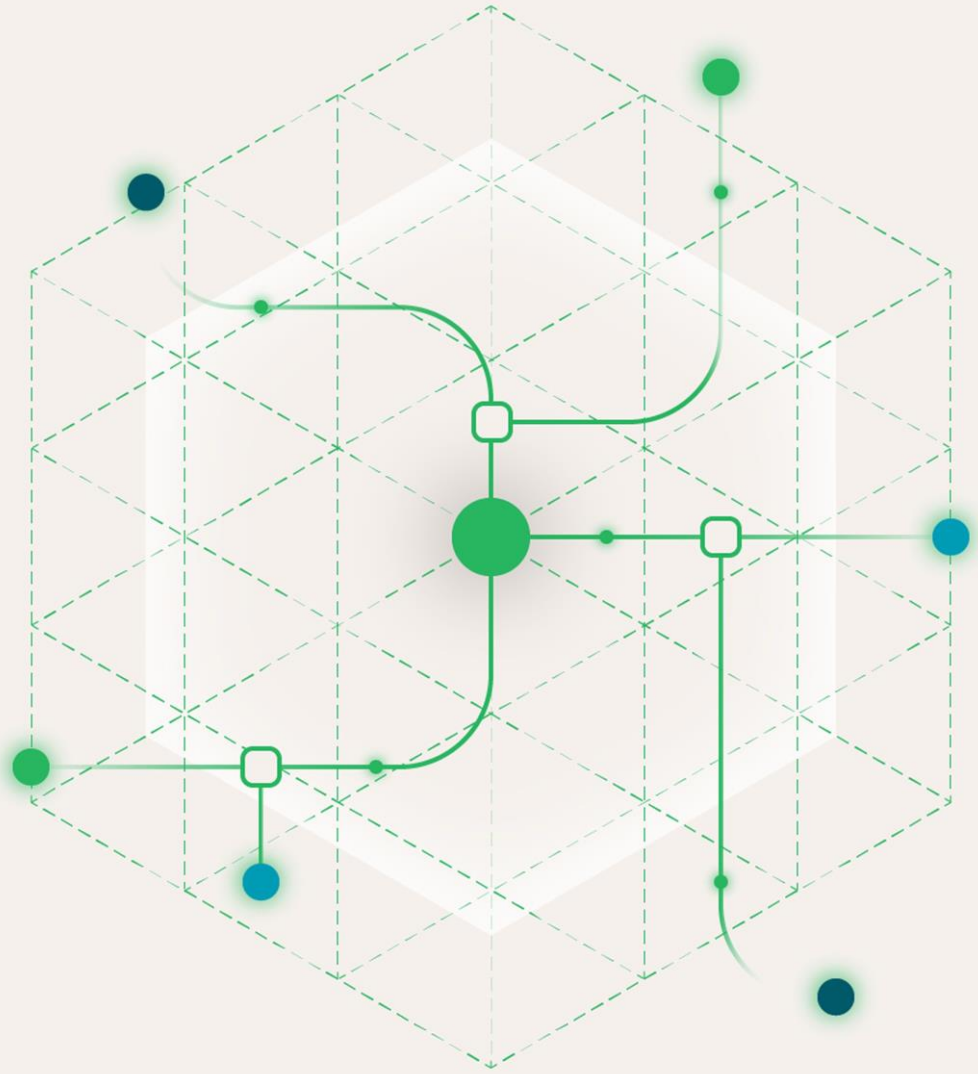
SYNECTICS SOLUTIONS



SERVICE DEFINITION

Orion

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

Orion is a network visualisation and analysis service designed to help organisations identify, investigate and respond to organised fraud and financial crime. It enables users to uncover hidden connections between applications, policies, claims, accounts or parties, providing greater visibility of complex fraud networks and exposure.

Orion operates by analysing linked data at both a local organisational level and, where applicable, across nationally shared intelligence. The service supports both manual and automated network creation, allowing investigators to understand the full context of suspicious activity and prioritise investigative effort.

Orion is part of the Synectics Solutions fraud prevention and intelligence suite and can be deployed either as an integrated capability alongside SIRA or as a standalone service using third-party or proprietary data sources.

2 SERVICE OVERVIEW

Orion is a web-based data visualisation and network analysis service that helps organisations identify organised fraud patterns and interconnected risk that may not be apparent through single-transaction or single-application review.

The service analyses relationships between data elements such as individuals, addresses, devices or accounts, using configurable matching criteria defined by the customer. These relationships are presented visually as networks, enabling investigators to explore connections, assess risk and manage investigations more efficiently.

Network analysis can be performed:

- **Manually**, where users create and explore networks as part of an investigation
- **Automatically**, where defined behaviours or triggers generate networks without manual intervention

Orion is designed to be configurable and usable by operational teams, without requiring specialist technical skills.

3 CORE SERVICE CAPABILITIES

3.1 NETWORK CREATION AND ANALYSIS

Orion supports the creation and analysis of networks in multiple ways, including:

- Manual creation of networks from selected cases, parties or events
- Automated generation of networks based on defined behavioural or risk profiles
- Use of configurable matching rules to determine how entities are linked
- Ability to apply different visual representations to support investigation

Networks can be analysed to identify central or high-risk entities and to understand the structure and scale of organised activity.

3.2 AUTOMATION AND CONFIGURATION

The service provides a high degree of configurability, including:

- Definition and management of automated network-building strategies
- Control over trigger events and matching criteria
- Deployment of multiple targeted profiles to proactively identify emerging networks
- Configuration of network scoring models and investigative task workflows

This allows organisations to tailor Orion to their specific fraud risks, operating models and investigative priorities.

3.3 INTEGRATION WITH SIRA AND OTHER DATA SOURCES

When deployed alongside SIRA, Orion can analyse and visualise networks using underlying SIRA data, including the ability to identify links via nationally shared intelligence where appropriate.

Orion can also operate independently of SIRA and ingest data from a wide range of third-party or internal data sources, enabling flexible deployment within an existing fraud and financial crime ecosystem.

4 KEY BENEFITS

- **Improved Visibility of Organised Fraud:** Helps uncover complex and previously hidden connections between related cases or parties.
- **Operational Efficiency:** Reduces investigative effort by presenting linked activity visually and prioritising high-risk networks.
- **Flexibility and Control:** Configurable rules, automation strategies and visualisations aligned to organisational needs.
- **Scalable Deployment:** Suitable for both targeted investigative use and broader, proactive network detection.

5 SERVICE DELIVERY AND SUPPORT

5.1 IMPLEMENTATION AND ONBOARDING

Orion is delivered as a hosted service. Implementation and onboarding are supported by Synectics Solutions, including:

- Configuration of data sources and matching criteria
- Support for integration with SIRA or other systems
- User training for investigators and operational teams

The service is designed to operate for extended periods without manual intervention once configured.

5.2 SUPPORT AND SERVICE LEVELS

Support is provided via telephone and email.

- **Standard support hours:**
  07:00–19:00 GMT, Monday to Friday (excluding public holidays in England and Wales)

- **Out-of-hours support:**
  Severity 1 and 2 incidents may be reported outside core hours, including evenings, weekends and public holidays, with on-call support available. Extended 24-hour support can be provided by agreement.

- **Service availability:** minimum 99.0%

Planned maintenance is scheduled outside UK core business hours (07:00–20:00) and typically does not exceed:

- 3 hours per month for infrastructure maintenance

- 3 hours per quarter for software releases

All planned maintenance is agreed in advance where possible.

5.3 INCIDENT MANAGEMENT

Incidents are managed through a structured support model, including:

- **Severity 1 (Critical Incident):**
  Examples include system-wide outages or severe degradation. Immediate response with sustained effort until resolution.

    - Target resolution: within 4 hours

    - Status updates provided at regular intervals

6 TECHNICAL OVERVIEW

Orion is delivered as a secure, web-based service hosted by Synectics Solutions. It is built on resilient, industry-standard infrastructure with redundant components to support high availability and fault tolerance.

The service can be accessed through standard web technologies and integrated with upstream systems and data feeds as part of a broader fraud prevention architecture.

7 DATA SECURITY AND ASSURANCE

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

The organisation is committed to ensuring that:

- Information is protected against unauthorised access

- Confidentiality, integrity and availability of data are maintained

- Applicable regulatory and legislative requirements are met

Security controls and risk management processes are reviewed regularly to ensure continued alignment with best practice and customer 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

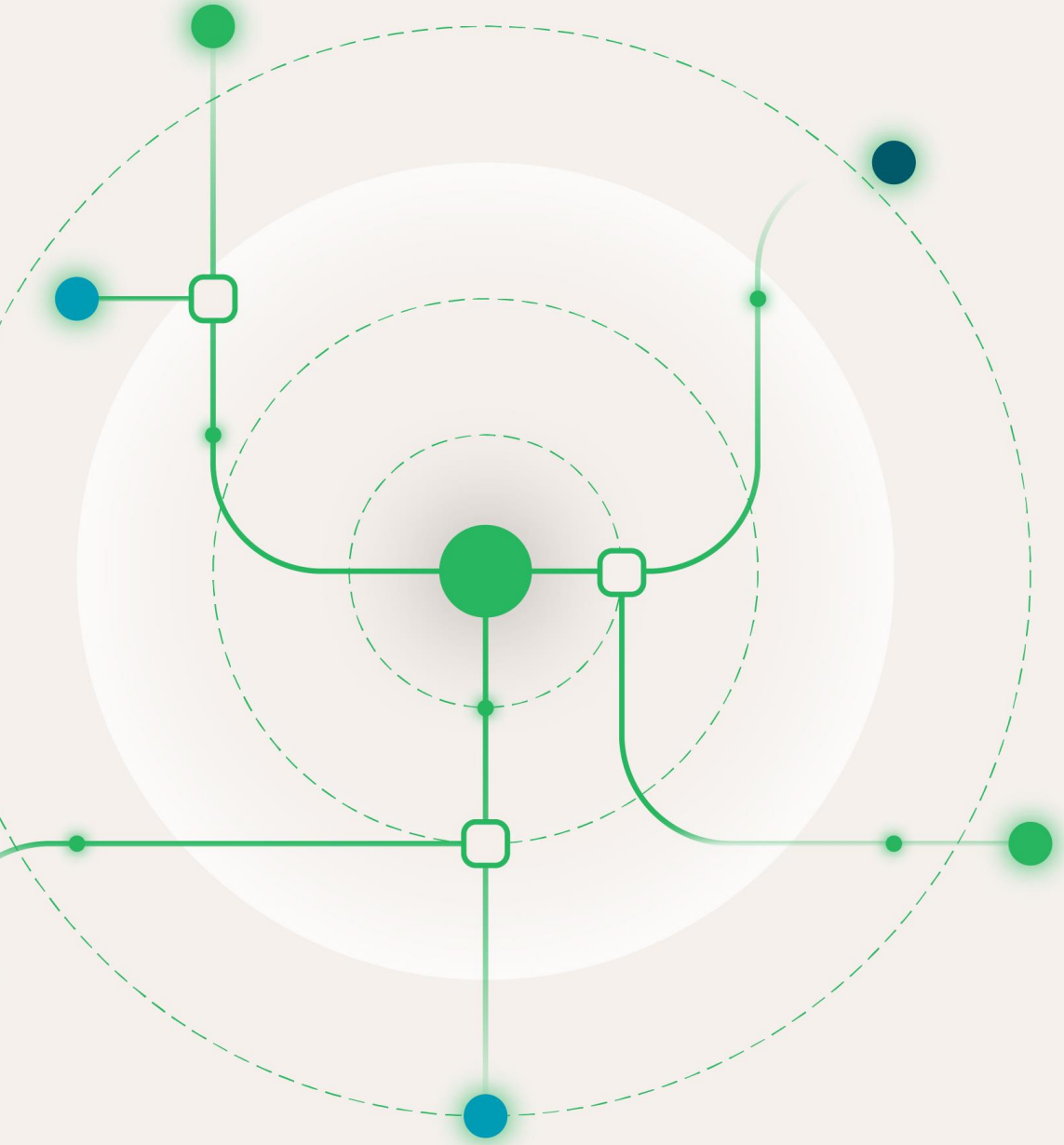
In the event of a critical service failure, documented procedures are followed to:

- 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