ZINFINITY™

SOLUTION BRIEF

SpyCloud

Build your continuous **Zero Trust policy engine** with actionable cybercrime telemetry that meets your compliance requirements, mitigates risk, and optimizes resources and operational costs

CONTINUOUS ZERO TRUST

THE CHALLENGE

Common implementations of Zero Trust fail to include high-fidelity darknet telemetry in their policy engine. Without this critical input, organizations fall short at preventing cybercriminals from using compromised identity credentials to sidestep traditional safeguards like MFA and SSO using session hijacking. Protecting your digital perimeter brings challenges in maintaining continuous identity validation without straining security teams or expanding risk. As organizations look to advance their Zero Trust strategy, security leaders are shifting to a continuous authentication model – one that expands the scope to protect against the use of compromised account information and cookies to bypass Zero Trust Architecture Controls.

PASSWORD REUSE RATE

74% for users exposed in two or more breaches

RECAPTURED BREACH DATA

61% was malware-related

RECAPTURED COOKIES

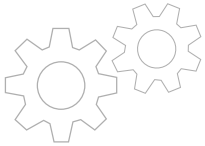
SpyCloud recaptured **20B+** in 2023, averaging **2,000+** per malware-infected device

SOLUTION OVERVIEW

As the Cybercrime Analytics leader, SpyCloud delivers a continuous Zero Trust solution that accelerates Zero Trust initiatives – with darknet telemetry and automated remediation for always-on authentication. SpyCloud streamlines your security operations by feeding definitive evidence of compromise into your policy engine for actionable insights that optimize access and protect against evolving identity threats. With SpyCloud, security teams confidently adapt and strengthen cyber resiliency, with seamless integrations into existing workflows to augment incident response.

MEET COMPLIANCE REQUIREMENTS

Enable adherence to regulatory and compliance requirements to maintain business productivity



OPTIMIZE CAPEX/OPEX

Free up resources by preventing targeted cyberattacks without adding headcount or overburdening resources

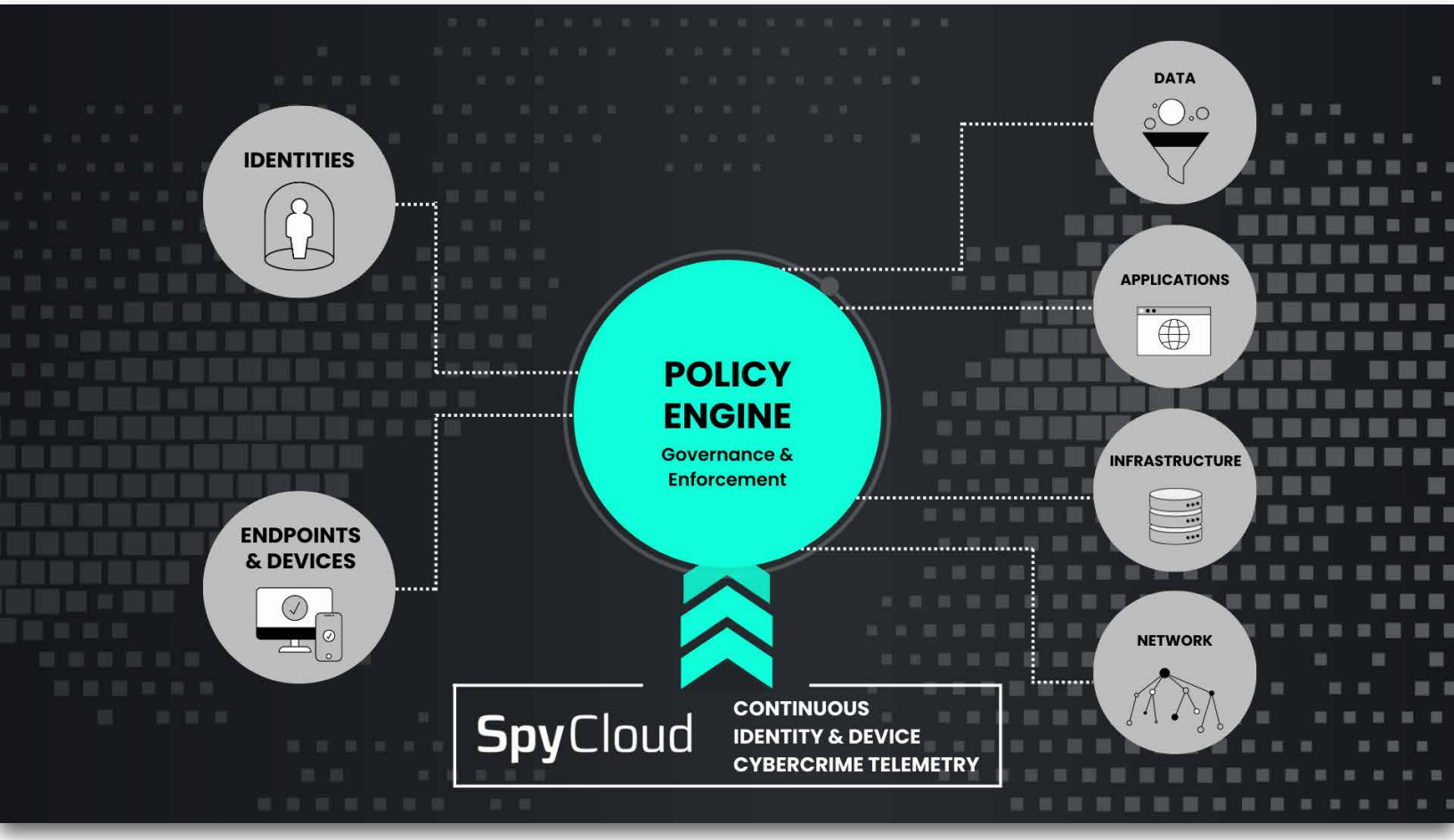
MITIGATE RISK

Automate protection from employee identity exposures to prevent costly cyberattacks

PREVENT NEXT-GEN THREATS

ENHANCE YOUR ZERO TRUST POLICY ENGINE WITH SPYCLOUD DARKNET TELEMETRY

SpyCloud's darknet telemetry offers a more comprehensive and enriched data set – cleansed, analyzed, and correlated for rapid delivery to enable teams to confidently optimize policy engines for always-on Zero Trust.



Continuous Identity Exposure Monitoring

EARLY DETECTION AND ACTION | Act on recently exposed credentials to shut down entry points and prevent targeted account takeover

REMOVE EXPOSURE BLINDSPOTS | Expand visibility into malware-infected employees to uncover unauthorized access across business applications, credentials, and stolen session cookies

CONVERT DARKNET DATA TO DEFENSE | Base your response on actionable insights with prompt action on exact-match compromised passwords and identities, with contextual information into the breach source

REAL-TIME POLICY UPDATES | Continuously refresh your policy engine with the latest exposure data, ensuring dynamic and effective threat response

Always-On Access Authentication

- **ENHANCED SESSION VISIBILITY |** Broaden security oversight beyond devices and applications, focusing on compromised user sessions to safeguard identities at their most vulnerable points
- **PREVENT LATERAL MOVEMENT |** Block cybercriminals from exploiting trusted devices by remediating the hidden scope of malware infections, including compromised third-party cloud applications
- **SECURE USER SESSIONS |** Defend against criminals exploiting authenticated sessions, bypassing MFA and passkeys to take over employee accounts, and stop targeted attacks where criminals impersonate employees to access sensitive information and escalate privileges
- **DAILY IDENTITY CHECKS |** Automatically scan directory services to identify compromised or weak credentials among active employees, flagging or resetting risky accounts

Automated Exposure Remediation

- **REDUCE ALERT FATIGUE |** High-fidelity alerts that prioritize investigations to remediate compromised credentials and shorten the attack window
- **DECREASE MEAN-TIME-TO-REMEDIATION (MTTR) |** Dynamic data enrichment for unparalleled insights into potential threats for a comprehensive understanding of identity exposures
- **STREAMLINE OPERATIONAL WORKFLOWS |** SIEM/SOAR integrations take quick action on compromised credentials from third-party breaches and malware infections to adjust policies accordingly
- **OPTIMIZE INCIDENT RESPONSE |** Take an identity-centric approach to shut down entry points and invalidate active sessions to reduce risk across all employee devices and applications

STREAMLINE REGULATORY COMPLIANCE

Actionable and relevant darknet telemetry is critical to your risk management frameworks

- **800-207 ZERO TRUST ARCHITECTURE |** Telemetry to enhance identity governance and trust algorithm
- **NIST CSF 2.0 |** Darknet intelligence for threats and potential likelihoods
- **NIST 800-053 |** Includes continuous monitoring and threat awareness
- **CIS TOP CONTROLS V8 |** Actionable data to restrict unathorized access and remediate malware-affected applications

SCALE ENTERPRISE EXTENSIBILITY

INTEGRATE HIGH-FIDELITY CYBERCRIME DATA INTO EXISTING WORKFLOWS

SpyCloud integrates with top vendors across SIEM, SOAR, XDR, TIPs and more – delivering darknet analytics at scale to inform decisions and navigate all known records of identity exposures.

SPYCLOUD CUSTOMER EXPERIENCE

SpyCloud

PAYBACK PERIOD

3.5

MONTHS

AVERAGE PAYBACK PERIOD FOR SPYCLOUD CUSTOMERS

lendingtree

TIME SAVINGS

UP TO

60%

TIME AND RESOURCES SAVED FOR LENDINGTREE'S SOC TEAM

ATLASSIAN

IDENTITY PROTECTION

7,000

EMPLOYEES

PROTECTED FROM IDENTITY-BASED ATTACKS AT ATLASSIAN

ZINFINITY

WHY SPYCLOUD

FASTER ACCESS TO CYBERCRIME TELEMETRY	SpyCloud continuously monitors for compromised credentials and identity exposures to analyze and publish faster than traditional threat intel, delivering evidence of compromise closest to the crime.
ACTION-DRIVEN ALERTS	Alerts you want more of to save time on tedious discovery and correlation, based only on exposed credentials that truly pose risk.
AUTOMATED WORKFLOWS & DATA ENRICHMENT	Free up resources and reduce the need for interpreting data to defend against identity-based threats with integrations across top vendors to decrease MTTR and deliver unparalleled insights.
LAYERED INTELLIGENCE	Layer SpyCloud's cybercrime telemetry into your existing tech stack and policy engine for improved efficacy and protection against next-gen attacks that bypass Zero Trust for a coordinated response across Identity + IT + Security teams.
DEDICATED CUSTOMER SUPPORT	SpyCloud technical and customer success account managers work with you for a smooth onboarding process to align on your desired outcomes, providing ongoing support to maximize your investment.

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, successful phishes, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include more than half of the Fortune 10, along with hundreds of global enterprises, mid-sized 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**