SpyCloud

WORKFORCE THREAT PROTECTION

STAY AHEAD OF ACCOUNT TAKEOVER AND TARGETED ATTACKS
BY PROACTIVELY DETECTING AND REMEDIATING COMPROMISED IDENTITIES

THE PROBLEM

Cybercriminals are exploiting exposed identities to bypass defenses, using compromised credentials for account takeover to access corporate networks and sensitive data. Employees often prioritize convenience over security, reusing passwords across their online personas, increasing the risk of exposure and compromise. Traditional monitoring tools miss these hidden identity exposures, leaving organizations vulnerable for targeted attacks. Organizations must automatically detect and reset compromised credentials, shutting down entry points for criminals.

PRODUCT OVERVIEW

SpyCloud Workforce Threat Protection reduces your organization's risk with real-time alerts when employee identity data is exposed on the darknet, delivering definitive evidence of compromise. With the world's largest collection of recaptured identity data, SpyCloud continuously checks employee credentials against billions of recaptured breach, malware, and phishing records for matches. Security teams can quickly identify exposed users and reset compromised passwords before criminals have a chance to use them. Easy to implement through a SaaS-based portal and seamless integrations, SpyCloud Workforce Threat Protection greatly reduces the effort it takes to keep identities safe, and corporate data secure.

BENEFITS AT A GLANCE

Decreased Exposure Window ▪
Reset exposed employee credentials early in the attack lifecycle, shutting down criminal entry points and safeguarding corporate resources

Continuous Credential Monitoring ▪
Gain unmatched visibility into recaptured darknet data with access the world's largest, continuously updated repository of breached, malware-exfiltrated, and successfully phished data

Automated Remediation ▪
Minimize security team workload and automate remediation of exposed passwords in existing workflows

Prioritize Critical Threats ▪
Focus on the most urgent risks with advanced filtering options, enabling quick identification and resolution of the exposures that matter most

SpyCloud

KEY CAPABILITIES

COMPROMISED CREDENTIAL MONITORING

Monitor your watchlist of domains, IPs, and emails for exposures against the largest repository of recaptured darknet data

REAL-TIME EXPOSURE ALERTS

Receive alerts when a new exposure is detected for any of the items in your watchlist

EXPOSED PASSWORD REUSE

Identify employees reusing exposed passwords and pinpoint top offenders to address trends and improve password hygiene

SECURE SSO-PORTAL

Access an intuitive portal with a user-friendly dashboard with detailed exposure data and organizational analytics to prioritize and streamline security efforts

ADMIN CONTROL

Administrators can add or remove domains, email addresses, and IP addresses to the SpyCloud Watchlist for tailored protection

EXECUTIVE REPORTING

Generate high-level reports on exposures and ATOs prevented to share with executive leaders – available on-demand or as a monthly email

DATA EXPORT

Export anything as a CSV for deeper analysis or to create custom reports based on individualized or use case metrics

DOMAIN-SPECIFIC MONITORING

Focus on critical areas of concern with domainspecific exposure insights, enabling faster, targeted responses to identity threats

FLEXIBLE INTEGRATIONS

Make the most out of your existing security stack, and enable rapid remediation by sending SpyCloud data to your preferred tools – with seamless integrations into SIEMs, SOARs, Identity Providers, and TIPs

ACTIONABLE SPYCLOUD EXPOSURE DATA, TIMELY INSIGHTS –
SHIFT TOWARDS HOLISTIC IDENTITY THREAT PROTECTION

SpyCloud continuously ingests and analyzes more than 25 billion pieces of stolen identity data every month – delivering exposure data for rapid remediation in 5 minutes from discovery. Preventing targeted employee ATO requires a view into exposures using a holistic identity lens - an interconnected web of darknet data that helps you understand the risk to your business.

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, 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 seven 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**.