ALLIED ESM

HALO OFFICIAL PARTNER

# Halo Security & Compliance

## Certifications, Controls & Data Protection

A technical overview for IT security and governance teams.

# Security You Can Verify

Independently audited. Continuously monitored. Fully documented.

Halo Service Solutions holds a comprehensive set of independently audited security certifications and maintains a real-time security monitoring programme across 70+ controls. This document provides a structured overview of Halo's certifications, data protection practices, hosting architecture, and the documentation available to support procurement, information governance, and due diligence processes.

All certifications listed in this document are active and current as of May 2026. Full copies of certificates and audit reports are available on request via Allied ESM.

## Certification Summary

| Certification | Standard | Status |
|---|---|---|
| **SOC 2 Type 2** | AICPA Trust Service Criteria — Security, Availability, Confidentiality | **Active — Audited Annually** |
| **ISO 27001:2022** | ISO/IEC Information Security Management Systems (current edition) | **Active — Surveillance Audits** |
| **Cyber Essentials Plus** | NCSC UK — independently tested (enhanced tier) | **Active — 2026 Certificate** |
| **Cyber Essentials** | NCSC UK — baseline tier | **Active — 2026 Certificate** |
| **UK GDPR** | UK General Data Protection Regulation — Data Processing Agreement available | **Compliant** |
| **DSPT Certificate** | NHS Data Security and Protection Toolkit — Standards Exceeded | **2026-27 — Active** |

## Certifications in Detail

S

### SOC 2 Type 2 — Independently Audited Annually

SOC 2 (Service Organisation Controls 2) is the gold standard for SaaS security assurance. The Type 2 designation is critical: it means an independent auditor has reviewed Halo's security controls in operation over a defined audit period and confirmed they work effectively in practice — not just that they are designed correctly. SOC 2 Type 2 reports for 2024 and 2025 are available under NDA. A SOC 3 public summary report is also available without an NDA.

I

### ISO 27001:2022 — Current Edition Certified

ISO/IEC 27001:2022 is the current version of the international standard for Information Security Management Systems (ISMS). Certification requires an accredited third-party audit of people, processes, and technology. Maintaining certification requires passing annual surveillance audits. The 2022 edition includes updated controls aligned to modern cloud and SaaS environments. The 2025 certificate is available publicly.

C

### Cyber Essentials Plus — Independently Tested

Cyber Essentials Plus is the UK government's enhanced cyber security certification, backed by the National Cyber Security Centre (NCSC). Unlike the baseline Cyber Essentials (self-assessed), Cyber Essentials Plus requires hands-on technical testing by an accredited assessor across five control areas: firewalls, secure configuration, user access control, malware protection, and patch management. Certificates for 2025 and 2026 are available publicly.

U

### UK GDPR — Data Hosted in the UK

UK and EU customer data is hosted exclusively in the AWS London region and is isolated from other geographic regions. Halo provides a full Data Processing Agreement (DPA) on request. Customer data is permanently deleted upon contract termination. Data classification policies and formal retention and disposal procedures are in place and continuously monitored.

D

### DSPT Certificate 2026-27 — Standards Exceeded

The NHS Data Security and Protection Toolkit (DSPT) is the NHS's own data security framework. Halo holds the DSPT Certificate 2026-27 at Standards Exceeded level — the highest tier. This is required or strongly preferred for NHS trust, ICB, healthcare provider, and social care deployments. Certificate available under NDA via Allied ESM.

## Continuous Security Monitoring

Halo's security controls are monitored continuously — not just at annual audit time. 70+ controls are tracked across five categories in real time, with all controls currently passing.

| Category | Controls | Examples |
|---|---|---|
| **Infrastructure Security** | 16 | Production DB authentication, encryption key access restricted, firewall access restricted, network authentication enforced, access control procedures. |
| **Organisational Security** | 14 | Asset disposal, production inventory, portable media encryption, anti-malware deployed, employee background checks, code of conduct, confidentiality agreements. |
| **Product Security** | 5 | Data encryption at rest (AES-256), annual control self-assessments, annual penetration testing, data transmission encrypted (TLS 1.2+), vulnerability monitoring. |
| **Internal Security Procedures** | 33 | BC/DR plans established and tested, cybersecurity insurance, change management enforced, formal SDLC, whistleblower policy, board-level security oversight. |
| **Data and Privacy** | 3 | Data retention procedures, customer data deleted upon leaving, data classification policy established. |

**All 70+ controls are currently passing. Controls are verified continuously — not just at the point of annual audit.**

## Data Protection & Encryption

Halo applies multiple layers of encryption to protect customer data at rest and in transit.

**1**

### Data in Transit — TLS 1.2+ with HSTS

All traffic between customer browsers and the Halo application is encrypted using HTTPS and TLS 1.2 or higher. HTTP Strict Transport Security (HSTS) is enforced on all application servers to ensure no unencrypted traffic can reach the application.

**2**

### Databases and Backups — AES-256 at Rest

All databases and all backups are encrypted at rest using AES-256 key encryption. This applies to production databases, replica nodes, and backup storage (Amazon S3). Even if backup files were accessed externally, the data would not be readable without the encryption keys.

**3**

### Sensitive Fields — X509 Certificate Encryption

Database fields storing sensitive data (passwords, client secrets, custom encrypted fields) carry additional X509 certificate encryption on top of database-level AES-256. Data protection keys are also X509-encrypted, ensuring sensitive data can only be read or written by authorised Halo application servers.

**4**

### Access Control — Principle of Least Privilege

Access to production infrastructure is restricted to Halo infrastructure engineers with a legitimate business need. No logical access is provided to third parties. Any Halo personnel outside this group must go through a formal approval process, with access automatically revoked after a set period.

**5**

### Multi-Factor Authentication

MFA is enforced across all systems used by Halo staff with a public domain. Password policy enforcement follows industry standard best practices. SSO via Azure AD manages access levels centrally across all required software.

## Hosting Architecture & Availability

Halo is hosted on AWS infrastructure, configured for high availability with no single points of failure across the database, application, and network layers.

| Component | Specification |
|---|---|
| **Cloud Platform** | Amazon Web Services (AWS). UK customers hosted in AWS London region, isolated from other geographic regions. |
| **High Availability** | Production-replica database cluster across multiple AWS availability zones. Automatic failover on single node or availability zone failure — zero downtime. |
| **Application Layer** | Blue-green deployment model. Auto-scaling application servers with load balancing. Unhealthy instances removed automatically. |
| **Network Security** | All internal components held in private subnets. Web Application Firewall (WAF) across all regions using managed AWS rules. Public NAT gateway for outbound traffic only. |
| **Intrusion Detection** | AWS GuardDuty, CloudTrail, Security Hub, Inspector, Config, CloudWatch, and Security Lake deployed. Automated alerts and remediation in place. |
| **Availability Target** | 99.95% availability of production instances. |

# Business Continuity & Disaster Recovery

**RTO — Recovery Time Objective**

## 4 Hours

In the event of a large-scale system failure, Halo targets a recovery time objective of 4 hours to restore functionality of production instances.

**RPO — Recovery Point Objective**

## 1 Hour

Halo targets a recovery point objective of 1 hour, ensuring minimal data loss in business-critical circumstances. Transactional backups run every hour (retained 3 days), daily backups are retained for 2 weeks, and monthly backups for 60 days. All backups are tested monthly.

# Requesting Security Documentation

Available on request via Allied ESM.

The following documents are available on request. Some require a Non-Disclosure Agreement (NDA) to be signed before release. Allied ESM can facilitate all requests and provide supporting context for your information governance or procurement team.

- ISO 27001:2022 Certificate — publicly available, no NDA required.
- Cyber Essentials and Cyber Essentials Plus Certificates — publicly available, no NDA required.
- SOC 3 Report (public summary) — publicly available, no NDA required.
- Halo SOC 2 Type II Bridge Letter — publicly available.
- SOC 2 Type 2 Report (2024 and 2025) — requires NDA. Full audit report.
- DSPT Certificate 2026-27 — requires NDA.
- Data Processing Agreement (DPA) — available on request.
- Hosting Architecture Overview — available on request.
- Penetration Test Results — available under NDA on request.
- Full Security Documentation Pack — compiled by Allied ESM on request.

## Get in Touch

info@alliedesm.com | alliedesm.com