RitAPI

Real-time AI Defense
Stopping API Attacks in Milliseconds

BY

IT Security is
Our Main Concern

Sydeco

Introduction

APIs are the engine of modern business. They connect your services, empower your developers, and drive your growth. But as their importance grows, so does the risk. Attackers are no longer just knocking at the front door; they're exploiting the intricate connections your APIs create. Yesterday's security, built on static rules and manual tuning, simply can't keep up, leaving you exposed to data breaches, service disruptions, and brand damage.

It’s time for security that operates at the speed of your business—intelligent, automated, and built for the API economy.

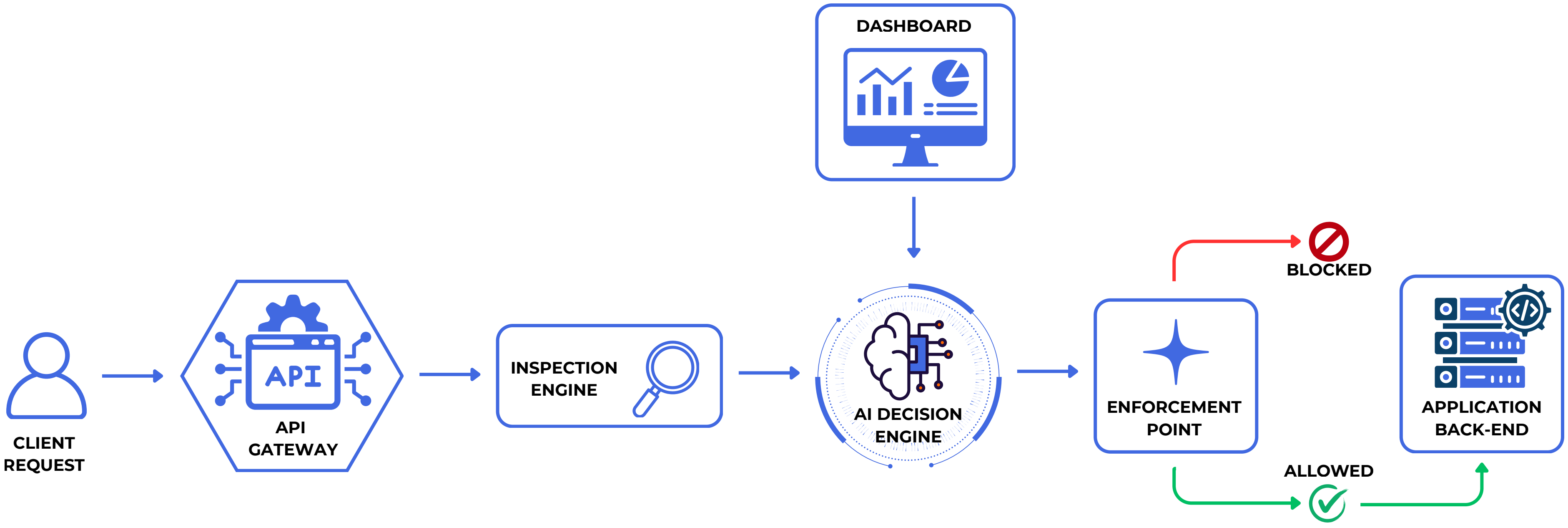
Meet RitAPI

RitAPI is a next-generation API security platform built for real-time protection. Using advanced machine learning, it inspects every API call, detects hidden anomalies, and blocks threats instantly—within a single millisecond. Unlike reactive tools, RitAPI offers proactive defense against both known and emerging attacks, ensuring your APIs stay secure, reliable, and always available.

Architecture

RitAPI's architecture is designed for maximum performance, scalability, and ease of integration. It operates as a seamless layer in your existing environment, providing robust security without introducing complexity or performance bottlenecks. The data flow is simple and effective.

1. **Inspection Engine**: Deployed as a lightweight agent, the Inspection Engine passively captures and normalizes API traffic without impacting performance. It reconstructs the full request context, including headers, payloads, and parameters.
2. **AI Decision Engine**: The normalized data is streamed to our core AI engine. This is where advanced machine learning models, trained on trillions of data points and fine-tuned on your specific traffic patterns, analyze behavior in real-time. It detects subtle anomalies that signal an attack.
3. **Enforcement Point**: When the AI engine identifies a threat with high confidence, a decision is sent to an enforcement point at the edge (e.g., API Gateway, load balancer, or the agent itself) to block the malicious request before it reaches your application.
4. **Dashboard & Analytics**: All events, legitimate and malicious, are logged and visualized in a comprehensive dashboard. Security teams get deep insights, actionable intelligence, and the ability to fine-tune policies without writing complex rules.



Detection Methods

RitAPI moves beyond signature-based detection to provide holistic, behavior-based protection against a wide spectrum of API attacks.

- **SQLi/NoSQLi Injection**: Detects attempts to manipulate backend database queries through malicious payload injection in parameters or JSON bodies.
- **Brute Force & Credential Stuffing**: Identifies anomalous login attempt rates and patterns, automatically blocking suspicious IP addresses or users targeting authentication endpoints.
- **Broken Authentication & Token Replay**: Our engine understands the context of authentication tokens (like JWTs) and can detect attempts to reuse stolen tokens or bypass authentication logic.
- **Zero-Day Attack Prevention**: This is the core strength of our AI engine. By establishing a baseline of normal API behavior, RitAPI can detect novel, never-before-seen attack patterns as deviations from that baseline, providing proactive defense against emerging threats.

Adaptive Learning

RitAPI’s models are not static. The system continuously learns from your unique API traffic patterns. This adaptive learning process dramatically reduces false positives over time, ensuring that legitimate user requests are never blocked while hardening defenses against genuine threats.

Performance Benchmarks

Security should be an enabler, not a bottleneck. RitAPI is engineered from the ground up for high-throughput, low-latency environments.

Tier	Throughput (requests/sec)	Added Latency (p99)	Description
RitAPI Guard	Up to 25,000 req/s	< 2ms	Ideal for high-performance microservices.
RitAPI Advanced	Scalable to 50,000+ req/s	< 2ms	For enterprise-grade, high-traffic API gateways.

Example Policy Snippet

While RitAPI works autonomously out-of-the-box, security teams can easily define custom rules in a simple, declarative format. This allows you to tailor enforcement actions based on the AI's confidence score.

Here is an example of a policy that blocks any request the AI flags as anomalous with a confidence score above 85%:

```
rule:
    name: block_high_confidence_anomalies
    type: anomaly_detection
    action: block
    confidence: >0.85
```