

An aerial photograph of a winding asphalt road through a dense, lush green forest. A river flows through the forest on the right side of the road. The road has white dashed lines and a solid white line on the edge. The forest is vibrant green, and the river is a clear blue. The overall scene is serene and natural.

# Eyes wide shut

Investigation challenges for  
trust and safety teams

FALKOR



## Introduction

Trust and safety teams are no strangers to the complexities of investigations. In fact, those complexities are their bread and butter.

Tasked with ensuring the safety of their company, its products, and its user base, trust and safety teams drive significant change in their company and its products.

They introduce on-platform safeguards and enforcement mechanisms to prevent the uploading of harmful content, before it reaches users, and remove harmful content discovered retroactively. To do this, they hone their investigative tradecraft, creating robust teams and building expertise in investigative reporting.

Some trust and safety teams have even developed in-house specialized monitoring and investigation systems, tailored to their unique platforms and threat landscapes. These systems utilize closed-source and proprietary data, along with platform-specific methodologies, to effectively carry out investigations. In doing this, they automatically protect users from the evolving and ever-present threats facing platforms and their users. These threats range from account hijacking by malicious cyber actors, to disinformation and brigading campaigns, to extremist organizations disseminating hateful content online. The list goes on.

Trust and safety teams have the skills and tools to investigate effectively on their own platforms, as certain platforms such as Facebook and Google have shown. However, they often lack the resources necessary to investigate emerging external threats.



## On and Off-Platform Investigations

Trust and safety investigations are ideally preventative by nature. But in reality, they are both preventative and reactive, and must be completed as quickly as possible to minimize the potential risk to not only end-users but also to the company. For example, preventing the spread of child abuse content is critical for trust and safety teams, not only to protect the public, but also to avoid regulatory and legal punishment. The longer illegal content is on-platform, the greater the potential harm to users and the platform itself.

Off-platform investigations complicate this element greatly, as the relevant data is, by definition, not visible to the trust and safety team of a given platform. Thus, their success is instead reliant on gathering open-source intelligence from various sources. Inter-platform cooperation is thankfully growing, but this alone is not capable of solving the problem.

While on-platform investigations can be difficult, even with the benefit of full data visibility, the difficulties of off-platform investigations are even greater. Below, we look at some of the key challenges facing trust and safety teams.



## Key Challenges of Trust and Safety Teams

### 1. Threat awareness

# Trust and safety teams lack the signals needed to detect off-platform threats effectively

Many trust and safety investigations originate via user reports or complaints about malicious on-platform activity. This enables trust and safety teams to quickly take action, often utilizing automated enforcement and protective algorithms.

For off-platform threats, there is no signal or warning. Therefore, trust and safety teams must be constantly vigilant to the dynamic threat vectors from an infinite number of potential sources.

For example, cybercriminals could sell users' personal identifiable information (PII), including their compromised on-platform data, on messaging applications or the dark web. For many platforms, no reasonable or convenient reporting system exists for off-platform threats, making it a huge challenge to detect or prevent them.





## 2. Data collection

### Off-platform data is varied, complex, and difficult to access

Off-platform investigations may span dozens of disciplines and specialties. Often, they require highly trained personnel to map out relevant data sources such as forums, messaging applications, closed groups and channels, corporate records, and more.

Additionally, analysts must know how to acquire access when data is otherwise inaccessible. For example, they may need to collect identifiers, suspicious accounts or entities, company registration information, and more.

Moreover, it is impossible to rapidly gather data from other platforms, databases, and websites at scale without automated collection methods and infrastructure.



### 3. Data analysis

## Tools for trust and safety data analysis are slow, inefficient, and unintuitive

Gathering masses of data is challenging enough, but analyzing it effectively, efficiently, and at scale is orders of magnitude more difficult.

Many platforms used by analysts today claim to aid them in analyzing data on a larger scale than manual analysis allows, but these systems are often disadvantaged in numerous ways. Often these systems are comparatively old and unintuitive in design, so they don't deliver the speed and efficiency promised.

Investigation and analysis systems available now are heavily skewed towards specific industries, such as law enforcement and financial investigations, and aren't optimized or suitable for the trust and Safety domain.

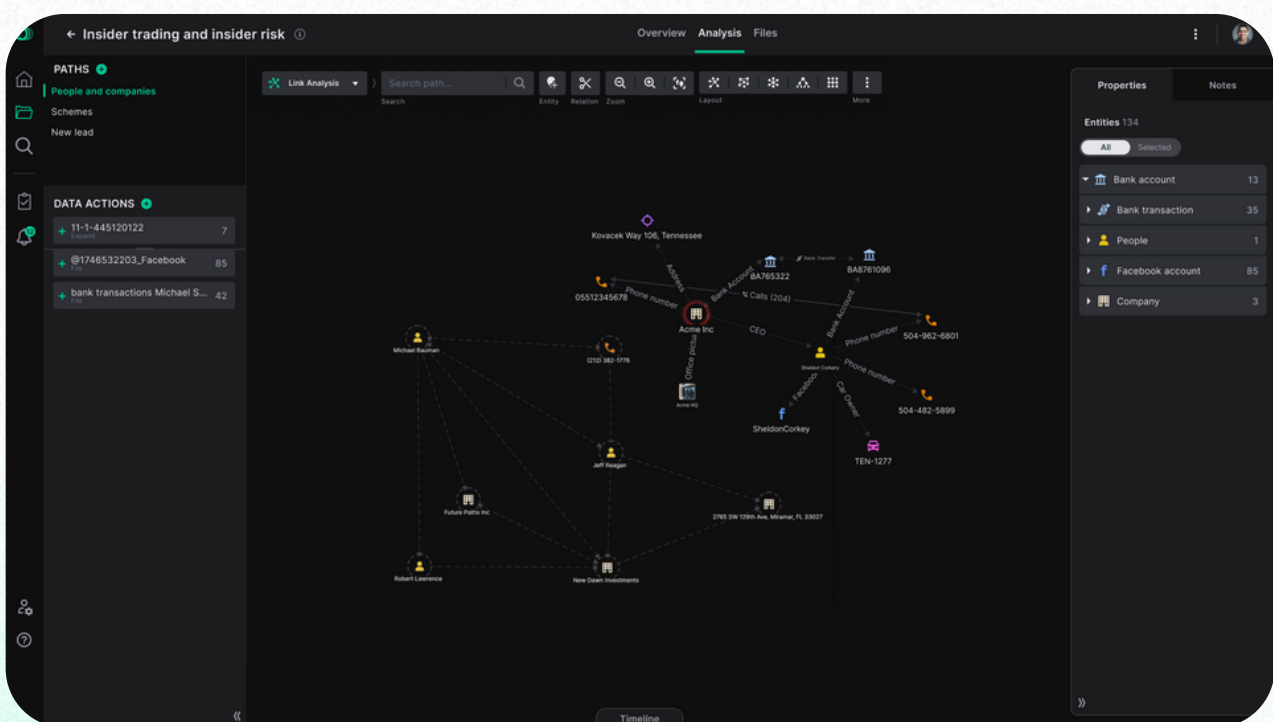
Trust and safety is an emerging industry with its own specific needs, and these platforms are simply not built to meet these needs. Trust and safety analysts thus spend much of their time and resources either retrofitting legacy systems or learning overly complex new data analysis tools.

Trust and safety teams require data analytics and investigative platforms that are versatile and flexible. They need platforms capable of providing full data visibility, including historical data, and which are able to ingest and analyze any file type while filtering out irrelevant noise.



# The Falkor difference

Falkor's analyst platform uses advanced automation to speed up analytics and cut down on repetitive tasks, so trust and safety teams can see the full picture – without drowning in data.



Falkor system user interface - showing a link analysis graph of various data types



#### 4. Data visibility

## Silos make it hard to collaborate and access complete, up-to-date data

Data persistence and utility are additional parts of the puzzle for trust and safety teams. Threats to platforms are dynamic and persistent, and recidivism is rampant. Alex Jones' evasion of permabans from Facebook, YouTube, and Instagram, even in the face of their Herculean anti-ban-evasion enforcement, is a salient example of this.

Trust and safety teams, however, are regularly siloed for reasons outside of their control, such as company bureaucracy and excessive data storage regulations. These can result in the need to store raw data, final intelligence, and investigative products away from other investigative teams. Overly siloed trust and safety teams are less inclined, and less able, to collaborate with teams on their own platforms, greatly reducing their efficacy.

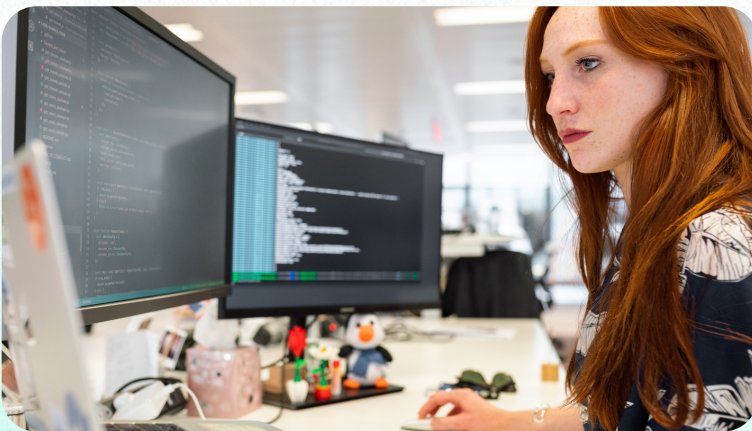
Centralized storage of relevant selectors of unique and persistent information (such as email addresses, IP addresses, and other technical indicators) is key to effectively tracking the activity of threat actors. This centralized storage can provide trust and safety teams with better knowledge management and full data visibility, helping them work far more efficiently. While this type of storage is not currently the standard, it is set to become a critical part of future Trust and Safety work.



## 5. Regulatory risk

Trust and safety teams must protect the privacy of both users and those they investigate

Trust and safety investigations prevent harm on platforms and contribute to creating a safer online space for the public. However, they are still subject to the various data collection and storage regulations protecting those being investigated, as well as any impacted users. To avoid legal challenges, and to protect user privacy, trust and safety teams must therefore ensure that any data they handle is used and stored both responsibly and securely.

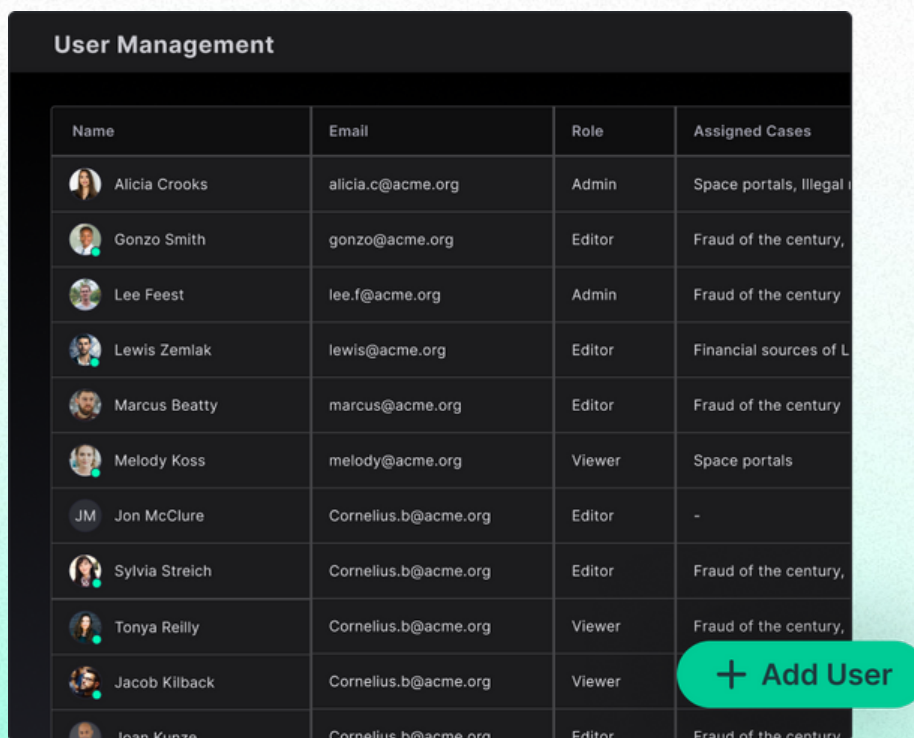














# The Falkor difference

Falkor gives analysts one unified form of access to data and standardizes the way data is gathered, stored, categorized, and accessed, making it easy to work collaboratively across teams.

It's easy to manage permissions for different members of staff and ensure that only the right people see the right data at the right time.



Name	Email	Role	Assigned Cases
 Alicia Crooks	alicia.c@acme.org	Admin	Space portals, Illegal i
 Gonzo Smith	gonzo@acme.org	Editor	Fraud of the century,
 Lee Feest	lee.f@acme.org	Admin	Fraud of the century
 Lewis Zemlak	lewis@acme.org	Editor	Financial sources of L
 Marcus Beatty	marcus@acme.org	Editor	Fraud of the century
 Melody Koss	melody@acme.org	Viewer	Space portals
JM Jon McClure	Cornelius.b@acme.org	Editor	-
 Sylvia Streich	Cornelius.b@acme.org	Editor	Fraud of the century,
 Tonya Reilly	Cornelius.b@acme.org	Viewer	Fraud of the century,
 Jacob Kilback	Cornelius.b@acme.org	Viewer	
 Ioan Kunze	Cornelius.b@acme.org	Editor	Fraud of the century

[+ Add User](#)



## 6. Vendor management

### Collaborating with other companies adds confusion and complexity

Trust and safety teams often work with an overwhelming quantity of data on a daily basis. Many teams outsource some of their workload to investigative firms and vendors.

These vendors provide trust and safety teams with (often excessively) complex reports and data sets. These are regularly in CSV or XLSX formats, which trust and safety teams must then manually analyze, wasting valuable time and resources.



## 7. Cross-platform cooperation

### Trust and safety teams struggle to work with other companies

Trust and safety teams in various companies are increasingly recognizing the advantages of cooperation with their counterparts in other companies – a practice shared by many law enforcement agencies and financial institutions. This cooperation is an effective way to share important information and tackle cross-platform threats.

However, there are limitations to such cooperation. For example, legal and regulatory constraints on sharing on-platform information can prevent or delay information sharing. Additionally, trust and safety teams at various firms have diverse workflows, with different tools, different formats, and different data. This can also work to delay and inhibit information sharing, as trust and safety teams have to ensure the compatibility of data with their systems and workflows.

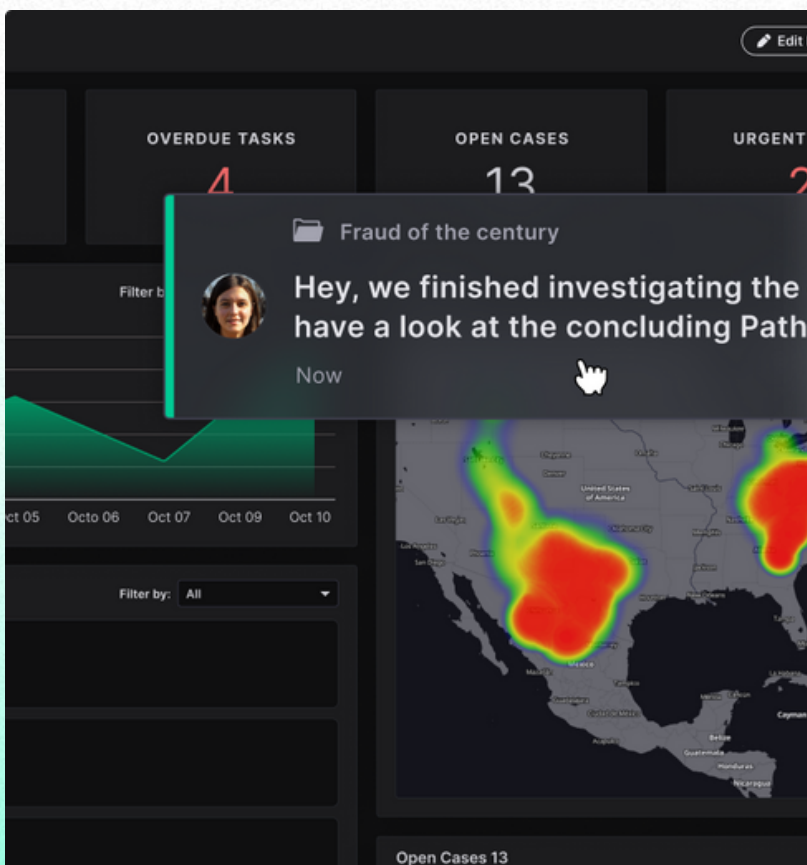




# The Falkor difference

With Falkor, trust and safety teams can share selective, permission-based access to key data or projects with other companies.

By working in one shared environment, teams can effortlessly share data, stay up to date with the investigation, and generate easily interpretable reports.





# Trust and safety teams need a platform built for them

The above challenges are by no means limited to trust and safety teams. Any team of investigative analysts or policy managers can face similar issues on a daily basis.

Tackling these challenges, and in particular the diverse and dynamic threat landscape facing trust and safety teams, requires a holistic, data-driven approach.

Multidisciplinary trust and safety teams must be able to effectively collect, store, and analyze data on and off their platforms at scale. This data must be visible to those who need access, helping them protect their platforms, comply with relevant regulations, and stay secure. This data must also be persistent and easy to analyze, providing trust and safety teams and decision-makers with data-driven and actionable insights.

Currently, the market for investigative and analytical platforms for analysts is lacking, forcing trust and safety teams to make do with legacy or otherwise inadequate software solutions. These teams need scalable solutions, built for their specific needs, allowing them to be proactive against threats and pre-empt harm to their platforms and user bases.



# One platform for every trust and safety investigation

Falkor provides trust and safety analysts with an intuitive, organized, and workflow-oriented investigative system, empowering them to focus on what's really important: protecting their platforms and users.

Falkor puts trust and safety analysts in the driving seat, giving them the tools they need to ingest, enrich, and analyze data sets of any size through one centralized, optimally visible analyst operating system.



## Discover the future with Falkor

Visit [falkor.ai](https://falkor.ai) or contact us at [hello@falkor.ai](mailto:hello@falkor.ai)