Solution Overview

How to Discover, Test and Continuously Monitor APIs

Multiple lenses of API discovery is a critical element of F5 Distributed Cloud API Security, dramatically improving API visibility, delivering continuous oversight, and identification of APIs.

It is widely recognized that you cannot protect what you cannot see, get a handle on your APIs today.

In today's rapidly evolving digital landscape, organizations are increasingly reliant on APIs to drive innovation, enhance connectivity, and streamline operations. In F5's latest research we found that 41% of organizations are managing at least as many APIs as apps today. As businesses integrate a multitude of APIs—both internal and external—into their apps and systems, the complexity of understanding, managing and securing these interfaces grows exponentially.

Not all APIs are known or well documented leaving many organizations flying blind. Within many organizations there may be multiple teams developing services and APIs across an increasingly diverse, distributed set of environments. As modern app environments grow more complex, and the number of APIs grows, it's imperative for organizations to keep up, ensuring they have a consistent and complete understanding of their API endpoints, and risks associated with the critical data and business processes these interfaces support.

They should be striving to get this visibility as early in the software development lifecycle as possible, before apps and APIs are released into production, limiting the exposure time of vulnerabilities and any sensitive data. Organizations should look to maintain centralized, continuous discovery, consistent documentation and monitoring of all web app and API endpoints that are present in their environments. This serves as the starting point for a complete, full API lifecycle security solution.

From Code Through Production, Seamlessly Discover, Document and Test APIs

API discovery forms the baseline of security for APIs. It helps organizations understand their complete threat surface, helping them stay on top of their APIs, as software development cycles continue to evolve. Having complete visibility and documentation, allows for consistent, continuous testing and monitoring which is paramount to stay on top of the constantly changing threat surface and the blind spots created by the new and evolving API endpoints.

With F5 Distributed Cloud API Security organizations get this complete visibility and insights into their APIs, paired with continuous API testing, and the ability to act through the implementation of API specific security controls. This includes discovery from code, dynamic API discovery from application traffic and client-side web crawling with automatic OpenAPI spec file generation. Organizations can easily enable code-based discovery across various developer repositories to scan, map and document their APIs and any vulnerabilities earlier in the development lifecycle.

Key Benefits

Improve API Visibility
Single, centralized console for identification and monitoring of all API endpoints including anomalous or malicious activity.

Reduce Exposure of API Vulnerabilities
Begin discovery, testing and monitoring of APIs earlier, improves visibility and understanding of vulnerabilities, so exposure can be limited.

Limit Data Loss
Better understand and monitor for sensitive data being exposed by APIs including PII and critical compliance related sensitive data types.

Reduce Time Documenting APIs
Automatically learn and continuously generate OpenAPI spec (OAS) files for all APIs to minimize manual tracking.

Complete and Precise API Inventory
Easily manage API inventory–providing a more accurate view into all endpoints, streamlining application of security policies and controls across the right API endpoints.

41% of organizations today say they are managing as many APIs as they are apps.

–F5 State of Application Strategy Report 2024

Key Features

Code Analysis and Discovery

Integrates with common code repositories including BitBucket, GitHub, GitLab and more to automatically scan, learn and map APIs.

Crawler Based Discovery

Automatically crawls external domains to detect and scan for exposed API endpoints.

Traffic Based Discovery

Analyzes API requests and responses in production to automatically learn and map APIs.

API Testing

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

Automatic API Documentation

Learns and automatically generates OpenAPI spec files from code and traffic, which can be used to enforce positive security and exported to improve source code.

Sensitive Data Detection

Discovers and maps data being exposed via APIs including common PII, hundreds of data types relevant to critical compliance frameworks (e.g. PCI-DSS, HIPAA, GDPR etc.) and custom sensitive data patterns.

Rich API Monitoring and Visualization

Identify the most used and attacked API endpoints, usage patterns including behavioral anomalies, plus any sensitive data, to inform response and optimize controls and security policies for APIs.

Inventory Management

Seamlessly group and tag discovered APIs, move endpoints to and from inventory, helping maintain a clearer picture of the API landscape.

Traffic-based discovery is also an option, which will analyze production traffic, looking at API requests and responses. And finally, intelligent web crawling which represents a third discovery mechanism that will intelligently and automatically crawl any web based application from the client-side—filling in any gaps that code or traffic analysis might not capture. When combined, these three different lenses into APIs with API testing helps form a more complete picture of any organizations API threat surface, including uncovering unknown (shadow APIs), unused (Zombie APIs) and any other discrepancies in their APIs including old or deprecated endpoints, versioning issues, anomalous behavior and vulnerabilities. All of this helps organizations manage their API inventory, identify and act on suspicious activity and weaknesses in API security, including unauthorized access, issues with authentication, identification of unintended sensitive data and personal identifiable information (PII) exposure and misconfiguration.

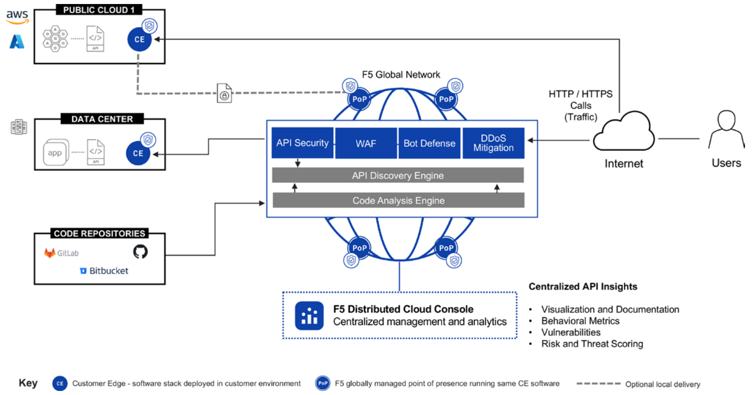
aws
PUBLIC CLOUD 1
CE
DATA CENTER
app
CE
CODE REPOSITORIES
GitLab
Bitbucket
F5 Global Network
PoP
PoP
PoP
PoP
API Security
WAF
Bot Defense
DDoS Mitigation
API Discovery Engine
Code Analysis Engine
HTTP / HTTPS Calls (Traffic)
Internet
Users
F5 Distributed Cloud Console
Centralized management and analytics
Centralized API Insights
• Visualization and Documentation
• Behavioral Metrics
• Vulnerabilities
• Risk and Threat Scoring
Key
CE Customer Edge - software stack deployed in customer environment
PoP F5 globally managed point of presence running same CE software
Optional local delivery

Figure 1: Easily combine code-based discovery across various developer repositories with continuous traffic analysis and intelligent web crawling to form a complete picture of any organizations APIs regardless of where and how the apps are deployed.

The service allows organizations to visualize and monitor usage over time for various metrics such as request size and response size, latency, request and error rates, and response throughput creating critical benchmarks used for behavioral analysis. The discovery and learning of the API endpoints and associated metrics is continuous, helping to maintain constant, reliable oversight of all endpoints. This visualization and the corresponding metrics are critical to helping organizations identify anomalies and changes in behavior over time, which may be indicators of potential attacks, or compromise. These baselines can also be used to inform, the implementation of layer 7 API protection policies to control access to and limit API functionality.

With these discovery capabilities comes critical inventory management functionality allowing organizations to seamlessly group and tag APIs plus move individual endpoints to and from inventory. They can effortlessly promote discovered or shadow API endpoints into a centralized inventory, while discoveries can quickly be marked as "non-API" when mistakenly detected and removed from inventory. This helps organizations maintain a clean and precise inventory, painting a more complete picture of their API threat surface—making it easier to manage the application of protections and controls applied to their APIs.

Properly documented and deployed API versions, inventory management, and tracking, plus continuous API discovery and testing from code through production play an important role in protecting organizations–mitigating API vulnerabilities and securing sensitive data.

Conclusion

As organizations increasingly leverage modern applications to drive innovation, the applications themselves enabled by APIs grown more dynamic and with rapidly evolving development cycles, it can be hard for operations, security, development and IT teams to keep up. Modern apps with APIs are exposing more endpoints that change more rapidly than traditional web applications, which makes having well-documented, on-going visibility and hygiene of APIs important. Properly documented and deployed API versions, inventory management, and tracking, plus robust, continuous API discovery and testing from code into production, play an important role in protecting an organization and mitigating API vulnerabilities, securing sensitive data or dealing with unknown, outdated, and deprecated APIs. All of which represent risks to any organization.

F5 Distributed Cloud API Security can help do just that with complete API discovery–providing a continuous, comprehensive view of all active endpoints their interactions, dependencies, and vulnerabilities giving organizations a roadmap to controlling and protecting their APIs–filling critical gaps in their security posture. The visibility that can be achieved with this insight not only helps in maintaining efficient operations and ensuring security, but also aids in identifying opportunities for optimization of and hardening of code and continued innovation. By adopting a robust API discovery solution, organizations can continue to stay agile, while reducing risk, and unlocking the full potential of their new, modern apps and evolving digital ecosystem.

Try the interactive demo or check out the website.