RedShield

2025

Third Horizon DoS & Bot Defense Advanced Patch

The Business Challenge

Sophisticated bots, including those powered by generative AI, now accurately mimic human behavior, rotate IPs, and can readily bypass CAPTCHAs. Attackers use these bots to harvest credentials, take over accounts, scrape pricing and content, and exfiltrate data.

During DoS and surge conditions, simple rate limits or behavioral checks often block legitimate users or let attackers through. What's needed, especially as attackers use generative AI to evade detection and break through defenses, is an identity challenge that can be applied in-session and only when risk rises - without changing the protected application's code.

Organizations need a managed, low-friction control that works alongside existing edge and behavioral defenses to keep services available, protect revenue, and preserve customer trust.

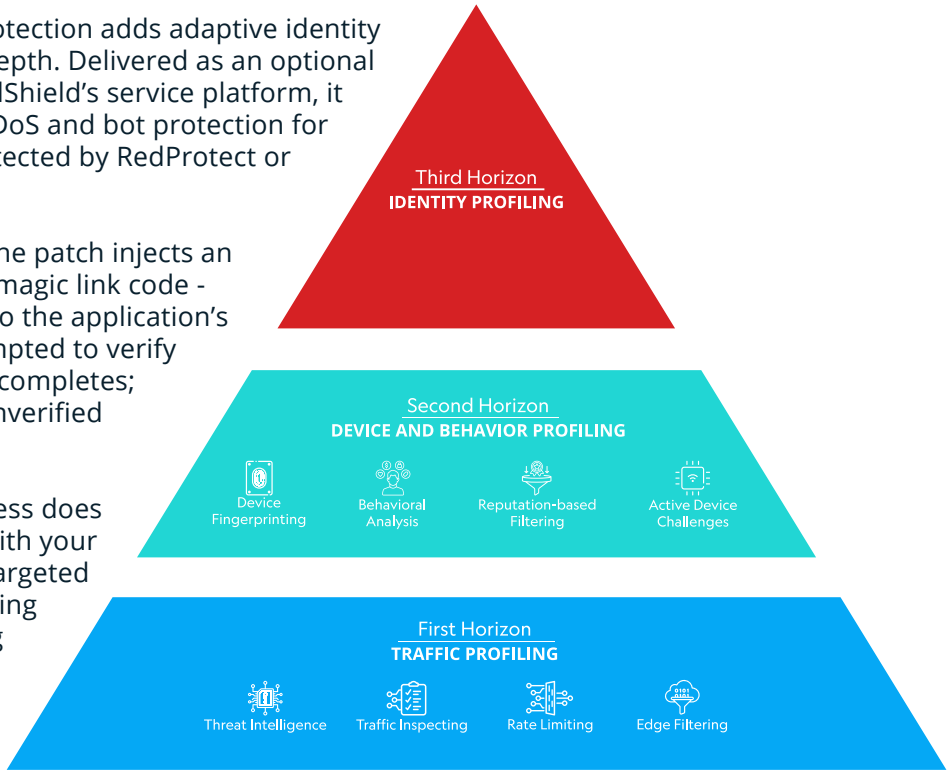
RedShield's Solution

The "Third Horizon" of DoS & bot protection

RedShield's Third Horizon of protection adds adaptive identity challenges to your defense-in-depth. Delivered as an optional Advanced In-Flight Patch on RedShield's service platform, it provides an additional layer of DoS and bot protection for critical applications already protected by RedProtect or RedSecure.

When risk thresholds are met, the patch injects an in-session email verification - a magic link code - without requiring any changes to the application's code. Suspicious users are prompted to verify inbox control before the action completes; verified users continue, while unverified sessions are blocked.

This is not MFA. The email address does not need to be pre-registered with your application. The goal is to add targeted friction only when needed, slowing and disrupting attackers, raising their cost, and preserving availability for legitimate users.



What are the Three Horizons of DoS & bot protection?

- **First Horizon – Traffic profiling:** absorb/deflect volumetric traffic at the edge via AWS' global infrastructure (eg L3/4 floods, noisy HTTP).
- **Second Horizon – Device & behavior profiling:** fingerprinting, invisible checks, Captcha-type challenges, and rate limits to deter commodity automation.
- **NEW! Third Horizon – Identity profiling:** adaptive email verification that is active when conditions require it, to further increase attacker cost while allowing legitimate users to continue.

Key attributes of the Third Horizon advanced patch

Risk-based & event-driven

Only triggers on suspicious sessions or sensitive actions.

Tuning controls

adjustable rate limits and geo-based triggers.

In-session

No re-login; users verify and continue the original task.

No code changes

Deployed and tuned by RedShield engineers.

How It Works

In-flight interception
The patch inserts a verification step before the action completes.

Decision
Successful verification allows the action to proceed; failed attempts, timeouts, or email over-use result in blocked sessions.

1 — 2 — 3 — 4

Risk detected
Triggers include suspicious activity or rates detected.

Email challenge
The user receives a magic link or one-time code and proves mailbox control.

Business Value

- **Reduce automated abuse and fraud** by requiring inbox proof that bots and toolkits struggle to complete quickly or at scale.
- **Protect availability** during DoS/bot pressure by combining identity checks with edge absorption and behavioral controls.
- **Time-to-Value - deploys** as a RedShield in-flight patch; production-ready in hours or days, not weeks.
- **Deploys without code changes** for the protected application, including legacy and third-party applications - no access to application code is required.
- **Managed outcome** with 24×7 monitoring, tuning, and actionable reporting from RedShield.

At-a-Glance

Challenge types	Email magic link; optional step-up patterns.
Trigger signals	Device/geo change; velocity/volume spikes; headless/browser anomalies.
Response modes	Sub-second policy check; email round-trip only for challenged users.
Latency impact	Up to 1,000 concurrent 10 MB uploads
Compatibility	Web applications protected by RedShield's application security service (RedProtect, RedSecure).
Security	Signed links/codes; short token TTLs; rate-limited retries.
Operations	24×7 monitoring, incident response, monthly reporting.
Tuning	Risk scoring and triggers managed by RedShield; adaptive tightening during active attacks.

Included Services

Onboarding & policy design

risk model, trigger points, user-experience design, test plans.

Deployment

Patch deployment and configuration on RedShield's service platform; no application code changes required.

Run & respond

24×7 monitoring, incident response, and adaptive tuning during attack windows.

Reporting

Dashboards and monthly reports - challenge counts, pass/fail rates, false-positive review, tuning changes.

Change management

Safe-rollout controls and rollback.

Post-incident review

Attack analysis and recommendations.

Learn More

Talk to RedShield about enabling Third Horizon protection on your most targeted applications. Please contact us at sales@redshield.co.