SERVICE DEFINITION DOCUMENT
WIRELESS NETWORK 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

Local authority campus — Guest/corporate segregation weaknesses

On multi-building estates, we found guest SSIDs bridging into corporate address space because teams mis-mapped VLANs and set overly permissive inter-SSID routing. JUMPSEC uncovered that administrators exposed controller admin interfaces over management subnets, which made them accessible from user networks. We also spotted signal overspill extending to public walkways, increasing the risk of evil-twin attacks near council entrances and libraries.

To address these issues, we re-mapped SSIDs to dedicated VLANs, enforced client isolation, and restricted routing to explicit flows. JUMPSEC hardened controller access, enforced MFA, and closed legacy services. We used floor-plan overlays to guide AP power adjustments. Our verification confirmed we achieved effective separation and reduced the attack surface in public areas.

Central government office — Enterprise EAP and certificate validation gaps

JUMPSEC identified devices that accepted unauthorised RADIUS endpoints because teams had not enforced strict server certificate validation and had configured mixed EAP methods. We observed client probes leaking historic SSIDs, and found that certain builds reverted to legacy protocols without PMF. JUMPSEC noted that administrators relied on shared accounts for controller access.

We standardised EAP-TLS with strict certificate pinning, enabled PMF, and removed legacy fallback options. JUMPSEC rotated administrative credentials to unique, role-scoped accounts with comprehensive logging. Our follow-up assessment confirmed that authentication was more resilient and that opportunities for credential capture had reduced.

Hospital campus (NHS) — Overspill and clinical isolation

JUMPSEC conducted RF surveying and discovered that clinical SSIDs bled into public concourses and exterior areas. We found that guest networks routed to internal services for convenience, and that imaging admin interfaces responded across shared subnets. JUMPSEC also identified that controller firmware lagged behind vendor security advisories.

We retuned RF power and relocated APs to limit overspill, carved clinical traffic into restricted zones, and brokered guest access through controlled gateways. JUMPSEC updated firmware and hardened configurations to address management exposure. Our verification demonstrated that we contained wireless coverage and enabled safer inter-zone flows supporting clinical operations.

Airport operator (CNI) — Rogue/evil-twin exposure near landside areas

JUMPSEC monitored the arrivals and retail zones and repeatedly detected rogue beacons. We found that travellers' devices auto-joined look-alike SSIDs, which exposed their probes and credentials. JUMPSEC also observed that admin portals were present on flat management ranges accessible from contractor networks.

We enabled rogue AP detection with alerting, required certificate validation on clients, and JUMPSEC segmented management away from contractor ranges while enforcing MFA on all admin paths. Our subsequent validation confirmed that we achieved faster rogue response and reduced susceptibility to evil-twin attacks in public zones.

Service Overview

JUMPSEC conduct independent security testing of enterprise and guest wireless networks to identify weaknesses in authentication, encryption, segmentation, and the management plane. The engagement assesses over-the-air controls, client behaviours, controller/AP configurations, and site coverage. Outputs provide reproducible evidence and a prioritised remediation plan suitable for network and security teams.

Objectives

- Validate enterprise authentication (EAP types, certificate trust, credential handling)
- Confirm isolation between guest, contractor, and corporate SSIDs/VLANs
- Identify signal overspill, rogue APs, and evil-twin susceptibility
- Harden controller/AP management, firmware posture, and default services

Approach

Testing runs on-site and, where relevant, from adjacent public areas using non-destructive techniques and agreed windows. Activities combine controlled association attempts, credential capture simulations, management-plane review, and targeted RF surveying. Findings reflect real-world abuse paths while respecting safety and change control.

Method

- **Plan** — objectives, locations, test windows, health and safety, escalation, evidence handling
- **Discover** — enumerate SSIDs, ciphers, EAP methods, management interfaces, and RF posture
- **Validate** — attempt controlled associations, credential capture/relay simulations, and isolation checks
- **Configuration review** — analyse controller/AP settings, firmware, logging, and admin access patterns
- **Debrief** — classify severity, document precise fixes, and sequence changes with rollback points
- **Improve** — optional verification to confirm remediation outcomes

Deliverables

- Executive briefing (slide deck + debrief): key risks, likely abuse scenarios, and priority actions
- Wireless Security Report:
    - Authentication & Encryption: EAP types, certificate validation, credential protection, PMF adoption

  - Segregation & Isolation: guest/corporate separation, VLAN mapping, inter-SSID routing checks
  - RF Posture: signal overspill, coverage anomalies, susceptible areas for evil-twin attacks
  - Rogue/Evil-Twin Findings: detections, dwell times, and response considerations
  - Management Plane: controller/AP hardening, admin access, firmware/version hygiene, logging
  - Client Behaviour: auto-join risks, probe leaks, legacy protocol fallback
- Exposure register (CSV/XLSX): issues, severity, owners, due dates, acceptance criteria
- Floor-plan overlays (where feasible): annotated RF/coverage and hotspot indicators
- Standards and alignment (embedded): NCSC enterprise Wi-Fi guidance, vendor hardening references, CIS control context for network management

Outcomes and benefits

- Stronger enterprise authentication and credential protection
- Reliable guest/corporate separation and reduced lateral exposure
- Lower susceptibility to rogue/evil-twin attacks near public spaces
- Hardened controller/AP management with clearer operational guardrails

Pricing model

Fixed price per site/campus or time-and-materials aligned to SFIA. Price drivers: site count, floor-area/coverage, SSID complexity, management-plane scope, artefact depth, and optional verification.

Timelines

- Planning and access: up to 1 week
- On-site testing and configuration review: 2–5 days per site (scope dependent)
- Report issue: 5–10 working days after testing completion
- Optional verification review based on findings and recommendations

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
- **Wireless Security Specialist(s)** — on-site testing, RF survey, configuration review
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead
- Arrange site access, escorts, and floor plans/coverage maps
- Provide controller access (read-only), config exports, and change windows
- Confirm health and safety requirements and any third-party consents

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Conduct a non-disruptive discovery and minimise operational impact
- Secure handling and time-boxed retention of data and artefacts

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-disruptive activities performed in approved windows
- Live credential replay to production services is out of scope
- Third-party and landlord permissions obtained where areas are shared

Related services

- Internal Network Penetration Testing
- Firewall / Segmentation Review
- Network Architecture / Asset Discovery

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com