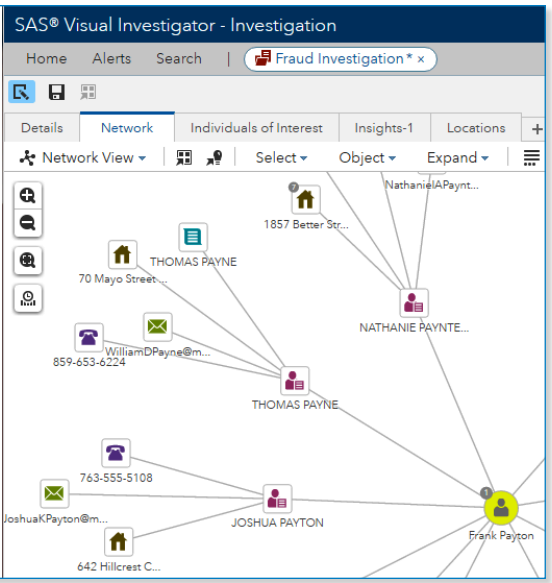
SAS® Visual Investigator

Fast and effective intelligence analysis and investigation



What does SAS® Visual Investigator do?

SAS Visual Investigator is a cloud-ready investigation and incident management solution that combines large, disparate, structured and unstructured data sources. Users can define, create, triage and manage alerts; perform detailed investigations; and customize the platform to meet their individual and organizational needs.

Why is SAS® Visual Investigator important?

Dealing with mounting complexity, analysts and investigators need to boost their efficiency to make sense of the velocity of alerts and far-reaching networks. With SAS Visual Investigator, you can perform deep investigations to uncover hidden behaviors and activities, then share them across your organization for optimal team coordination.

For whom is SAS® Visual Investigator designed?

SAS Visual Investigator is designed for banks and financial institutions looking for fraud and money laundering, national security and law enforcement organizations looking for terrorism and criminal activities, legal firms conducting discovery, and hospitals and public health organizations guarding against disease outbreaks.

Providing the full power of SAS advanced analytics and machine learning, our solution has an interactive interface for investigators to conduct visual and directed investigations. This self-service approach can reach throughout your organization so that users can perform any number of activities, such as simple data import, point-and-click exploratory analysis and access to third-party systems.

Streamlined deployment options and IT administrative functions allow you to evolve the solution as your user community changes. To adapt to market conditions and organizational changes, business process owners can tailor the solution to their needs and specific business objectives without expensive customization.

Features include text and geospatial search and analysis, data visualization, interactive network building, entity generation and transaction analysis. All of this enables you to proactively identify areas needing further investigation, respond to anomalous and suspicious activity as it is happening, and address the demands of regulatory compliance and internal audits.

When all your data is easily accessible, well-governed and up-to-date, analysts and investigators can gain a holistic view of people, relationships, networks, patterns, events, trends and anomalies to keep your organization one step ahead.

Benefits

- **Tailor the configurable solution platform to each user's requirements without expensive customization**. An open, data-driven approach in a hub-and-spoke topology ensures solution capabilities can be configured, enabling you to respond to new trends and business problems, access new data sources, and expand the use of the solution across your business as needed.
- **Empower your users and increase efficiency**. Our solution automates much of the data management, triage and workflow to streamline your operations and enable analysts to make decisions quickly. With an easy-to-use interface in a single solution, users can import data, perform advanced searches, and apply temporal or geospatial methodologies while investigating business problems or search results.
- **Harness data in place**. Unlike traditional approaches that require the added expense of data models, ETL, on-site engineers and ad hoc customizations, the SAS approach takes advantage of your data where it lives – regardless of size, structure and format. To meet your unique challenges, you can tailor the solution so that large numbers of analysts and investigators can actively analyze and make decisions from deep investigational searches on data residing throughout your organization.
- **Minimize your total cost of ownership through cloud deployment options and configuration**. Our architecture is engineered to run your analytics processing wherever you need; you can deliver key functions with your preferred deployment model.
- **Understand deep, simply presented analytical insights**. Analysts shouldn't be expected to know the difference between a p-value and a t test. We deliver descriptive and understandable reasons why an event has occurred or an alert is generated to broaden the reach of analytics throughout your organization.

Overview

SAS Visual Investigator is an easy-to-use solution to identify, investigate and govern the end-to-end life cycle of an investigation, search or inquiry. The span of capabilities provides organizations with the ability to acquire, analyze, identify, make decisions and act on events of interest and suspicious activities. Designed with productivity and efficiency in mind from the start, SAS Visual Investigator provides:

- **Alerting and event management**: Analysts and investigators can investigate and disposition alerts and events; initiate cases for deeper investigation; and actively route or make decisions on events of interest as they occur, virtually eliminating information lag.
- **Streamlined alert administration and workflow**: Managers and domain experts can prioritize analyst activities, monitor productivity and effectiveness, and adapt surveillance strategies to new and emerging patterns.
- **Agility to adapt to changing business needs**: Without any custom interfaces to develop, administrators can quickly design and deploy new intelligence assets using an interactive, drag-and-drop page builder.
- **Targeted investigations**: The Insights module is an easy-to-use interface that captures views of a workspace and search visualizations (e.g., maps, timelines, grids and networks), as well as notes and images documented by the analyst. Dynamic workspaces provide analysts with the ability to gather pertinent data and interact with visualization components as part of an investigation.

Capabilities

Search and discovery

Perform free-text or geospatial searches across all data (from internal and external sources). Then filter and visualize search results in different ways to aid investigations and discover pertinent information about entities, resolved entities and relationships, and initiate actions such as adding results to investigation workspaces for further analysis.

Features include:

- **Free-text search**: Discover data that is pertinent to an investigation with powerful search capabilities.
- **Search filters/facets**: Refine search results using interactive filters and facets.
- **Form search**: Perform a field-based search for a specific entity type, such as first name and surname for an individual or registration/license plate number to find a specific vehicle.
- **Query Builder**: Construct complex queries through an intuitive interface without the need to understand specific syntax. For example, use fuzzy searching, proximity searching and field boosting while restricting searches to specific entity types, fields, comments or insights.
- **Inspector**: Preview and refine details of search results interactively.
- **Selection tools**: Highlight and collate objects for further investigation.

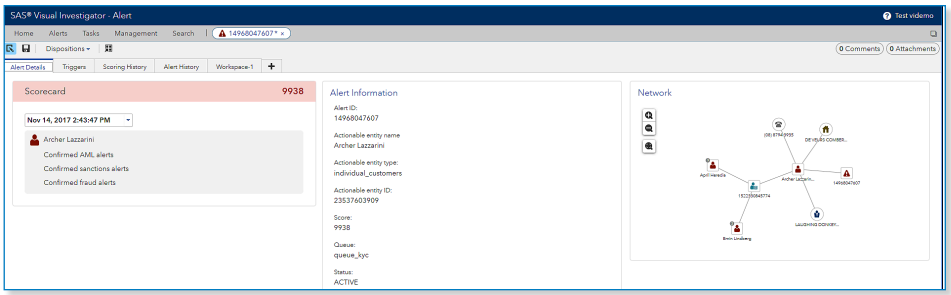


Figure 1: Analysts can view details of the rules that caused this alert to be created and the overall alert score. They can explore the associated social network and view other information helping them triage the alert and take action.

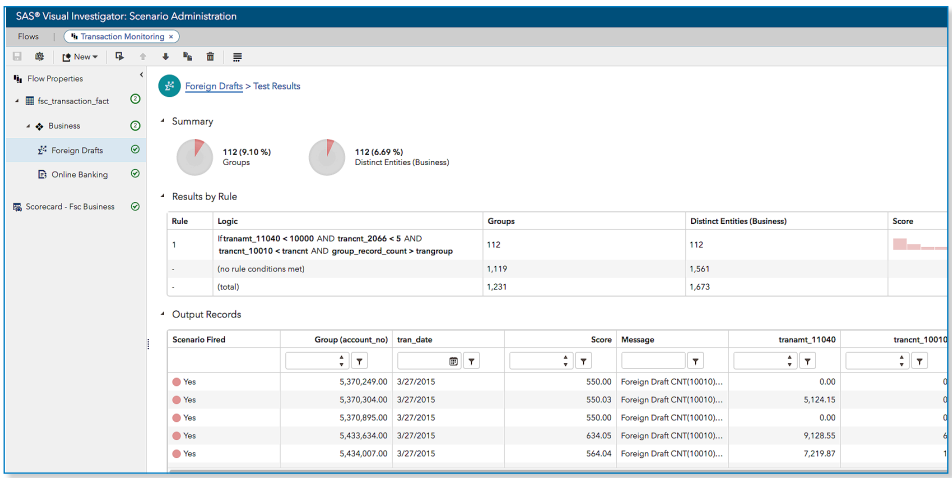


Figure 2: Analysts can author and test surveillance scenarios to identify suspicious events and anomalies in the data and generate alerts.

Surveillance

Using an intuitive user interface, you can author scenarios generating alerts in alert management queues for analyst review. Advanced SAS users can create rules.

- Author scenarios using rule builder, decision table or SAS code.
- Restrict defined scenarios for parameter adjustment by role.
- Test scenarios.
- Create a score based on scenario(s).
- Execute in batch or on demand.

Alert and event management

SAS provides a comprehensive decision management function where alerts and events of interest can be discovered and triggered through the deployment of advanced analytic models, business rules, scenarios or integration with third-party

systems (communicating back and forth). The alerts and event management capabilities enable you to:

- Prioritize alerts.
- Visualize alerts in different views to gain context.
- Enhance alerts by adding entities and integrating and connecting data.
- Escalate by routing alerts or changing their priorities.
- Set up auto-disposition options.
- Provide a management overview of disposition activity.
- Designate an alert to prompt a deeper investigation.

Entity analytics

SAS is set apart by interactive entity resolution capabilities that help analysts get the most accurate picture of complex relationships. SAS entity analytics supports and directs analysts and investigators by showing entity closeness, betweenness and influence to highlight areas of potential interest. Seeing the complex network of relationships between people, places, things and events over time and across multiple dimensions helps analysts identify relationships that aren't obvious, traverse and query complex relationships, and uncover patterns and communities interactively.

Analysts can also interact through the network viewer to see entire social networks. They can expand or trim the network as required, explore communities and individual relationships, and manipulate the network layout. Finally, they can take snapshots and clips of the insights that they develop, collaborate with other investigators and document their findings.

Features include:

- **Network viewer/node link diagram (NLD)**: Visualize and interactively explore networks and network layout, develop communities, and identify relationships that aren't obvious.
- **Link expansion**: Visualize complete networks and relationships through multilevel expansion.

Key Features

Search and discovery
- Free-text search.
- Form search and Query Builder.
- Filters and facets.
- Geospatial search, exploration and visualization.

Alert and event management
- Governance, audit and compliance.
- Prioritized queuing model.
- Enrichment.
- Scenario-fired event model, including scenario context.
- Disposition options and management overview.
- Case creation from alerts.

Entity analytics
- Entity resolution.
- Network analytics and visualization.
- Network link expansion.
- Network node decorator and enrichment.

Transaction analysis
- Transaction network visualization.

Targeted investigations
- Interactive investigator workspaces.
- Insights to record findings.
- Print Insights.
- Data visualization (grids, maps, timelines, networks, detailed views).

Case management
- Workflow.
- Ability to add attachments.
- Role-based home pages with cascading grid layout.
- Structured printing.

Surveillance engine
- Author scenarios using rule builder, decision table or SAS code.
- Restrict defined scenarios for parameter adjustment by role.
- Scenario testing.
- Creation of score based on scenario(s).
- Batch or on-demand execution.

Administration and configurability
- Open data model.
- Easy addition of new data sources.
- Page/home page design with a drag-and-drop interface.
- Defining of links/relationships (i.e., what types of links users can create).
- Application configuration import/export.
- Data import or query by reference from internal or external sources.
- Search configuration.
- Define entity-level security model.
- Events model for maps and timelines.
- Link traversals.
- User permissions.
- Monitor back-end processes, workflows and tasks.
- Detailed auditing of user actions and activity.

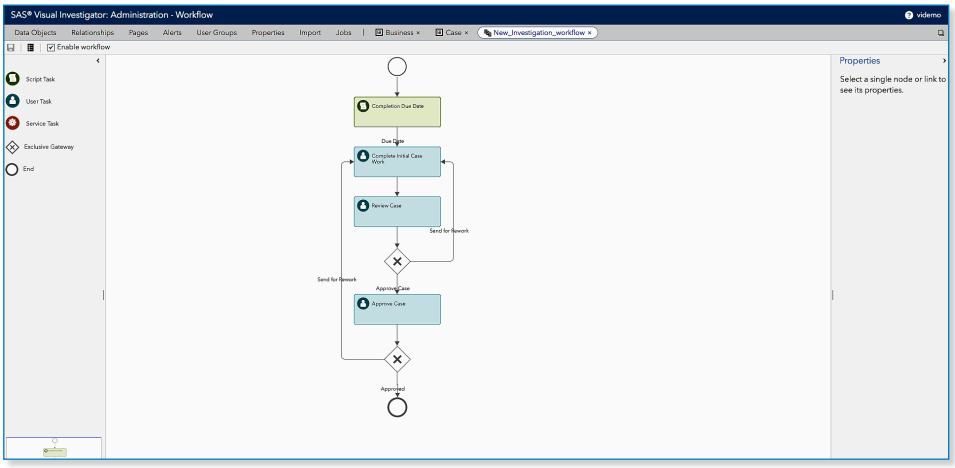


Figure 3: Administrators design workflows to guide users through defined tasks as they carry out their everyday work.

- **Network analytics**: Identify areas of interest and centrality within the network by showing entity closeness, betweenness, influence and so on.
- **Node decorators**: Help analysts and investigators understand network data by highlighting useful information on the node icon view, for example, to indicate different customer accounts held at different banks. Analysts can identify entities at a glance and better understand their data.

Investigative workspaces

The investigative workspaces offer analysts collaboration, compliance and efficiency. The interactive visualization and search components help analysts build, gather, explore, visualize and manipulate data that's pertinent to their investigation or research. They can take static clips of visualizations and add them to the Insights module to narrate maps, timelines, networks and other content with self-service features. Users can also print the Insights they create.

Product configurability

Organizations can take advantage of the solution's flexibility to respond to different business needs or evolving trends. SAS Visual Investigator supports an open data model and provides a straightforward mechanism for administrative configuration – including designing interfaces, components and screens used to display and work with data.

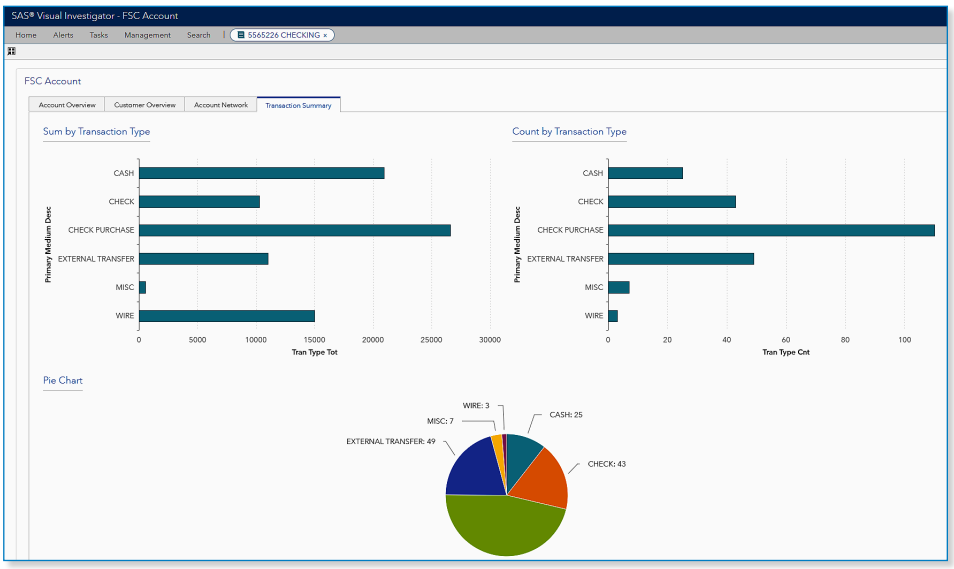


Figure 4: Analysts and investigators can view details of an object and related information in page views best configured to display and work with the data.

Administrators have access to:

- An open data model to meet different or evolving business requirements and situations.
- A dynamic page designer and viewer.
- The ability to configure and manage alerts and events with a streamlined, lightweight workflow.
- A solution configuration import/export component that makes it easy to develop, maintain and deploy solutions.

In addition, administrators can perform ad hoc data imports, analysis, indexing and data visualization with self-service features.

TO LEARN MORE »

To learn more about SAS Visual Investigator, download white papers, view screenshots and see other related material, please visit sas.com/vi.

To contact your local SAS office, please visit: sas.com/offices

THE POWER TO KNOW®