SERVICE DEFINITION DOCUMENT
MICROSOFT SECURITY CONFIGURATION REVIEW

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

Central government agency — Conditional access and privileged access strategy

JUMPSEC conducted an estate-wide review, which revealed that user groups used a mix of MFA strengths, break-glass accounts operated with overly permissive settings, and some services still allowed legacy protocols. We found that role scoping granted standing admin rights where just-in-time access would have been sufficient. Although Sentinel ingested sign-ins, it did not include rules to track misuse of emergency access.

We consolidated conditional access templates, enforced phishing-resistant MFA for administrators, and placed emergency accounts under strict usage and monitoring rules. JUMPSEC replaced standing admin rights with PIM and added Sentinel rules to highlight high-risk sign-ins and role activations. Our verification demonstrated that policies were applied consistently and that accountability for privileged actions became clearer.

Local authority — Email security and collaboration controls

JUMPSEC reviewed the Microsoft 365 configuration and identified weak authentication on shared mailboxes, permissive external sharing in Teams and SharePoint, and incomplete Safe Links and Safe Attachments policies. We also found that audit logs retained data for too short a duration to support investigations. We hardened shared mailbox access, applied sensitivity labels and scoped external sharing policies, and enabled Safe Links and Safe Attachments for priority groups. JUMPSEC extended retention settings to improve audit coverage. When we carried out our subsequent assessment, we saw fewer risky shares, enhanced phishing resistance, and improved investigative depth.

NHS Shared Service — Defender/XDR and Sentinel coverage

We identified gaps in Defender sensor deployment on non-persistent endpoints, found that ASR rules were disabled in clinical images, and observed that duplicate Sentinel analytics led to alert fatigue. JUMPSEC also discovered that connector configuration missed several Microsoft sources and key third-party logs.

We drove full sensor coverage, staged ASR enablement with compatibility testing, and JUMPSEC rationalised rules using suppression logic and watchlists. We added additional connectors to improve coverage of identity and endpoint events. Our follow-up review showed higher-quality incidents and enhanced containment readiness.

Energy utility (CNI) — Azure guardrails and key governance

We analysed subscriptions and found inconsistent policy baselines, identified overly permissive role assignments at the management group level, and discovered that deployment pipelines relied on long-lived credentials. JUMPSEC also observed that Key Vault permissions lacked separation of duties, and noticed that alerting failed to capture key rotation failures.

JUMPSEC remediated these issues by applying deny-by-default guardrails, narrowing roles to workload boundaries, and moving pipelines to use short-lived credentials. We also adopted dual control for key governance and implemented rotation alerts. Our verification confirmed that we achieved constrained privilege paths, reliable rotation, and clearer audit trails.

Service Overview

JUMPSEC conduct an independent configuration review and uplift across Microsoft 365, Entra ID, Defender, Azure, and Sentinel. The engagement aligns identity, endpoint, cloud, and SIEM settings with current hardening guidance. Outputs prioritise high-value changes with clear owners, acceptance criteria, and change checkpoints.

Objectives

- Strengthen identity controls: MFA, conditional access, role scoping, break-glass
- Improve endpoint and XDR posture: sensor coverage, response, attack surface reduction
- Apply cloud guardrails: policy/SCPs, segmentation, secrets and key governance
- Raise SIEM value: relevant connectors, analytics, suppression, and retention

Approach

Evidence-led review using read-only access, exports, and configuration snapshots. Delivery runs in agreed windows without disrupting production. Stakeholders usually include Technology, Security, Endpoint, Identity, Cloud, and SOC teams.

Method

- **Plan** — objectives, tenants/subscriptions, artefacts, windows, escalation, evidence handling
- **Discover** — capture identity, endpoint, cloud, and Sentinel configurations and usage
- **Validate** — confirm risk and effort; assess change impact and rollback needs
- **Debrief** — prioritise fixes with owners, pre-requisites, and acceptance criteria
- **Improve** — optional verification to confirm posture change

Deliverables

- Executive briefing (slide deck + debrief): top risks, value drivers, and priority actions
- Microsoft Security Uplift Report, covering:
    - Identity (Entra ID/M365): conditional access, MFA (including phishing-resistant), privileged access strategy/PIM, emergency access, legacy auth and risky protocols
    - Endpoint/XDR (Defender): sensor coverage, response actions, ASR policies, attack surface features, tamper protections
    - Cloud (Azure): role design/privilege paths, policy/Blueprints/SCPs, network and key/secrets governance, logging

    - SIEM (Sentinel): connectors, normalisation, analytic rules, watchlists, incident rules, SOAR opportunities, retention/cost controls

- Issue register (CSV/XLSX): severity, owners, due dates, acceptance criteria
- Optional 30/60/90-day Configuration Roadmap: change sequence, rollback points, and test gates
- Standards and alignment (embedded): Microsoft and NCSC hardening guidance, CIS Microsoft 365/Azure references, and ATT&CK technique names used for rationale

Outcomes and benefits

- Measurably stronger identity assurance and privileged access governance
- Higher detection and containment confidence from Defender and Sentinel
- Clear guardrails that reduce configuration drift and operational risk
- Actionable backlog with agreed ownership and verification steps

Pricing model

Fixed price per scoped tenant/subscription set or time-and-materials aligned to SFIA. Price drivers: tenant/subscription count, tool coverage, artefact depth, and optional verification

Timelines

- Planning and access: 3–5 working days
- Testing and reviews: 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
- **Microsoft Security Specialist(s)** — technical assessment and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead
- Provide read-only access/exports and relevant architecture documentation
- Confirm change windows and arrange third-party consents where required

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Use non-destructive validation 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
- Third-party involvement requires prior written consent
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Cloud Infrastructure Penetration Testing
- Active Directory / Entra ID Configuration Review
- Detection Engineering and Use Case Tuning

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com