

# SESSION IDENTITY PROTECTION FOR EMPLOYEES

PREVENT AUTHENTICATION BYPASS & STOP SESSION HIJACKING BY SECURING YOUR EMPLOYEE IDENTITIES

## THE CHALLENGE

Employee accounts continue to be compromised at a staggering rate by cybercriminals. Malware-siphoned cookies allow bad actors to bypass all forms of authentication and hijack employee accounts using an advanced method of account takeover. Once a threat actor has stolen active session cookies, they often bypass SSO on trusted devices, with lateral access across the network.

## PRODUCT OVERVIEW

**SpyCloud Session Identity Protection for Employees** provides early warning for employees who are victims of malware infections, sometimes well before their credentials or cookies have been used to hijack active sessions. By checking your domain against SpyCloud's continuously-updated feed of compromised session cookies and recaptured malware logs, security teams can detect when employee's authentication cookies are stolen and in the hands of criminals.

Security teams can intervene to rapidly remediate before criminals leverage stolen browser fingerprints to access their accounts and traverse the enterprise network. Powered by SpyCloud's Cybercrime Analytics - compromised cookies relevant to your domains are parsed, enriched with contextual information to help you identify the affected system for remediation, and delivered via our high-volume, REST-based API.

Using recaptured data from SpyCloud, enterprises can:

— **Invalidate active sessions** identified by a compromised cookie, to prevent session hijacking and MFA bypass, keeping the account safe - even when employees log into your corporate SSO provider from an infected personal device.

— **Flag vulnerable accounts** with known compromised devices 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 already-authenticated sessions – bypassing credentials, MFA and passkeys, to take over employee accounts, and stop targeted attacks where criminals impersonate employees to access sensitive information and escalate privileges

#### Lock Out Bad Actors

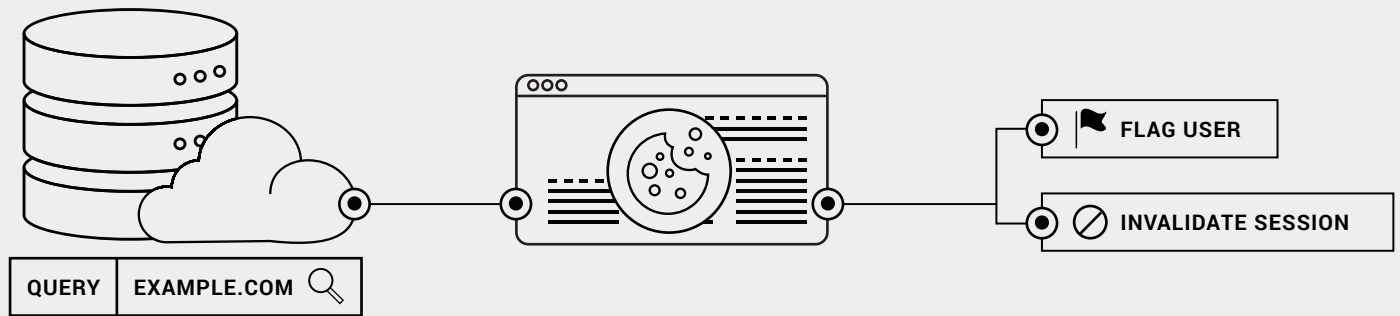
Receive alerts when an employee's active web session is compromised to log them out, expire the session, and level the playing field with criminals

#### Scalable Remediation Options

Choose how to intervene to protect exposed employees by invalidating the compromised cookies or flagging accounts with known compromised devices and applications

## 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 which accounts are vulnerable and determine how to intervene.



### QUERY SPYCLOUD API

1. 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

### RECEIVE RESULTS

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

#### Results include:

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







### CHOOSE INTERVENTION

3. 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.

## KEY CAPABILITIES

---

-  **TIMELY ALERTS**  
Receive actionable alerts when compromised cookies appear in the darkweb to stop active threats to your employees
-  **ENRICHED DATA, READY FOR ACTION**  
Compromised cookies relevant to your domains are enriched with information to help identify the affected system or user for remediation
-  **SECURE THIRD-PARTY WORKFORCE SERVICES**  
Prevent unauthorized access when cookies from critical workforce services are stolen from infected personal or managed devices
-  **SCALABLE REMEDIATION OPTIONS**  
Choose how and when to intervene by invalidating the compromised cookies or flagging user accounts with known compromised devices
-  **CONTEXTUAL INFORMATION**  
Determine the severity and privilege level with cookie domain, subdomain, name, value, and expiration values
-  **FLEXIBLE API**  
High-volume API with simple configuration helps to integrate with your preferred tech stack

## 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](https://spycloud.com).