

THIRD PARTY INSIGHT

MONITOR SUPPLY CHAIN ATO RISKS AND **PROTECT YOUR CORPORATE DATA**

THE CHALLENGE

Third-party vendors with privileged access to your data and systems pose risk of opening unauthorized access to your enterprise network if their employees or operations are compromised. If employees within your vendors have exposed credentials in the darkweb, criminals have an easy path to targeting your employees for ATO or following up with costly cyberattacks.

PRODUCT OVERVIEW

SpyCloud Third Party Insight draws from the largest repository of recaptured breach and malware data to help you understand risk of potential exposures across your third party vendors to prevent employee ATO. By reviewing SpyCloud's defined security risk levels, you can proactively take action to defend against any threats to your employee identity and company data.

With SpyCloud's interactive dashboard, you can monitor your third parties' ATO risk at-a-glance and view trends over time to identify spikes to help optimize your security posture. Additionally, you can provide critical partners with access to the compromised data they need to remediate incidents, including usernames and plaintext passwords. **SpyCloud Third Party Insight** continuously updates the security risk rating of your vendors so you can proactively defend against next-gen threats.



BENEFITS AT A GLANCE

IDENTIFY VENDOR EXPOSURES EARLY

Identify compromised credentials within your supply chain early, before criminals can exploit and target your employees

GET DEEP VISIBILITY

Gain insight into your third parties' ATO exposure, including when and why their risk level has changed over time

TAKE ACTION

Enable remediation by sharing detailed access to exposure data within a vendor-provisioned portal, including affected usernames and passwords

CLOSE THE LOOP

Report on your third parties' remediation actions to confirm whether they have acted on your recommendations to reduce exposure

HOW IT WORKS

1. Select your third-party vendors from a list to add to your SpyCloud watchlist for ongoing monitoring.
2. View high-risk security relationships at a glance with SpyCloud's indicator of High, Medium, or Low risk.
3. SpyCloud alerts you whenever credentials tied to your partners appear in breach or malware records, increasing their risk of ATO – enabling you to keep track of when and why a third-party vendor's security risk has changed.
4. Understand SpyCloud risk factors such as exposed corporate credentials, vulnerable C-level executives and VIPs, potentially infected employees, combo list collisions, and password reuse rates.
5. Invite third parties to access their own SpyCloud portal for the data needed to validate and remediate, including exposed usernames and plaintext passwords.
6. Monitor vendors who take action to resolve their exposures and remediate on their end, which will lower their SpyCloud security risk.

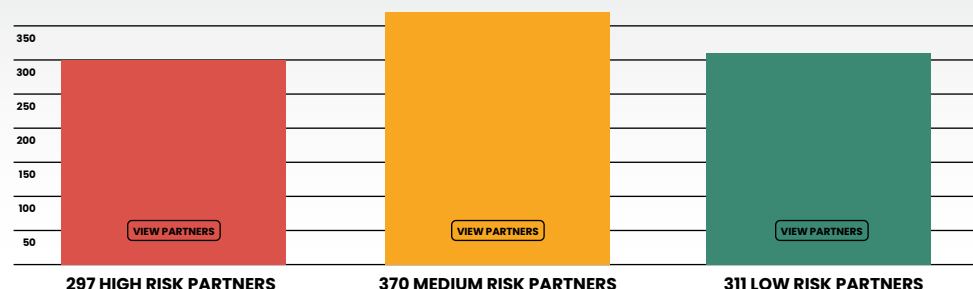
SpyCloud

Third Party Insight
VIEW THIRD PARTY INSIGHT

Third Party Insight
DASHBOARD

SECURITY RATING DISTRIBUTION

ADD PARTNERS



Changes in the Last 30 Days

↑ INCREASED RISK

10%

106 partners increased their risk

VIEW PARTNERS

↓ DECREASED RISK

1%

19 partners decreased their risk

VIEW PARTNERS



KEY CAPABILITIES

- **CONTINUOUS MONITORING** | SpyCloud continuously monitors domains, IPs, and emails and checks for exposures against the largest repository of recaptured darknet data
- **COMPLETE VISIBILITY** | Quickly identify high-risk third parties with a summary dashboard that groups vendor domains by high, medium, and low security ratings
- **RISK SCORING** | Understand SpyCloud's risk assessment categorized by the levels of exposed plaintext credentials, VIP and C-level executives exposed, potentially infected employees, combo list collisions, and password reuse rates
- **SHARE FINDINGS** | Invite your partners to their own vendor-provisioned portal to access their exposure data
- **SECURITY ALERTS** | Receive alerts from SpyCloud when your third parties' credentials are exposed in recaptured breach or malware logs
- **CHANGES AT-A-GLANCE** | View trends in third-party risk over time in dashboards to see which vendors are lowering their exposure

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 >