DATASHEET

SpyCloud

SESSION IDENTITY PROTECTION FOR EMPLOYEES

PREVENT AUTHENTICATION BYPASS & STOP SESSION HIJACKING

BY SAFEGUARDING YOUR EMPLOYEES' HOLISTIC DIGITAL IDENTITIES

THE CHALLENGE

Employees' identities continue to be compromised at a staggering rate, and cybercriminals are leveraging automation to exploit exposed identity data for follow-on attacks. Traditionally, security teams visibility has focused only on breach-exposed credentials, but malware-siphoned session cookies allow a shortcut to bypass all forms of authentication using an advanced method of ATO. Once a criminal has their hands on active session cookies, they can bypass SSO on trusted devices, gaining unrestricted lateral access across the network.

PRODUCT OVERVIEW

SpyCloud Session Identity Protection delivers early detection of malware-infected compromised employees, well before their credentials or session cookies have been used to hijack active sessions. By checking your domain against SpyCloud's continuously-updated database of recaptured identity data, security teams can verify when exposed authentication cookies are in the hands of criminals.

Security teams can use Session Identity Protection to rapidly remediate identity threats, preventing criminals from using stolen browser fingerprints to impersonate employees and gain unauthorized access. SpyCloud normalizes and enriches compromised cookies relevant to your domains, publishing contextual details to pinpoint exposed identities and affected systems. Delivered via a high-volume, REST-based API, SpyCloud Session Identity Protection prevents next-gen ATO caused by session hijacking.

USING RECAPTURED IDENTITY DATA FROM SPYCLOUD, ORGANIZATIONS CAN:

- **Invalidate active sessions** identified by a compromised cookie, to prevent session hijacking and MFA bypass, keeping the employee identity safe - even unauthorized SSO access from any infected personal device.
- **Flag vulnerable accounts** with known compromised identities for increased scrutiny of future logins/access - even if the session has already expired.

BENEFITS AT A GLANCE

Prevent Authentication Bypass
Defend against criminals exploiting active, authenticated sessions - bypassing credentials, MFA and passkeys, to take over employee accounts, and stop targeted attacks where cybercriminals impersonate employees to access sensitive information and escalate privileges

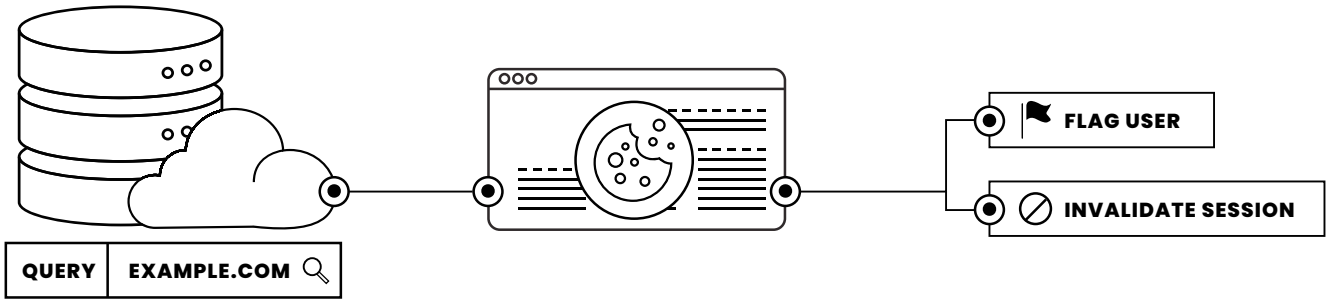
Lock Out Bad Actors
Receive alerts when an employee's active web session is compromised to log them out, expire the session, and shut down entry points for criminals

Scalable Remediation Options
Choose how to intervene to protect exposed employees by invalidating the compromised cookies or flagging known compromised accounts faster

SpyCloud

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 accounts and determine how to intervene.



1. QUERY SPYCLOUD API

Query the Session Identity Protection API for your target domains of interest, such as mycompany.com, app.mycompany.com, or mycompany.okta.com.

Query options include:

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

2. QUERY SPYCLOUD API

SpyCloud returns compromised cookie data associated with your domain, including the information you need to identify which accounts are vulnerable.

Results include:

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

3. QUERY SPYCLOUD API

Choose how and when to intervene to protect these accounts. For example, you can invalidate the compromised cookies, expire the session and log the user out, and even force a password reset, depending on the amount of risk perceived and friction that's tolerable for your organization.

For cookies from third-party sites such as SSO providers, response options may vary by provider. Some identity brokers like Okta, provide the ability for admins to look up and deactivate specific sessions.

SpyCloud

KEY CAPABILITIES

TIMELY ALERTS
Receive actionable alerts when compromised cookies tied to your domains appear in the darknet, stopping active threats to your employee identities

ENRICHED DATA, READY FOR ACTION
Compromised cookies are enriched with contextual information to identify the extent of the domain exposure and aid remediation efforts

PROTECT VENDORS AND SUPPLY CHAIN
Prevent unauthorized access stemming from malware-infected vendors and supply-chains, even those using personal devices

TAKE ACTION TO REMEDIATE
Chose how to remediate by invalidating compromised cookies, expiring sessions, forcing logouts, or resetting passwords to stop unauthorized access

CONTEXTUAL INFORMATION
Determine the severity of risks and privilege level with Cookie Domain, Subdomain, Name, Value, and Expiration values

FLEXIBLE API
Integrate SpyCloud's high-volume, REST-based API into your preferred tech stack with simple configuration that match your organization's needs

ABOUT SPYCLOUD

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

SPYCLOUD SESSION IDENTITY PROTECTION FOR EMPLOYEES