multi-vector attack campaigns by using fully vetted attack campaign signatures developed by F5 threat researchers. These signatures help protect organizations from a variety of injection attacks and other critical vulnerabilities and attack types, including DoS, bots, and automation, which are trying to exploit vulnerabilities that exist in the underlying code.

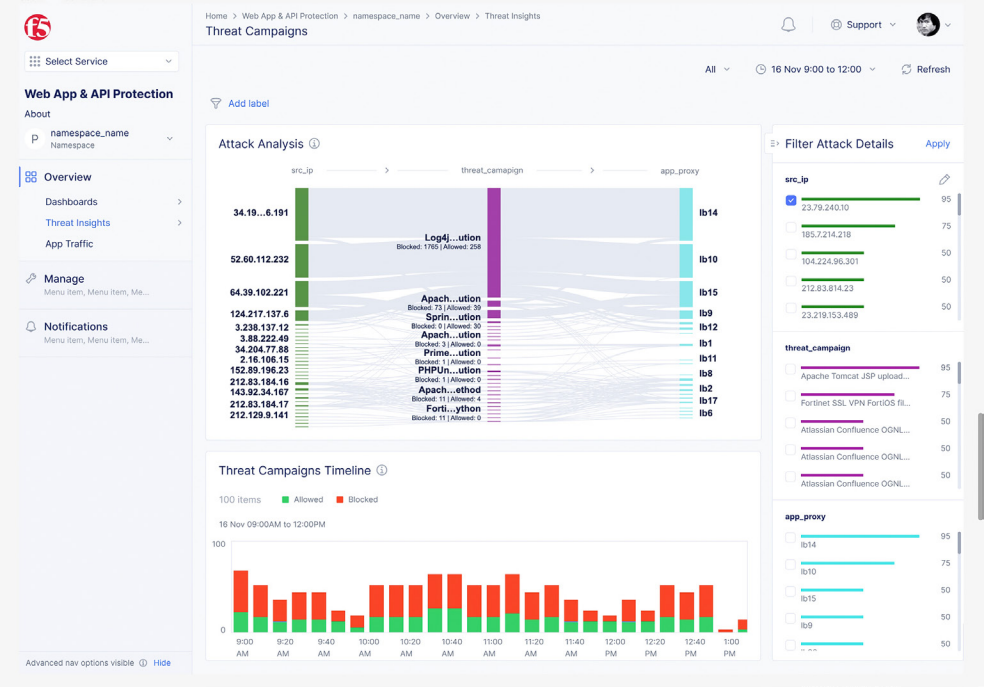

Figure 2: Threat Campaigns correlates singular attack incidents as extensive and sophisticated attack campaigns developing signatures to protect web apps and APIs from persistent attempts to exploit their code.

The WAF engine and Threat Campaigns are yet more elements that Distributed Cloud WAAP delivers to protect applications and their APIs from exploitation, tightening up critical vulnerabilities in code while development teams work to review, patch, and improve code over time.

Gaps in Access and Authorization of APIs

When it comes to handling access and authorization threats, Distributed Cloud WAAP 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 and the back-end systems and data they connect. The service learns, models, and maps all app and API endpoints, including the status and type of authentication present.

API Authentication Discovery identifies and baselines the authentication state of all APIs within an environment. The service can learn and document authentication types based on OpenAPI spec or their location within each API call, easily associating this data with app endpoints for analysis. Authentication information which is part of a known OpenAPI spec can be automatically enforced, and unauthenticated traffic can be stopped at very early stages, removing the need for origin API gateways to handle requests.

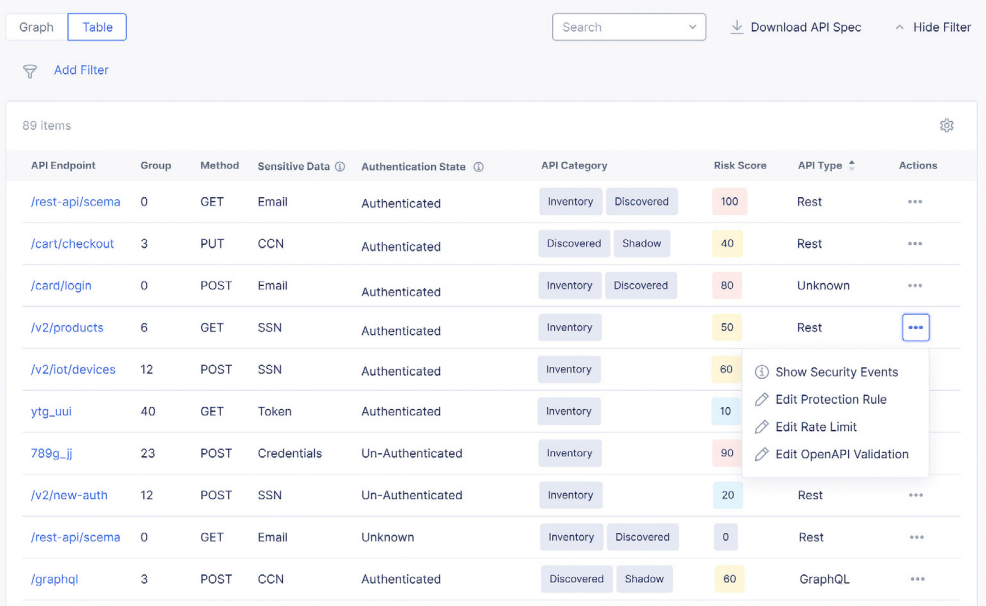

Figure 3: API Authentication Discovery and Validation—discover and view authentication status, details and risk score of all APIs including the ability to create protection or blocking rules.

In addition to this, for endpoints with JSON Web Token (JWT) authentication type, Distributed Cloud WAAP can evaluate existing authorizations within tokens. This further helps organizations understand the security of their API posture, enabling swift action to take place where and if gaps are identified. The service can discover and validate headers, payloads, and signatures within JWTs which may be indicators of compromise. It can detect user role or user ID, identifying sensitive data in JWT payloads, ultimately producing an API endpoint threat level and risk score, which can be used to guide remediation efforts to shore up insecure endpoints. The API threat level developed for JWTs is composed of a variety of inputs, including these potential vulnerabilities:

- Missing digital signature algorithm
- Expected signature algorithm is not enforced
- Inadequate JWT expiration policy
- Expired tokens are accepted
- Tokens with invalid signature are accepted
- Sensitive data found in JWT token

This discovery and analysis of authentication within API endpoints delivers remediation insights to organizations, so they can easily view the distribution of authentication types across API endpoints, including those endpoints where authentication isn't in place. The insights are delivered with rich filter and drill-down capabilities, so that operations and developer teams can act quickly react via existing API gateway(s) or with Distributed Cloud WAAP layer 7 policies to update authentication or block unauthenticated clients.

API Access Control

Another key element is the control of access to APIs, accomplished with import OpenAPI spec functionality and API protection rules (layer 7 policies). These are used to define a specific API endpoint, API groups or Base path, then set policies to enforce granular API access control, enabling implementation of a positive security model for applications and APIs. This includes preparation of OpenAPI spec files with discovered APIs, API definitions and groups which can be exported into an existing API gateway where authentication and enforcement can be applied and appropriate API behavior can be monitored. These capabilities help organizations ensure only API connections and client requests to operations that are specified in the OpenAPI spec file are allowed and all other requests, including those where users are trying to guess objects, parameters or other unspecified operations, are denied.

If there are applications with flaws in the design of their authentication for any of their APIs, Distributed Cloud WAAP with layer 7 application security policies can be configured as a proxy to allow or block requests, thereby preventing attempts to bypass access and authentication functions.

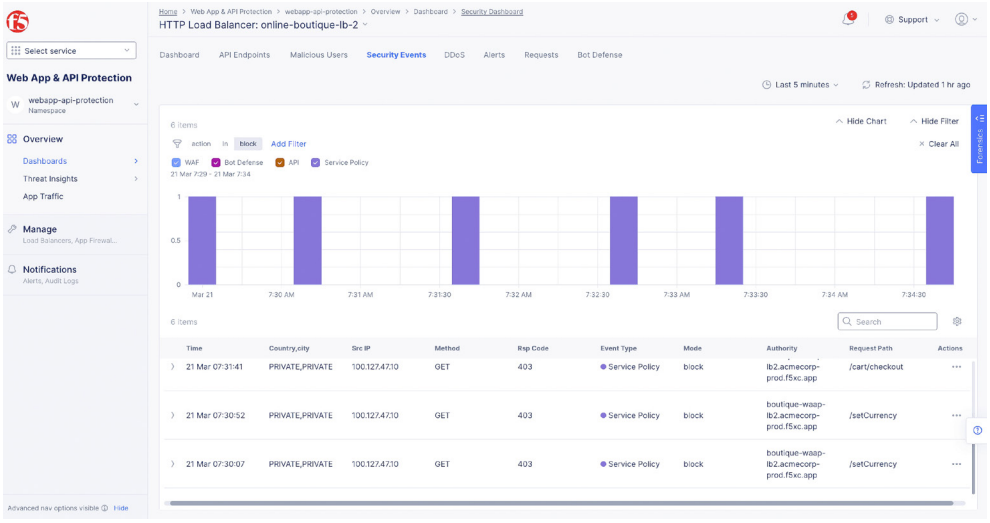

Figure 4: Protected API endpoint where request is returning 403 response code to client(s) who are not authorized to access.

Malicious User Detection and Mitigation

The final feature that supports access and authorization of applications and APIs is malicious user detection and mitigation, backed by the AI/ML. All client interactions, including those of APIs, are analyzed for an organization's applications over time, and outliers are identified. Then, each client is given a risk score (High, Medium or Low) based on all their interactions with a given app and API endpoints.

Based on a client's activities with respect to a set of problem categories, a client's threat level will rise or fall. The AI/ML engine learns client behavior from traffic generated across all endpoints in an organization's environment. There are various methods for malicious user detection, including forbidden activity via configured layer 7 protection policies (including HTTP methods, paths, query parameters, headers, and more), failed login attempts, WAF and threat campaigns signatures, IP reputation database triggers, and invalid or nonexistent URL/request activity (404 not found response codes).

When it comes to API security and protecting against unauthorized access via APIs, either through credential stuffing, brute force, or other forceful login attempt mechanisms, the AI/ML engine can help by identifying failed login attempt activity or attempts to discover API parameters, and flag that to operations teams. The feature keeps track of the number of login attempts that have failed (specifically 401 unauthorized response codes) for all clients. When the number of login failures from a client exceeds the limit set, and/or there is a large spike based on historical, learned behavior, the client will be classified as malicious and can be blocked.

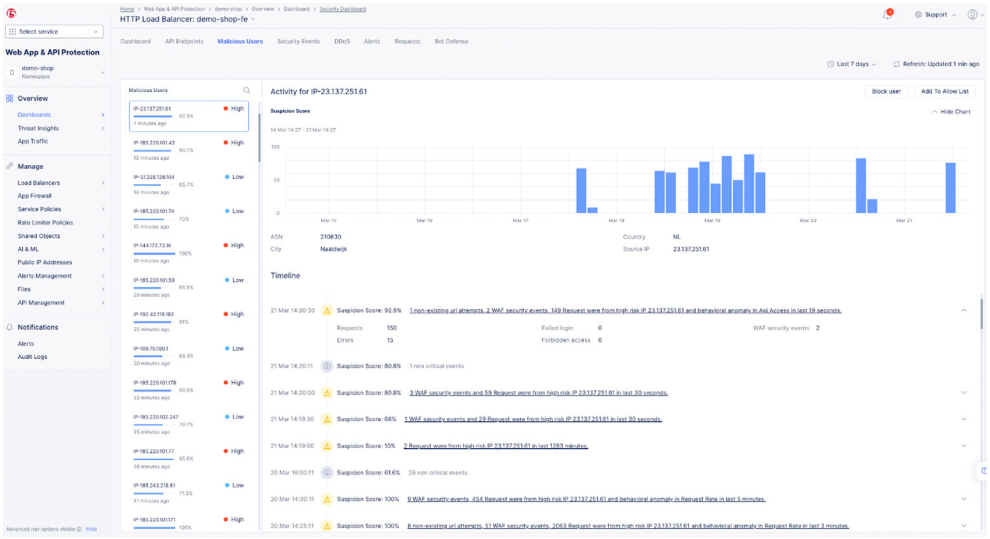

Figure 5: Malicious User functionality—correlates WAF events, abnormal API access behavior, failed login attempts, and so forth, for app and API endpoints, flagging these for operations teams with the ability to quickly take action including block/allow list, rate limit, and more.

Distributed Cloud WAAP can help organizations shore up API security, including validating connections and access, monitoring and alerting on behavior over time, and helping to identify unusual client behavior to pinpoint potential areas of compromise. Not only will the service test and report on API authentication mechanisms and potential access issues, but it includes critical enforcement mechanisms to easily act (block/allow/limit) against unwanted client or API activity quickly. The service can play a huge role in modern application security by augmenting the efforts of API gateways in controlling client interactions and enforcing appropriate access to API endpoints.

Improper Asset Management and Security Misconfiguration

Another critical component of API security is ongoing management of APIs. This can take many forms. Some of this is handled by API gateways, but modern web app and API protection capabilities are necessary to aid in this, as modern applications driven by APIs can be very dynamic with quick and rapidly evolving development cycles. It can be hard for operations, security, or IT teams to keep up, as modern apps with APIs tend to expose more endpoints than traditional web applications, making well-documented and ongoing hygiene of APIs important. Properly documented and deployed API versions, inventory management, and tracking, plus API discovery, play an important role in protecting an organization and mitigating issues such as old, deprecated APIs or API versions, and unknown or shadow APIs. Distributed Cloud WAAP allows organizations to easily deploy and enforce a positive security model when it comes to API security. This ability, combined with rich web app and API path discovery, helps identify, model, and baseline unknown or undocumented APIs.

Positive Security with Import and OpenAPI Spec Validation

Organizations can leverage Distributed Cloud WAAP to enforce proper API behavior based on valid API definitions through imported OpenAPI specs. Documented API characteristics are used 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 the spec file.

Dynamic API Endpoint Discovery and Schema Learning

Not all APIs are known or well documented. As a result, it's imperative for organizations to be able to continuously discover and monitor all web app and API endpoints that are present in their environments. Dynamic API endpoint discovery and schema learning is also part of the service. This enables markup and analysis of API endpoints for applications, including authentication status, determining which API paths are communicating with all application endpoints and the authentication state of their APIs. This can augment what is already known as part of an existing OpenAPI spec to update legitimate API endpoints or to uncover unknown/shadow APIs that don’t have the benefit of OpenAPI spec documentation.

Behavioral Analysis Through Machine Learning

Distributed Cloud WAAP has the capabilities to discover and perform behavioral analysis on the various logs collected from endpoints and APIs of an application using ML. The schema structure of APIs and authentication elements is learned by analyzing sampled request and response data examples for each API. This provides learning of the behavior of these paths, including request and response schemas and sensitive data detection. The discovery and mapping capability shows the complete inventory of learned application and API paths, including shadow sets, with development of an OpenAPI spec for exporting and usage by development teams. Downloaded OpenAPI spec files for learned API schemas can be rendered at a variety of levels, including HTTP load balancer, app type and per API. The file is an exportable JSON file.

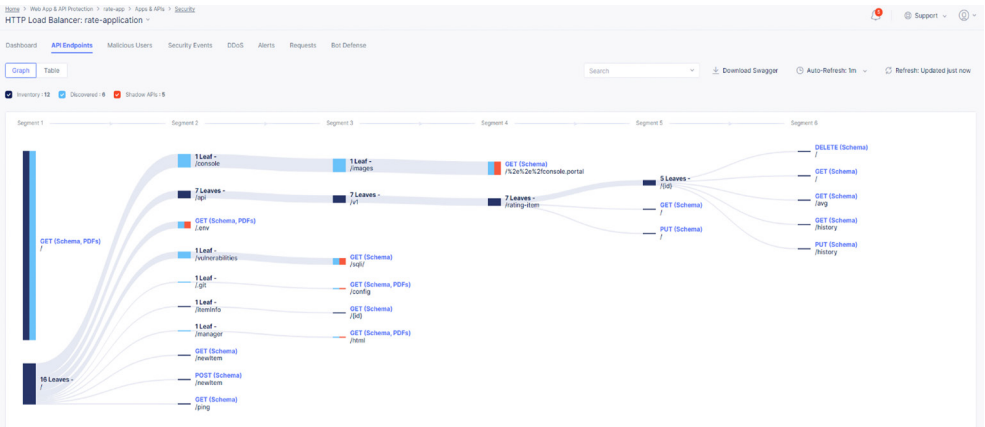

Figure 6: Learned app and API path visualization includes Inventoried APIs, Discovered APIs and Shadow APIs. The endpoint paths are shown in a hierarchical structure with root and leaf relationships presented in segments.

As application paths and API endpoints are discovered and monitored, probability distribution functions related to each endpoint are generated for metrics such as request size and response size, latency with and without data, request rate and error rate, and response throughput. Analysis is performed periodically, and these baseline metrics are updated. Learning of the API endpoints and associated metrics is incremental in nature and updated periodically. This visualization and the corresponding metrics can be used to create layer 7 security policies to control access to and functions of APIs. These resulting rules can be applied to all APIs, including unknown/shadow APIs, to block or limit activity.

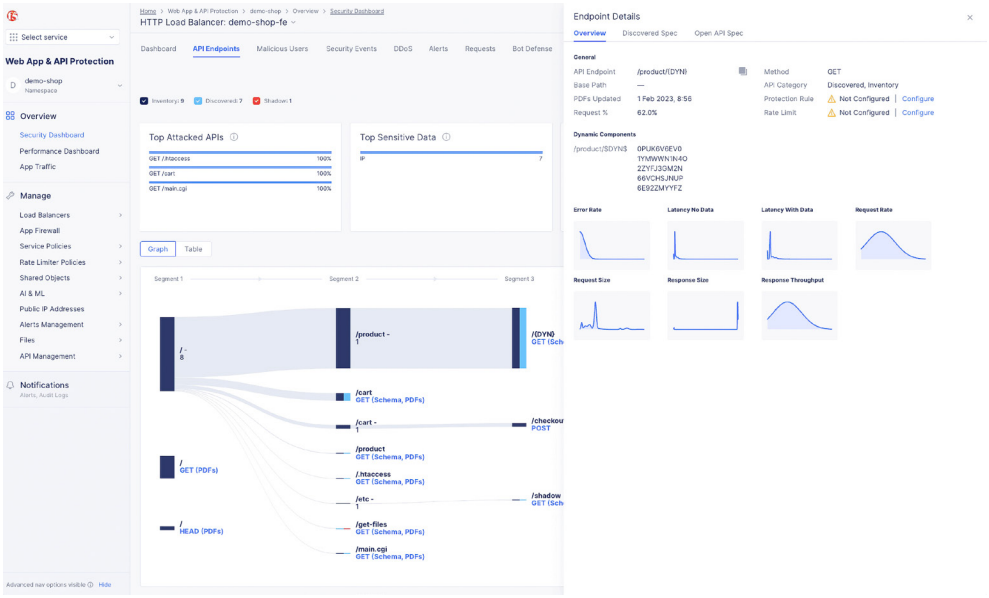

Figure 7: Endpoint details include metrics such as request size and response size, latency with and without data, request rate and error rate, and response throughput.

There are a variety of rule types that can be applied to web application paths and APIs when using Distributed Cloud WAAP. They include:

- **Protection rules for APIs (allow/deny, rate limit, and more)—**allow/deny or rate limit API endpoints, using API endpoint path and method(s) for applying protection rules
- **Update/configure API request parameters—**HTTP query parameters, HTTP headers, web cookie and/or TLS fingerprint match criteria/parameters to limit functionality of specific API endpoints
- **IP reputation—**client access can be allowed/denied based on IP reputation categories—all F5 categories, specific groups, or individual IPs—so organizations can select options to match by IPv4 prefix, IP prefix, ASN list, or BGP ASN sets

Not only can organizations easily discover unknown or shadow APIs, as well as upload and enforce positive application and API security, but Distributed Cloud WAAP can deliver more holistic visibility with a comprehensive API endpoints dashboard. This includes all discovered and imported API endpoints for each domain, with views into Top Attacked APIs, Top Sensitive Data, Total API Calls, Most Active APIs, plus threat scores for each API endpoint in a given domain. This centralized view allows operators or engineers to move quickly, identifying potential issues within their API environment, with the capability to easily drill down, investigate, and take action as appropriate to neutralize any anomalies or threats that could impact connectivity, availability, or app and API security.

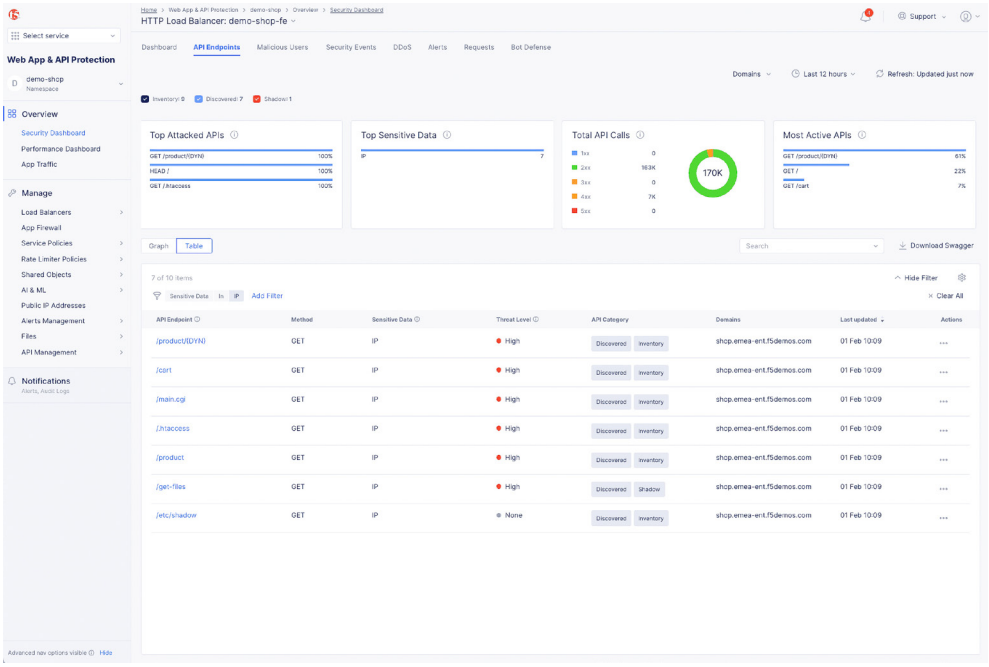

Figure 8: API endpoints dashboard—all discovered and imported API endpoints for each domain with views into Top Attacked APIs, Top Sensitive Data, Total API Calls, Most Active APIs plus threat scores for each API endpoint in a given domain.

Conclusion

Deliver superior digital experiences with performant, effective, and scalable application and API security with F5 Distributed Cloud WAAP

Applications and increasingly APIs 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 WAAP 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.

With Distributed Cloud WAAP, organizations benefit from comprehensive application and API security to more effectively secure and manage APIs, helping drive business velocity by enabling extensive, modern application and API deployments with the necessary management and protection against API-specific threats. Organizations can seamlessly augment existing API management and gateway functionality to secure API vulnerabilities, access, and authentication gaps, enabling API security for all critical threat categories. With Distributed Cloud WAAP, customers can pair rich API discovery and mapping to identify unknown or shadow APIs, with the necessary enforcement tools, in one global, SaaS-delivered solution.

This innovative and accessible service helps reduce app and API security gaps and enables consistent coverage across an organization's entire application portfolio. With Distributed Cloud WAAP, organizations can simplify their path to effective security while fostering the innovation their business and customers demand.

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

DC 04.2023 | WP-X-PILLAR-1064838504-xc-api-security-technical-whitepaper