Cyber Security
Defence Consultants

Cyber Security Consultancy

January 2026

G-Cloud 15 Service Description

Cyber Security Defence Consultants Limited
St John's Innovation Centre Cowley Road
Cambridge CB4 0WS
T: 01223 421577
W: cybersecuritydefence.co.uk

Secure Apple Privileged Access and Device Management Service

Cyber Security Defence Consultants

Table of Contents

Service Definition Document

Secure Apple Privileged Access and Device Management Service

1 OVERVIEW

Cyber Security Defence Consultants delivers a comprehensive Apple device management and security service powered by Jamf, specifically designed for UK government and public sector organisations requiring secure privileged access from Apple devices.

Our service provides Privileged Access Workstation (PAW) configurations for Tier 0, Tier 1, and Tier 2 administrative access, ensuring that privileged operations are performed from hardened, continuously monitored devices that meet GovAssure requirements and NCSC device security guidance.

All service delivery is performed by SC-cleared UK-based professionals with extensive experience deploying secure Apple environments across central government departments.

1 SERVICE DESCRIPTION

1.1 Tiered Access Model

The Privileged Access Workstation model segments administrative access to contain credential exposure and limit blast radius in the event of compromise:

1.1.1 Tier 0 — Identity Infrastructure

Direct control over domain controllers, certificate authorities, and identity systems. Requires dedicated hardware with maximum isolation, hardware-bound authentication, and the strictest security controls.

1.1.2 Tier 1 — Server and Application Administration

Management of servers, applications, and cloud services. Requires separation from end-user activities with enhanced monitoring and restricted network access.

1.1.3 Tier 2 — Workstation and Helpdesk Administration

Desktop support and helpdesk functions with limited administrative scope. Standard hardened configuration with privilege elevation controls for specific tasks.

1.2 Technical Implementation

Our MAC PAW implementation combines Jamf platform capabilities with security best practices:

- **Apple Managed Device Attestation:** Hardware-bound device trust using the Secure Enclave
- **Jamf Connect:** Zero Trust Network Access with identity provider integration and Conditional Access
- **Jamf Protect:** Real-time threat detection, behavioural analytics, and compliance monitoring
- **Privilege Elevation:** Time-limited administrator rights with full audit logging
- **Smart Groups:** Dynamic device segmentation by privilege tier with automatic policy enforcement

2 SERVICE COMPONENTS

2.1 Device Management (Jamf Pro)

- Zero-touch deployment via Apple Business Manager integration
- Configuration profile management and enforcement
- Application deployment and patch management
- Inventory and asset management
- Full device lifecycle including secure wipe and retirement

2.2 Endpoint Security (Jamf Protect)

- Real-time malware and threat detection
- Behavioural analytics and anomaly detection
- CIS benchmark compliance monitoring
- SIEM integration for centralised security monitoring
- Automated threat response and remediation

2.3 Identity and Access (Jamf Connect)

- Zero Trust Network Access (ZTNA)
- Integration with Microsoft Entra ID, Okta, and Google Workspace
- Conditional Access based on device compliance state
- Single sign-on and passwordless authentication options
- Device trust attestation for resource access decisions

3 COMPLIANCE AND STANDARDS

3.1 NCSC Device Security Guidance

Our service deploys NCSC-published macOS configuration profiles designed to counter commodity threats within the UK Government OFFICIAL Threat Model. Configurations include certificate transparency enforcement, firewall rules, disabled risky features (iCloud, Siri where appropriate), password policies, and FileVault encryption.

3.2 GovAssure and CAF Alignment

The service supports GovAssure compliance across Cyber Assessment Framework objectives:

- **Objective A (Managing Security Risk):** Asset inventory, configuration management
- **Objective B (Protecting Against Cyber Attack):** FileVault encryption, access controls, patching
- **Objective C (Detecting Security Events):** Jamf Protect monitoring, SIEM integration
- **Objective D (Minimising Impact):** Remote wipe, incident response procedures

4 PRICING

Service is priced per device per month with tiered options based on security requirements. Volume discounts apply at 100, 250, and 500+ device thresholds. See separate Pricing Document for full pricing matrix.

4.1 Managed Service Tiers

- **Foundation:** Device management, zero-touch deployment, inventory, standard support
- **Professional:** Adds Jamf Protect endpoint security, compliance monitoring, threat detection
- **Enterprise:** Adds Jamf Connect ZTNA, identity integration, Conditional Access
- **PAW-Secured:** Full privileged access workstation configuration for Tier 0/1/2 access

4.2 Professional Services

Implementation, migration, PAW architecture design, and training services are available at SFIA day rates (£500-£1,150 depending on consultant level). Fixed-price implementation packages available for standard deployments.

5 SUPPORT

Standard Support (included): Named SC-cleared analyst, UK business hours monitoring, monthly reports, policy changes within 2 working days, quarterly reviews.

Enhanced Support (additional cost): Extended hours, priority response, dedicated TAM, custom reporting.

Response Times: 4 business hours initial response. Critical security incidents escalated immediately.

6 QUALIFICATIONS AND CERTIFICATIONS

- All assessors hold Security Clearance (SC)
- Staff screening to BS7858:2019
- Cyber Essentials Plus certified
- Professional certifications: CISSP, CISM, ISO 27001 Lead Auditor/Implementer
- Engagement process aligned to NCSC Certified Cyber Security Consultancy Standard