SERVICE DEFINITION DOCUMENT
THICK CLIENT / DESKTOP APPLICATION PENETRATION TESTING

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

Local authority — offline mode and business-logic abuse

We supported a records application that enabled offline edits with subsequent synchronisation. JUMPSEC discovered that client-side validation permitted users to manipulate payloads, which bypassed server-side checks when synchronisation resumed. Our assessment found that the application's timestamp and sequence handling accepted out-of-order updates, which risked overwriting authoritative records.

To mitigate these issues, JUMPSEC introduced signed payloads with server-side validation, enforced sequence controls, and implemented idempotency keys during synchronisation. We redesigned error models to be generic, with correlation for support purposes. Our verification confirmed that the system now rejected tampered payloads and handled conflicts in a predictable manner during reconnection.

Energy supplier (CNI) — IPC and privileged service exposure

JUMPSEC discovered that the desktop client communicated with a privileged helper over a named pipe, and we found that the access control lists permitted untrusted processes to request privileged operations. We determined that the helper deserialised untrusted objects, which enabled local code execution and allowed lateral movement.

To address these issues, JUMPSEC restricted the pipe ACLs to signed client processes and replaced unsafe deserialisation with vetted formats. We also added command allow-lists with parameter validation. In our subsequent assessment, JUMPSEC confirmed that we blocked privilege bridging and ensured safer inter-process communication paths.

Service Overview

JUMPSEC conducts manual-first security testing of Windows, macOS, and Linux desktop applications to identify exploitable weaknesses in authentication, authorisation, storage, transport, inter-process communication, update mechanisms, and business logic. Testing maps priority user journeys, validates exploitability using safe techniques, and produces backlog-ready fixes with clear acceptance criteria.

Objectives

- Identify and validate high-impact vulnerabilities with reproducible evidence
- Harden authentication, session, and authorisation between client and backend
- Reduce exposure from insecure local storage, IPC, and update channels
- Provide prioritised remediation with rationale suitable for audit and assurance

Approach

Testing runs in agreed windows using representative builds, test licences, and controlled accounts. Activities include static and dynamic analysis, inspection of installers and updaters, API and protocol testing, and targeted reverse-engineering within the rules of engagement. Findings focus on impact clarity and practical remediation aligned to delivery pipelines.

Method

- **Plan** — objectives, platforms/builds, roles, environments, escalation, evidence handling
- **Discover** — enumerate attack surface, local stores, IPC mechanisms, protocol flows
- **Validate** — confirm exploitability for authn/authz, storage, transport, deserialisation, signing, logic
- **Analyse** — document root cause and preventive patterns for future releases
- **Debrief** — prioritise fixes, owners, and acceptance criteria; agree re-test scope
- **Improve** — optional re-test to confirm remediation and prevent regression

Deliverables

- Executive briefing (slide deck + debrief): key risks, business impact, and priority actions
- Thick Client Security Report: evidence, reproduction steps, and precise fixes per issue; coverage notes for installation/update, storage, IPC, transport, and server interactions
- Issue register (CSV/XLSX): severity, owners, due dates, acceptance criteria
- Backlog-ready remediation guidance: aligned to CI/CD, code-signing, and release processes

- Optional re-testing: confirming remediation outcomes
- Standards and alignment (embedded): OWASP MSTG/ASVS references where applicable, CWE mappings, code-signing best practice, and relevant NCSC guidance for citizen-facing software

Outcomes and benefits

- Lower risk of account takeover, data exposure, and local privilege escalation
- Stronger update channels, code-signing integrity, and client-server trust
- Backlog-ready actions that land cleanly in engineering sprints
- Assurance artefacts suitable for governance, audit, and software escrow

Pricing model

Fixed price per site or zone set, or time-and-materials aligned to SFIA. Price drivers include site count, OEM/integrator coordination, allowable test depth, and verification during maintenance windows

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 Security Tester(s)** — desktop testing, reverse-engineering, evidence capture
- **Coordinator** managing logistics, supplier comms, and action tracking

Buyer responsibilities

- Nominate a single engagement lead and executive sponsor

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control

- Provide representative builds/installers, signing approach, test accounts/licences, and backend access
- Arrange third-party consents where suppliers or payment providers are in scope
- 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
- Store policies, EULA, and licence constraints respected for test builds
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- API Penetration Testing
- Source Code Review
- Secure SDLC / DevSecOps Assessment

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com