

# ENTERPRISE PROTECTION FOR MICROSOFT SENTINEL

ACCELERATE INCIDENT RESPONSE TIME TO SAFEGUARD EMPLOYEE IDENTITIES

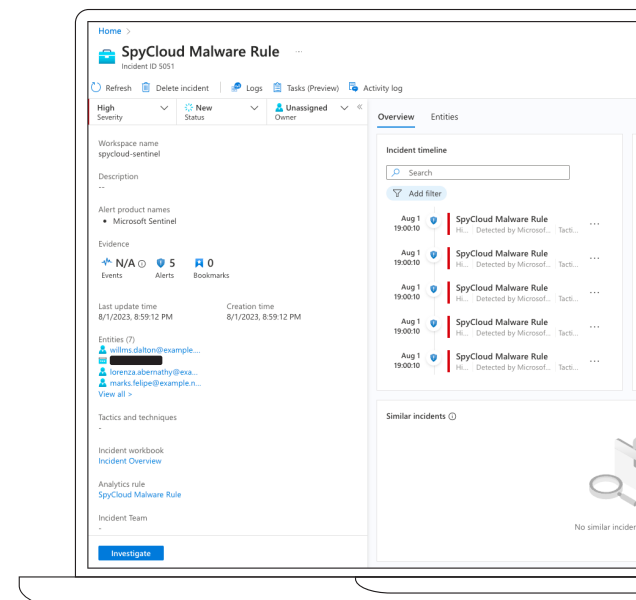
**SpyCloud Enterprise Protection for Microsoft Sentinel** helps security teams triage and remediate identity-related exposure incidents – shutting down threats to prevent targeted account takeover and cyberattacks. SpyCloud publishes exposed employee credentials from billions of recovered breach, malware and phished data records before they even hit the dark web – decreasing the exposure window and allowing for rapid action against compromised identities while disrupting cybercrime.

With SpyCloud Enterprise Protection for Microsoft Sentinel, breach and malware data from SpyCloud is ingested into Sentinel to create incidents and automate remediation. Security teams can take advantage of built-in incident response playbooks, or create their own automated steps for responding to breached credentials and malware and phishing exposures – calling SpyCloud's API directly to gather enriched data for specific incidents.

## DECREASE MTTR WITH RECAPTURED DARKNET DATA, READY FOR ACTION

Automate and analyze recaptured darknet data into your workflows:

- Query SpyCloud's complete set of recaptured breach or malware and phishing records for enriched details
- Automatically create high-priority incidents for new breach, malware or phishing records, correlated with employee identities
- Perform comprehensive analysis at scale on normalized, recaptured data to investigate and identify trends
- Expand visibility of malware exposures into all possible business applications
- Streamline SOC workflows with SIEM/SOAR integrations to accelerate remediation of compromised credentials and malware-infected devices, users, and applications
- Reduce alert fatigue with high-fidelity alerts that prioritize investigations to remediate threats and shorten the attack window



## HOW IT WORKS

---

Microsoft Sentinel performs a daily ingest of the freshest, high quality darknet data published from SpyCloud – curated breach, malware-exfiltrated data, and successfully phished data that is clean, normalized, and free of irrelevant information and duplicates. This includes the data source, description and plaintext passwords which is then saved into a custom table in Sentinel. Teams can use Sentinel's SIEM capabilities for full analysis or run the included response playbooks.

### INCIDENT REMEDIATION

SpyCloud's Analytic Rules in Sentinel generate high priority incidents when certain criteria are met for new records.

- ▶ **BREACHES:** In the event of a breach where a plaintext password was exposed, SpyCloud creates and flags the event as a high priority incident in Sentinel. SpyCloud offers several automation steps available through a built-in playbook to streamline the incident response process for credentials exposed in data breaches.
- ▶ **MALWARE:** For infostealer malware exposures, SpyCloud removes all blindspots across users, applications, and devices that would normally hinder post-infection remediation. All records associated with a specific malware infection are combined into a single high priority incident, grouped for analysis. Additional malware records outside the primary enterprise watchlist can be brought in to gain visibility across all exposed applications and devices.

## UNLOCK ADDITIONAL ACTION USING SPYCLOUD'S PLAYBOOKS

---

Additional ways to remediate:

### BREACHED CREDENTIALS

- Check if the employee is still active or if the breached password length meets your requirements; if not, close the incident
- Check against your IAM tool to determine if the exposed password is in use on key applications
- Automate a password reset trigger if the password is in use

### MALWARE INFECTIONS

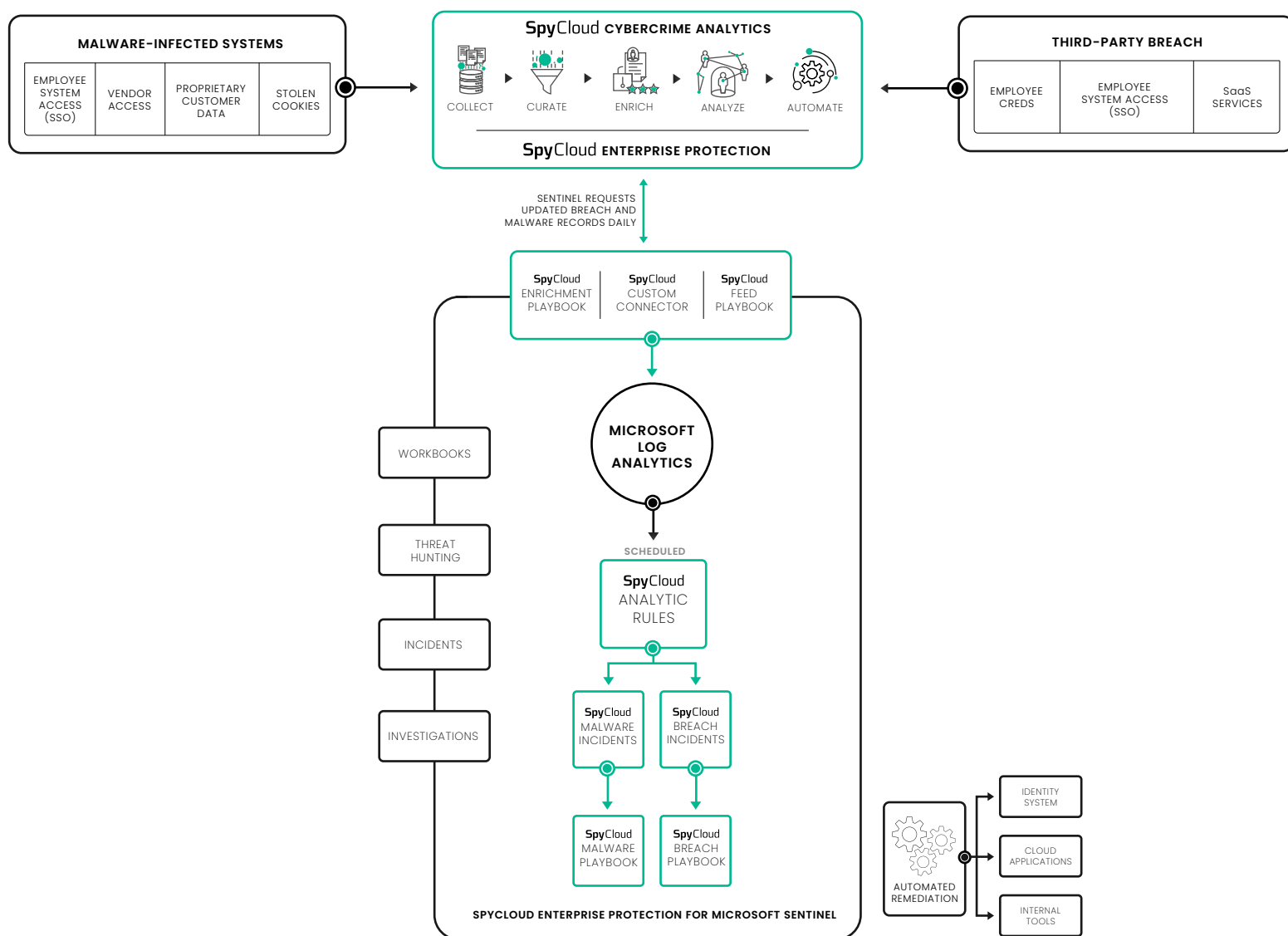
- Decide the appropriate response based on whether the infection is related to a managed device or a personal/unmanaged device accessing work applications
- Ingest additional malware records for a specific incident to better understand the extent of the exposure

## DEEP DIVE INVESTIGATIONS

Enhance your incident response by querying SpyCloud's API to pull additional context to build out further automation. Search the entire SpyCloud database by domain, email, IP, username, or passwords to pull entire user records of recaptured darknet data. Or search for specific applications or subdomains to identify any exposed credentials to enrich your **Post-Infection Remediation**.

## SPYCLOUD ENTERPRISE PROTECTION FOR MICROSOFT SENTINEL

Reference Diagram



Streamline SOC workflows using SpyCloud's complete integration with Microsoft Sentinel for rapid response, incident analysis, threat hunting, and automation.

## TECHNICAL REQUIREMENTS

---

- » **SpyCloud Enterprise Protection for Microsoft Sentinel** requires a Microsoft Power Apps or Power Automate plan with custom connector feature, along with an active Azure subscription.
- » Analyzing SpyCloud breach, malware and phishing data requires a license for SpyCloud Employee ATO Prevention, and an additional SpyCloud Compass license is required to ingest malware records for applications outside the primary enterprise watchlist.

## 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).

