

## SPYCLOUD CONSOLE

# SpyCloud Cybercrime Investigations

Automate and accelerate cybercrime and identity threat investigations.

## 01 THE PROBLEM

### Analysts are drowning in data and starved for clarity

The sheer volume of compromised identity assets and OSINT data makes it nearly impossible to correlate digital breadcrumbs, attribute threats, or spot insider risks – before damage is done. Most tools demand deep expertise, limiting success to only the most seasoned investigators.

SpyCloud Cybercrime Investigations changes that. It gives teams a faster, smarter path from raw exposure to finished intel – helping organizations **act before cybercriminals do**.

## 02 PRODUCT OVERVIEW

### An AI-powered force multiplier for every analyst

SpyCloud Cybercrime Investigations is an AI-powered, SaaS-based module that lets cyber threat intel, security operations, fraud and risk, and trust and safety teams uncover, analyze, and act on identity exposures with speed and confidence. It transforms malware-exfiltrated, phished, and breached data into deep identity intelligence – revealing holistic views of exposed users and infrastructure.

Four capabilities work together as a layered system. **IDLink** automatically correlates fragmented identity data into a complete picture of a digital identity. **Research Agent** plans and runs the investigation on the analyst's behalf, sequencing pivots the way a senior analyst would and returning finished intelligence grounded in verified recaptured records. **Log Analysis** digs into the full telemetry from an infected device, including stealer logs, browser history, cookies, and other captured artifacts, for forensics. **AI Insights** then transforms those findings into clean, exportable reports in seconds, built on decades of SpyCloud's investigative tradecraft. Each layer builds on the one before it.

#### BENEFITS AT A GLANCE

What Cybercrime Investigations delivers for your team.

##### See the full picture, instantly

Query SpyCloud's vast collection of recaptured data to rapidly construct digital identities and uncover sophisticated insider and external threats.

##### Accelerate investigations

Find answers faster with AI that detects suspicious identity patterns and relationships often missed by other solutions, significantly reducing discovery time from hours to seconds.

##### Deliver finished intel

Research Agent returns finished intelligence grounded in verified recaptured records, every finding traceable to a specific source. AI Insights transforms those findings into clean, exportable reports with the click of a button.

##### Amplify analyst impact

Senior analysts close cases faster and go deeper. Junior analysts operate at increased efficiency from day one. Research Agent encodes decades of investigative tradecraft so every analyst on your team runs the same quality investigation, regardless of experience level.

### 03 BUILT FOR EVERY TEAM

## Exposed identity data and AI-driven context for faster investigations

SpyCloud gives teams the exposed identity data and AI-driven context to investigate with speed and precision – across cyber threat intelligence, security operations, fraud and risk, and trust and safety.

### Cyber Threat Intel

Attribute adversaries and map digital identities across campaigns and infrastructure.

### SOC & IR

Accelerate investigations and pivot faster from detection to decisive action.

### Fraud & Risk

Uncover compromised identities and stop fraud tied to phishing and malware exposures.

### Trust & Safety

Protect users and platforms by identifying identity abuse and account compromise early.

### 04 USE CASE SPECTRUM

## Cover the full spectrum of identity threats and investigations

From attribution to insider risk, SpyCloud Cybercrime Investigations covers the investigation use cases analysts face most.

■ Threat actor attribution

■ Identity resolution

■ Platform abuse

■ Synthetic identity analysis

■ Supply chain exposures

■ Insider threats – malicious & unwitting

■ Hard-to-detect fraud

■ Pattern of life analysis

■ Employment fraud

■ Know Your Customer (KYC)

■ VIP exposures

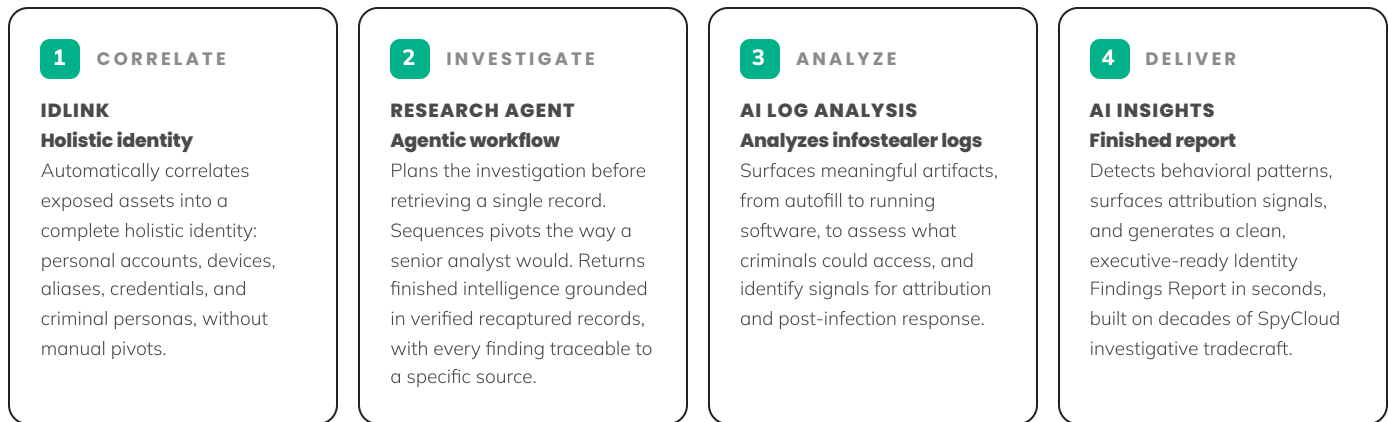
■ Infected host identification

■ Trust & safety escalations

05 HOW IT WORKS

## Connected layers, from exposure to finished intel

SpyCloud Cybercrime Investigations combines deep recaptured data from the criminal underground with automated correlation, agentic investigation planning, and AI-driven finished intelligence. Investigations begin with any selector analysts rely on, like an email, phone number, domain, or IP address, and move through four connected layers.

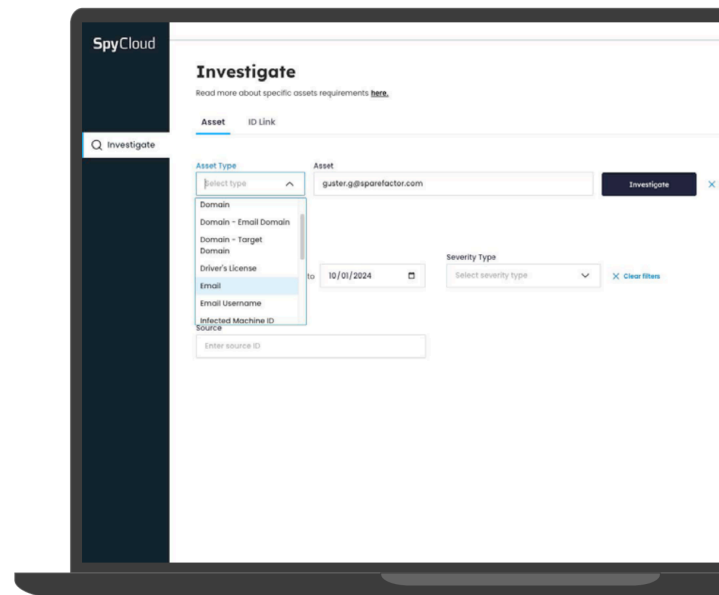


### INVESTIGATE USING THESE ASSET TYPES, AND MORE

- |                       |                           |
|-----------------------|---------------------------|
| ✓ Domain              | ✓ Email address           |
| ✓ Password (hashed)   | ✓ Phone number            |
| ✓ Infected machine ID | ✓ Log ID                  |
| ✓ Social media handle | ✓ Username                |
| ✓ SSN                 | ✓ Driver's license number |

#### RECAPTURED AT CRIMINAL SPEED

Findings are based on continuously delivered recaptured identity assets from malware-infected devices, successful phishes, and third-party breaches – often accessible within minutes of discovery in criminal communities.



06 IDLINK

## Automated identity correlation that drives analysis to attribution

SpyCloud Cybercrime Investigations includes proprietary IDLink™ advanced analytics, which automatically build holistic identities – giving you the speed and resources to drive analysis to attribution while filtering out the irrelevant records that bog analysis down.

1

### Automatic background pivots

After matches on an email, username, phone number, or 9 other selectors, IDLink **automatically runs pivots in the background**, looking for connections across everything that makes up a digital identity – matching emails and backup emails, shared and exposed PII, usernames, passwords, and over a dozen other asset types.

2

### Only high-relevance results

IDLink returns only **new, highly-relevant results**, removing any out-of-scope identity asset that slows down analysis – so your team stays focused on what matters.

3

### Context-enhanced intelligence

Raw data is enhanced with additional context to give you a **broader view of exposed identities and threats**, turning scattered records into a coherent picture.

8×

MORE IDENTITY  
RECORDS

2×

MORE MALWARE  
RECORDS

14×

MORE PLAINTEXT  
PASSWORDS

5×

MORE EMAIL  
ADDRESSES

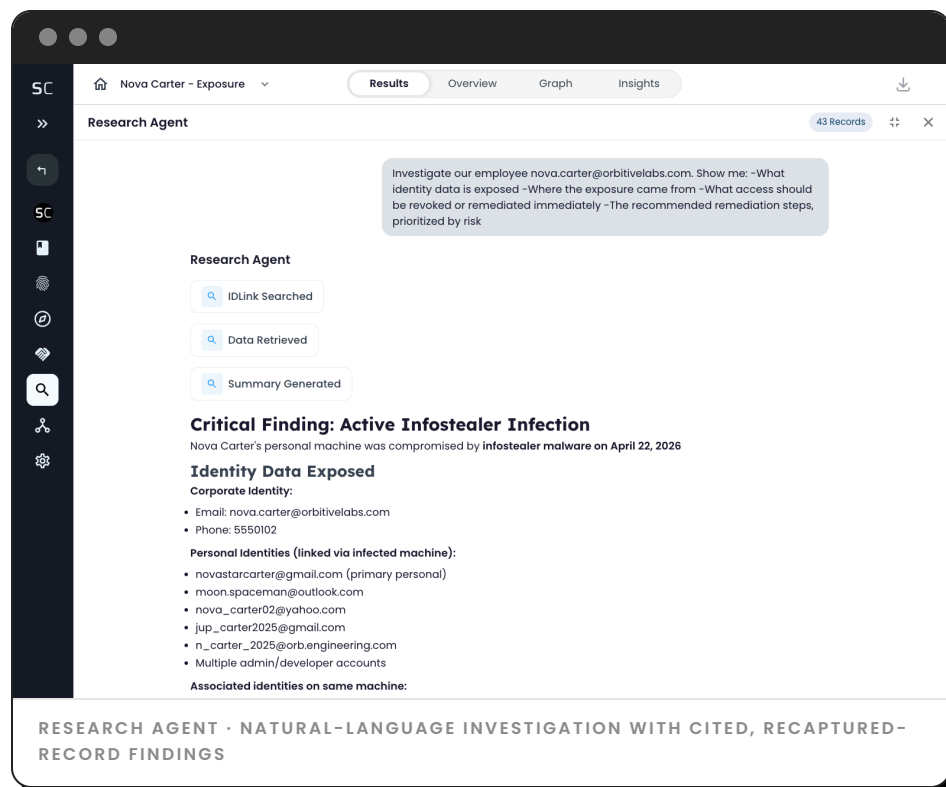
## 07 RESEARCH AGENT

### Amplify investigations with agentic workflows

Research Agent is SpyCloud's agentic investigation workflow, built on over **one trillion recaptured criminal-source assets** and the investigative methodology SpyCloud's team has spent decades developing. Give it a question, a hypothesis, or a batch of mixed assets in natural language, and it runs the investigation from start to finish.

- ✓ **Plans and adapts as it investigates**  
Determines which pivots are worth running and in what order, then retains context as the investigation develops so each step builds on prior findings.
- ✓ **Correlates identities automatically**  
Every interaction triggers IDLink holistic identity matching to surface connected personal accounts, devices, aliases, and criminal personas, even across mixed asset types.
- ✓ **Keeps agentic and hands-on investigation in sync**  
Searches and pivots analysts run themselves become part of the agent's context automatically, while analysts can remove dead-end queries and records so the agent stops reasoning on them.
- ✓ **Shows the evidence behind every finding**  
Every finding cites the specific recaptured record behind it, making results explainable and verifiable.

Senior analysts close cases faster and go deeper. Junior analysts operate at increased efficiency from day one. The investigation sequence that closes your most complex attribution case becomes replicable through the Prompt Library, not locked inside one analyst's head.



08 AI INSIGHTS

## Finished intelligence in seconds

From subtle patterns to finished intelligence, AI Insights uncovers the threats others miss. It automates the final step of the investigation – turning complex identity exposures into actionable summaries without manual analysis. Built on SpyCloud's investigative tradecraft, it synthesizes relationships and risk indicators across malware, phished, and breached data to generate a **SpyCloud Identity Findings Report** in seconds.

1

### Analyze every asset in context

After pivoting across your dataset, AI Insights flags suspicious patterns such as identity reuse, credential overlap, and suspicious browser activity.

2

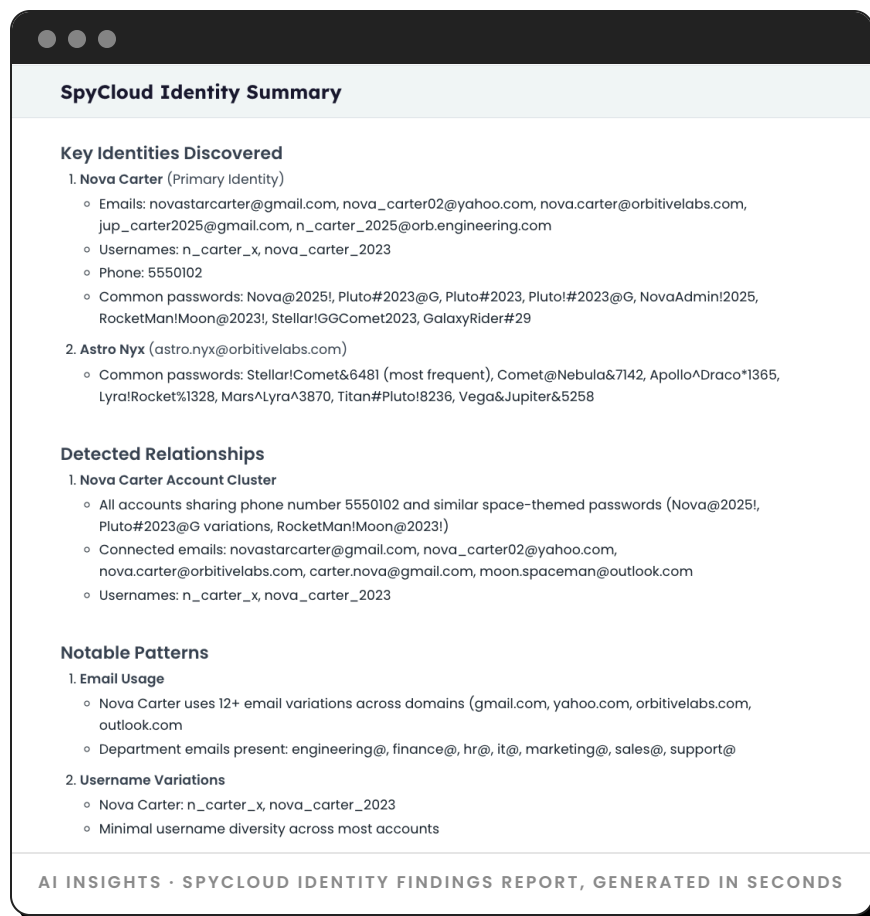
### Identify unique signals

SpyCloud's AI model surfaces patterns commonly tied to insider threats, synthetic identities, and coordinated fraud by evaluating every data point returned in your queries.

3

### Generate an exec-ready report

A streamlined PDF summarizes the investigation's scope, key risks, and notable associations – ready to export for escalations, incident response, or stakeholder briefings.



09 KEY CAPABILITIES

## From unknown exposure to decisive action

A powerful, easy-to-use SaaS module that makes it faster and more efficient to analyze and remediate cybercrime and identity threats.

### Query

Broaden your understanding of exposure risks across your workforce and supply chain.

- Perform unlimited queries against SpyCloud's rich dataset of identity assets from tens of thousands of third-party breaches, millions of malware-infected devices, and successful phishing attacks, with over 200 data types.
- Start investigations using 19 asset types, including email address, domain, IP, password, and more, or reconstruct holistic identities fast by querying IDLink analytics to reveal broader identity exposure.

### Pivot

Pull in the most relevant identity data points for your investigation and analysis.

- Pivot off query results for a full picture of identity exposures, enabling analysts to swiftly assess internal and external risks to the organization.
- IDLink analytics filters out irrelevant data to focus only on high-signal relationships to accelerate investigations.
- Pivot across underlying infostealer log data to investigate what was captured from the infected device.

### Graph

Visualize holistic identities across employees, customers, and your supply chain.

- Quickly build a picture of exposed identities by viewing visual relationships across data to reveal previously unknowable connections.
- Perform follow-up pivots in the graph, finding direct matches, wildcard searches, or broader identity views with IDLink analysis that reveal patterns other tools miss, all without losing your place.

### Investigate

Run investigations in natural language, at senior analyst quality, on every case.

- Describe a subject, hypothesis, or drop in a batch of mixed assets; Research Agent plans the investigation, sequences the pivots, and returns finished intelligence with every finding traceable to a specific source.
- Automatically triggers IDLink holistic identity correlation on every interaction, surfacing connections analysts would otherwise spend hours tracing manually.
- Retains context across the full session so analysts can pursue new leads and build on prior findings without starting over.
- Prompt Library of proven investigation workflows covering insider threat, threat actor attribution, fraud, synthetic identity, infected host identification, and more.

### Analyze

Dive into the full infostealer log to understand exactly what was exposed at time of infection.

- Examine credentials, cookies, autofill data, browser history, files, running software, and other device telemetry to understand what criminals could access and use.
- Run AI-assisted log analysis to quickly identify meaningful artifacts, scope potential impact, and surface evidence for attribution and post-infection response.
- Export the raw log for deeper analysis in your own tools and workflows.

### Act

Get finished intel for attribution and analysis in a report ready for analysts to use.

- Research Agent returns verified, evidence-grounded finished intelligence; AI Insights summarizes key risk factors, digital habits, and exposure patterns into clean reports without needing to sort through raw data or perform manual analysis.
- Generate clean, consumable summaries for executives, IR teams, and external stakeholders.

10 LICENSING OPTIONS

## Three tiers for the Cybercrime Investigations Module

|                                 | Pro Tier                                                                                                                                                                                         | Core Tier                                                                                                                                                                          | Light Tier                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WHEN TO USE IT</b>           | <ul style="list-style-type: none"> <li>Advanced investigations</li> <li>Integrated AI-enhanced analysis</li> <li>Complex insider threat cases</li> <li>Comprehensive threat analysis</li> </ul>  | <ul style="list-style-type: none"> <li>Standard investigations</li> <li>Accelerated threat hunting</li> <li>Routine incident response</li> <li>Core security operations</li> </ul> | <ul style="list-style-type: none"> <li>Basic searches</li> <li>Limited fraud verification</li> <li>Limited risk assessment</li> <li>Entry-level research</li> </ul>         |
| <b>WHO COULD USE IT</b>         | <ul style="list-style-type: none"> <li>Investigation specialists &amp; insider threat teams</li> <li>CTI teams handling complex cases</li> <li>Multi-disciplinary investigation units</li> </ul> | <ul style="list-style-type: none"> <li>SOC analysts &amp; incident responders</li> <li>Security operations teams</li> <li>Standard threat hunting teams</li> </ul>                 | <ul style="list-style-type: none"> <li>Junior analysts &amp; fraud researchers</li> <li>Entry-level security analysts</li> <li>Basic research &amp; triage teams</li> </ul> |
| <b>DATA &amp; ACCESS</b>        |                                                                                                                                                                                                  |                                                                                                                                                                                    |                                                                                                                                                                             |
| <b>DEPLOYMENT / PRICING</b>     | SaaS-based console · Per-seat annual                                                                                                                                                             | SaaS-based console · Per-seat annual                                                                                                                                               | SaaS-based console · Per-seat annual                                                                                                                                        |
| <b>QUERY VOLUME</b>             | Unlimited (in-app)                                                                                                                                                                               | Unlimited (in-app)                                                                                                                                                                 | Unlimited (in-app)                                                                                                                                                          |
| <b>ENDPOINT ACCESS</b>          | All 18 endpoints                                                                                                                                                                                 | All 18 endpoints                                                                                                                                                                   | Limited – email, username, phone, IP address, domain, machine ID, log ID                                                                                                    |
| <b>ANALYTICAL CAPABILITIES</b>  |                                                                                                                                                                                                  |                                                                                                                                                                                    |                                                                                                                                                                             |
| <b>INTERACTIVE AI WORKFLOWS</b> | ✓                                                                                                                                                                                                | –                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>IDLINK ANALYTICS</b>         | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>LOG ANALYSIS</b>             | ✓                                                                                                                                                                                                | –                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>INVESTIGATIVE FEATURES</b>   |                                                                                                                                                                                                  |                                                                                                                                                                                    |                                                                                                                                                                             |
| <b>GRAPHING</b>                 | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>PIVOTING</b>                 | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>AI INSIGHTS</b>              | ✓                                                                                                                                                                                                | –                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>RESEARCH AGENT</b>           | ✓                                                                                                                                                                                                | –                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>LOG DATA</b>                 | ✓                                                                                                                                                                                                | –                                                                                                                                                                                  | –                                                                                                                                                                           |
| <b>CASE MANAGEMENT</b>          | ✓                                                                                                                                                                                                | ✓                                                                                                                                                                                  | ✓                                                                                                                                                                           |

## ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions use advanced analytics and AI to accelerate investigations and protect workforce, consumer, and supplier identities from the threats that matter most: authentication bypass, session hijacking, malicious insiders, account takeover, ransomware, and fraud. Its data from malware-infected devices, successful phishing, combolists, and third-party breaches also powers many popular dark web monitoring and identity theft protection offerings. Customers include 7 of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 250 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

### Get a demo

Looking to perform larger-scale queries or combine SpyCloud identity data with other OSINT sources?  
Explore the SpyCloud Cybercrime Investigations API.

[SPYCLOUD.COM](https://spycloud.com) >