

# RapidScale Application Protection

Secure the applications and APIs that power your business with expert-managed protection

Your web applications and APIs carry customer data, process payments, and run your business, which is exactly why attackers go there first.

Application Protection combines AI-driven detection with expert management to help protect your web applications and APIs from application-layer attacks.

## Application security requires continuous oversight

After deployment, protection must keep up as applications evolve, traffic shifts, and threats become more sophisticated.



### Policies drift

Each release changes what normal traffic looks like, so rules start blocking legitimate customers and letting threats through.



### Exposure expands

APIs, endpoints, scripts, and customer-facing services can grow faster than teams can inventory and secure them.



### Response depends on ownership

When accountability is unclear, detection can become a delayed handoff instead of a coordinated response.

## Solution benefits



### Applications stay online

Customer transactions and revenue-generating services stay available through an attack.



### Teams stay focused

Offload tuning, certificate oversight, and response coordination so internal teams can stay on priority work.



### Risk stays visible

Turn traffic, attack, and policy data into clearer evidence for audits, reporting, and control validation.



### Threats stay contained

Managed updates and threat intelligence help defend against emerging techniques and automation abuse.

## Protection across every entry point

Protect your web applications and APIs with managed security powered by AI-driven behavioral analysis that learns your normal traffic patterns and adapts in real time as threats evolve.

### WEB APPLICATION FIREWALL

Defend public-facing applications from OWASP Top 10 threats, zero-day attacks, and malicious traffic.

### API PROTECTION

Discover, monitor, and protect APIs from abuse, data exposure, and attacks targeting application logic.

### CLIENT-SIDE PROTECTION

Reduce risk from unauthorized scripts, browser-side threats, and client-side data exposure.

### DDOS PROTECTION

Help maintain availability during volumetric, protocol, and application-layer attacks.

### LOAD BALANCER- AS- A- SERVICE (LBAAS)

Keep applications reachable with automatic origin health checks, active-active traffic distribution, and session persistence across visits.

### BOT MANAGER

Distinguish real customers from automated traffic in real time, stopping credential stuffing, scraping, and account takeover before they turn into fraud.

## Protection is tuned as your applications change

RapidScale manages setup, validation, tuning, certificate oversight, and support escalation across your protected applications.



### Onboard

RapidScale gathers DNS, domain, origin, and SSL/TLS details, then defines the records needed to route protected traffic.



### Validate

Policies are configured, tuned, and tested with your team to confirm routing, availability, and protection behavior.



### Operate

Ongoing management includes policy reviews, certificate notifications, post-attack analysis, chat support, and RapidScale-owned escalation.

## Uncover hidden exposure across your applications and APIs

Gain clear insight into the attack surface across applications and APIs, mapped to your business impact and security requirements.

*Speak to a RapidScale cloud security expert today*

[meet@rapidscale.com](mailto:meet@rapidscale.com) 