SOLUTION BRIEF

SpyCloud

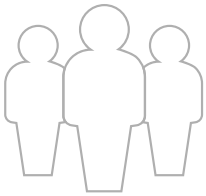
Safeguard your employees' digital identities and prevent targeted cyberattacks

ENTERPRISE PROTECTION

THE CHALLENGE

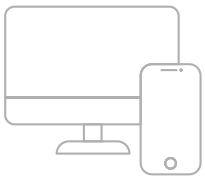
From account takeover to session hijacking and ransomware, cybercriminals are constantly finding new attack vectors and technology that use stolen credentials to gain access to enterprise networks and data. People and their digital identity are the new perimeter of your security framework. To safeguard employee identities and protect your data and critical IP, security teams need to move beyond legacy threat intel and device-centric remediation. With SpyCloud, take an identity-centric approach that elevates your response and remediation workflows towards identity-based exposures with flexibility and scale.

ACCESS CYBERCRIME ANALYTICS TO CLOSE GAPS IN YOUR DEFENSE



HUMAN-DRIVEN RISKS

82% of breaches are initiated by **human error**



UNMANAGED DEVICES

36% of organizations allow personal devices to **access business apps and systems**

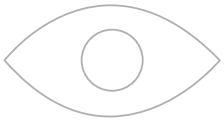
EXPOSED APPLICATIONS

Malware infection exposes access to an average of **26 business apps**

SOLUTION OVERVIEW

SpyCloud's Enterprise Protection provides actionable, identity-centric solutions for disrupting cybercrime. We empower security teams to rapidly respond to exposed credentials and proactively prevent evolving threats to employees and corporate data. Strengthen cyber resiliency and mitigate risk with seamless integrations into existing workflows to optimize incident response.

DEEPER, DARKER, BETTER – INSIGHTS FROM THE DARKEST LAYERS OF THE CRIMINAL UNDERGROUND

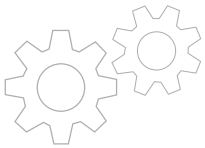


MONITOR & DETECT

Safeguard employees' digital identities with **continuous monitoring of compromised credentials** to protect corporate data

PROTECT & PREVENT

Reduce enterprise risk with **automated protection** against exposures to prevent costly cyberattacks



RESPOND & REMEDIATE

Optimize SOC efficacy to rapidly respond to exposures through **automated remediation**

SPYCLOUD ENTERPRISE PROTECTION

The right data, at the right time – to protect employee identities

MONITOR & DETECT

Safeguard employees' digital identities with **continuous monitoring of compromised credentials** to protect corporate data

- Detect, recover, and act on exposed credentials with the earliest data available, shutting down entry points for targeted cyber attacks and preventing account takeover.
- Remove blindspots in ransomware prevention with visibility into unauthorized access to business applications via malware-exfiltrated credentials and authentication cookies.
- Schedule scans of Active Directory credentials to detect compromised and weak passwords currently in use by active employees.

PREVENT & PROTECT

Reduce enterprise risk with **automated protection** to prevent costly targeted cyberattacks

- Reduce risk of data loss by resetting compromised passwords, invalidating stolen web sessions, and identifying password reuse.
- Optimize CapEx/OpEx and free up limited and valuable resources to focus on innovation and other high priority initiatives.
- Prevent criminals from bypassing authentication on trusted devices and moving laterally by remediating previously unknown malware infections.

"SpyCloud's data is more specific and actionable than any other solution we've found, giving us employee, account-level and source detail we need to mitigate the threat and take immediate action."

- Global Specialty Chemical Company

USE CASES

AUTOMATED ACCOUNT TAKEOVER PREVENTION

Proactively detect and reset compromised credentials as soon as SpyCloud publishes freshly recaptured breach and malware data. Plug into existing workflows and integrate with directory services and SOARs to prevent account takeover.

PROACTIVE RANSOMWARE PREVENTION

Monitor for active malware exfiltrated data in the hands of criminals. Shut down opportunities for follow-on attacks by resetting stolen credentials and expiring session cookies to fully remediate the exposed identity.

SPYCLOUD ENTERPRISE PROTECTION

Layer Cybercrime Analytics into & onto your existing tech stack

RESPOND & REMEDIATE

Rapidly respond to breach and malware exposures with **automated remediation**

- Streamline SOC workflows with SIEM/SOAR integrations to accelerate remediation of compromised credentials and malware-infected devices, users, and applications.
- Reduce alert fatigue with high-fidelity alerts that prioritize investigations to remediate threats and shorten the attack window.
- Optimize incident responses with an identity-centric approach to shutdown entry points and invalidate active sessions to reduce risk across all employee devices and applications.

EXTENSIBILITY YOUR WAY WITH OUT-OF-THE-BOX INTEGRATIONS

Leverage your existing tech stack to centralize recaptured dark web data and make informed, actionable decisions. SpyCloud integrates with top technology vendors across SIEM, SOAR, XDR, TIPs and more – delivering Cybercrime Analytics at scale.

splunk> Chronicle tines

Active Directory Microsoft Sentinel SECURE X

USE CASE

POST-INFECTION MALWARE REMEDIATION

Post-Infection Remediation is SpyCloud's crucial addition to malware infection response that prevents follow-on attacks. View all third-party applications exposed by malware, including shadow IT apps, to reset credentials and invalidate stolen session cookies.

"Because the solution is fully automated, we are able to process 14,000 unique credentials per month. This scalability allows us to use our resources efficiently.

We don't have to do any manual processing of public breaches anymore, which took a lot of time with the constant stream of new breaches. SpyCloud's amazing API allows us to automate the entire process."

– Niels Heijmans
Principal Security Intelligence Analyst
Atlassian

DEEPER, DARKER, BETTER INSIGHTS WITH SPYCLOUD

Shift away from shallow, directionless data with the power of the SpyCloud Cybercrime Analytics Engine. Here's how it works.

SPYCLOUD'S CYBERCRIME ANALYTICS ENGINE

COLLECT

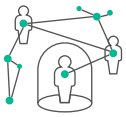
Continuous monitoring for compromised credentials identifies stolen and leaked assets very early in the attack timeline

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**.