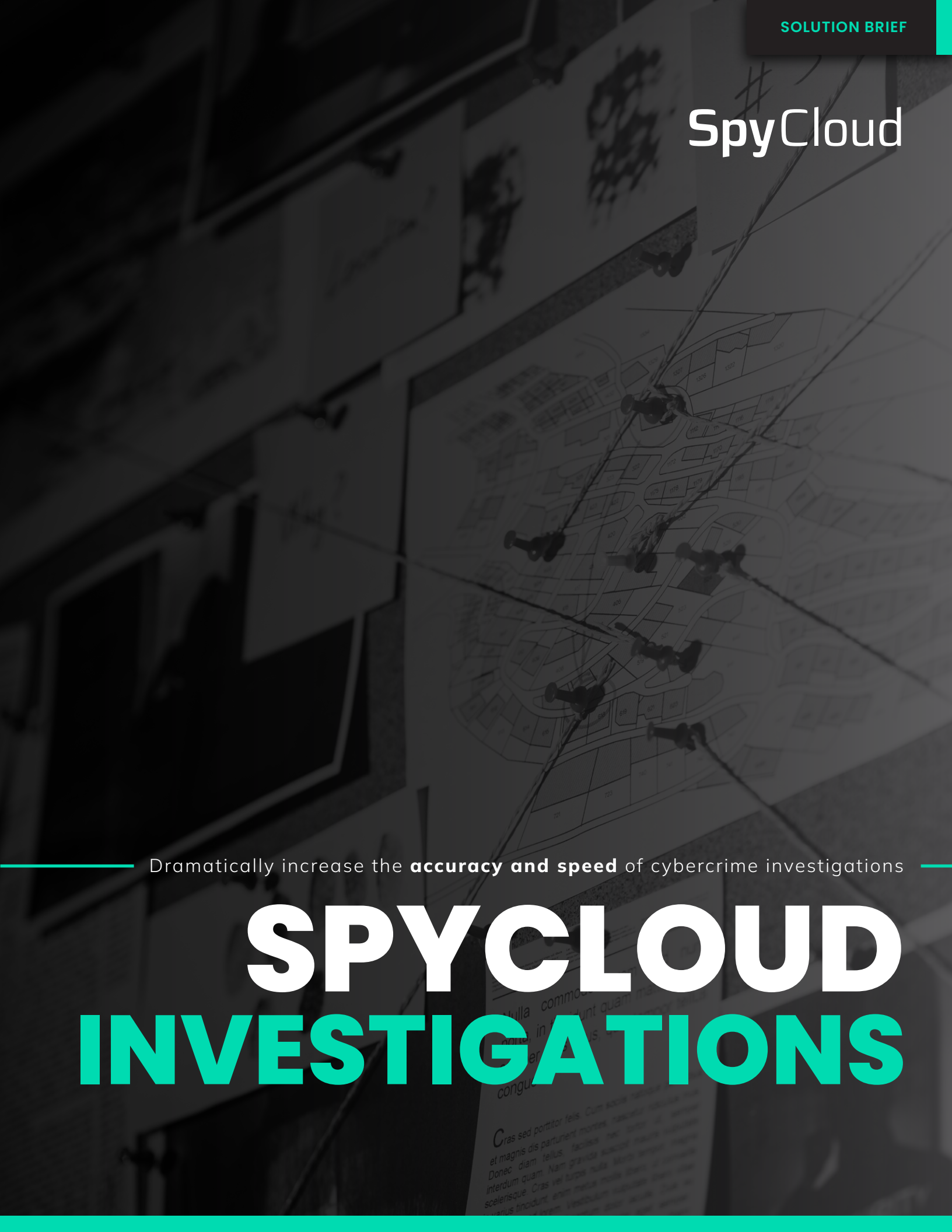
SOLUTION BRIEF

SpyCloud



Dramatically increase the **accuracy and speed** of cybercrime investigations

SPYCLOUD INVESTIGATIONS

UNRAVELING THE COMPLEXITY OF CYBERCRIME AND IDENTITY THREATS

Hidden digital identities make the jobs of analysts and investigators harder – and we're doing them a disservice if we don't give them the proper tools to uncover the full scope of identity-related threats across their organization and supply chain. Today, analysts face the daunting task of correlating massive volumes of OSINT data with other sources, often missing hidden exposures. Investigating the holistic identity of any given user – legitimate or criminal – is time-intensive, requires specialized skills, and extensive manual analysis. Even so, hidden exposures often go unnoticed.

In the face of growing cybercrime and identity threats, analysts and investigators need easy access to the right answers. SpyCloud illuminates the hidden connections to help visualize holistic identities, reduce risk, decrease MTTD and MTTR, and complete cybercrime investigations successfully.

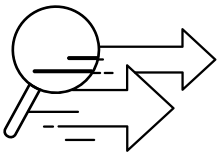
SOLUTION OVERVIEW

CYBERCRIME AND IDENTITY THREAT INVESTIGATIONS

Other tools require advanced skills to navigate through overwhelming amounts of data. **SpyCloud Investigations** is the opposite: a powerful SaaS-based solution that enables analysts and investigators to quickly build holistic identities to respond to exposures and identity-based cyber attacks. From analyzing corporate compromise to online fraud, SpyCloud Investigations offers the right answers.

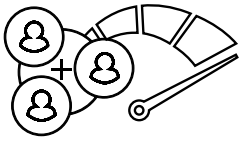
INVESTIGATIONS POWERED BY IDLINK ADVANCED ANALYTICS

SpyCloud accelerates investigations with automated analysis of connected identity assets, uncovering hidden threats to accelerate remediation.



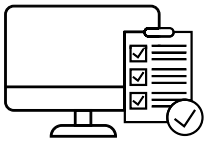
ACCELERATE INVESTIGATIONS

Find answers faster with automated identity correlation, uncovering hidden exposures and reducing discovery time



UPLEVEL YOUR ANALYSTS

Drive team efficiency and focus on high-impact work by removing dead ends with SpyCloud's proprietary holistic identity matching



GET ANSWERS, TAKE ACTION

Use a holistic identity lens to act on exposures across your organization and supply chain with speed and accuracy

BIGGEST THREATS TO ORGANIZATIONS

MALWARE ENTRY POINTS
expose a broad range of corporate applications and network access

EXPOSED EMPLOYEES
malicious or negligent, create significant risk to your organization

COMPROMISED SUPPLY CHAIN
accounts with privileged access pose risks of unauthorized access

FRAUDULENT ACCOUNTS
exploit exposed access for fraudulent activity and platform abuse

HIDDEN ADVERSARIES
bypass security measures and exploit exposed access for fraudulent activity and platform abuse

USE SPYCLOUD INVESTIGATIONS FOR

INFECTED HOST IDENTIFICATION
determine where actors have stolen access to your corporate environment for comprehensive Post-Infection Remediation

INSIDER RISK ANALYSIS
research the risk level of specific employees based on recaptured breach, malware, and successfully phished data

VENDOR & SUPPLY CHAIN EXPOSURE
analyze risk of unauthorized access from reused credentials to malware-infected vendors

FINANCIAL CRIME ANALYSIS
uncover identities with indicators of fraud and criminal activity

THREAT ACTOR ATTRIBUTION
deanonymize, profile, and understand threat actors, their capabilities, and the infected infrastructure used by the actor

SUPPORT MULTIPLE TEAMS

CYBER THREAT INTEL + SOC TEAMS

CYBER THREAT INTEL + SOC TEAMS

CYBER THREAT INTEL + SOC TEAMS

FRAUD & RISK TEAMS

CYBER THREAT INTEL

CYBER THREAT INTEL TEAMS

Deanonymize, profile, and understand **threat actors**, their motivations, and their capabilities.

Identifying **exposed employees and infected infrastructure** used by the threat actor.

SOC TEAMS

Review **malware infected employees and supply-chain** incidents to optimize tools and processes for evolving threats.

Discover and analyze potential identity threats from **insider risks** within the network.

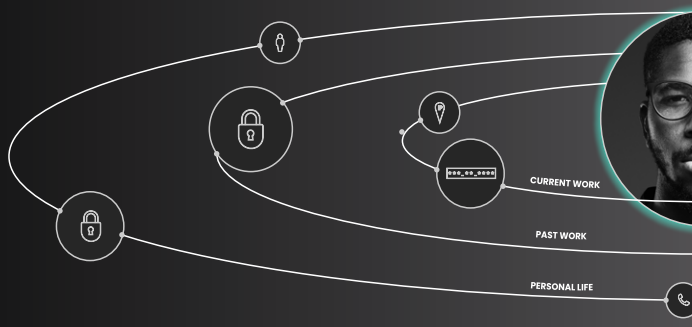
FRAUD & RISK TEAMS

Investigate indicators of **financial crime and platform abuse** without requiring technical expertise.

Uncover emerging trends of **identifying patterns that indicate fraudulent activity** at scale alongside existing data.

WHAT IS A HOLISTIC IDENTITY?

A holistic identity provides a complete view of risk by analyzing a user's darknet exposure. This goes beyond the lens of combining OSINT data with threat intel, and SpyCloud offers insights into exposures that would otherwise remain hidden, reducing unseen risk like never before.



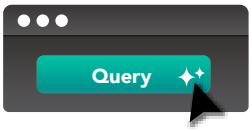
SPYCLOUD IDLINK ADVANCED ANALYTICS

UNDERSTAND THE SCOPE OF AN IDENTITY, FASTER

WHAT IS IDLINK?

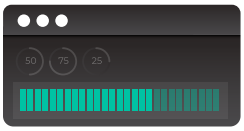
As you query SpyCloud Investigations, IDLink analytics automatically connects the dots between exposed identity assets, building relationships related to your user often missed in other tools.

By exposing the overlap of personal and professional identity data - both past and present - SpyCloud IDLink helps analysts verify identity exposures, remediate compromised identities, investigate financial crimes, and more.



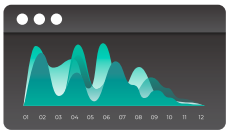
AUTOMATED IDENTITY CORRELATION

Seamlessly connect the dots between hidden identity records, with no effort



NO DEAD END ANALYSIS

Removing investigative dead end roadblocks with crucial insights and identity analytics



NO NOISE

Automatically sift and drop unrelated identity records — reducing noise from low confidence linked identities

TYPICAL FINDINGS WITH **IDLINK ANALYTICS** vs EXACT MATCH QUERIES

8X
MORE IDENTITY RECORDS

2X
MORE MALWARE RECORDS

14X
MORE PLAINTEXT PASSWORDS

5X
MORE EMAIL ADDRESSES

HOW IT WORKS: UP-LEVELING EXPOSURE ANALYSIS & INVESTIGATIONS

MULTIPLE STARTING POINTS, ONE DESTINATION

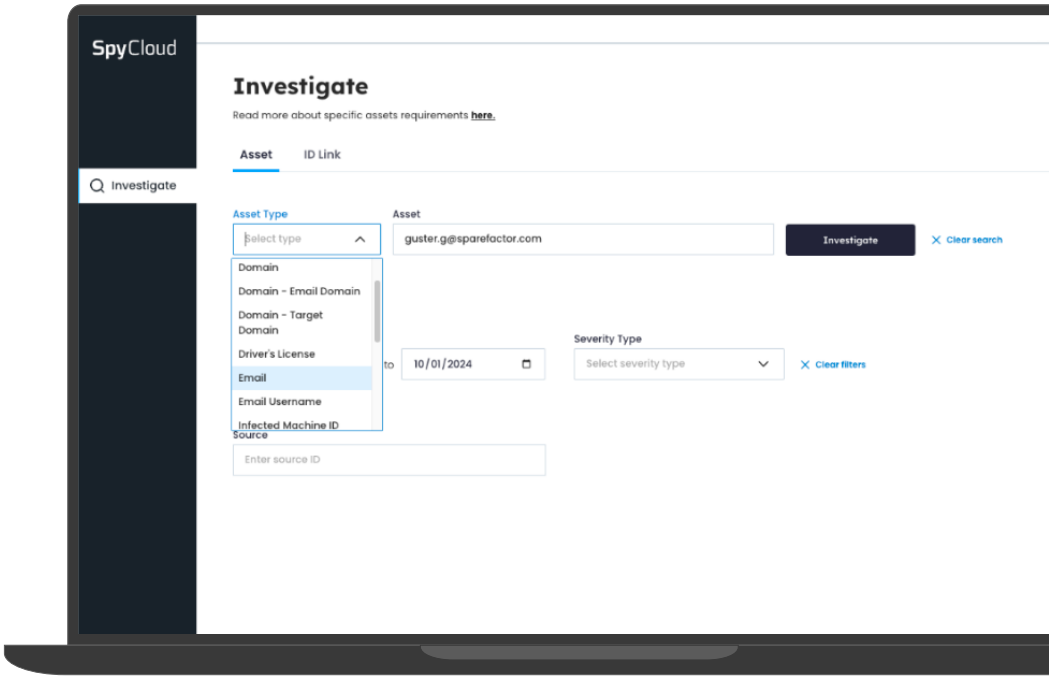
SpyCloud Investigations is the ultimate force multiplier for analysts, automating identity analysis with IDLink to accelerate investigations. Understand risk of exposure, open up new angles to investigate, and illuminate hidden connections within a single portal.

Leverage the world's largest collection of recaptured identity data, with 25+ billion assets ingested and analyzed monthly, providing unparalleled depth and speed to get the answers you seek.

SpyCloud offers multiple asset types for initial searches, advanced identity analytics for clues along the way, and graphical link analysis to complete your investigation.

INVESTIGATE USING THESE ASSET TYPES, AND MORE

- Domain
- Email address
- Password (hashed)
- Phone number
- Infected machine ID
- Social media handle
- Username
- SSN
- Drivers license number



GET STARTED WITH SPYCLOUD INVESTIGATIONS

SEE MORE

Uncover risks with a holistic identity lens

VISUALIZE YOUR RESEARCH SUBJECT

Visualize holistic identities of exposed employees, customers, vendors, and threat actors themselves, using connected recaptured darknet data.

- Uncover hidden connections within a single interface to remove investigative hurdles
- Easily correlate previously unknown information, assets, and other digital exhaust for a holistic view of your user
- Turn unknowns into knowns with a click, unmasking alternate identities and unseen exposures

KNOW MORE

Analyze hidden connections among exposed identities

UNCOVER HIDDEN CONNECTIONS, FASTER

Quickly uncover hidden relationships and connections across identity assets for comprehensive understanding of exposures.

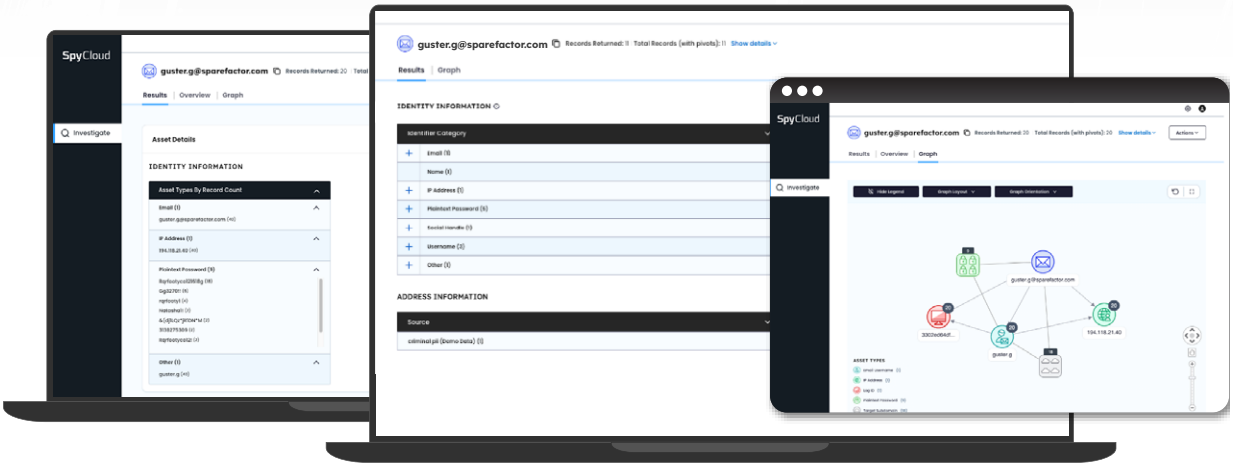
- Identify relationships and overlap across identity assets to understand definitive evidence of compromised identities
- Jumpstart an investigation from a single selector, with 19+ options including email address, IP address, password, & more
- Use IDLink analytics to pivot seamlessly, expanding your view of exposed identity data in the same graph and table, without losing your place

DO MORE

Get impactful answers to rapidly complete investigations

GET ANSWERS THAT MATTER

- Enhance and boost investigations and root-cause analysis – getting answers in the easiest to use format, ever, for decision makers to interpret
- Make high-confidence decisions with a complete view of identity exposures impacting your organization
- Reduce errors and streamline investigations with robust, identity analytics delivered in an easy to use, SaaS-based portal for analysts of all experience levels



API DEPLOYMENT OPTIONS

Looking to integrate SpyCloud Investigations into your existing tools and workflows? SpyCloud offers REST-based APIs to combine our recaptured breach, phished, and malware-exfiltrated records with your internal data and other OSINT sources.

SPYCLOUD INVESTIGATIONS API INTEGRATIONS

MALTEGO

Accelerate investigations with 80+ Maltego Transforms for SpyCloud identity data

splunk>

Query SpyCloud's recaptured identity assets or write custom search commands for enrichment

jupyter

Prebuilt notebooks offer advanced visualizations, pivot options, and drill downs to exact answers

Vertex

Access SpyCloud identity data with custom Storm commands within Synapse to enrich nodes

WHY CUSTOMERS CHOOSE SPYCLOUD

ELEVATE SECURITY STANDARDS

Senior Director of Global Security & Privacy

Samsonite

"With SpyCloud Investigations, we have been able to uncover and address gaps we would have never known about in our suppliers' cybersecurity practices. Now we can enforce higher security standards across our entire supply chain."

CHRIS WINGFIELD
CTI Managing Director

360 PRIVACY

"SpyCloud automates the manual investigation pivots through an advanced algorithm, drastically ***reducing our workflow time by 50%*** and increasing the efficiency and scalability of our analysis."

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven 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 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

To learn more and see insights on your company's exposed data, visit **spycloud.com**.

"SpyCloud is the best service in their industry and I really don't know why you would use another vendor or competitor."

MANAGER
IT Security & Risk Management

Gartner Peer Insights™