DATASHEET

SpyCloud

INVESTIGATIONS PORTAL

DRAMATICALLY INCREASE THE ACCURACY AND SPEED OF INVESTIGATIONS WITH IDLINK ADVANCED ANALYTICS

THE PROBLEM

The volume and complexity of OSINT data available to analysts and investigators makes it hard to quickly find the right information to remediate identity and supply chain exposures, mitigate insider threats, and complete cybercrime investigations. Investigating often requires experience that looks more like data science, existing tools are challenging to set up, and analyzing the results of a query takes time – assuming there are no hidden exposures.

PRODUCT OVERVIEW

SpyCloud Investigations Portal is a powerful investigations solution that enables rapid resolution of cybercrime activity and identity-based threats – for analysts and investigators to quickly respond to exposures and identity threats, preventing targeted cyber attacks and reducing organizational risk.

SpyCloud Investigations is the ultimate force multiplier for analysts, providing a wealth of quality identity analytics for a deeper understanding of the risks to your organization by viewing holistic identities of exposed users and infrastructure. SpyCloud's unique IDLink analytics accelerates investigations with automated analysis of identity assets, uncovering hidden threats across your organization and supply chain, making it faster and easier to get the answers you seek.

BENEFITS AT A GLANCE

Advanced Identity Correlation
IDLink automatically pivots on highly-relevant identity assets to build holistic identity profiles

Rapid Results
Query SpyCloud's recaptured identity database for a full picture of exposed identity data to swiftly assess internal and external risks to the organization

Deeper Context
Easily correlate previously unknown identity information and other digital exhaust for a contextualized view of users

Accelerate Investigations
Find answers faster, pulling out hidden identity exposure and reducing time spent in discovery

KEY USE CASES

- THREAT ACTOR ATTRIBUTION
- INFECTED HOST IDENTIFICATION
- FINANCIAL CRIMES ANALYSIS
- SUPPLY CHAIN EXPOSURE ANALYSIS
- INSIDER RISK ANALYSIS
- IDENTITY EXPOSURE ANALYSIS

CYBERCRIME INVESTIGATIONS POWERED BY RECAPTURED DATA

SpyCloud

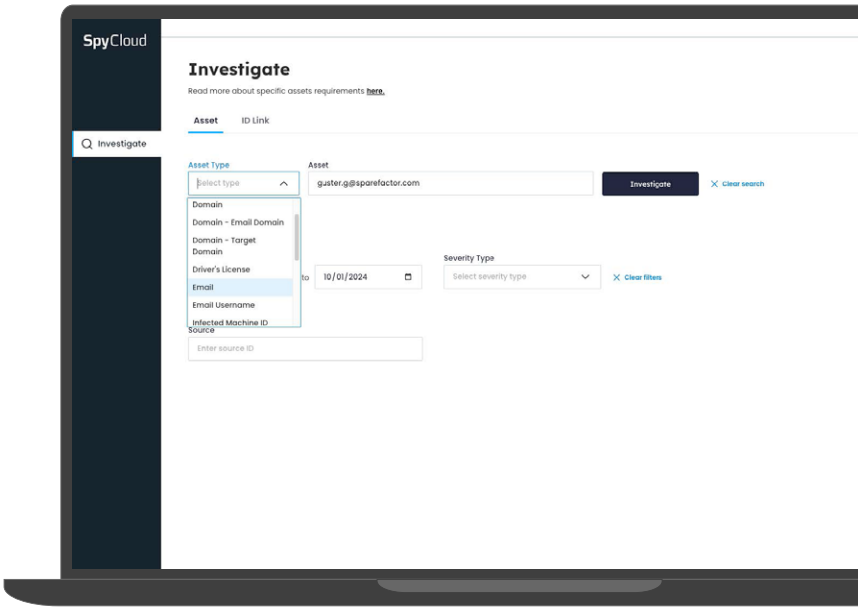
HOW SPYCLOUD INVESTIGATIONS WORKS

SpyCloud Investigations streamlines the steps needed to analyze hidden risks, identify holistic identities of users, and protect your organization from targeted identity attacks. Analysts and investigators - of all skill levels - have access to SpyCloud's leading repository of originated recaptured darknet data with powerful querying capabilities to delve into a wide range of identity data and uncover crucial insights, even with only a single thread to pull.

Start with multiple asset types for initial exact match searches, pivot with IDLink identity analytics for automated analysis along the way, and use graphical link visualization 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



Leverage the world's largest collection of originated recaptured identity data, with 25+ billion assets analyzed monthly, providing unparalleled depth.

SPYCLOUD INVESTIGATIONS PORTAL

SpyCloud

GET ANSWERS FASTER WITH IDLINK POWERED INVESTIGATIONS

Unlocking and unblocking investigations is now easier than ever. SpyCloud Investigations includes our proprietary IDLink advanced analytics – which automatically builds holistic identities to give you the speed and resources you need to drive analysis to attribution.

8x MORE IDENTITY RECORDS

2x MORE MALWARE RECORDS

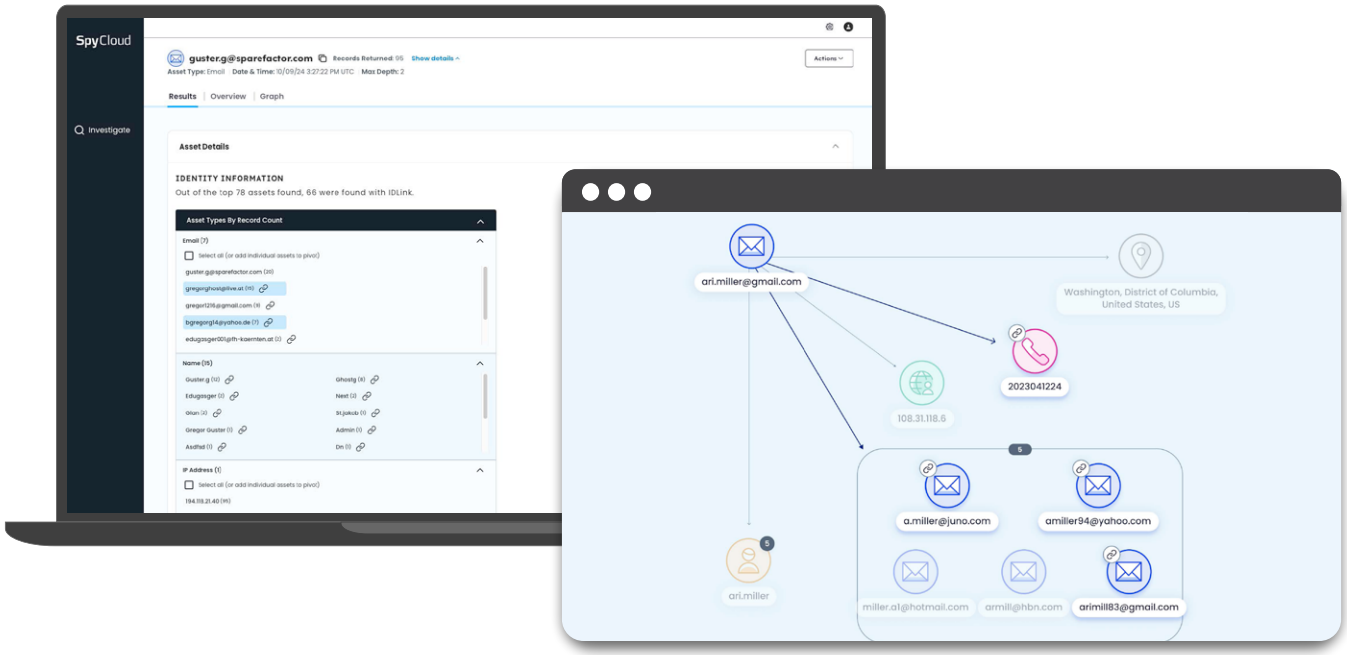
14x MORE PLAINTEXT PASSWORDS

5x MORE EMAIL ADDRESSES

HOW ID LINK WORKS

IDLink speeds up the process of investigating exposed identities, and reduces the manual effort to filter out irrelevant records that bog down analysis:

- After searching exact matches on an email, username, or phone number, IDLink automatically runs pivots in the background, looking for connections on everything that makes up a digital identity – from matching emails and backup emails, to shared and exposed PII, usernames, passwords, and over a dozen other asset types
- SpyCloud Investigations with IDLink only returns new, highly-relevant results, removing any out-of-scope identity asset that slows down analysis
- SpyCloud Investigations enhances raw data with additional context to give you a broader view of exposed identities and threats



SPYCLOUD INVESTIGATIONS PORTAL

SpyCloud

KEY CAPABILITIES

SEE MORE, KNOW MORE, DO MORE WITH SPYCLOUD INVESTIGATIONS

SpyCloud Investigations is a powerful, easy to use SaaS-based portal that makes it faster and more efficient to analyze and remediate cybercrime and identity threats.

QUERY | Broaden your understanding of exposure risks across your organization 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 for a direct match using 19 asset types, including email address, domain, IP address, password, and more, or reconstruct holistic identities faster by querying IDLink analytics on an email, username, or phone number

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

- Pivot off query results for a full picture of exposures and identity compromise, and enable analysts to swiftly assess internal and external risks to the organization
- IDLink analysis remove out-of-scope identity assets to focus investigations on relevant information, filtering out noise

GRAPH | Visualize holistic identities across employees, customers, and your supply chain

- Powerful link analysis graph to perform pivots and quickly build a picture of users with previously unknowable connections
- Perform follow up pivots in the same graph and tables so analysts don't lose their place, finding direct matches, wildcard searches with fuzzy pivots, or broader identity views with IDLink analysis

ACT | Get impactful information for attribution and remediation in a format that is easy for analysts to use

- Gain answers through widgets with enriched identity data that answer threat of exposure risk without needing to sort through raw data or manual analysis
- Reduce errors and missed data points when analyzing risk to act on exposures comprehensively

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**.