SERVICE DEFINITION
ACTIVE DIRECTORY / DOMAIN 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

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 — Legacy trusts and broad admin roles

We worked with a tiered council estate that had inherited legacy trusts from a historic merger and broad domain admin assignments to shared IT groups. During our discovery, we identified unconstrained delegation on service accounts, machine accounts with SPNs that enabled ticket abuse, and Conditional Access policies that exempted key admin roles from strong MFA. We also found that mail hygiene permitted external auto-forwarding, which increased the risk of consent-then-rule attack sequences.

To address these issues, we removed unconstrained delegation or isolated services where it was required. We replaced persistent admin rights with Privileged Identity Management (PIM) and approval workflows, and enforced phishing-resistant MFA with session controls on admin roles. We ensured that Conditional Access excluded only break-glass accounts, and implemented time-boxed elevation for administrators. Additionally, we blocked external auto-forward in mail flow and introduced sequence detections. Our re-testing provided evidence of collapsed escalation routes, auditable elevation, and safer defaults for mail and consent.

NHS-adjacent provider — Hybrid join and service account hygiene

We supported a shared services organisation that relied on hybrid Azure AD join with a combination of key trust and certificate trust. Our team identified that service accounts were running with interactive logon enabled and non-expiring passwords. In addition, several autoloaded GPOs applied conflicting settings across VDI and clinical devices, which led to inconsistent telemetry and enforcement.

We normalised the hybrid join approach, disabled interactive logon where it was unnecessary, and rotated service account secrets. Where feasible, we introduced managed identities. We also rationalised and hardened GPOs, establishing a clear precedence model. Furthermore, we set logging and EDR posture to consistent baselines across all device pools. Our verification confirmed that device identity became reliable, the privilege footprint reduced, and detection coverage improved.

Central government agency — Conditional Access and consent posture

We found that a programme team maintained permissive consent for unverified publishers to facilitate rapid trials. Admin roles inherited from legacy groups synchronised from on-prem AD, which allowed them to bypass PIM policies. We also identified that several emergency access accounts lacked periodic validation and had stale backup methods.

To remediate these issues, our recommended actions tightened publisher trust and required security admin approval for new publisher registrations. We decoupled legacy groups from privileged cloud roles, making PIM mandatory with approval and logging. We enhanced break-glass accounts by implementing strong, out-of-band authentication, conducting periodic drills, and introducing a sealed-secrets process. Our evidence packs demonstrated improved consent governance and clean, just-in-time privileged access.

Service Overview

Active Directory and Domain Configuration Reviews provide a deep, configuration-led assessment of Microsoft Entra ID (Azure AD) and on-premises Active Directory, including hybrid identity, to reduce privilege sprawl, collapse escalation routes, and strengthen authentication and administrative boundaries.

The review examines identity lifecycle processes, trust relationships, Kerberos/NTLM usage, Group Policy design, tiering and segmentation of admin rights, Conditional Access design, app registration and consent posture, Privileged Identity Management (PIM/JIT) configuration, service account hygiene, device join and hybrid key trust settings, and key controls that influence blast radius during ransomware and business email compromise. Findings translate directly into low-risk hardening actions, supported by evidence, rollback points, and verification tests that land cleanly through change control.

Objectives

- Create an accurate baseline of identity and domain configuration across Entra ID and AD DS.
- Eliminate unnecessary privilege and legacy trust that enable lateral movement or rapid escalation.
- Strengthen authentication, admin tiering, and break-glass design to protect critical services.
- Deliver precise, auditable changes with owners, acceptance criteria, and verification artefacts.

Approach

Delivery is evidence-led and non-disruptive. The engagement begins with a short planning session to confirm target tenants, domains, forests, privileged access patterns, and any time-sensitive risks. Read-only configuration export and console reviews establish the baseline. Analysis focuses on controls that break multiple attack paths with minimal operational friction—admin tiering, PIM/JIT, Conditional Access, consent and publisher trust, device and hybrid join posture, Kerberos delegation and encryption settings, service account controls, and Group Policy hardening. Recommendations are sequenced for safety, include rollback steps, and align to the buyer's change windows.

Method

- **Plan** — confirm scope, artefacts, authority, evidence handling, and safe change windows.
- **Discover** — capture tenant and domain configuration, trusts, role assignments, Conditional Access, consent posture, service accounts, GPOs, device join, and logging.
- **Validate** — perform non-destructive checks to confirm feasibility and business impact; identify quick wins and prerequisite dependencies.
- **Analyse** — map weaknesses to realistic attack paths and business risk; define exact configuration changes with acceptance criteria and rollback.
- **Debrief** — present actions, owners, sequencing, and verification checks; agree follow-up and optional re-test.

Deliverables

- Executive briefing for senior stakeholders explaining material risks, likely attack paths, and the expected reduction in blast radius after change.
- Configuration & Hardening Report with evidence, exact change steps (e.g., policy names, role IDs, GPO paths), rollback notes, and acceptance criteria tied to each recommendation.
- Admin Tiering & Access Model update covering role definitions, break-glass accounts, PIM policies, approval and logging requirements, and separation of duties.
- Conditional Access and Authentication Pack describing MFA strength, session controls, device posture use, emergency bypass, and publisher trust settings for app consent.
- Verification artefacts: test scripts or steps, before/after screenshots, log/alert references etc
- Standards and alignment embedded in reporting: references to NCSC identity and design principles, Microsoft security baselines and hardening guidance, OWASP ASVS control families for authentication and access control, and ISO/IEC 27001 Annex A themes for governance mapping.

Outcomes and benefits

- Reduced identity attack surface and fewer viable escalation routes across tenant and domain boundaries.
- Clear, enforceable administrative boundaries with just-in-time elevation and auditable break-glass use.
- Higher confidence during incident response through predictable isolation choices and stronger logging.
- Changes that persist, with verification evidence that satisfies governance, audit, and insurers

Pricing model

Fixed price per tenant/forest and major scope area, or time-and-materials for complex multi-forest estates. Price drivers include number of domains/tenants, legacy features in use (e.g., ADFS, unconstrained delegation), service account volume, GPO complexity, and required verification depth.

Timelines

- Planning and access preparation: 3–5 working days.
- Discovery and analysis: typically 5–10 working days depending on estate size and hybrid complexity.
- 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 Identity Specialist(s) conducting configuration review, modelling attack paths, and designing changes.
- Coordinator — call-out handling, logistics, document control.

Buyer responsibilities

- Nominate a single engagement lead and technical owner for Entra ID and AD.
- Provide read-only access or exports for tenant and domain configuration, including Conditional Access, roles, app registrations, logging, and GPOs.
- Align change control contacts to schedule safe adoption of priority fixes.

JUMPSEC responsibilities

- Operate within agreed authority and follow non-destructive, evidence-led methods.
- Minimise operational impact and provide rollback notes for each material 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 credential harvesting, password spraying, or destructive testing.
- Third-party or hosted identity components require prior written consent.
- Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Microsoft 365 / Entra ID / Azure AD Tenant Review
- Attack Path Mapping
- Response Playbook Development

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com