SERVICE DEFINITION DOCUMENT
NETWORK ARCHITECTURE / ASSET DISCOVERY

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 agency — Unknown internet-facing assets**

We confirmed web endpoints and APIs existed outside change control by conducting discovery across multiple domains. JUMPSEC uncovered stale DNS records, identified forgotten VIPs on legacy load balancers, and located cloud front-ends still connected to old trial subscriptions. Our teams found that external scanners had indexed these assets with outdated headers and permissive TLS.

We consolidated DNS, retired orphaned VIPs, and routed all public exposure through a controlled ingress tier as part of our remediation efforts. JUMPSEC registered assets in the inventory with renewal and patch cycles. Our verification confirmed that we had reduced the external footprint and established clear accountability for the remaining services.

- **NHS Trust — Flat routing between clinical and corporate segments**

We identified unrestricted routes from user subnets into systems that supported clinical workflows and imaging repositories. JUMPSEC found that shared services resided on mixed-purpose subnets, and jump paths traversed unmanaged endpoints. Our team saw that backup networks accepted traffic from broad address ranges.

We re-stated trust boundaries, carved out service-specific VLANs, and constrained routes to allow only explicit flows. JUMPSEC moved critical services behind controlled gateways with logging enabled on privileged pathways. Our follow-up validation showed that we had reduced traversal options and established clearer dependency chains.

- **Housing association — Shadow networks and orphaned VLANs**

We discovered legacy VLANs still trunked across the core and intermittently observed hosts responding to ARP. JUMPSEC noted that network diagrams had fallen behind several changes, and CMDB entries did not specify owners. We also found that devices were advertising management interfaces on mixed-purpose subnets.

JUMPSEC removed unused VLANs, detached dormant trunks, and relocated management to dedicated subnets. We then updated the inventory to record ownership and lifecycle checkpoints. Our verification showed that we had simplified spanning domains, reduced broadcast noise, and achieved faster fault isolation.

- **Airport operator (CNI) — Third-party links bypassing central controls**

JUMPSEC conducted flow sampling and identified supplier connections that terminated deep within internal zones. We discovered that historical projects had introduced split tunnelling and direct access to admin interfaces. JUMPSEC reviewed change records and found that expired access windows were still active.

We remediated the situation by rerouting suppliers through brokered gateways with least-privilege rules and strict logging. JUMPSEC closed expired windows and updated contracts to reference the new control pattern. Our subsequent validation confirmed that we established controlled entry points and significantly lowered exposure from partner networks.

Service Overview

JUMPSEC conduct independent discovery and mapping of networks, routes, and assets to establish a reliable view of what exists, how it communicates, and where controls apply. The engagement identifies unknown assets, shadow networks, risky paths, and misaligned trust boundaries. Outputs provide an authoritative inventory, dependency maps, and a pragmatic roadmap to simplify, segment, and govern the estate.

Objectives

- Build a verified inventory of address space, subnets, devices, and services
- Map data flows, trust boundaries, and privileged pathways
- Identify exposure: unknown internet-facing assets, legacy protocols, risky routes
- Recommend a staged simplification and segmentation plan with ownership

Approach

Evidence-led discovery using safe interrogation of routing, ARP/DHCP, device configs, CMDB exports, cloud inventories, and passive DNS. Sampling validates critical flows without disrupting production. Stakeholders usually include Network, Security, Operations, and key suppliers..

Method

- **Plan** — confirm address space, artefacts, windows, and evidence handling
- **Discover** — enumerate subnets, gateways, devices, VIPs, DNS, and services
- **Validate** — sample critical flows and confirm ownership of disputed assets
- **Debrief** — reconcile inventory, highlight exposure, and prioritise actions
- **Improve** — optional verification to confirm clean-up and control placement

Deliverables

- Executive briefing (slide deck + read-out): key exposure themes, material risks, and recommended priorities for leadership.
- Authoritative asset inventory (CSV/XLSX): subnets, devices, roles, ownership, business criticality, environment tags, and exposure flags; import-ready for CMDB/IPAM.
- Network topology and data-flow diagrams: L3/zone maps, key dependencies, privileged pathways (admin/jump/backup), and third-party connectivity.
- Exposure register (CSV/XLSX): unknown internet-facing assets, risky services, shadow networks, orphaned VLANs, legacy routing/protocols, and misaligned trust boundaries—ranked with rationale.

- Ownership and stewardship pack: contact matrix, support groups, and joiners-movers-leavers touchpoints for asset lifecycle.
- CMDB reconciliation pack: variances between discovered reality and CMDB; ready-made updates and import templates.

Outcomes and benefits

- Single source of truth for assets, ownership, and exposure
- Smaller blast radius via clearer trust boundaries and routes
- Faster incident triage with dependable maps and contact points
- Leaner networks with lower operational overhead and audit friction

Pricing model

Fixed price per defined address space/site or time-and-materials aligned to SFIA. Price factors: site count, device/vendor mix, artefact availability, cloud/on-prem scope, and optional verification

Timelines

- Planning and pre-requirements gathering: up to 1 week
- Discovery and validation: 1–2 weeks (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
- **Network Security Consultant(s)** — discovery, validation, evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control

- Provide exports (routing, ARP/DHCP, device configs), CMDB/cloud inventories, and diagrams
- Confirm change windows and supplier participation where required
- 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-destructive activities performed in approved windows
- Third-party participation requires prior written approval
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Firewall / Segmentation Review
- Continuous Attack Surface Management (CASM)
- Internal Network Penetration Testing

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com