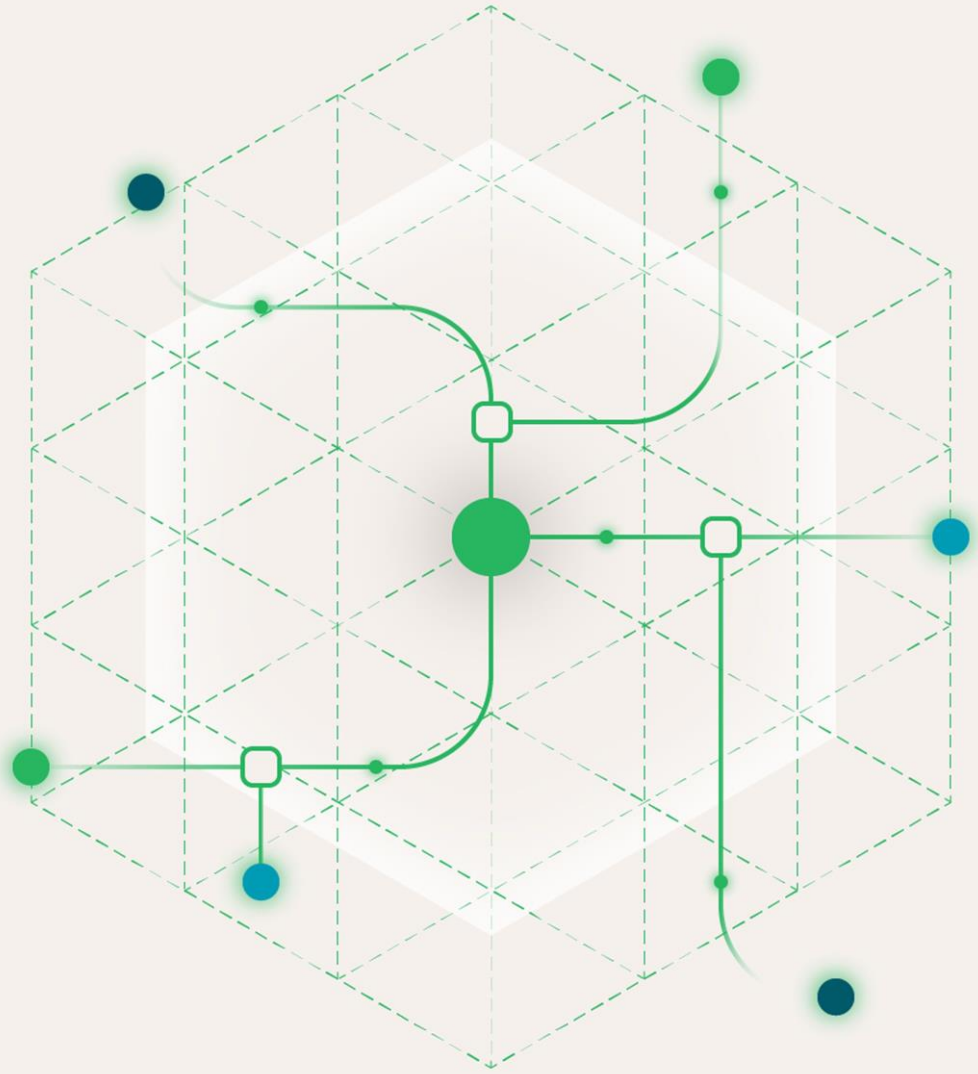
SYNECTICS SOLUTIONS



SERVICE DEFINITION

SynDOC

Synectics Classification: Public

Classification Status: Public

In the UK, please contact:

Synectics Solutions
Hamil Road
Burslem
Stoke-on-Trent
ST6 1AJ

Tel: 0333 234 3409

Synectics Solutions website: http://www.synectics-solutions.com

Document Information	
Document Owner	Jake Harley
Effective Date	14/04/2022
Last Reviewed Date	27/01/2026
Next Review Date	27/01/2027
Classification	Public

Document Control				
Date	**Issue**	**Name**	**Details**	**Sign-off**
27/01/2026	V2	Jordan Roberts	G-Cloud 15	

CONTENTS

1 EXECUTIVE SUMMARY

SynDOC is a document and image analysis service designed to help organisations identify fraudulent or manipulated evidence submitted as part of customer interactions. It supports the automated assessment of unstructured data, including images and documents, to detect potential fraud indicators and repeat misuse.

The service leverages both analytical techniques and syndicated intelligence to identify patterns of fraudulent document submission across participating organisations. This enables organisations to detect serial or cross-sector fraud that may not be visible when reviewing documents in isolation.

2 SERVICE OVERVIEW

SynDOC is a digital image forensics and unstructured data analysis service designed to address the increasing prevalence of fraudulent documentation, including altered, counterfeit or reused evidence.

The service analyses submitted documents and images to identify indicators of manipulation, duplication or reuse. Where permitted, it compares submissions against syndicated repositories to identify repeat patterns across contributors, supporting the detection of organised or serial fraud.

SynDOC can be deployed as a standalone investigative tool or integrated with other Synectics services, including National SIRA, to support broader fraud prevention and intelligence workflows.

3 CORE SERVICE CAPABILITIES

3.1 DOCUMENT AND IMAGE ANALYSIS

SynDOC supports the analysis of a wide range of document and image formats and provides capabilities including:

- Detection of potential image or document manipulation
- Identification of duplicate or reused fraudulent evidence
- Comparison against known authentic and counterfeit document templates
- Analysis of embedded metadata to identify inconsistencies or anomalies

These capabilities support both automated screening and investigator-led review.

3.2 SYNDICATED INTELLIGENCE AND MATCHING

Where applicable, SynDOC enables matching of document and image submissions across a multi-sector contributor network. This supports the identification of repeat submissions and shared fraudulent templates across organisations.

Participants cannot directly access other organisations submitted data; however, relevant matches and associated risk indicators are surfaced to support investigation and decision-making.

3.3 ADVANCED ANALYTICAL FEATURES

Additional analytical capabilities can be enabled where required, including:

- Enhanced similarity matching using proprietary matching techniques

- Advanced manipulation detection using trained tamper detection models
- Reverse image searching against publicly available sources

These features are available subject to agreed scope and commercial terms.

4 KEY BENEFITS

- **Detection of Emerging Evidence Fraud:** Supports identification of manipulated or artificially generated documents and images.
- **Protection Against Repeat Submissions:** Identifies reuse of fraudulent evidence across applications, products or organisations.
- **Improved Consistency and Fairness:** Supports proportionate, timely decision-making by prioritising higher-risk submissions while reducing manual effort for lower-risk cases.
- **Collaborative Intelligence:** Enables cross-sector sharing of fraud patterns and document intelligence within a governed framework.

5 SERVICE AND DELIVERY SUPPORT

5.1 IMPLEMENTATION AND ONBOARDING

Implementation of SynDOC is supported by a dedicated Project Manager who will:

- Manage the project plan and onboarding activities
- Configure data ingestion and analysis settings
- Lead production deployment
- Deliver training for operational users

The service can be configured to align with investigative workflows and organisational risk appetite.

6 TECHNICAL OVERVIEW

6.1 ACCESS AND CONNECTIVITY

SynDOC is a secure, web-based service accessible via modern browsers. Access is restricted to authorised users and may be controlled through pre-approved network and IP-based controls.

6.2 DATA INGESTION AND PROCESSING

SynDOC supports multiple methods of data submission, including:

- Real-time API integration
- Batch uploads
- Ad hoc submissions via the user interface

The service can operate as a standalone investigative tool or be integrated with National SIRA and other Synectics services.

Typical response times for real-time analysis are within seconds, subject to agreed service scope.

6.3 DATA STORAGE

SynDOC provides centralised storage for ingested unstructured data using secure cloud-based services. Data access is controlled to ensure that organisations cannot view other contributors' underlying documents, while still benefiting from relevant match indicators where applicable.

7 DATA SECURITY AND ASSURANCE

Synectics Solutions operates a formal Information Security Management System aligned with ISO/IEC 27001.

The organisation is committed to:

- Protecting information against unauthorised access
- Maintaining confidentiality, integrity and availability of data
- Meeting applicable regulatory and legislative requirements

Risk management activities and periodic assessments are undertaken to ensure ongoing alignment with recognised good practice and evolving security requirements.

8 SUPPORT AND SERVICE MANAGEMENT

Synectics Solutions provides ongoing support for its services to ensure availability, performance and continuity in line with agreed service levels.

8.1 SUPPORT AVAILABILITY

Standard application support is available:

- Monday to Friday, 07:00–19:00 (UK time)
- Excluding public holidays in England and Wales

Support services are delivered in accordance with ITIL-aligned service management practices. Services are actively monitored, and incidents are managed using structured processes to ensure timely restoration, effective communication and appropriate escalation. Where required, incident summary reports and root cause analysis are provided, and outcomes are used to drive continuous service improvement.

Extended support hours, including out-of-hours and weekend support, can be agreed on request, subject to commercial and service agreement.

8.2 ACCOUNT MANAGEMENT

All customers are provided with a dedicated account team, which typically includes a Client Success Manager, Service Delivery Manager and Account Development Manager.

This team acts as a trusted extension of the customer's fraud and financial crime function and supports:

- Ongoing optimisation of the service
- Alignment of service configuration with business objectives
- Strategic planning, benchmarking and roadmap development
- Industry collaboration and knowledge sharing

This engagement model ensures customer requirements are reviewed on a continual basis and that services evolve in line with operational and regulatory needs.

9 DISASTER RECOVERY AND BUSINESS CONTINUITY

Synectics Solutions maintains a formal disaster recovery and business continuity framework designed to ensure service continuity, data protection and controlled recovery in the event of a major incident.

9.1 RECOVERY ARCHITECTURE

Services are delivered from a primary UK-based private cloud environment, supported by a separate secondary disaster recovery environment.

Data and system components are protected through backup and recovery mechanisms aligned to the following standard recovery objectives:

- Recovery Time Objective (RTO): 48 hours
- Recovery Point Objective (RPO): 24 hours

Improved RTO and RPO targets can be agreed on request, subject to service scope and commercial agreement.

9.2 DISASTER RECOVERY PROCESS

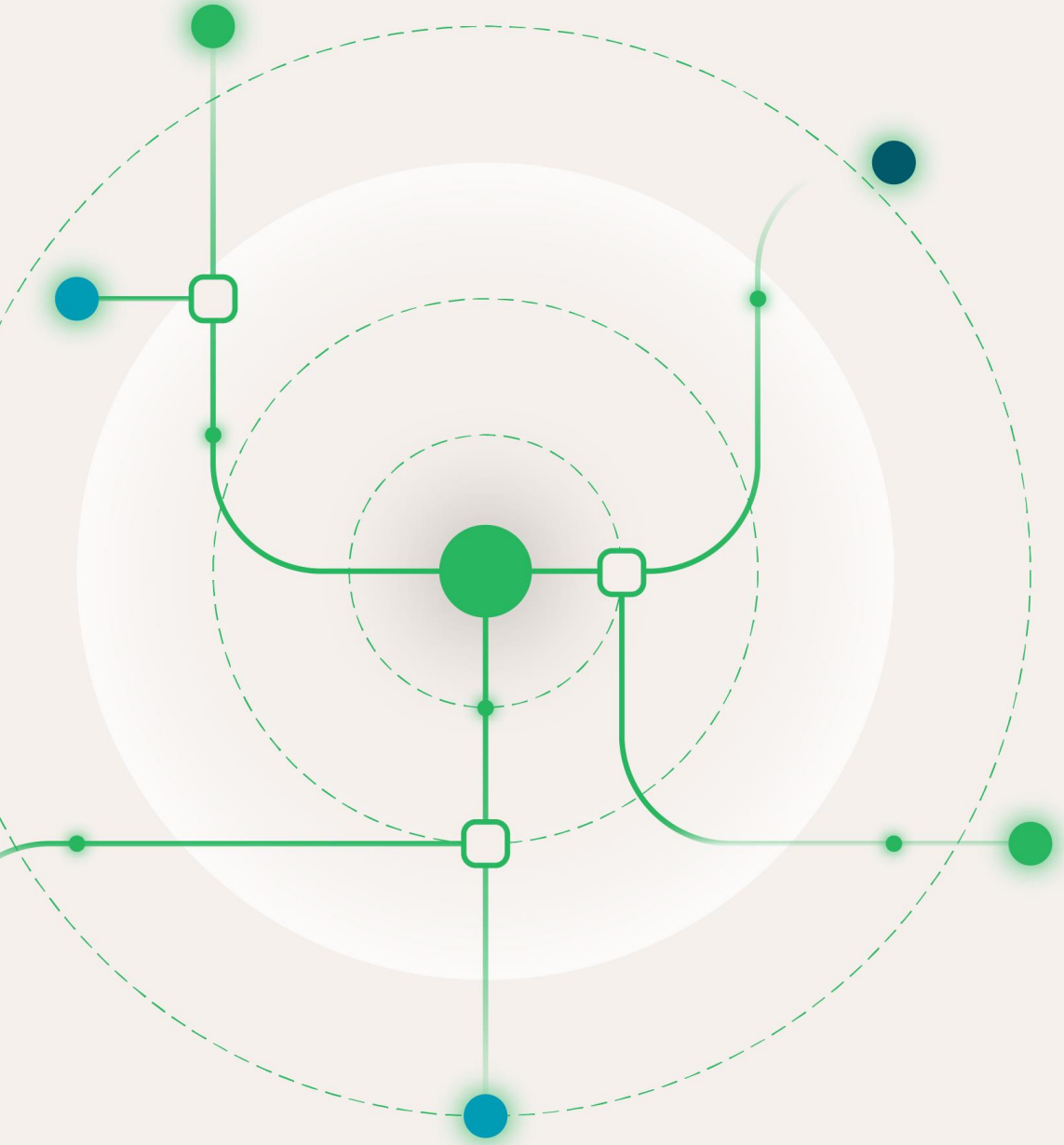
In the event of a critical service failure, documented procedures are followed to:

- Assess the nature and impact of the incident
- Invoke disaster recovery controls where required
- Restore services using the secondary environment and available backups
- Validate system integrity and data consistency prior to resuming normal operations

Recovery activities are governed by documented runbooks, clear escalation paths and defined roles and responsibilities to ensure a controlled and auditable response.

9.3 TESTING AND GOVERNANCE

Disaster recovery procedures are tested periodically to ensure effectiveness and operational readiness. Test outcomes are reviewed and used to strengthen resilience, refine recovery processes and support continuous improvement of the overall service.



SYNECTICS SOLUTIONS