DATASHEET

SpyCloud

CONTINUOUS DARK WEB MONITORING

REAL-TIME PUSH ALERTS DELIVERED AS A SERVICE
POWERED BY THE INDUSTRY'S LARGEST COLLECTION OF DARK WEB DATA

THE PROBLEM

The dark web has become a marketplace for stolen data, where cybercriminals buy, sell, and trade sensitive information – putting millions of individuals at risk of account takeover, identity theft, and fraud. Traditional dark web monitoring solutions often fall short – having mainly access to either commoditized data that has been exposed for months or even years, or limited to no insight into malware-exfiltrated or successfully phished data.

Although high-quality data is critical for effective monitoring, many teams lack the engineering resources to efficiently implement scalable dark web monitoring solutions. So how do teams balance increasing business productivity, and safeguarding consumer experiences to build loyalty and trust, without adding friction to already limited resources?

THE SOLUTION

SpyCloud Continuous Dark Web Monitoring goes beyond traditional dark web monitoring – offering a seamless way to maximize the value of your products and services, decrease your engineering footprint, and adhere to governance, risk, and compliance concerns. Our service does the heavy lifting for you, by continuously monitoring and alerting on new identity exposures with the right data, at the right time – giving you flexibility to implement tiered pricing and valued added services within your offering. Powered by the industry's largest collection of recaptured data, SpyCloud Continuous Dark Web Monitoring gives you instant visibility into users' exposures from breaches, malware infections, and successful phishing attacks – enabling them to take action and mitigate appropriately.

BENEFITS AT A GLANCE

Push Alerts for Rapid Remediation
Combat identity exposures and generate new revenue streams with real-time push notifications powered by the industry's largest repository of dark web data

Reduce Costs and Save Time
Decrease your engineering footprint and let SpyCloud offload the majority of the data processing and matching logic – saving compute and general processing time by dealing only with assets that have new data

Increase Customer Loyalty
Augment your products and solutions to include differentiated matching of recaptured identity assets as quickly as possible to increase customer acquisition and retention

TAKE YOUR DARK WEB MONITORING TO THE NEXT LEVEL

Arm your product teams with world’s largest and most actionable collection of recaptured identity data – speeding the delivery of critical exposure data to your application for rapid action and continuous protection

CONSUMER DARK WEB MONITORING SERVICE PROVIDERS

IDENTITY THEFT PROTECTION SERVICES

PASSWORD MANAGER PROVIDERS

ECOMMERCE APPLICATIONS

B2B APPLICATIONS WITH ATO CONCERNS

WHY SPYCLOUD

THE RIGHT DATA

- SpyCloud built and maintains the largest, most diverse, and highly actionable breach, malware-exfiltrated and successfully phished data repository in the industry.
- We deliver insights that you can act on quickly – via our highly flexible and scalable API that seamlessly integrates into your products, tools, and workflows – to shut down identity-based attacks.
- The variety and depth of assets we provide enables product teams to design a wide range of monetized value-adds within their solutions – making it easy to tier pricing to unlock new levels of coverage.
- Through our partnership, your solution will integrate SpyCloud data, exposing certain pieces of information to your users to educate them and to act on to secure themselves online.
- Some examples of data you may share include: date of breach, compromised website, exposed email address / username, plaintext password, specific personally identifiable information (PII) such as phone number, physical address, SSN, international ID, credit card, bank account number, etc.

AT THE RIGHT TIME

- We offer the earliest possible access to dark web-exposed data so it can be actioned on quickly, thwarting criminals from using it to take over accounts and perpetrate fraud.
- Our team of experienced researchers collects and rapidly ingests data from criminal communities other companies can't access, often months or even years ahead of anyone else in the industry.
- You choose when and how to deliver it to your users, but rest assured that SpyCloud's speed of delivery gives you an edge.

700B+ RECAPTURED ASSETS | **46k+** BREACHES | **25B+** ASSETS INGESTED MONTHLY | **60+** MALWARE FAMILIES | **90%** PLAINTEXT PASSWORDS

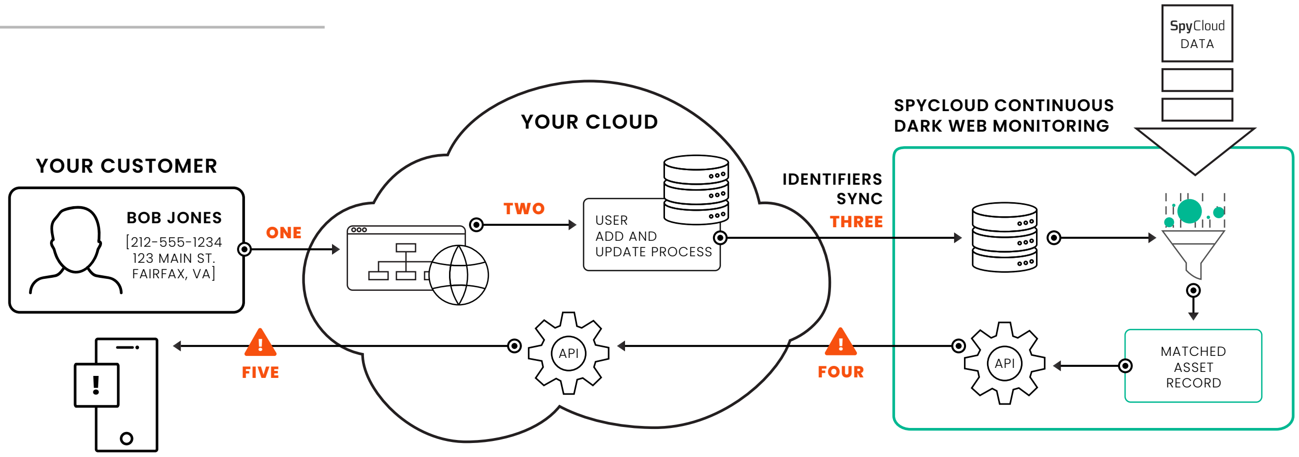
BEST PRACTICES FOR MAXIMUM SUCCESS

We provide best practices around notifying your users of exposures, with insight into:

- Choosing the appropriate level of transparency
- Why timing matters
- Educating on password reuse and MFA
- Suggested methods of malware remediation

We offer email template guidance that shows how you can display information to your user – with localized translations available to meet needs across a variety of geographies.

HOW IT WORKS



ONE Your user registers for monitoring via your website or application

TWO Your internal processes update your local store of their monitored assets, and then you call SpyCloud's API to register this user for exposure monitoring

THREE SpyCloud takes that registration data and updates our filter in our system that continuously monitors our data pipeline for relevant matches

FOUR When a match is identified, a matched record is sent via our PUSH API to your endpoint, alerting you of the match and corresponding details

FIVE You take those details and send an appropriate alert to your user

DATA DELIVERY OPTIONS

- **PUSH API WITH RECORD |** This combines the alert and the record into a single API PUSH alert
- **PUSH API WITH CALLBACK |** This separates the alert workflow from the record delivery and is suited for environments wishing to keep alerting infrastructure separate from data-access components

HOW TO INTEGRATE WITH OUR API

FULL PRODUCTION DATA FOR NEW USERS

- For every new user who signs up, call our services to collect exposure details and cache for reference when the user navigates through your UI

CONTINUOUS MONITORING FOR ALL YOUR USERS

- For all users with configured identity assets, our service continuously monitors for exposures of those assets, generating an alert when a match is found

BREACH CATALOG INITIAL PULL

- The breach catalog allows you to match individual exposure records to the exposure source details
  - Where this data is from
  - When the exposure took place
  - Other contextual background information
- You will want to access our breach catalog and cache the details for matching our data in your UI

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 more than half 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**.