SOLUTION BRIEF

SpyCloud

Prevent targeted cyberattacks with identity threat protection across your workforce, endpoints, and supply chain

ENTERPRISE PROTECTION

THE CHALLENGE

Identity is the primary attack surface – and it extends far beyond your managed workforce.

Employees, contractors, endpoints, and third-party vendors all create exposure paths that traditional IAM, EDR, ITDR, and MFA weren't designed to see. Criminals don't break in anymore – they log in using recaptured credentials, stolen session cookies, and malware-exfiltrated identity data circulating the criminal underground.

When identity exposures go undetected across work and personal accounts, managed and unmanaged devices, and vendor ecosystems, attackers gain trusted access – leading to account takeover, session hijacking, and ransomware.

To stop targeted attacks, security teams need visibility across the holistic identity – and the ability to act before criminals do.

UPLEVEL YOUR DEFENSES – VISUALIZE & ACT ON EXPOSED IDENTITIES TO STOP CYBERCRIMINALS

RISKY HUMAN BEHAVIOR

82% of breaches involve a **human element**

EXPOSED APPLICATIONS

A single malware infection can expose access to an average of **26 business apps**

SUPPLY CHAIN BLIND SPOT

Third-party involvement in breaches doubled YoY from **15%** to **30%**

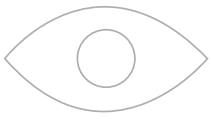
SOLUTION OVERVIEW

SpyCloud Enterprise Protection prevents identity-based attacks by turning recaptured darknet data into automated remediation. Powered by the world's largest repository of breach, malware, phishing, and combolist data, SpyCloud correlates exposures across employees, contractors, endpoints, and vendors to connect work and personal identities and uncover hidden risk.

When new identity exposure data appears, SpyCloud triggers automated action within minutes – resetting compromised credentials, invalidating session cookies, and remediating infected devices before attackers gain access.

SpyCloud integrates directly into your identity providers, EDR, SIEM, and SOAR tools – reducing manual effort, accelerating response, and closing identity-driven entry points across your workforce and supply chain.

DEEPER UNDERGROUND INSIGHTS, CLEAR ANSWERS, AND AUTOMATED ACTION

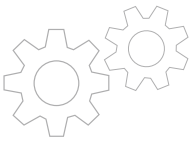


MONITOR & DETECT

Continuously monitor your workforce's **holistic identities** – inclusive of employees, contractors, and vendors – with real-time insight into recaptured data circulating in the criminal underground

PROTECT & PREVENT

Strengthen your workforce and supply chain with automated protection against identity-based attacks – **increasing control and reducing risk**



RESPOND & REMEDIATE

Rapidly remediate identity exposures **within 5 minutes** of discovery to optimize SOC workflows – decreasing MTTD and MTTR

SPYCLOUD ENTERPRISE PROTECTION

Move beyond detection to automated remediation. Protect identities across your extended workforce to secure every access point.

MONITOR & DETECT IDENTITY EXPOSURES

CONTINUOUS MONITORING
Access the world's largest, continuously updated repository of breach, malware, phished, and combolist data recaptured from the criminal underground – delivering visibility into exposures early in the attack timeline

MONITOR EXPOSURES ON ANY DEVICE TYPE
Detect exposures from managed, unmanaged, and personal devices, including BYOD, to shift from account-centric security to identity-focused protection

UNCOVER PREVIOUSLY HIDDEN IDENTITIES
Connect hidden or unknown exposure data across employees' work and personal personas, malware-infected endpoints, and vendor employees to reveal hidden threats

SECURE DIRECTORY STORES
Automatically scan Active Directory, Entra ID, and Okta to detect compromised and weak passwords currently in use and eliminate password reuse across accounts

PREVENT & PROTECT AGAINST TARGETED IDENTITY ATTACKS

PREVENT ACCOUNT TAKEOVER
Validate identities when exposure data appears in newly recaptured underground records and trigger resets before unauthorized access

ELIMINATE PASSWORD REUSE
Prevent password reuse and recycling of passwords that are in any way correlated to the user's holistic identity, complying with NIST guidelines

SECURE YOUR SUPPLY CHAIN
Identify vendors whose employees have exposed credentials or active malware infections before attackers use them as entry points

PROTECT AGAINST SESSION HIJACKING
Prevent criminals from bypassing authentication on trusted devices and gaining unauthorized access by resetting compromised session cookies associated with your domains

"We discover anywhere from 3,000 to 11,000 direct matches per hour. Every one of those exposed accounts could have led to account takeover."

- Financial Services Company

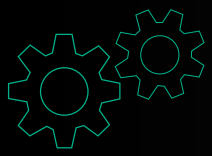
USE CASES

AUTOMATED ACCOUNT TAKEOVER PREVENTION

Detect and reset exposed credentials as soon as SpyCloud publishes newly recaptured identity records – including exposures outside traditional monitoring visibility – finally preventing password reuse and recycling of passwords any way correlated to the holistic identity.

PROACTIVE RANSOMWARE PREVENTION

Remove blind spots in ransomware prevention with visibility into unauthorized access to business applications via malware-exfiltrated credentials and authentication cookies, and successful phishing attacks. SpyCloud delivers an expanded view of exposed identities that illuminate a path to ransomware prevention.



RESPOND & REMEDIATE COMPROMISED IDENTITIES

REMEDIATE EXPOSED IDENTITIES
Streamline SOC workflows with IDP, EDR, SIEM, and SOAR integrations to accelerate remediation of compromised credentials, malware-infected devices, users, and applications

AUTOMATE PASSWORD RESET
Rapidly remediate exposures ***within 5 minutes*** of discovery with automated workflows for Active Directory, Entra ID, and Okta - including exposures tied to employees' personal identities

REMEDIATE MALWARE INFECTIONS
Address identity exposures resulting from malware infections with contextual details including infection path, IP address, and target URLs to close entry points

REDUCE ALERT FATIGUE
Reduce alert fatigue with high-fidelity alerts with enriched data to remediate identity threats and shorten the attack window

INVESTIGATE DEEPER WHEN THREATS ESCALATE

Effective remediation starts with understanding the full scope of identity compromise and putting that intelligence in the hands of the people responsible for stopping it.

SpyCloud Cybercrime Investigations connects fragmented identity data to uncover and contextualize threats – starting with a single selector like an email address or username. SpyCloud's integrated AI applies decades of investigative tradecraft to surface high-risk exposure patterns and hidden relationships, uplevelling the output of your analysts.

The result: finished, contextualized intelligence in seconds so you can understand and end identity threats.

Learn more about Cybercrime Investigations>

USE CASE

INSIDER THREAT DETECTION

Insider threats, whether malicious or negligent, can often be tied back to exposed or misused identity data. SpyCloud combines investigative tradecraft and identity analytics to identify employees, vendors, and job candidates who are compromised, infected, or using stolen identities.

VENDOR RISK DETECTION

Third-party vendors can introduce hidden risk through exposed credentials, malware infections, or phishing attacks that extend access into your environment. SpyCloud uncovers compromised vendor identities across your supply chain to identify risky partners and act before that access is exploited.

"By combining speed, clarity, and depth of intelligence, SpyCloud Investigations with AI Insights sets a new benchmark for how modern security teams should approach threat investigations."

– Jacques Chitarra
Sr. Director of Global Security & Privacy

Samsonite

LARGEST ORIGINATOR OF RECAPTURED DARKNET DATA

SpyCloud continuously ingests and analyzes more than 25 billion pieces of stolen identity data every month – delivering exposure data for rapid remediation **within 5 minutes** from discovery.

SpyCloud accesses freshly stolen and traded identity data from all layers of the criminal underground, and at a speed and volume that no other vendor can match. Using advanced analytics, SpyCloud enriches and correlates to individuals in your organization to understand the impact, delivering instantly actionable alerts.

This unmatched data collection enables continuous monitoring not just across your employee base, but extending to your vendor ecosystem and endpoint visibility – providing enterprise-wide identity threat protection from a single intelligence source.

SUCCESSFULLY PHISHED DATA

Detect and remediate threats with millions of recaptured credentials from successful phishing attacks. Early intervention stops identity-driven threats before criminals escalate privilege or deploy malware.

MALWARE-EXFILTRATED DATA

Gain unmatched visibility into malware-exfiltrated identities, compromised devices, exposed applications, and stolen session cookies. SpyCloud's enriched malware data provides contextual details to accelerate comprehensive post-infection remediation.

THIRD-PARTY BREACH DATA

Access billions of compromised credentials recaptured from third-party breaches, including breach source details and plaintext passwords to prevent account takeover attempts.

REPACKAGED COMBOLISTS

Stay ahead of emerging combolist trends generated from infostealer logs. Repackaged credentials often include actively used passwords sourced from URL:Login:Password (ULP) lists, increasing enterprise risk.

KNOW MORE – WITH IDLINK ANALYTICS

FIND UP TO 8X MORE IDENTITY RECORDS PER USER

SpyCloud's IDLink leverages our proprietary advanced identity analytics to detect all exposed credentials tied to your employees' personal identities - even those outside your monitoring visibility looking for every compromise that makes up a holistic identity.

SpyCloud's holistic identity matching finds, on average, per user:

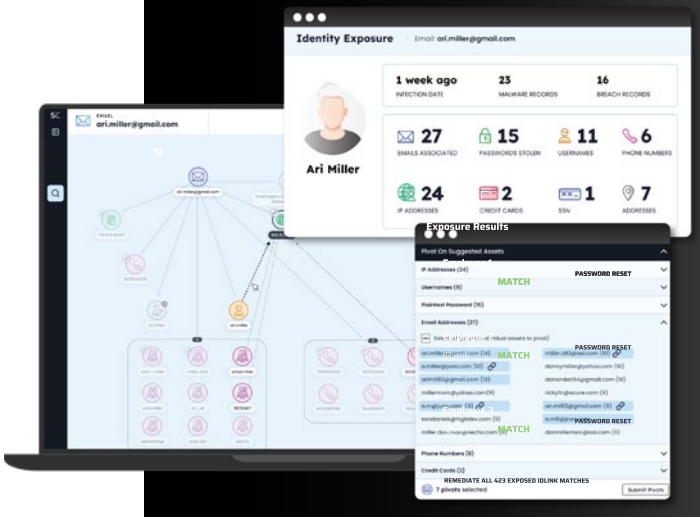
8x MORE RECORDS

14x MORE PLAINTEXT PASSWORDS

2x MORE MALWARE RECORDS

5x MORE EMAIL ADDRESSES

These analytics deliver significantly more exposed identity data to stop identity-based cybercrimes, with less noise. Our analytics drive action to mitigate attacks, ensure no false positives, and over 90% of passwords are delivered in plaintext.



AUTOMATED REMEDIATION WITHIN YOUR EXISTING TOOLS

Centralize recaptured darknet identity data and make informed, actionable decisions with SpyCloud's out-of-the-box, native integrations.

INTEGRATE WHERE IDENTITY HYGIENE HAPPENS

Whether you manage on-prem directories or cloud-based identities, SpyCloud Identity Guardians integrate directly into your environment to automate credential remediation and session termination in real time. Automatically detect exposed passwords, reset compromised credentials, and invalidate stolen session cookies to improve password hygiene across your workforce and vendor ecosystem.

Scan your directory store with IDLink analytics to uncover up to **14x more exposed passwords** per user.

IAM INTEGRATIONS

Active Directory · Microsoft Entra ID · okta · PingIdentity

DO LESS – WITH SEAMLESS INTEGRATIONS AND HOSTED AUTOMATION

Layer SpyCloud into your existing tools and workflows for identity threat protection across your workforce and supply chain.

EDR INTEGRATIONS

CROWDSTRIKE

Microsoft Defender for Endpoint

SIEM INTEGRATIONS

splunk> · elastic

Microsoft Sentinel · Google Security Operations

SOAR INTEGRATIONS

Microsoft Sentinel · CORTEX XSOAR

tines · Google Security Operations

SpyCloud CONNECT

Need help with automation and creating custom workflows across your security tools? Our hosted automation service builds custom workflows with almost any technology vendor to maximize your existing technology investments and automate at scale with confidence.

Ready to see it in action?
Take a self-guided tour in our Demo Center or request a custom demo today.

DEMO CENTER › **REQUEST DEMO ›**

ABOUT SPYCLOUD

SpyCloud protects businesses from the stolen identity data criminals are using to target them now. 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.

To learn more about its holistic identity approach and see your company's exposed identity data, visit **spycloud.com**.