SOLUTION BRIEF

SpyCloud

Safeguard consumer identities and prevent targeted attacks tied to malware

CONSUMER RISK PROTECTION

THE CHALLENGE

Upholding consumer account integrity to prevent account takeover (ATO) and keep personal and sensitive information safe is of utmost importance to security teams. Businesses are challenged with navigating consumers' poor password practices and managing the consequences of their digital identities being exposed within the criminal underground. Existing solutions often fall short, providing outdated and insufficient data, leaving security teams with only a piece of the puzzle in protecting their business from monetary loss while ensuring safe digital journeys for their valuable consumers. Meanwhile, cybercriminals continually evolve, side-stepping safeguards like MFA or bypassing authentication entirely, and maliciously exploiting and profiting off of the stolen data.

SOLUTION OVERVIEW

SpyCloud Consumer Risk Protection empowers security teams to secure their consumers' digital identities by staying ahead of next-gen account takeover threats – with insights from the criminal underground to preemptively protect consumers against targeted and automated ATO attacks, as well as session hijacking. SpyCloud offers actionable insights on breached credentials, malware-exfiltrated authentication data, and exposed PII to ensure unwavering account security for your consumers. By integrating SpyCloud into your security workflows, you can enhance efficiency, strengthen account security, and mitigate risk – all while delivering a seamless, friction-free customer journey.

THE SPYCLOUD DIFFERENCE: CYBERCRIME ANALYTICS

Making raw data recaptured from breaches, malware, and other underground sources actionable

SpyCloud has the largest repository of recaptured data tied to digital identities in the world, yet we still value quality over quantity – giving you more of the right data, at the right time, powered by Cybercrime Analytics.

SpyCloud's Cybercrime Analytics Engine delivers high volume recaptured data from the deepest layers of the darknet – curating, analyzing, and enriching it with actionable insights to deliver only the most relevant and high quality information to security teams. Businesses can in turn increase operational efficiency by reducing noise and streamlining otherwise manual processes.

COMPLETE VIEW OF A USER'S RISK

200+

supporting data types tied to a user's digital identity

UNMATCHED ABILITY TO CRACK PASSWORDS

90%

of passwords in the SpyCloud database are available in plaintext

KEY FEATURES & FUNCTIONALITY

SECURING DIGITAL IDENTITIES TO PREVENT ACCOUNT TAKEOVER

When criminals gain access to your consumers' credentials and exposed PII, they can effortlessly take over accounts, steal sensitive data, execute fraudulent transactions, and even lock legitimate users out of their accounts. SpyCloud delivers the visibility you need into your consumers' risk, with deep insights into exposed data available to criminals in the underground.

SpyCloud's high-volume, REST-based APIs are easily integrated into your application to fortify account security across a customer's entire lifecycle.

- **Defend against credential stuffing & targeted attacks** by enforcing strong passwords at the point of account creation and preventing the reuse of exact credential combinations that have been previously breached
- **Act on consumer risk at account login** by determining whether the consumer has been exposed, the nature of the exposures, and if their credentials align with those used to access their account
- **Identify exposed financial data or PII** that can be used for identity theft (ex: SSN, National ID, DOB, Address, Driver's License) or to facilitate fraud (ex: Credit Card Numbers, CSVs, Bank Accounts)
- **Detect malware-infected consumers** to shut down novel entry points to high-risk accounts that otherwise remain undetectable

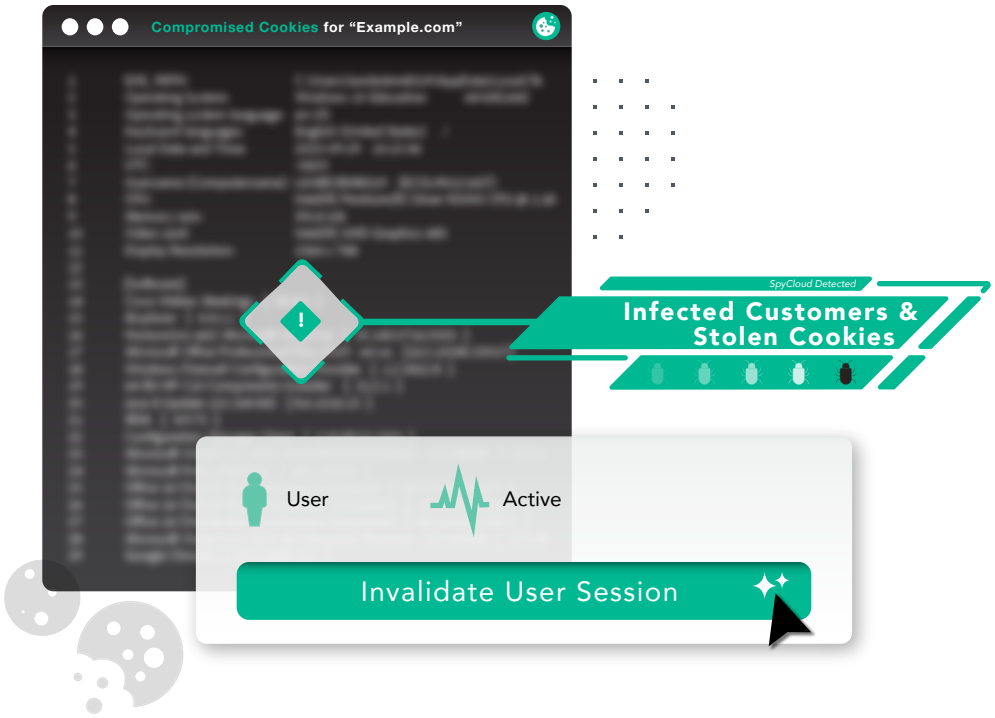
PREVENT AUTHENTICATION BYPASS & STOP SESSION HIJACKING

Cybercriminals excel at concealing malware within enticing links and downloads, causing a surge in consumers falling victim to malware infections – with more modern and sophisticated malware executing and auto-deleting before antivirus tools can even detect it. Cybercriminals perceive session cookies as the most actionable and highest value authentication data stolen, due to their potential for session hijacking – an advanced method of ATO that extends beyond the realm of traditional credentials.

Criminals have discovered ways to bypass all forms of authentication by using malware-exfiltrated cookies in anti-detect browsers to mimic a trusted consumer's device – defeating the need for a password, passkey, or any form of MFA. As long as a cookie stays valid, the gate to that consumer's account remains wide open.

SpyCloud identifies infected consumers and monitors malware logs for compromised session cookies tied to your application that can be used for session hijacking – alerting your business so you can act quickly to protect these high-risk accounts. With SpyCloud you can:

- **Identify compromised sessions** that must be invalidated to prevent authentication bypass, locking criminals out, and optionally requiring legitimate users to take additional steps to secure their accounts
- **Safeguard high-value accounts** and build trust by notifying consumers of their risk while advising them on how to devalue their stolen data to deter fraud



INCREASE OPERATIONAL EFFICIENCY WITH AUTOMATION

Security teams must make rapid decisions without impacting operational workflows and wasting resources on discovery. SpyCloud enables seamless prioritization of high-risk threats based on definitive indicators that cybercriminals have compromised data tied to your consumers. Our easy-to-implement APIs are flexible, catering to how your team prefers to structure their alerts and remediation workflows. Rest easy, knowing that SpyCloud delivers quality analytics, ready for action, to help reduce alert fatigue by converting noise to signal – delivering what your team needs to automate workflows, safeguard customer journeys, and streamline remediation.

- **Accelerate investigations** with robust query results that deliver a full picture of consumer risk and enable security teams with up tp 200+ data asset types per user – even providing counts of exposures, recency, severity, breach details, or PII exposed – all of which can be used in decision making
- **Easily adhere to compliance requirements** like NIST, and improve password protocols and governance by incorporating breach data into account creation security requirements to include the inability to use weak and previously compromised credentials
- **Protect valuable resources by alleviating time and headcount** dedicated to darknet data collection, data cleaning, parsing, and password cracking
- **Set it and forget it** with automated ATO prevention workflows that increase confidence to address risk and reduce monetary losses

SpyCloud Helps You Automate:

DARKNET DATA COLLECTION	Collect data from all darknet layers, including closed criminal communities where the most sinister cyber threats originate – compared to legacy tools that usually collect data from the darknet's surface or public sources, often retrieving outdated information.
DATA CLEANSING, PARSING, AND CRACKING	Reduce the noise, act on the signal – SpyCloud's Cybercrime Analytics Engine returns only clean and actionable data relevant to your consumers, with 90% of passwords available in plaintext.
SECURITY CHECKS	Check your customer database on a frequent basis against our continuously updated repository of third-party breaches and malware victim logs to proactively detect new exposures that put your consumers at risk, regardless of if the users have been active.
ATO PREVENTION EFFORTS	Integrate SpyCloud APIs into workflow applications, SIEMs, and TIPs to automate credential resets and invalidate active session cookies for high-risk or malware-infected accounts.
SESSION HIJACKING PREVENTION	Automate the invalidation of active stolen session cookies that are detected for your users, preventing authentication bypass and stopping hard-to-detect fraud.

11K

EXACT MATCHES PER HOUR

-Top 10 travel booking company

$10M+

FRAUD LOSSES PREVENTED

-Global fintech company

20M

ACCOUNTS RESET

-Global job hunting company

HOW IT WORKS

Flexibility is key when integrating SpyCloud's Consumer Risk Protection APIs into your workflows. Whether implemented at account creation for new customers, login for active users, or checking your customer database regularly for inactive accounts and general risk insights for all consumers, SpyCloud's high-volume REST-based APIs return up to 200+ data asset types per user. These insights include counts of exposures, recency, severity, breach details, and PII exposed, and identify malware-infected consumers and compromised session cookies.

Checking for Exposed Passwords, Credentials, and PII:

SpyCloud offers two complementary high-volume, performant APIs that can be used together or separately to help detect consumer risk and prevent traditional account takeover via the use of stolen credentials.

1. **PASSWORD ONLY CHECKS**

   Checking hashes of your consumers' passwords against billions of passwords in the SpyCloud database to identify if that **specific password** has been exposed (regardless of username), without compromising password secrecy.

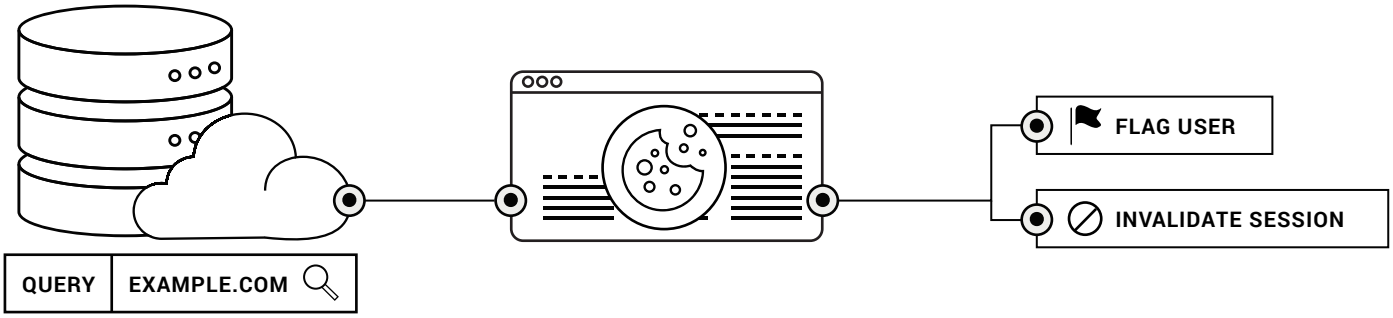
2. **USER EXPOSURE CHECKS**

   Checking the SpyCloud database for an identifier like email address, username, phone number, or IP address to determine if your **consumers' credentials and data** have been exposed in a breach or malware log. Aside from detecting credential exposures tied to the queried identifier, SpyCloud provides up to 200+ additional data types associated with the user (ex: SSN, National ID, Driver's License, DOB, Address, IP Address, Financial Data, etc.).

Both APIs include easy-to-understand, resource-oriented URLs, and use HTTP response codes to indicate API transaction status. All API responses return JSON, including those with errors.

Checking for Stolen Session Cookies from Malware Victims:

SpyCloud analyzes malware logs for appearances of your users' data and parses out the compromised cookies relevant to your application. Our Engine then enriches those records with information to help you identify the affected system for remediation, and delivers results via our high-volume REST-based API.



1. Query the API for your target application domain. Query options include:

- Cookie Domain (required)
- Cookie Name
- Cookie Expiration Date
- Source ID
- SpyCloud Publish Date

2. SpyCloud returns compromised cookie data associated with your application domain, including the information you need to identify which accounts are vulnerable. Results include:

- Source ID
- Cookie Domain
- Cookie Name
- Cookie Value
- Cookie Expiration
- SpyCloud Publish Date
- Infected Machine ID
- IP Addresses
- User Hostname
- User System Registered Owner

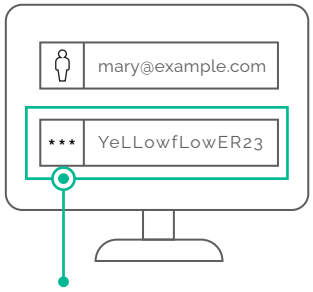
3. Choose how and when to intervene to protect these accounts. SpyCloud recommends you invalidate the compromised cookies, or flag consumer accounts with known compromised devices for increased scrutiny.

SECURITY & COMPLIANCE

Customer IP addresses accessing the SpyCloud APIs must be authorized, and all data is encrypted while in transit and at rest. We allow flexibility in the data points returned from our API, allowing you to obscure fields that shouldn't be accessible to your application. In addition, we can further secure the outputs by hashing and salting the values returned to you.

POPULAR IMPLEMENTATION OPTIONS

CREATE ACCOUNT

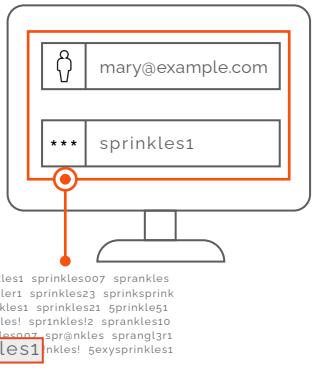


NO EXPOSURES DETECTED

PREVENT BAD PASSWORDS

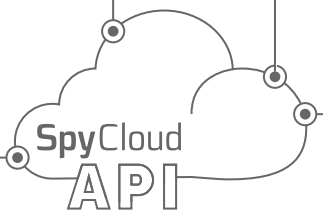
Head off weak/common passwords by checking consumer credentials for previous exposures during account creation and password resets.

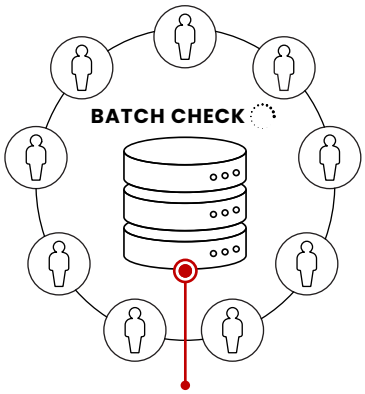
LOGIN



TEST USER LOGINS IN REAL TIME

Check credentials in real time as consumers log into your application, in parallel with an enhanced authentication procedure for high-risk accounts.





EXPOSURES DETECTED FOR **2,743 CONSUMERS**

CHECK YOUR ENTIRE DATABASE FOR EXPOSURES PROACTIVELY

Check your entire customer database on a frequent basis to detect new exposures, whether or not your consumers have been active.

14,372 COMPROMISED SESSION COOKIES

AUTOMATE COMPROMISED COOKIE CHECKS

Query the SpyCloud API frequently to identify newly-compromised session cookies for your application.

90%

REDUCTION IN ATO

-Global airline

6K

INFECTED CUSTOMERS IDENTIFIED

-Global hotel search site

20%

PERFORMANCE INCREASE

-Fortune 100 technology company

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to protect businesses from cyberattacks. Its products operationalize **Cybercrime Analytics** (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to nearly 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

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

"This was amazing. We were able to respond quickly, invalidate cookies, and protect millions of customer dollars."

- Financial Services Company