



RedSecure

Managed Application Security Service

Reduce application risk in days, not months. Keep your business running and releases moving. Warranted, measurable security outcomes.



What is RedSecure?

RedSecure is a web application and API security service for organizations that need rapid, comprehensive security for business-critical web apps and APIs (including legacy apps) - without slowing delivery or expanding headcount.

RedSecure is designed to address the challenge of today's agentic, AI-enabled attackers whose GenAI-powered attacks evade WAF signatures and exploit logic flaws faster than teams can ship code fixes. Instead of waiting months for code fixes, vulnerabilities and logic flaws can be neutralized in hours, keeping applications secure and available.

The 24/7 managed service combines perimeter protection (DDoS, bot management, and a tuned WAF) with RedShield-developed in-flight patches that fix application-specific issues, without needing any code changes. Assurance is continuous, with regular scans, correlated reporting, and dashboards that prove mitigations are effective.

RedSecure's outcome-based service typically reduces total cost of ownership for application security by ~70-80%. It frees scarce experts for strategic work while delivering board-ready evidence of control effectiveness - backed by a warranty.



Why RedSecure over DIY?



Tools alone don't fix logic flaws or keep pace with change. RedSecure does both, by applying expert people and proven processes.



With process maturity, experience and scale comes efficiency, and thus lower cost to serve. RedShield's application security service typically reduces TCO by ~70-80% compared with in-house threat and vulnerability programmes.



Backed by an outcome warranty: RedShield stands behind the effectiveness of its security from identified exploits.

Why Now? Gen-AI Adversaries



Evasive automation: AI-driven bots rotate behavior and infrastructure to overwhelm published services (DDoS, scraping, credential stuffing).



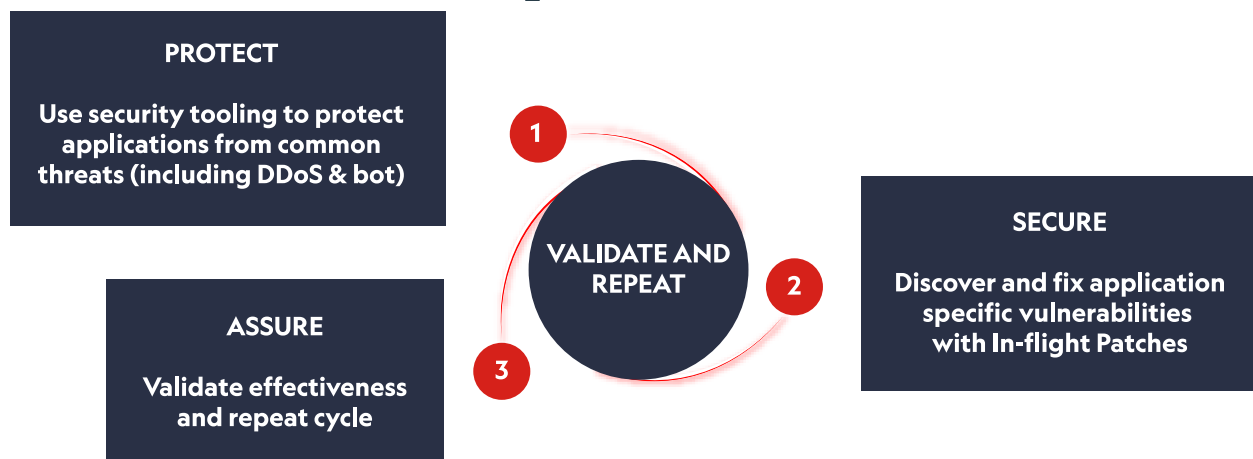
WAF evasion: Models fuzz syntax/ semantics and exploit parser quirks to slip past signature and simple policy checks.



Faster reconnaissance: Attackers mine leaked credentials and tech fingerprints, then race to exploit before fixes land.

WAFs still have a role in threat management, but for vulnerability management you need edge compute (in-flight) patches. RedSecure includes both.

The RedSecure Cycle



- **Protect:** DDoS protection (via AWS global infrastructure), advanced bot management, and expertly tuned WAF rules.
- **Secure:** RedShield develops and applies in-flight patches to neutralize application-specific vulnerabilities and logic flaws - no code change required.
- **Assure:** Regular scans, attack/vulnerability correlation, dashboards, analyst commentary, and SLAs to prove mitigations remain effective.

Business Outcomes

- Cut exposure from months to hours while keeping releases on track.
- Lower cost by replacing DIY tooling and staffing with one managed service.
- Minimize false positives and user disruption - without weakening security.
- Board-ready assurance with measurable risk reduction and warranted protection.



What's Included in RedSecure?

1 Protect

- **DDoS protection:** Always-on AWS-powered global defense (100+ Tbps) with scrubbing and absorption for volumetric, protocol, and app-layer attacks (including TLS).
- **Bot protection:** Detects and stops credential stuffing, scraping, and fraud using reputation, device, and behavior signals - including AI-driven evasive bots - without disrupting legitimate users.
- **Managed WAF:** 9000+ rules expertly managed, continuously researched signatures, RFC compliance, header/cookie hardening, rapid CVE response, and expert tuning to reduce parser blind spots that GenAI fuzzing seeks to exploit.

2 Secure

- **In-flight patches:** Request/response transformations fix issues such as SQLi, XSS, IDOR, CSRF, session weaknesses, insecure redirects, spoofing, weak headers, and more.
 - RedShield has 14,000+ pre-built patches for fast remediation, plus rapid bespoke development when needed.
- **Clean retirement:** In-flight patches are easily removed once permanent fixes are deployed.
- **Change-tolerant base policy:** Avoids disruption as apps evolve.

3 Assure


- **Regular scans:** Run with and without security in-path to confirm mitigation.
- **Correlated reporting:** Links prevented attacks to known vulnerabilities, with analyst commentary and monthly summaries.
- **Dashboards & integration:** Portal access, SIEM/syslog export, and helpdesk support for rare false-positive reviews and change control.



Service Levels & Operations

- 24x7 incident detection, response, and notification.
 - Response target: P1 <1 hour, P2 <4 hours.
- Deployment: baseline/UAT typically within ~10 business days.
- Operated from RedShield's AWS-powered global platform with geo-redundancy and performance optimization.

Next step

Sound too good to be true? Let us show you how easy it can be. Call us for a free trial today. We apply targeted security out of path for one application - with no production impact. You'll receive a report showing the reduction in risk and operational effort. 

Learn More

For a deeper dive into the challenges of web application security and how RedShield helps organizations address them, download our whitepaper and visit us at [RedShield.co](https://redshield.co).