# SERVICE DEFINITION
## HARDWARE / EMBEDDED SYSTEMS ASSESSMENT


**Our address**
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

**Give us a call**
0333 939 8080

**Send us a message**
hello@jumpsec.com

**Find out more**
www.jumpsec.com

# About JUMPSEC

**JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.**

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- **to reduce the risk of significant security incidents**
- **to speed up the detection and containment of threats, and**
- **to demonstrate robust governance to stakeholders such as boards, auditors, and insurers**

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

# Example use cases

### Central government digital service — Alternate origin path exposes admin utilities

JUMPSEC mapped ingress and identified a maintenance origin that we could reach via a legacy DNS record, which bypassed the WAF. We sent requests to predictable admin paths and received login prompts accompanied by verbose headers. Logging at the edge failed to capture traffic using the legacy host, so we lost visibility during incidents.

We remediated the issue by retiring the legacy origin, restricting admin utilities behind authenticated ingress, and standardising logging across all paths. JUMPSEC verified that we blocked access to admin routes and achieved consistent telemetry.

### NHS provider — JSON and GraphQL evasions

We blocked classic form-encoded attacks at the edge, but JSON and GraphQL variants with altered casing and nested structures still bypassed our defences. JUMPSEC left introspection exposed, and we did not apply anomaly scoring to specific content types.

JUMPSEC enabled JSON-aware inspection, restricted or authenticated introspection, and tuned anomaly thresholds with targeted exclusions. In our follow-up, we accurately blocked evasions without impacting legitimate traffic.

### Energy supplier (CNI) — API gateway exclusions and method smuggling

JUMPSEC excluded health and utility routes from gateway inspection, which allowed attackers to exploit method and path smuggling to reach sensitive handlers. We observed that the origin accepted TRACE requests and an undocumented verb, both of which bypassed controls.

We removed broad exclusions, JUMPSEC disabled unsafe methods, and we introduced normalisation before inspection. During our re-assessment, JUMPSEC blocked smuggling attempts and ensured consistent inspection across all routes.

### Local authority — CDN rules and cache poisoning risk

We found that the CDN permitted wide origins and cached responses based on unkeyed headers. JUMPSEC crafted requests that poisoned the cache, causing attacker-controlled content to be served to citizens. We checked the WAF logs and saw that no related alerts were triggered.

To mitigate the issue, we tightened the cache keys, enforced strict CORS, and JUMPSEC added negative caching rules for suspicious responses. We then verified the changes and demonstrated stable cache behaviour along with appropriate alerting for poisoning attempts.

# Service Overview

JUMPSEC conduct an independent, manual-first assessment of edge protections to determine whether a determined attacker can bypass the WAF or related controls. The engagement enumerates ingress paths, tests evasion techniques, validates rule coverage, and confirms whether blocking, logging, and alerting behave as intended. Outputs focus on exploitable routes, precise fixes, and changes that improve protection without excessive false positives.

## Objectives

- Identify practical bypass paths using encoding, transformation, fragmentation, and protocol quirks
- Validate coverage for web and API traffic across all ingress routes and origins
- Reduce risk from misconfigurations, exclusions, and unmanaged paths
- Provide backlog-ready changes with acceptance tests and rollback points

## Approach

Testing runs in agreed windows against production or production-equivalent edges using non-destructive payloads. Activities cover primary and alternate ingress (CDN, reverse proxy, load balancer, API gateway), origin fallbacks, geo and bot controls, virtual patching, custom rules, and logging/alerting flows. Findings emphasise exploit feasibility and operationally safe remediation.

## Method

- **Plan** — objectives, in-scope domains and ingress, change windows, escalation, evidence handling
- **Discover** — map routing, origin policies, bypass candidates, exclusions, and unmanaged paths
- **Validate** — exercise evasions (encoding, case, path and parameter smuggling, chunking, multipart, JSON/XML variants, HTTP/2 quirks) against known vulnerability classes and sample real findings where available
- **Analyse** — confirm exploitation paths, rule gaps, origin behaviours, and monitoring visibility
- **Debrief** — prioritise fixes, owners, acceptance criteria; agree verification checks
- **Improve** — optional re-test following rule changes or edge reconfiguration

## Deliverables

- Executive briefing describing material bypass routes, probable attacker behaviours, and priority actions
- WAF Bypass Assessment Report with evidence, reproduction steps, exact configuration changes, and verification steps

- Issue register (CSV/XLSX) listing severity, owners, due dates, and acceptance criteria
- Rule and policy change set for virtual patching and durable configuration improvements, including logging and alerting checks
- Optional re-test confirming effective mitigation after change
- Standards and alignment embedded in reporting, referencing vendor best practice for the target WAF/CDN, OWASP ASVS and OWASP Testing Guide for context, and ATT&CK technique names where edge evasions inform rationale

## Outcomes and benefits

- Higher confidence that the edge blocks real attack traffic
- Reduced false negatives from overlooked ingress and exclusions
- Operationally safe rules that minimise false positives
- Clear verification tests ensuring protections remain effective

## Pricing model

Fixed price per application or domain set and ingress mix, or time-and-materials aligned to SFIA. Price drivers include ingress diversity, API coverage, custom rule volume, and verification depth.

## Timelines

- Planning and access: 3–5 working days
- Execution based on scope and complexity
- Report issue in 5–10 working days after testing completion
- Optional re-test by agreement

## Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

## Team and roles

- **Engagement Lead** — scope, governance, quality management, stakeholder alignment
- **Application/Edge Security Tester(s) -** testing and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

## Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Provide edge configuration exports, change windows, and test headers or tokens
- Arrange third-party consents for CDN, WAF, and hosting providers where required

## JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Use non-destructive validation and minimise service impact
- Handle evidence securely and retain only for agreed periods

## Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

## Constraints and assumptions

- Non-destructive techniques; no denial-of-service or volumetric testing
- Third-party coordination required for managed edges and CDNs
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

## Related services

- Web Application Penetration Testing
- API Penetration Testing
- Continuous Attack Surface Management (CASM)


Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com