

EMPLOYEE ATO PREVENTION

STAY AHEAD OF ACCOUNT TAKEOVER AND TARGETED ATTACKS
BY PROACTIVELY DETECTING AND RESETTING COMPROMISED PASSWORDS

THE PROBLEM

Stolen credentials remain the #1 way criminals gain access to corporate networks and the sensitive information within. Employees often prioritize convenience over security and reuse credentials across multiple sites, increasing the odds of criminals acquiring them from third-party breaches or malware infections and using them to gain unauthorized access. Organizations must find ways to detect and reset compromised credentials to shut down entry points

PRODUCT OVERVIEW

SpyCloud Employee ATO Prevention offers an easy to implement solution that continuously monitors and alerts on any employee exposures within the criminal underground – helping enterprises reduce risk of identity-based cyberattacks and data breaches. SpyCloud checks employee credentials against billions of recaptured breach and malware records in the SpyCloud database, and proactively notifies security teams when a match is found to take swift action to remediate any vulnerable, compromised accounts. Security teams can quickly identify exposed users and reset compromised passwords before criminals have a chance to use them – greatly reducing the effort it takes to keep corporate assets secure.

TAKE CONTROL OF YOUR CORPORATE EXPOSURE

Monitor multiple domains for exposed employee logins, checking each set of credentials against the largest, most continuously updated, and most actionable repository of recaptured darknet data.

STAY A STEP AHEAD OF CRIMINALS

Reset exposed passwords before criminals have a chance to use them. SpyCloud provides fast, high-volume access to recaptured data early in the breach lifecycle.



BENEFITS AT A GLANCE

Decreased Exposure Window

Early notification of new exposures enables security teams to swiftly reset exposed employee credentials and protect corporate resources from criminals

Continuous Credential Monitoring

World's largest repository of recaptured breach and malware data helps detect exposed credentials to automate password resets









Automated Remediation

Minimize security team efforts and enhance existing workflows to automate the remediation of exposed passwords

Flexible API Integrations

Custom, high-volume APIs with simple configuration to integrate SpyCloud data with your current tech ecosystem to streamline account takeover prevention

KEY CAPABILITIES

-  **COMPROMISED CREDENTIAL MONITORING**
Monitor your watchlist domains, IPs, and emails and checks for exposures against the largest repository of recaptured darknet data.
-  **REAL-TIME ALERTS**
Receive alerts when a new exposure is detected for any of the items in your watchlist.
-  **PREVENT PASSWORD REUSE**
Stop employees from reusing a password that was previously exposed in the criminal underground.
-  **SSO PORTAL**
Secure access to a user-facing portal to view breach and malware activity.
-  **ADMIN CONTROL**
Admins can add or remove domains, email addresses, and IP addresses to the watchlist.
-  **GRANULAR ATTRIBUTION**
Seamless context and correlation of compromised data sources to decrease dwell time and enable rapid response.
-  **EXECUTIVE REPORTING**
High level report exposures and ATOs avoided to share with executive leaders – available in the portal or as a monthly email.
-  **DATA EXPORT**
Export anything as a CSV to enable your desired level of analysis and create custom reports based on individualized or use case metrics.

OUT-OF-THE-BOX API WORKFLOW INTEGRATIONS



Integrate SpyCloud breach and malware alerts with common directory services, SIEMs, SOARs, and ticketing platforms to automate response and help prevent employee account takeover. Trigger alerts in internal detection software to optimize incident response processes. SpyCloud can integrate with any preferred application via custom integrations.

ACTIONABLE DATA, TIMELY INSIGHTS – POWERED BY SPYCLOUD'S CYBERCRIME ANALYTICS ENGINE



COLLECT

Continuous monitoring for compromised credentials identifies stolen and leaked assets very early in the attack timeline



CURATE

Cleansed and curated breach and malware data removes irrelevant files, identifies duplicate records, and curates data to ensure relevance, including count of unique data collected from third-party data breaches



ENRICH

Contextual information includes compromised data sources, with breach description and plaintext password, improves actionability and enables rapid response



ANALYZE

Unique insights into the severity risk of exposures help security teams determine the appropriate response



AUTOMATE

Drive action to protect digital identities with flexible APIs that can be embedded into your workflows and applications, or via integrations to popular directory services, SIEMs, SOARs, and TIPs

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.