DATASHEET

SpyCloud

CONSUMER ACCOUNT TAKEOVER PREVENTION

STRENGTHEN ACCOUNT SECURITY & REDUCE ATO

Account takeover (ATO) risks are at an all-time high, as users continue to use weak or previously compromised passwords across multiple sites – making them vulnerable to both targeted attacks and credential stuffing.

SpyCloud Consumer ATO Prevention strengthens account security by providing direct insights into breached and malware-exfiltrated consumer credentials circulating in the criminal underground.

SpyCloud offers a proactive approach to mitigating ATO risk and reducing monetary losses by monitoring your consumers' logins for exposure against the industry's largest, continually-updated repository of recaptured darknet assets. When matches are detected, security teams can automate workflows to reset passwords or leverage enhanced authentication for at-risk accounts, without adding unnecessary friction for low-risk accounts. Implementation into your existing applications and workflows is easy, and allows you to quickly up-level account protections to cover previous blindspots.

> *"Now that we have SpyCloud, we can protect hundreds of millions of people and prevent them from choosing passwords that have already been exposed."*
>
> **LEADING WEB DEVELOPMENT COMPANY**

20M

ACCOUNTS RESET

Global Job Hunting Company

High-volume access to billions of fresh plaintext passwords to help detect matches, reset exposed credentials, and support your overall ATO and fraud prevention strategy

20%

PERFORMANCE INCREASE

Fortune 100 Technology Company

Expedite investigations with access to 200+ data asset types providing counts of exposures, recency, severity, breach details, and more that can be used in workflows for decision making.

$10M+

FRAUD LOSSES PREVENTED

Global Fintech Company

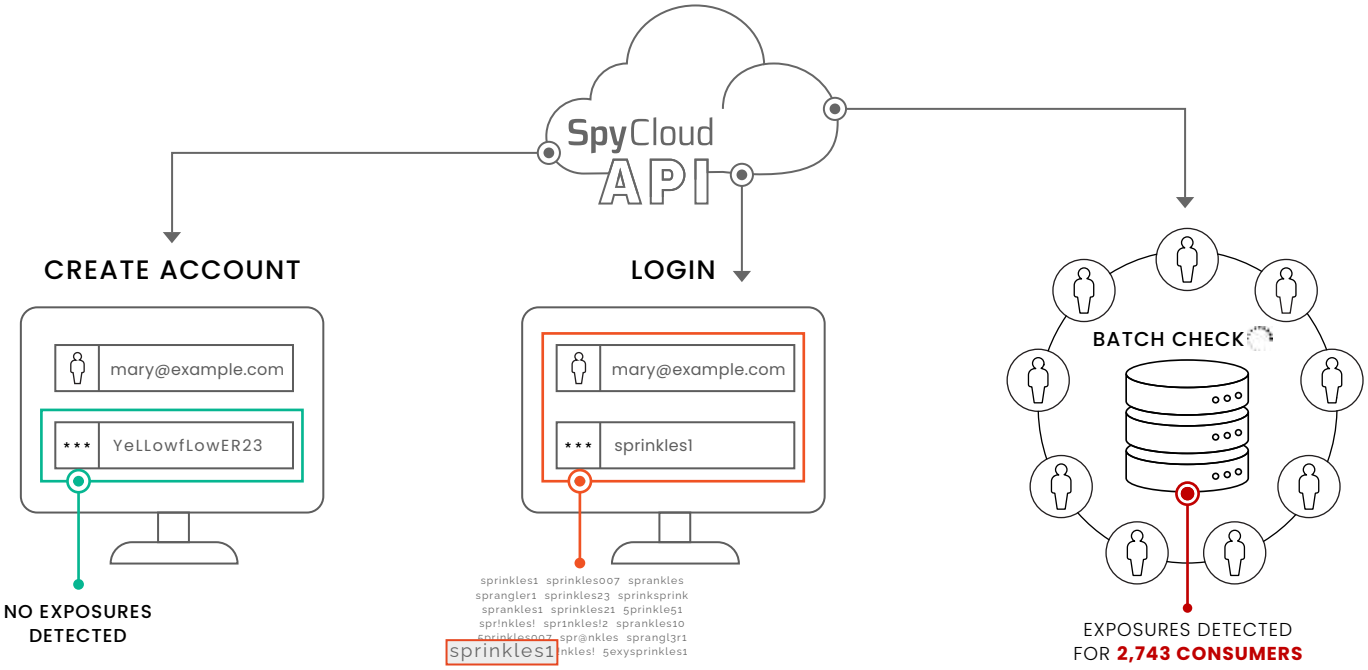
Visibility into otherwise undetectable threats victims of malware pose (over 22 million unique infected machines detected by SpyCloud in 2022 alone).

SPYCLOUD CONSUMER ATO PREVENTION

SpyCloud

HOW IT WORKS

SpyCloud Consumer ATO Prevention operationalizes SpyCloud's extensive database of recaptured darknet assets using high-volume, REST-based APIs. Depending on your organization's requirements, you can check consumer logins using identifiers (such as email address, username, phone number, or IP address), passwords (partial hashes), or a combination of both. Alternative solutions are available for organizations that must satisfy a high volume of API calls or specialized privacy requirements.



PREVENT BAD PASSWORDS

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

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.

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.

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 more than 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.