SERVICE DEFINITION
CLOUD-HOSTED APPLICATION 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

Copyright (c) 2026 JUMPSEC Ltd | All Rights Reserved: This document or any part of it should not be duplicated or the contents transmitted to any third party without the express approval of JUMPSEC Ltd.

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

Local authority — Multi-tenant SaaS extension with permissive ingress

JUMPSEC identified that ingress exposed admin utilities at predictable paths and that shared WAF rules permitted overly broad origins. The email flows did not have DKIM on a sub-domain used by the application. We brokered admin utilities behind authenticated ingress, tightened WAF and origin policies, and standardised SPF, DMARC, and DKIM. Our verification demonstrated safer administration surfaces and improved email trust for citizen messaging.

Housing association — Tenant services app with public storage

JUMPSEC reviewed an AWS serverless tier and discovered that S3 buckets exposed directory listings for uploaded documents and logs. Our team identified that Lambda functions accepted unauthenticated calls for pre-signed URL generation, and that CORS permitted wildcard origins.

We remediated these issues by closing public access with bucket policies, restricting URL creation to authenticated principals, and tightening CORS to trusted domains. Additionally, we implemented lifecycle rules to purge sensitive artefacts after processing. Our follow-up confirmed that directory listings were closed and invocation paths were properly controlled.

Higher education — Learning platform with multi-tenant leaks

We assessed an Azure-hosted LMS and uncovered predictable identifiers and missing server-side checks on assignment and grade endpoints. We found that GraphQL introspection was enabled in production, which disclosed hidden fields and mutation names. Additionally, we observed that error payloads included stack traces containing connection strings.

We addressed these issues by enforcing per-object authorisation, disabling unauthenticated introspection, and normalising error models. We ensured that API gateways validated audience, issuer, and nonce, and we moved secrets to managed stores with short-lived access. Upon re-testing, we confirmed correct tenant isolation and clean error handling.

National broadcaster — Streaming microsites with permissive ingress

JUMPSEC identified that GCP ingress exposed admin utilities at predictable paths, and that shared WAF rules permitted broad origins and methods. We discovered that service accounts for content pipelines held long-lived keys without rotation. We brokered admin utilities behind authenticated ingress, tightened WAF policies, and replaced long-lived keys with short-lived workload identities. We enhanced logging and alerting to detect admin path access. Upon re-assessment, we demonstrated safer administration and reduced risk of token misuse.

Service Overview

JUMPSEC conduct manual-first testing of applications hosted on Azure, AWS, or GCP, including serverless, managed databases, containers, and PaaS services. The engagement validates exploitability in authentication, authorisation, input handling, transport, and business logic, and assesses cloud service configuration that impacts the app's external risk. Findings include reproducible evidence and backlog-ready fixes aligned to engineering workflows and change control.

Objectives

- Identify exploitable weaknesses across app, API, and cloud service boundaries
- Reduce external exposure from misconfigured storage, functions, networking, and identities
- Harden token handling, object-level authorisation, and secret management
- Provide prioritised remediation with test steps and acceptance criteria

Approach

Testing reflects data sensitivity and provider specifics. Activities run in approved windows using non-destructive techniques and controlled accounts/clients. Coverage spans application behaviour and cloud configuration elements that directly affect the application's attack surface.

Method

- **Plan** — confirm objectives, environments, roles/clients, artefacts (diagrams, OpenAPI, IaC snippets), windows, escalation, evidence handling
- **Discover** — map app endpoints and critical workflows; enumerate public storage, functions, gateways, ingress, identity flows, and secrets handling
- **Validate** — confirm exploitability for authn/authz, input/serialization, transport, business logic; validate cloud misconfigurations affecting exposure (e.g., public buckets, permissive roles)
- **Analyse** — link issues to impact and root cause across app and platform
- **Debrief** — prioritise fixes, owners, and acceptance criteria; agree re-test scope
- **Improve** — optional re-test to confirm remediation

Deliverables

- Executive briefing (slide deck + debrief): key risks, abuse paths, priority actions
- Cloud-Hosted Application Security Report: evidence, reproduction steps, and precise fixes across application vulnerabilities and platform exposures impacting the app (storage, functions, networking, identity, secrets)

- Issue register (CSV/XLSX): severity, owners, due dates, acceptance criteria
- Optional re-testing: confirming remediation outcomes
- Standards and alignment (embedded): OWASP ASVS/Top 10 and OWASP API Security Top 10 where applicable, CIS cloud references, provider guidance (Azure/AWS/GCP), CWE mappings, CVE/CVSS severity rationale, and ATT&CK technique names for exploitation context

Outcomes and benefits

- Smaller public attack surface and stronger isolation of sensitive data
- Consistent token, session, and object-level controls across app and platform
- Actionable fixes that land cleanly in pipelines and IaC baselines
- Assurance artefacts suitable for governance, audit, and stakeholder review

Pricing model

Fixed price per application (and environment) or time-and-materials aligned to SFIA. Price drivers include environment count, service breadth (functions, storage, gateways, managed DBs), role/tenant complexity, artefact depth, and re-testing.

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

Fixed price per application and platform, or time-and-materials aligned to SFIA. Price drivers include platform count, feature complexity, offline modes, backend/API breadth, artefact depth, and re-testing requirements.

Team and roles

- **Engagement** Lead responsible for scope, governance, and quality
- **Application/Cloud Security Tester(s)** — testing, platform exposure validation, evidence capture
- **Coordinator** managing logistics, supplier comms, and action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor
- Provide builds/test accounts, diagrams, OpenAPI/collections, and read-only platform exports where feasible
- Arrange third-party consents for suppliers or managed service providers

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 testing only; no denial-of-service
- Third-party coordination requires prior written approval
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- API Penetration Testing
- Cloud Infrastructure Penetration Testing
- Secure SDLC / DevSecOps Assessment

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com