



API Security Radically Simplified

ProtectOnce's mission is to empower organizations to safely build, test, operate, and protect all of their APIs with radical simplicity.



API security that just works

1. API Security Complexities

Modern API-driven applications are extremely complex and ever-changing. While APIs fuel growth and development speed, they expose the business logic of the application and make it a prime asset for attackers to target. Legacy WAFs are not enough, while modern solutions are too complex and expensive to run.

2. What makes ProtectOnce different



Full lifecycle API security

Testing, inventory, posture management, threat detection and response.



Built for taking action

easy to customize response playbooks allows you to create security workflows in minutes and take remediation action.



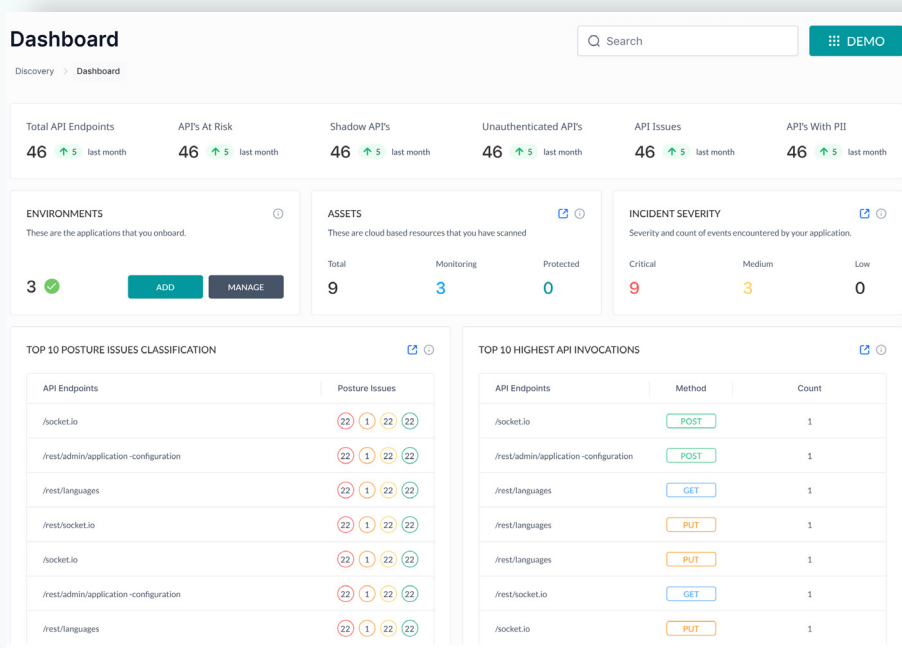
Agentless, automated deployment

ProtectOnce handles the complexities of deployment, so you don't have to.



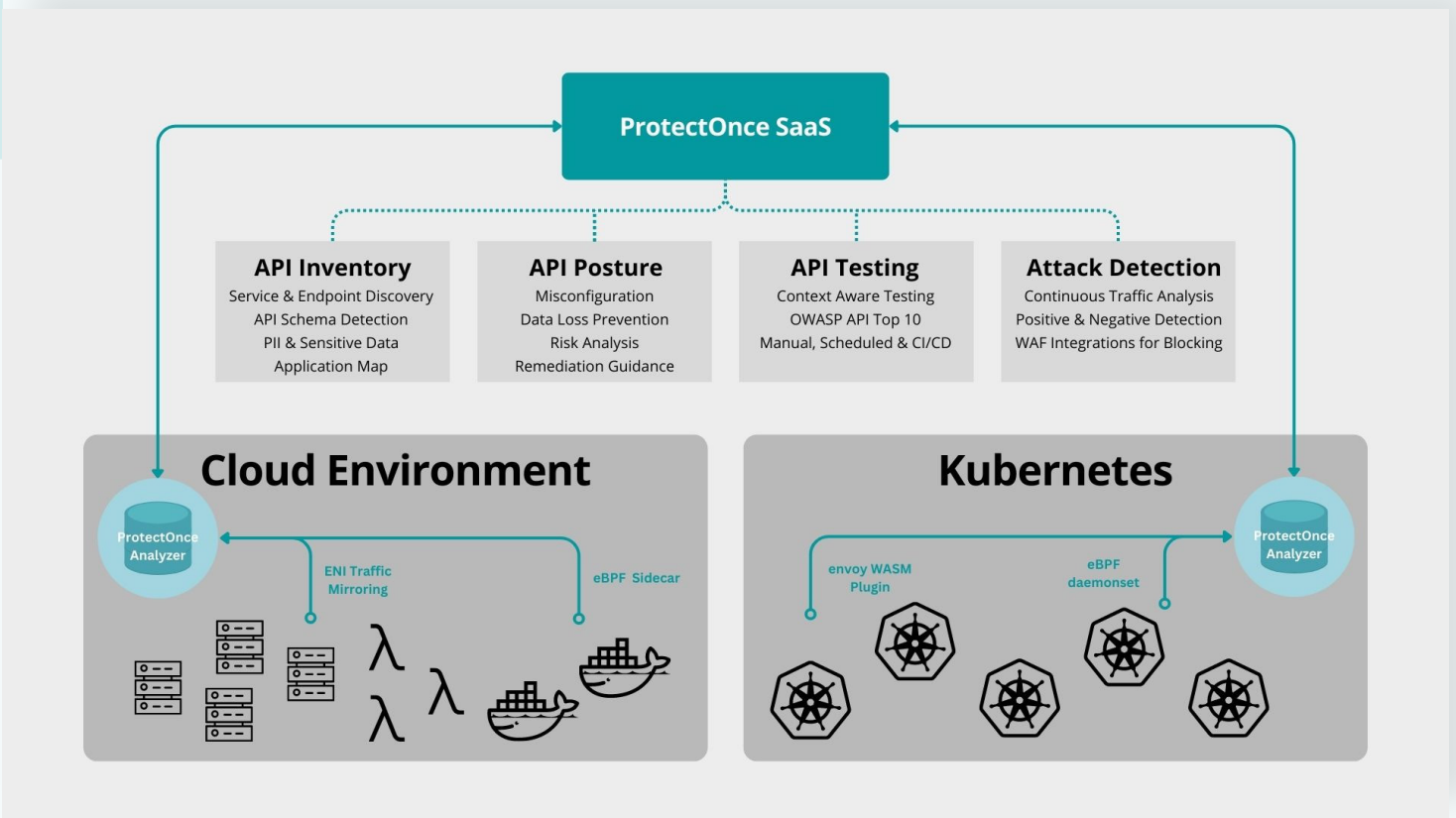
API Testing done right

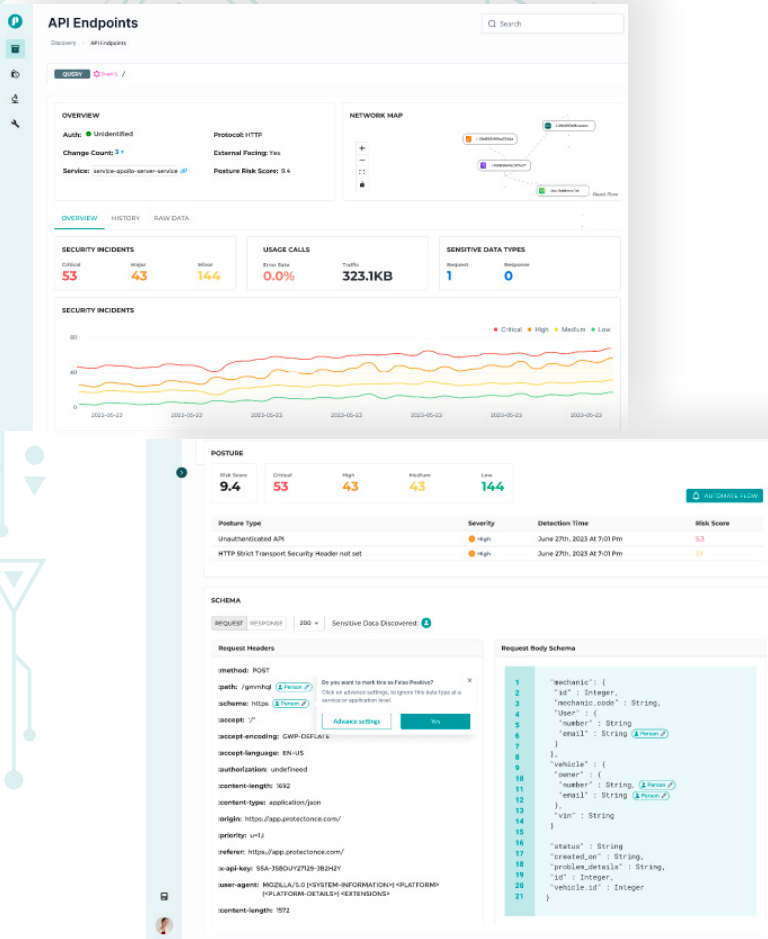
ProtectOnce is the first solution to use runtime discovery data to automatically craft test cases that are specific to your environment.



The ProtectOnce Platform

Our platform is specifically designed to provide the four essential functions that enhance your current API security, monitoring, and management systems. No matter the location or method of hosting your applications, ProtectOnce offers comprehensive protection that extends from your code to cloud.





1. API Discovery & Inventory

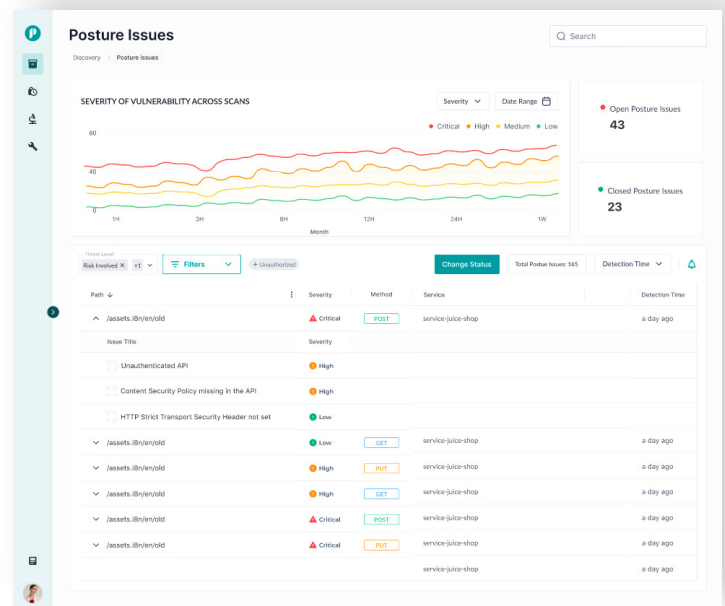
API endpoints change rapidly at certain parts of the application lifecycle, and security teams need a way to know what the up to date inventory is.

- Discover and catalog all your APIs, regardless of their setup or kind, such as RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC.
- Identify which APIs are able to access sensitive data.
- Identify inactive, outdated, and so-called zombie APIs.
- Pinpoint shadow domains and drift from your official API schema.

2. API Security Posture Management

Basic API misconfigurations can render you vulnerable to cyberattacks. Once hackers breach your defenses, they can easily obtain and steal your confidential information. Utilize our platform to:

- Run automatic scans of your infrastructure to detect misconfigurations and concealed risks.
- Develop tailored workflows to alert relevant stakeholders about vulnerabilities.
- Allocate severity levels to identified problems to streamline the prioritization of fixes.
- Leverage playbooks to automate actions



3. API Attack Detection & Response

The question isn't if your organization will face an attack, but when. This necessitates the ability to identify and halt attacks as they happen. Employ our AI/ML-driven anomaly detection system to:

- Detect complex API attacks such as Broken-Object-Level-Authentication with ProtectOnce's advanced threat detection.
- Go beyond OWASP top 10 to identify and block threat actors leveraging AI
- Agentless and out of band - ProtectOnce's applies real time detection will never interfere with your app's performance..
- Respond to security events using the platform's easy to customize security playbooks.
- Integrate with existing workflows (ticketing, SIEMs, etc) to alert security/operations team

The image shows two screenshots from the ProtectOnce interface. The top screenshot, titled 'Security Events', displays a table of security incidents. The bottom screenshot, titled 'Detect & Respond', shows a configuration page for various security playbooks.

Status Code	Path	Method	Activity Type	OWASP Category	Environment	IP Address	Date
200	/cart	GET	Sqli Injection	API10:2023 - Unsafe Consumption of APIs +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
200	/cart	POST	Mass Assignment	API10:2023 Broken Object Property Level Auth... +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
200	/api/v3/user/rid	DELETE	Web Tempering	API10:2023 Broken Function Level Authorization +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
200	/ftp	GET	Unauthenticated Api	API10:2023 - Unsafe Consumption of APIs +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
200	/cart	GET	Sqli Injection	API10:2023 - Unsafe Consumption of APIs +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
200	/api/v3/me/	GET	Cors Misconfiguration	API10:2023 Security Misconfiguration +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
200	/api/v3/me/	GET	Shell Injection	API10:2023 - Unsafe Consumption of APIs +1	DEFAULT_WORKLOAD	106.210.152.194	10 days ago
304	/api/v3/store/order/rid	GET	Web Tempering	API10:2023 Broken Function Level Authorization +1	DEFAULT_WORKLOAD	157.32.79.38	10 days ago
304	/api/v3/store/order/rid	GET	Web Tempering	API10:2023 Broken Function Level Authorization +1	DEFAULT_WORKLOAD	157.32.79.38	10 days ago
304	/api/v3/store/order/rid	GET	Web Tempering	API10:2023 Broken Function Level Authorization +1	DEFAULT_WORKLOAD	157.32.79.38	10 days ago
500	/api/v3/user	POST	Sqli Injection +1	API10:2023 - Unsafe Consumption of APIs +1	DEFAULT_WORKLOAD	62.225.226.579	10 days ago
500	/api/v3/user	POST	Sqli Injection +1	API10:2023 - Unsafe Consumption of APIs +1	DEFAULT_WORKLOAD	62.225.226.579	9 days ago
200	/api/admin/console/ping/rid	GET	Shell Injection	API10:2023 - Unsafe Consumption of APIs +1	7fad00e-e639-4e4e-9f0c-c6b08aa0055	154.138.44.973	7 days ago

NAME	CATEGORY	STATUS	MANAGE
spec-analysis-playbook	Specification Analysis	<input checked="" type="checkbox"/>	<input type="checkbox"/>
change-api-playbook	API Drift	<input checked="" type="checkbox"/>	<input type="checkbox"/>
posture-issues-playbook	Posture Issues	<input checked="" type="checkbox"/>	<input type="checkbox"/>
incident-playbook	Security Incident	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4. AI Powered API Security Testing

Shifting left is an integral part of API security. Some risks can't accurately be detected by posture analysis in runtime and sometimes, its just too late

- Unique 'purple team' approach uses runtime detected inventory and schema to dynamically craft test cases
- Automatically run tests that simulate malicious traffic, including the OWASP API Top 10
- Discover vulnerabilities before APIs enter production and reduce the risk of a successful attack
- Use mitigation information that helps patch vulnerabilities.
- Seamlessly integrate API scans and retests within CI/CD and progress towards shift left security.

The image shows a 'VULNERABILITY REPORT' interface. It lists various security issues on the left, with 'SQL Injection' highlighted. On the right, it shows details for the 'Owasp Category: API10:2023 Unsafe Consumption of APIs', including a table of vulnerable endpoints and a bar chart for 'RE-RUN STATISTICS'.

Path	Method	Status Code	Response Time
/api/Users	POST	201	34 ms
/api/Users	POST	201	57 ms
/rest/user/login	POST	200	34 ms

The image shows a detailed view of a 'SQL Injection' vulnerability. It includes a description, mitigations, and an impact statement.

Description
A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

Mitigations

1. Ensure that all user inputs are being sanitized and malicious characters are stripped with the help of a well known and maintained library.
2. Make use prepared statements with parameterized queries and stored procedures wherever applicable.
3. Ensure that the user account connected to the database is provisioned with the least privileges required.

Impact
An SQL injection allows an attacker to manipulate SQL queries being run by the server; potentially leading to exploitation of sensitive information or information being tampered in the database depending on the context of the query.

About ProtectOnce

As a group of SaaS developers and cyber security entrepreneurs, application & API security has always been a pain point.

In today's cloud-native world, developing and deploying web applications is easier than ever, however properly securing them has never been more complex.

This is why we built ProtectOnce. We believe that quality API security should be accessible to all companies, big and small, without having to invest endless resources and manpower. With ProtectOnce, growing SaaS companies can get API visibility, discoverability and protection for free, with an automatic, out-of-the-box approach.

Start for free:

app.protectonce.com/signup



ProtectOnce