

SpyCloud

# SpyCloud CONNECT

CUSTOM-BUILT WORKFLOWS FOR SEAMLESS AUTOMATION  
ACROSS YOUR PREFERRED SECURITY TOOLS

## THE PROBLEM

Enterprises depend on a variety of tools across diverse teams to operate and protect their companies. While use cases may be similar, each enterprise is unique in how they choose to work and the tech stack they prefer to get their work done efficiently and effectively. The key to scaling and maximizing efficiency depends on automating those workflows to help increase not only response times, but also offload manual workloads to save time and resources. Security teams may struggle to prioritize development resources for automation efforts and to have complete confidence in their data sources to allow for any automation.

## THE SOLUTION

With SpyCloud, you don't have to choose between quality data and automating your operations. SpyCloud Connect is a hosted custom automation solution that allows SpyCloud products to be seamlessly integrated with a wide variety of security tools and processes – enabling rapid remediation and scalable automation of compromised identities within a customer's preferred tech stack.

Whatever you want, wherever you want it – SpyCloud Connect builds out the workflows for your desired integrations to send SpyCloud data where and when you need it, all in the tools you are using today without needing to burden your existing resources with custom development work.



### BENEFITS AT A GLANCE

#### Custom Workflows

Define your preferred logic for ingesting and remediating identity exposures

#### Development Free

Alleviate your team's resources by having SpyCloud set up native connectors and build your desired custom workflows for you

#### Zero Maintenance

SpyCloud maintains and supports the custom workflow(s), giving you time to focus on what matters most

#### Any Data, Anywhere

Automate with confidence using the tools your teams already have in their stack – with endless possibilities to help you optimize and scale your operations

## YOU

CHOOSE YOUR  
DESIRED WORKFLOWS  
AND INTEGRATION  
DESTINATIONS

## SPYCLOUD



**BUILDS IT**

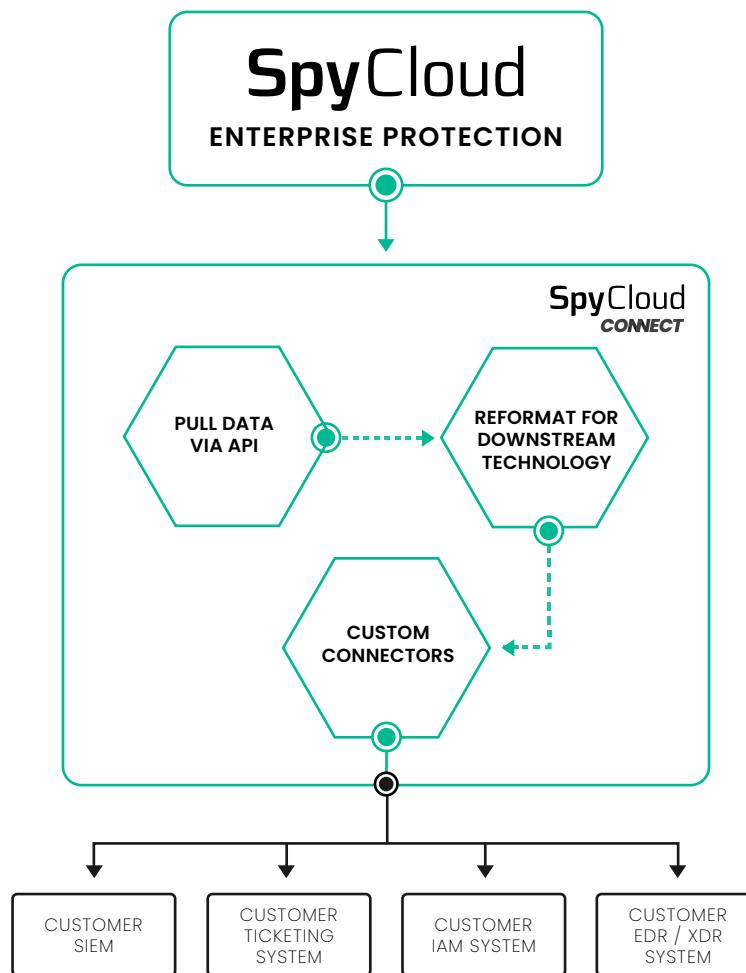


**MAINTAINS IT**



**SUPPORTS IT**

## HOW IT WORKS



### CHOOSE YOUR DESIRED WORKFLOW

Customers can specify desired custom workflows and integrate SpyCloud for a variety of use cases with any combination of their preferred tools – including SIEMs, SOARs, Ticketing Systems, Threat Intelligence Platforms (TIPs), Endpoint Detection & Response (EDR), XDR Platforms, Identity Providers, and more.

## WHAT'S INCLUDED

### THE SERVICE

- The SpyCloud Connect solution is inclusive of the development, support, and maintenance of the custom workflows – tailored to meet unique needs across diverse teams.
- The SpyCloud Connect SKU includes the build of a custom workflow with up to 3 integration destinations.
- Downstream data can be customized to:
  - ▶ Adhere to principle of least privilege (PoLP) and limit access to sensitive information for internal teams that don't require visibility into that data
  - ▶ Add descriptive elements to data returns
- All SpyCloud Connect custom workflows are dynamic and will automatically update as our data lake and ingestion grows in real-time.

### ADDITIONAL CUSTOMIZATION OR EDITS

- If further customization is required, as in the case of specific data transformations, SpyCloud can create those using the low-code SpyCloud Connect solution.
- If you change technology providers within your custom workflow at any point, we will swap the integration destination at no additional cost.

## DELIVERY CYCLE

- SLA for custom automation workflow delivery is 90 days.
  - ▶ However, typical delivery cycles for SpyCloud Connect deployments are 2-4 weeks, done in tandem with customer onboarding.

## COMPATIBLE PRODUCTS

### ► COMPASS MALWARE EXPOSURE REMEDIATION

React to malware-compromised devices, users, and applications

**LEARN MORE ►**

### ► EMPLOYEE ATO PREVENTION

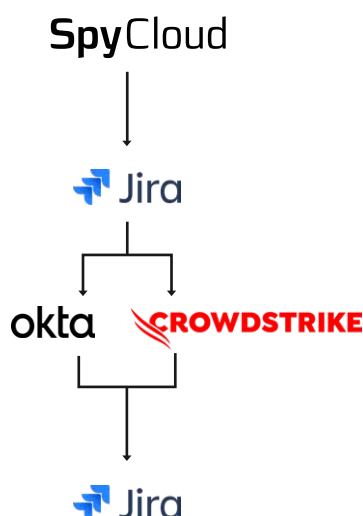
Stop targeted and automated account takeover

**LEARN MORE ►**

## CUSTOMER FAVORITE WORKFLOWS

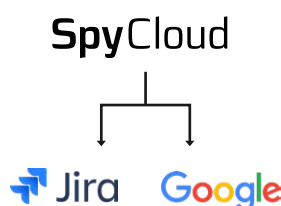
**1**

Receive exposed password alerts from SpyCloud and re-secure the accounts



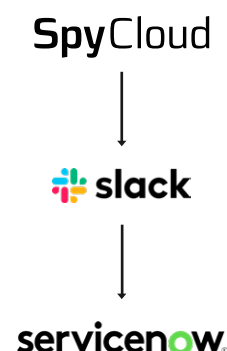
**2**

Disable Google accounts based on SpyCloud exposure data



**3**

Create ticket for malware-infected user and send alert to on-duty team in slack



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