SERVICE DEFINITION
MICROSOFT 365 / ENTRA ID / AZURE AD TENANT 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

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 — Consent and mailbox-rule sequence hardening

We observed that a council tenant permitted consent to unverified apps and enabled external auto-forwarding. JUMPSEC detected risky sign-ins, followed by delegated mailbox access and rule creation, which together created a realistic path to staged data loss. We reviewed and linked consent events directly to rule creation, highlighting where weak controls existed in mail hygiene.

JUMPSEC restricted publisher trust and required admin approval for new publishers. We configured mail flow to block external auto-forwarding and added holds for suspicious rules on finance and leadership mailboxes. We enforced PIM approval and logging for privileged roles. Our verification process showed that we successfully blocked consent attempts, triggered early alerts on risky rule creation, and ensured clear, auditable elevation.

Housing association — Safer external sharing and partner collaboration

JUMPSEC enabled permissive external sharing in SharePoint and Teams, which resulted in broad inheritance and unmanaged devices. We identified several guest accounts that held elevated permissions without clear ownership. JUMPSEC also noted that the DLP configuration did not include tested policies for sensitive document types.

We introduced managed defaults for external sharing, set expiry and review processes, and established guest access governance with regular attestation. JUMPSEC applied device-based controls for sensitive sites and implemented DLP policies, starting in monitored mode and moving to enforced mode. We provided evidence that showed we reduced exposure, attributed guest access to owners, and caused minimal disruption to partner workflows.

NHS provider — Privileged access and break-glass assurance

We found that privileged roles inherited from on-prem groups and bypassed PIM policies. JUMPSEC observed that break-glass accounts existed but did not undergo periodic validation or use a sealed-secrets process. We identified that Conditional Access excluded legacy protocols, which created blind spots.

JUMPSEC decoupled cloud roles from legacy groups, made PIM mandatory with approval and time-bound elevation, and formalised emergency access with regular drills and out-of-band authentication. We enhanced Conditional Access with session controls and enforced modern authentication. When we re-tested, we demonstrated auditable elevation, safe break-glass usage, and stronger session governance.

Service Overview

JUMPSEC conduct a configuration-led assessment of Microsoft 365 and Entra ID (Azure AD) that reduces identity compromise, data leakage, and administrative risk. The review examines authentication strength, Conditional Access design, privileged access and elevation, consent and publisher trust, collaboration and sharing posture, mail hygiene, device and session controls, and audit/monitoring. Recommendations focus on safe, low-friction changes that collapse common attack paths and improve day-to-day operations.

Objectives

- Establish a reliable baseline of tenant configuration and risky deviations.
- Harden authentication, consent, and privileged access to cut common compromise routes.
- Make collaboration safer without unnecessary friction for users and suppliers.
- Deliver exact, auditable changes with owners, acceptance criteria, and verification artefacts.

Approach

Work begins with planning to confirm target tenants, evidence handling, and change windows. Read-only configuration exports, portal reviews, and policy sampling create an accurate picture of roles, policies, apps, and sharing. Analysis prioritises changes that remove whole classes of risk: phishing-resistant MFA, Conditional Access with device and session context, just-in-time privileged access, restricted app consent and publisher trust, safe defaults for sharing and mail flow, and logging that supports rapid triage. Recommendations include rollback notes and align with change control.

Method

- **Plan** — confirm objectives, artefacts, authority, access, and safe adoption windows.
- **Discover** — capture Conditional Access, MFA strength, role assignments and PIM, app registrations, consent and publisher trust, sharing and DLP controls, Exchange Online hygiene, Teams/SharePoint settings, device posture, and logging.
- **Validate** — perform non-destructive checks to confirm feasibility and impact; identify quick wins and dependencies.
- **Analyse** — map weaknesses to realistic attack sequences and business risk; define precise changes with acceptance criteria and rollback.
- **Debrief** — present actions, owners, sequencing, and verification steps; agree re-test approach.

Deliverables

- Executive briefing for senior stakeholders summarising material risks, attack sequences, and expected reduction in business impact after change.

- Tenant Hardening Report with evidence, exact policy updates (policy names, role IDs, locations), rollback notes, acceptance criteria, and ownership.
- Privileged Access Pack covering role definitions, PIM policies and approvals, emergency access ("break-glass") design and drills, and auditing requirements.
- Collaboration & Mail Safety Pack describing safe defaults for sharing, external access, mail flow controls, authentication of senders, forwarding restrictions, and monitoring for risky sequences.
- Verification artefacts including before/after screenshots, policy exports, log references, and short re-test instructions.
- Standards and alignment embedded in reporting: references to Microsoft security baselines and hardening guidance; NCSC security design principles for UK buyers; OWASP ASVS control families for authentication/access control; ISO/IEC 27001 Annex A mapping for governance.

Outcomes and benefits

- Lower likelihood of identity compromise and mailbox-driven data loss.
- Clear, auditable privileged access with just-in-time elevation and controlled emergency access.
- Safer collaboration with suppliers and partners, retaining usability.
- Stronger logging and earlier, more precise alerting for incident response.

Pricing model

Fixed price per tenant and scope area, or time-and-materials for complex estates. Price drivers include tenant count, integration breadth, volume of registered apps, collaboration complexity, and verification depth.

Timelines

- Planning and access preparation: 3–5 working days.
- Discovery and analysis: typically 5–10 working days depending on scope and artefact availability
- Report issue: 5–10 working days after testing completion.
- Optional re-test and change assurance: by agreement.

Team and roles

- Incident Director / Manager — command and stakeholder comms.
- Microsoft Security Specialist(s) performing configuration review and designing changes.
- Coordinator — call-out handling, logistics, document control.

Buyer responsibilities

- Nominate an engagement lead and tenant owner(s).
- Provide read-only access or exports for relevant portals and policies.
- Align platform owners and change control for safe adoption of recommendations.

JUMPSEC responsibilities

- Operate within agreed authority using non-destructive, evidence-led methods.
- Minimise operational impact and provide rollback notes for each significant change.
- Handle materials securely with least-privilege access, time-boxed retention, and approved destruction/return.

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

- No destructive testing or simulated attack traffic.
- Third-party or managed components require prior written consent.
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Active Directory / Entra ID Configuration Review
- Detection Engineering and SOC Use Case Tuning
- Attack Path Mapping

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com