SOLUTION BRIEF

SpyCloud

Prevent targeted cyberattacks with holistic identity threat protection

ENTERPRISE PROTECTION

THE CHALLENGE

Safeguarding employee identities often focuses only on account or device protection. But criminals have no boundaries, and fast-growing access to exposed darknet identity data gives them plenty of opportunities to bypass IAM, EDR, ITDR, and MFA for session hijacking, ransomware, and other targeted attacks.

To fully protect employees and corporate data, security teams need insight into the **holistic digital identity** – actioning on exposures from past and present, work and personal personas that lead to unauthorized access. SpyCloud Enterprise Protection automates remediation of identity exposures – connecting every dot and allowing you to ***know more, and do less*** to secure the identity perimeter.

UPLEVEL YOUR DEFENSES – VISUALIZE & ACT ON EXPOSED IDENTITIES TO STOP CYBERCRIMINALS

RISKY HUMAN BEHAVIOR

82% of breaches involve a **human element**

DELAYED CONTAINMENT

Credential attacks result in **$4.8m per breach** and take **~292 days to contain**

EXPOSED APPLICATIONS

A single malware infection can expose access to an average of **26 business apps**

SOLUTION OVERVIEW

Secure your enterprise from targeted cyberattacks with holistic identity threat protection – acting on known points of exposure before they can be used by cybercriminals. ***Stop targeted attacks in 5 minutes from discovery to remediation.***

SpyCloud's Enterprise Protection provides actionable, automated, identity-centric solutions for preventing costly and disruptive identity-based cyberattacks. Protection requires a foundation of strong data and actionable analytics to power workflows, enhance decision-making, and automate remediation. SpyCloud empowers security teams with a holistic identity lens of a user's exposures - connecting datapoints across all digital personas; past and present, work and personal - to quickly assess the risk to your business and prevent evolving threats. SpyCloud offers maximum extensibility with seamless integrations into existing security tools and workflows to optimize incident response, accelerate triage, and shut down hidden entry points.

DEEPER DARKNET INSIGHTS, REAL ANSWERS, AND AUTOMATED ACTION

MONITOR & DETECT

Continuously monitor employees' **holistic identities** with real-time insights into recaptured darknet data in the hands of criminals

PROTECT & PREVENT

Dynamically secure your workforce with automated protection against costly cyberattacks – **increasing control and reducing risk**

RESPOND & REMEDIATE

Rapidly remediate identity exposures within 5 minutes from discovery to optimize SOC workflows – drastically **decreasing MTTD and MTTR**

SPYCLOUD ENTERPRISE PROTECTION

The right data, at the right time – protecting employee identities to secure corporate access

MONITOR & DETECT IDENTITY EXPOSURES

CONTINUOUS MONITORING

Access the world's largest, continuously updated repository of breach, malware-exfiltrated, and successfully phished data for real-time, recaptured darknet exposure data, early in the attack timeline

MONITOR EXPOSURES ON ANY DEVICE TYPE

Detect exposures from managed, unmanaged and personal devices, including BYOD, to shift from account-centric security to holistic identity threat protection

UNCOVER PREVIOUSLY HIDDEN IDENTITIES

Instantaneously connect hidden or unknown data that may expose your enterprise from targeted identity attacks

SECURE DIRECTORY STORES

Automatically scan Active Directory, Entra ID, and Okta credentials to detect compromised and weak passwords currently in use, and shut down password reuse across accounts

PREVENT & PROTECT AGAINST TARGETED IDENTITY ATTACKS

PREVENT ACCOUNT TAKEOVER

Automatically validate a user's identity when credentials appear in newly-recaptured darknet data, to automate resets before unauthorized access

ELIMINATE PASSWORD REUSE

Prevent password reuse and recycling of passwords that are in any way correlated to the user's holistic identity, complying with NIST guidelines

REDUCE EXPOSURES ACROSS SUPPLY CHAIN & EXECUTIVES

Uncover exposures that act as a follow-on attack for executives' personal accounts & even exposed domains managed by your supply chain

PROTECT AGAINST SESSION HIJACKING

Prevent criminals from bypassing authentication on trusted devices and moving laterally by resetting compromised session cookies associated with your domains

> ***"We discover anywhere from 3,000 to 11,000 direct matches per hour. Every one of those exposed accounts could have led to account takeover."***
>
> *– Financial Services Company*

USE CASES

AUTOMATED ACCOUNT TAKEOVER PREVENTION

Proactively detect and reset compromised credentials as soon as SpyCloud publishes recaptured identity records – even exposures you'd otherwise never see – finally preventing password reuse and recycling of passwords any way correlated to the holistic identity.

PROACTIVE RANSOMWARE PREVENTION

Remove blindspots in ransomware prevention with visibility into unauthorized access to business applications via malware-exfiltrated credentials and authentication cookies, and successful phishing attacks. SpyCloud delivers an expanded view of exposed identities that illuminate a path to ransomware prevention.

RESPOND & REMEDIATE COMPROMISED IDENTITIES

- **REMEDIATE EXPOSED IDENTITIES**
  Streamline SOC workflows with EDR, IdP, SIEM, and SOAR integrations to accelerate remediation of compromised credentials and malware-infected devices, users, and applications

- **AUTOMATE PASSWORD RESET**
  Rapidly remediate exposures ***within 5 minutes*** from discovery with automated workflows with Identity Provider integrations for Active Directory, Entra ID, and Okta - even those hidden behind an employee's personal identity

- **REMEDIATE MALWARE INFECTIONS**
  Remediate exposed identities from malware infections with critical information like infection details and path, IP address, and target URLs to shutdown entry points

- **REDUCE ALERT FATIGUE**
  Reduce alert fatigue with high-fidelity alerts with enriched data to remediate identity threats and shorten the attack window

HOW SPYCLOUD DELIVERS HOLISTIC IDENTITY THREAT PROTECTION

1. LARGEST ORIGINATOR OF RECAPTURED DARKNET DATA

2. COMPREHENSIVE & ACTIONABLE IDENTITY ANALYTICS

3. AUTOMATED REMEDIATION WITHIN YOUR EXISTING TOOLS

USE CASE

POST-INFECTION MALWARE REMEDIATION

Post-Infection Remediation is SpyCloud's crucial addition to complete malware infection response. Identity threat detection and response lacks the enriched identity data that prevents follow-on attacks, but SpyCloud provides the insights needed across all third-party applications exposed by malware, including shadow IT apps, even from unmanaged and personal devices to properly remediate malware-siphoned data from being used for other attacks.

> ***"Because the solution is fully automated, we are able to process 14,000 unique credentials per month. This scalability allows us to use our resources efficiently.***
>
> ***We don't have to do any manual processing of public breaches anymore, which took a lot of time with the constant stream of new breaches. SpyCloud's amazing API allows us to automate the entire process."***
>
> *- Niels Heijmans*
> *Principal Security Intelligence Analyst*
>
> **ATLASSIAN**

LARGEST ORIGINATOR OF RECAPTURED DARKNET DATA ▼

SpyCloud continuously ingests and analyzes more than 25 billion pieces of stolen identity data every month – delivering exposure data for rapid remediation **within 5 minutes from discovery**.

SpyCloud accesses freshly stolen and traded identity data from all layers of the darknet, and at a speed and volume that no other vendor can match. By applying data science, SpyCloud enriches and correlates to individuals in your organization to understand the impact, delivering instantly actionable alerts.

⚠ THIRD-PARTY BREACH DATA

Access billions of compromised credentials recaptured from third-party breaches. View critical insights like breach sources, descriptions, and plaintext passwords to prevent account takeover attempts.

MALWARE-EXFILTRATED DATA

Gain unmatched visibility into malware-exfiltrated identities, compromised devices, exposed applications, and stolen session cookies. SpyCloud's enriched malware data provides contextual details to accelerate comprehensive Post-Infection Remediation.

SUCCESSFULLY PHISHED DATA

Detect and remediate phishing threats with millions of recaptured credentials from successful phishing attacks. Early intervention stops identity-driven threats before criminals escalate privilege or deploy malware.

COMPREHENSIVE AND ACTIONABLE IDENTITY ANALYTICS ▼

SpyCloud's advanced analytics correlate identities - using exposed data from breaches, malware infections, and successful phishing attacks - of your workforce and their many online personas.

These analytics deliver significantly more exposed identity data to stop identity-based cybercrimes, with less noise. Our analytics drive action to mitigate attacks, ensure no false positives, and over 90% of passwords are delivered in plaintext.

KNOW MORE – WITH IDLINK ANALYTICS

Find up to 8x more identity records per user

SpyCloud's IDLink leverages our proprietary advanced identity analytics to detect all exposed credentials tied to your employees' personal identities – even those outside your monitoring visibility – looking for every compromise that makes up a holistic identity.

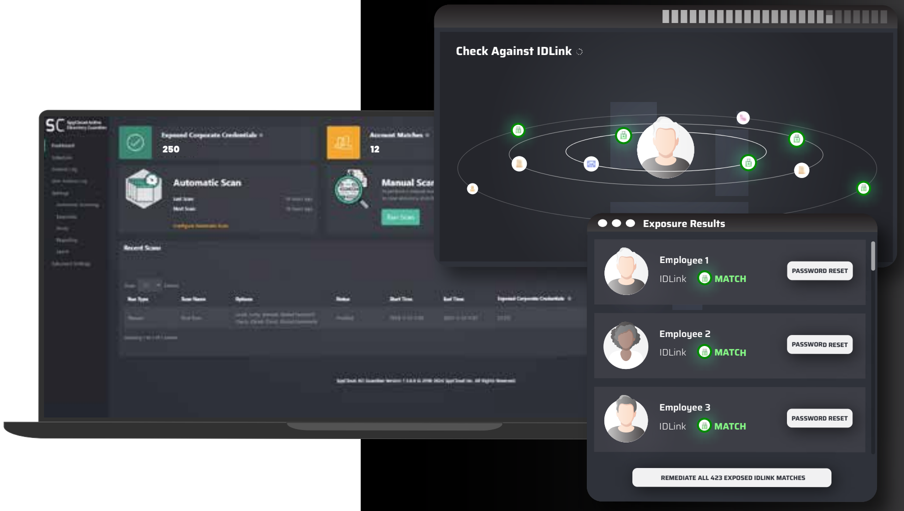
SpyCloud's holistic identity matching finds, on average, per user:

8x
MORE IDENTITY RECORDS

14x
MORE PLAINTEXT PASSWORDS

2x
MORE MALWARE RECORDS

5x
MORE EMAIL ADDRESSES



AUTOMATED REMEDIATION WITHIN YOUR EXISTING TOOLS

Centralize recaptured darknet identity data and make informed, actionable decisions with SpyCloud's out-of-the-box, native integrations.

Need help with automation and creating custom workflows across your security tools? Our hosted automation service builds custom workflows with almost any technology vendor to maximize your existing technology investments and automate at scale with confidence.

DO LESS – WITH SEAMLESS INTEGRATIONS AND HOSTED AUTOMATION

Layer SpyCloud into your existing tools and workflows for holistic identity threat protection at scale:

EDR INTEGRATIONS

- CROWDSTRIKE
- Windows Defender

SIEM INTEGRATIONS

- Microsoft Sentinel
- splunk>
- elastic

SOAR INTEGRATIONS

- tines
- CORTEX XSOAR BY PALO ALTO NETWORKS
- Microsoft Sentinel

IDENTITY PROVIDER INTEGRATIONS

- Microsoft Active Directory
- okta
- Microsoft Entra ID

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**.