

SESSION IDENTITY PROTECTION

PREVENT AUTHENTICATION BYPASS & STOP SESSION HIJACKING
BY SAFEGUARDING YOUR USERS' DIGITAL IDENTITIES

THE CHALLENGE

Cybercriminals increasingly use malware to steal high-value authentication data – especially active session cookies that allow them to impersonate legitimate users. Modern malware executes fast, evades detection, and often deletes itself, leaving organizations unaware that an account has already been compromised.

With a stolen session cookie, attackers can bypass every form of authentication – passwords, MFA, passkeys, even SSO – gaining frictionless access to consumer accounts, employee systems, and sensitive resources. This form of account takeover, session hijacking, turns traditional identity security ineffective: once a session is active, attackers simply walk in.

PRODUCT OVERVIEW

SpyCloud Session Identity Protection enables organizations to proactively safeguard both employees and consumers from next-generation account takeover by identifying malware-infected users with exposed authentication data. With early visibility into compromised sessions, security teams can quickly intervene to invalidate active sessions and lock criminals out before damage occurs.

SpyCloud's researchers continuously recapture malware logs from the criminal underground. From this data, we extract and enrich compromised cookies tied to your applications, providing the context needed to pinpoint affected users and impacted systems. Results are delivered via our high-volume REST API, enabling rapid action against your highest-risk accounts.

WITH SPYCLOUD SESSION IDENTITY PROTECTION, ORGANIZATIONS CAN:

- ▶ Stop targeted account takeover attacks by invalidating active sessions before criminals can exploit them.
- ▶ Prevent authentication bypass by detecting valid authentication cookies attackers can weaponize.
- ▶ Identify malware-infected users – employees or consumers – to protect accounts, advise users, and reduce fraud or lateral movement.
- ▶ Flag high-risk identities and devices for enhanced scrutiny of future logins or access attempts.

BENEFITS AT A GLANCE

Prevent Authentication Bypass

Block adversaries attempting to hijack active sessions to impersonate users, escalate privileges, commit fraud, or access sensitive systems

Lock Out Bad Actors

Receive alerts when web sessions tied to your domains appear in recaptured malware logs, enabling you to log users out, expire sessions, and shut down unauthorized access pathways

Scalable Remediation Options

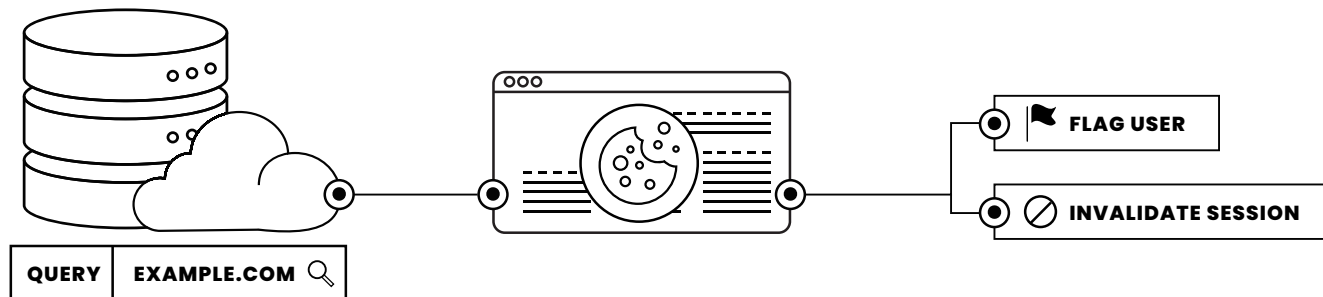
Choose how to intervene based on risk tolerance – invalidate compromised cookies, flag accounts, require reauthentication, or force a password reset

Protect Across Your Entire Ecosystem

Safeguard your customers, employees, vendors, and third-party users – even when they authenticate from unmanaged or personal devices where malware risk is highest

HOW IT WORKS

When you query the Session Identity Protection API, SpyCloud returns compromised cookie data associated with your domains, including the information you need to identify exposed employee and consumer accounts and determine how to intervene.



1. QUERY THE SPYCLOUD SESSION IDENTITY PROTECTION API

Send requests for domains relevant to your consumer applications, workforce systems, SSO brokers, portals, or any authenticated surface.

Query options include:

- ▶ Cookie Domain (required)
- ▶ Cookie Name
- ▶ Cookie Expiration Date
- ▶ Source ID
- ▶ SpyCloud Publish Date

2. RECEIVE ENRICHED COMPROMISED COOKIE DATA

SpyCloud returns detailed intelligence on compromised cookies tied to your domain,

including:

- ▶ Severity
- ▶ Source ID
- ▶ Cookie Domain & Subdomain
- ▶ Cookie Name & Value
- ▶ Cookie Expiration
- ▶ SpyCloud Publish Date
- ▶ Infected Time
- ▶ Infected Machine ID
- ▶ IP Addresses
- ▶ User Hostname
- ▶ User System Registered Owner

With this context, teams can identify affected users, determine session risk, and trace potential infection sources.

3. INTERVENE BASED ON RISK

Choose how and when to act:

- ▶ Invalidate compromised cookies
- ▶ Force users to reauthenticate
- ▶ Apply step-up verification
- ▶ Reset passwords where appropriate
- ▶ Deactivate or investigate SSO sessions (depending on provider capabilities, e.g., Okta session lookup)

Whether protecting a consumer account from fraud or preventing lateral movement from a compromised employee identity, the goal is the same: close the door before attackers walk through it.

KEY CAPABILITIES

TIMELY IDENTITY THREAT ALERTS

Detect compromised, active sessions quickly – reducing the attacker’s window of opportunity.

CONTEXTUAL RISK INSIGHTS

Understand severity, privilege level, and exposure across every authentication surface you own.

ENRICHED DATA, READY FOR ACTION

SpyCloud provides context around the compromised cookie and infected system to support rapid, targeted remediation.

FLEXIBLE API INTEGRATION

A high-volume, REST-based API that fits into your existing workflows, SIEM/SOAR integrations, fraud systems, or IAM stack.

PROTECT VENDORS AND SUPPLY CHAIN

Extend protection to vendors, contractors, and partners – even those using personal or unmanaged devices to access your ecosystem.

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