Blackdot Solutions Videris Services Definition

About Blackdot Solutions

Blackdot Solutions is a UK-founded and owned SME based in Cambridge. Our mission is to help investigators use OSINT for good by equipping them with the software they need to combat criminal activity effectively.

Our solution, Videris, was designed for investigators in UK law enforcement and government agencies, and is now used on a global scale. We combine our investigations expertise with the power of AI and automation to transform manual investigation processes.

About Videris

Videris is an end-to-end investigations platform that centralises and streamlines OSINT workflows with AI and automation, allowing investigators to work faster and improve effectiveness. We offer two solutions which can be combined for maximum impact and workflow coverage.

Videris Investigate

Videris Investigate is an investigator-driven complex investigations solution with flexible access to data sources, advanced visualisation and analysis tools. With Videris Investigate, investigators can:

- Search securely and anonymously across multiple hard-to-access sources at once, with hard-to-spot connections automatically flagged to ensure high accuracy levels and unique insight.
- Map networks from publicly available social media data to gain valuable context on subjects of interest.
- Improve global reach of investigations by using a platform that works in any language or script.
- Use an interactive AI-enabled investigative assistant (Videris Investigative Assistant /VIA) to expedite investigations.
- Analyse and report more easily, facilitated by advanced network visualisation tools with integrated AI and automation.
- Access integrations with multiple premium data providers and integrate internal data sources for seamless data access and visualisation.
- Benefit from Videris' full integration with Long Arm® Desktop for secure, end-to-end investigations.

Videris Automate

Videris Automate combines Blackdot's expertise in external data, investigations and intelligence with the latest in agentic automation technology. It expedites repetitive investigation processes by removing the time-consuming manual steps common in many investigations. With Videris Automate, investigators can:

- Create customisable playbooks per investigation type, including predefined data sources and investigation goals.
- Remove manual steps by using agentic AI to run initial investigations, keeping a human in the loop who retains full decision-making power.
- Trigger investigations headlessly or through a human investigator.
- Receive a fully sourced, explainable report covering key findings, connections and risks – in seconds or minutes.
- Escalate an automated investigation to Videris Investigate for a dynamic, human-driven investigation with flexible source access.
- Monitor investigations and be alerted to changes.

Why is Videris unique?

Single platform

Videris is an all-in-one, intuitive investigations platform which allows users to collect, analyse and visualise data in one place. Instead of focusing only on structured or curated data sets, Videris allows users to search across all relevant sources, including live unstructured internet data, in one platform. Any repository with an API can be accessed from within the platform, thanks to Videris Extension Builder. Investigators can quickly gain a single subject view, assisted by intelligent automation which allows them to get to the data they need faster and uncover hidden insights.

Unique chat investigator

Videris Investigative Assistant (VIA) is an AI-enabled interactive chat assistant designed to help investigators work more effectively with large volumes of case data. Users can ask VIA to identify connections, risks and possible avenues of investigation.

AI and automation

We are the experts in leveraging Open Source Intelligence to enhance public sector investigations. Our unique expertise in data and investigations means that we are well-positioned to support teams implementing AI and automation technologies in this security-conscious, high-stakes context. Videris differs from many commercially available AI solutions in four key areas:

Accuracy

- We ground our data in trusted curated data sets. This allows AI within Videris to build its reasoning on fact, safeguarding against hallucination and bias.

Evidence and auditability

- We use a 'chain of thought' reasoning process, providing a human-readable account of every step and decision the AI has taken, including sourcing of insights.
- Videris Automate allows organisations to define the sources and types of information they are interested in, creating consistency across enterprise investigations.
- We also provide prompt management capability, allowing admins to create approved prompts and review where they have been used.

Technology

- We combine LLMs with other technologies to achieve the context-aware reasoning across networks that is essential to many investigations.
- We provide unique, targeted 'playbooks' that help to direct AI technologies to identify clear, sourced and relevant insights investigators can trust.

Security and ethics

- We allow the human to remain in the loop so that sensitive decisions are not made without oversight.
- We never use customer data for AI training and store the minimal possible data from investigations for customer audit purposes.

Key Features

Videris can be deployed alongside and enhance the functionality of many commonly-used investigative technologies, or can operate as a standalone solution.

Videris Investigate

Search

- Search across multiple selected data sources simultaneously.
- View and filter results by source, topic, risk categories and extracted entities, and add relevant results to the chart. Use NLP to identify and extract entities (names, addresses, contacts, etc.),
- Apply contextual intelligence, entity extraction, and custom filters for specific key terms.

Visualisation

- Automatically map & visualise networks using data from sources such as publicly available social media, corporate records and more on the Videris chart.
- View and filter data in table format.

Reporting

- Export findings and charts in multiple formats (jncluding CSV, PDF, PNG and .docx).
- Create, customise and export entity-specific or full case reports.
- Users can attach positive results and free text to entity reports. Entity reports can be exported in Word or CSV format.

Analysis

- Automatic risk identification: Rapidly assess an entity's risk profile by automatically screening case data against risk databases and identifying potentially high-risk entity attributes on the chart.
- Automated detection and highlighting of similarities, duplicates and potential links.
- Leverage Watchlists to check case data automatically against user-defined lists (from Videris cases or uploaded CSV).

Explore web content securely

- Navigate the live internet anonymously and securely, including high-risk sources such as dark web content.
- Use optional integrated AI tools to summarise, translate, and extract entities from web content.
- Use built-in translation for online content.
- View public social media posts, comments, and profiles securely with the Social Media Explorer.

Videris Automate

- Automate searches across selected data sources using AI to speed up investigation tasks.
- Create standardised 'playbooks' to automate initial steps for each investigation type (such as vetting or enhanced due diligence) and define report output.
- Incorporate and customise investigation goals, predefined sources and desired output.
- Ensure efficient, standardised, accurate and human-readable reports or other desired output, including full sourcing and explainable step-by-step reasoning.
- Monitor topics to detect changes, patterns and trends by setting automated searches to periodically re-run based on user-defined frequency and term
- Build custom prompts/queries where they are supported and available from the target source.

Security and operations

User roles

- Share cases with colleagues to enable case collaboration and review, according to their user role and permissions.
- Videris offers 3 types of user roles: Administrator, Investigator and Reviewer.
- Each user with an "Investigator" role requires a Named User Licence to create cases and run investigations.
- Administrator (only) and Reviewer (only) roles do not require a Named User Licence. Reviewers are able to review cases which are shared with them in a read-only mode.

Case deletion and data retention

- Ability to manually delete and schedule the deletion of cases.
- Ability to schedule deletion of data.

Audit
All data is fully sourced to show the origin of the result. All user actions are tracked and logged, including CRUD (Create, Read, Update and Delete) activity, providing a comprehensive audit trail.

Access
Videris offers Single Sign On (SSO) and Multi-factor Authentication (MFA) to ensure data security and compliance with internal data security requirements.

Data Sources

Videris integrates with numerous providers of open source data, as well as search engines and premium data providers, allowing investigators to access them all securely from a single platform. Examples of these include:

Data source type	Examples:
Corporate registries	Moody's Orbis*, OpenCorporates
Search engines	Google, Yahoo
News media	Google News, Lexis Nexis News**
Social media	Profile searches and some content from major social media platforms (where publicly available) is included in every license. Additional public data from a range of mainstream and niche platforms available at an additional cost**
Dark web data	NA**
Risk databases	Moody's GRID*, LSEG World-Check One*
Breach and leaks data	ICIJ Offshore Leaks, OCCRP Aleph, District4**
Online profile data	GBG**, Pipl
Domain data	Hexillion, WHOIS

* Organisations must provide their own license key to use this source
** This source may incur an additional cost

Alongside the above sources, organisations can integrate additional sources (such as proprietary, internal or niche sources) using the Videris Extension Builder.

Deployment and Support

Secure Deployment

Videris is a fully secure SaaS platform. It is equipped with advanced security features which are tested regularly to stay ahead of evolving threats. These measures ensure that the platform is fully GDPR compliant and that all client data remains secure, private and accessible only to authorised personnel. Additionally, Blackdot Solutions is ISO/IEC 27001 and Cyber Essentials Plus Certified, demonstrating our unwavering commitment to exceptional security and data protection standards.

For Long Arm® customers, Videris can be accessed via the Long Arm® Desktop for additional security capabilities.

Ongoing Training and Support

Blackdot Solutions offers world-leading training and support. As part of the initial onboarding process, your team will receive dedicated, online training at a convenient time. Once a team is familiar with Videris, our Customer Success team provides up to two ongoing 2-hour training sessions to answer more detailed questions. They also conduct regular business reviews and users have access to automated in-app help to ensure maximum benefit from the product.

Our Support Team is available to offer advice, solve problems and report any issues. We respond quickly to these and take product feedback very seriously.

Additional Services

Blackdot offers a range of professional services to support every organisation's deployment, training and operational requirements. These can include:

- Additional training sessions with Subject Matter Expert
- Access to Subject Matter Expert for workflow and investigation support
- Beta testing and roadmap feedback sessions
- Technical consultancy including custom-built Videris Extensions

Videris SLA

Service Availability

We commit to a minimum 99.5% uptime per calendar month. Uptime is calculated as the percentage of total possible minutes that Videris was available to users during the calendar month. The uptime calculation excludes scheduled downtime, customer equipment or external network problems, unauthorised access, or issues which are related to third parties or otherwise outside of Blackdot's reasonable control. We use an independent third-party tool to continuously monitor whether Videris is available or not, and to automatically calculate the uptime percentage over a period of time.

Customer can report issues and raise support requests with Blackdot at any time by emailing support@blackdotsolutions.com

Blackdot will aim to respond to and resolve issues within the following time periods, during UK working hours (0800-1800 local, Monday to Friday, excluding UK public holidays)

Priority	Description	Response time	Resolution time
P1	• Service outage – Videris is unavailable to customer (service availability incident) • Data or security is compromised (data security incident)	1 hour	1 day
P2	• Functionality or performance is degraded such that typical usage is difficult. • Individual user access problem (e.g. disabled account)	3 hours	3 days
P3	• Functionality or performance is degraded such that typical usage is impaired. • New user accounts or account servicing.	1 day	10 days
P4	• Any other defect or concern. • General information or feature request.	3 days	As advised

Additional comments

- In the event of service or data loss (P1) the Recovery Time Objective is 1 working day. The Recovery Point Objective is up to 24 hours (i.e. restore to the most recent daily back-up).
- Blackdot shall assign a priority rating to each support request in line with its triage policies.
- Blackdot shall keep Customer informed of any relevant updates in a timely manner.
- Customer must commit necessary resources to support diagnosis and resolution of issues.
- Target resolution times may be impacted by external factors beyond Blackdot's control (e.g. third-party data source issues or force majeure events).