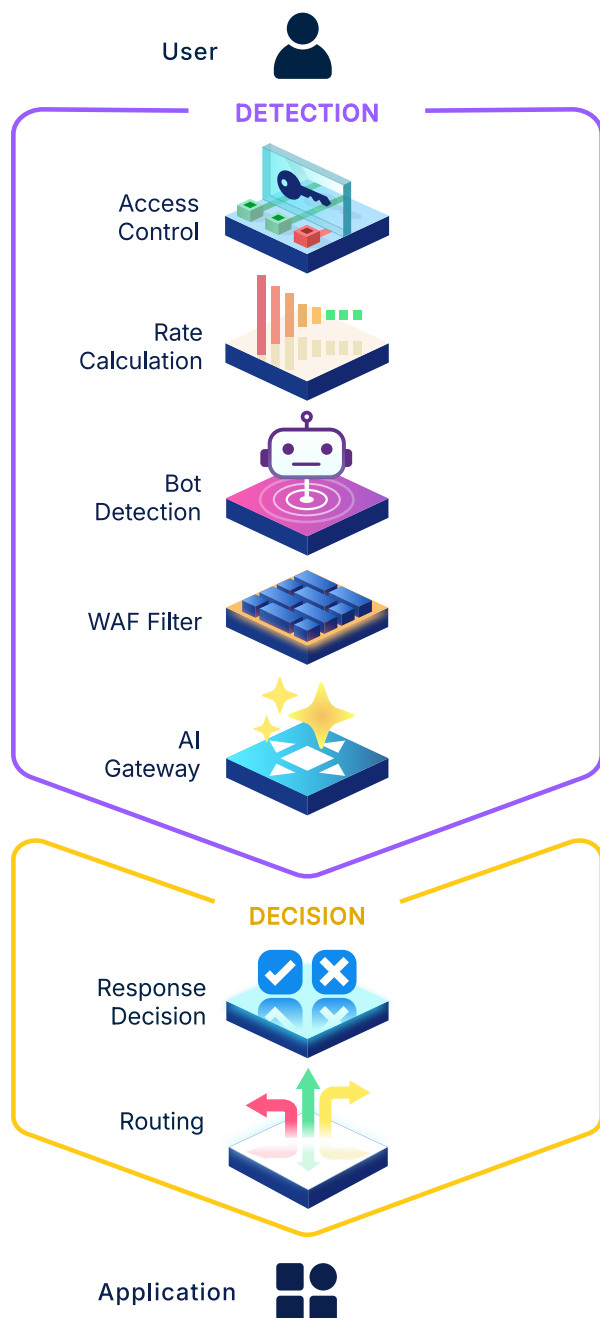# High-Performance Security for Apps and APIs

Every application is different. Instead of a one-size-fits-all solution, HAProxy Enterprise provides customizable security layers that form the building blocks of application and API security. We give you the power to build deep, targeted, and scalable security adapted perfectly to your infrastructure.

User

DETECTION

Access Control

Rate Calculation

Bot Detection

WAF Filter

AI Gateway

DECISION

Response Decision

Routing

Application

Harness defense in depth

A single line of defense will inevitably fail. Combine HAProxy Enterprise's high-performance security layers to form an ironclad defense against a broad spectrum of threats.

Line-rate packet filtering, Access Control Lists (ACLs), HAProxy Enterprise Bot Management Module, Global Rate Limiting, and HAProxy Enterprise WAF collaboratively share intelligence to make fast, accurate decisions.

Defeat evolving threats

From DDoS to fraud, automated bots threaten your business at a massive scale.

Wield the power of HAProxy's sophisticated security layers to inspect, filter, and protect real-time network traffic. Efficiently detect and block your biggest threats.

Implement adaptable security

Your traffic and threat profiles are unique. What looks normal for other businesses raises red flags for yours. HAProxy Enterprise lets you customize the security signals, weightings, and thresholds that determine responses at each layer.

Make informed decisions about the attacks and anomalous activity affecting your systems.

The Building Blocks of Application Security

Security incidents such as DDoS attacks, bot threats, and data theft cost companies millions in lost revenue. HAProxy's security capabilities leverage an extremely efficient, flexible, and dynamic code base—with a robust SSL/TLS stack, industry-leading ACL, and Stick Table tracking systems.

HAProxy Enterprise and **HAProxy Fusion** keep you ahead of threats by extending the core capabilities of HAProxy. Security enhancements include the HAProxy Enterprise Bot Management Module, the HAProxy Enterprise WAF, Global Rate Limiting (powered by the Global Profiling Engine), content inspection, adaptive response policies, plus centralized management of security policy, SSL/TLS certificates, and observability.
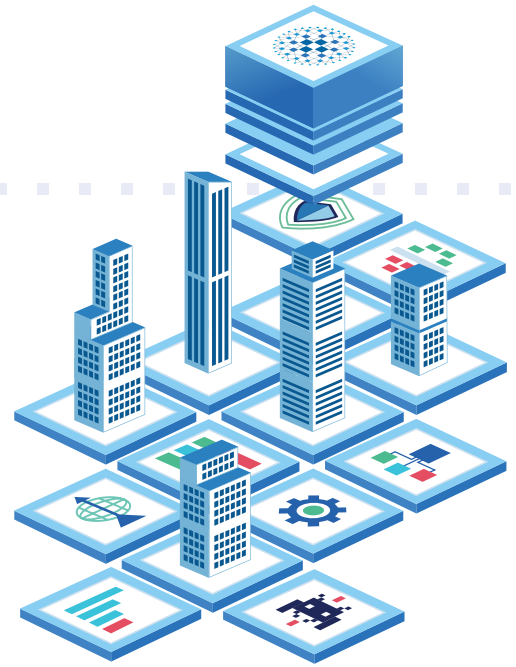
Advanced ACLs and tracking

▶ **Flexible Access Control Lists (ACLs) provide matching based on multiple options:**

- IP / CIDR
- SSL/TLS data
- Map file support
- Logical operator support
- Request/response headers and paths

▶ **Global Profiling Engine:**

- Generic key-value storage
- Combine any number of metrics
- Dynamic peer support
- Real time cluster-wide tracking for the following:
  - Request/error rate and counts
  - Unique page views per IP or User-Agent
  - Rate and counts of unique User-Agents per IP
  - Number of WAF violations per IP or User-Agent
  - ...and much more

DDoS and bot management

▶ **Detect and protect against:**

- Application DDoS
- GET/POST floods
- Web scraping
- Brute forcing
- Vulnerability scanning
- Advanced fingerprinting

▶ **Response Policies:**

- Threat Detection Engine (TDE) powered by data intelligence
- Request rate limiting, shadow banning, tarpitting, and dropping
- Native and flexible CAPTCHA module

▶ **Threat Detection Engine (TDE):**

- Detect, classify, and label high-impact threats such as application-layer DDoS, brute force attacks, web scrapers, and vulnerability scanners
- Strong out-of-the-box protection with minimal configuration or tuning
- Accurate, dynamic, and efficient with 100% local processing

HAProxy Enterprise WAF

- High throughput and low latency
- OWASP Core Rule Set (CRS) compatibility with massively boosted performance and low false positives
- Unmatched balanced accuracy (low false positives and low false negatives)
- Customizable WAF Profiles
- Allowlist/denylist/signature support
- Detailed logging

SSL/TLS

- ECC/RSA
- OCSP stapling
- AWS-LC library provides the best available performance
- TLS session resumption
- Built-in Heartbleed protection
- Zero round-trip time resumption (0-RTT)

Extra capabilities

- HTTP header sanitization
- Response body injection
- IP masking support
- Lua scripting support
- Runtime API
- Dynamic update support