

API SECURITY.

Every API is a direct line into application logic and data — **unauthenticated, unmonitored, or undocumented endpoints turn that convenience into an open door** for attackers to walk through.

- AUTHENTICATION & AUTHORIZATION
- RATE LIMITING
- SCHEMA VALIDATION
- API DISCOVERY

01 THE MECHANISM

Authentication & Authorization
Verifying caller identity and enforcing **what each token or key is allowed to access.**

Rate Limiting & Abuse Detection
Capping request volume and flagging **patterns that look like automated abuse.**

Schema Validation & Discovery
Enforcing expected input formats while **mapping every endpoint, including shadow APIs.**

02 THE FLOW

The Request Cycle CONTINUOUS

1

A caller presents credentials that are **authenticated and checked for scope.**

2

The request is validated against the **expected schema and rate limits.**

3

Traffic and responses are logged for **ongoing monitoring and anomaly detection.**

The Abuse Cycle LIVE EVENT

1

An attacker probes endpoints for **weak auth or missing input validation.**

2

Automated requests exploit a flaw **to scrape data or bypass business logic.**

3

The activity is detected, the endpoint is patched, and **access is revoked or rotated.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Authentication & Authorization	Confirms caller identity and restricts access to permitted scopes.
Rate Limiting	Caps request volume to prevent abuse and resource exhaustion.
Schema Validation	Rejects malformed or unexpected input before it reaches application logic.
API Discovery	Inventories every endpoint, including undocumented and shadow APIs.

04 API SECURITY APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Network Firewall Alone	No	Doesn't inspect API-layer logic or authentication flaws.
API Gateway Without Validation	No	Routes traffic but doesn't verify schema or intent.
Documentation-Only Inventory	No	Misses shadow APIs never added to the official catalog.
Static Code Review Alone	No	Doesn't catch runtime abuse or credential-based attacks.
API Security (Auth + Rate Limiting + Validation)	Yes	Verifies every caller, request, and endpoint continuously.

API SECURITY.

AUTHENTICATE · LIMIT · VALIDATE

05 PROGRAM OPERATIONS

Shadow APIs outnumber documented ones.

Undocumented endpoints ship constantly and rarely get security review.

Authentication isn't authorization.

A valid token doesn't mean the caller should reach every resource.

Rate limits need per-endpoint tuning.

A single global threshold misses abuse on sensitive, low-traffic endpoints.

Third-party integrations inherit risk.

A partner's compromised key becomes your exposure too.

06 CONTROL MAPPING

OWASP API TOP 10

Baseline risk categories specific to API-layer vulnerabilities and abuse.

NIST SP 800-204

Microservices security guidance for cloud-native, API-driven architectures.

PCI DSS

API access controls required wherever APIs touch cardholder data.

ISO 27001

Access control policies extended to machine-to-machine interfaces.

07 WHAT THIS DOES NOT SOLVE

Business logic flaws

Validated requests can still abuse legitimate functionality in unintended ways.

Third-party API risk

Securing your own APIs doesn't cover vulnerabilities in partner or vendor endpoints.

Credential compromise

A leaked or stolen API key looks identical to legitimate traffic.

Data exposure by design

Overly permissive responses leak data even when every control passes.

08 MYTHS VS. REALITY

MYTH	REALITY
"APIs behind a gateway are already secure."	Gateways route traffic; they don't validate business logic or intent.
MYTH	REALITY
"Internal APIs don't need the same scrutiny."	Internal APIs are a common lateral-movement path once inside.
MYTH	REALITY
"If it's not documented, it's not a risk."	Shadow APIs are often the least monitored and most exposed.
MYTH	REALITY
"Rate limiting alone stops abuse."	Attackers distribute requests to stay under the threshold.
MYTH	REALITY
"API keys are as safe as passwords."	Keys are often long-lived, over-privileged, and rarely rotated.

09 SPEAK THE PROGRAM — KEY TERMS

API

Application Programming Interface: a defined way for systems to exchange data.

SHADOW API

An endpoint that exists and runs but isn't documented or tracked.

RATE LIMITING

Restricting how many requests a caller can make in a given window.

SCHEMA VALIDATION

Checking that input matches the expected structure and type.

OAuth / API Key

Common mechanisms for authenticating and scoping API access.

BOLA

Broken Object Level Authorization: accessing another user's data via ID manipulation.