INTEGRATION DATASHEET

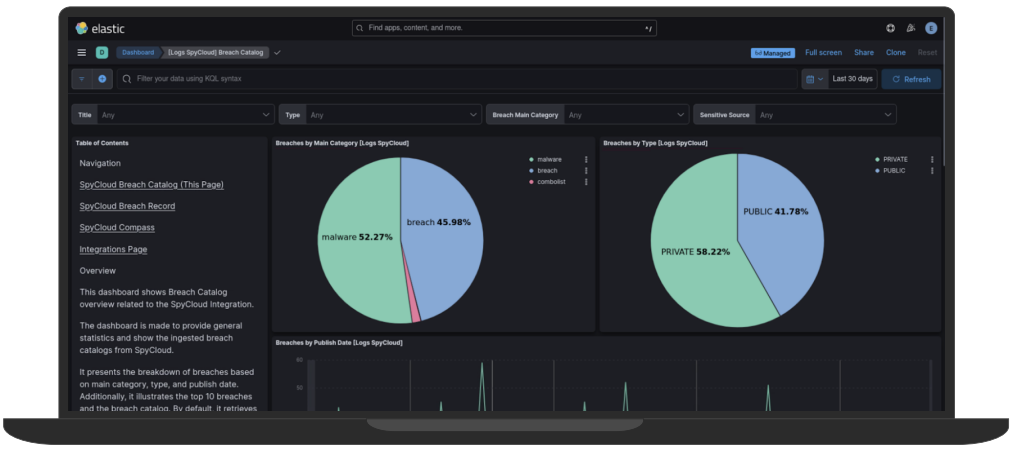
SpyCloud

ENTERPRISE PROTECTION FOR elastic

MAXIMIZE EXPOSURE VISIBILITY AND RESPONSE WITH SPYCLOUD + ELASTIC

PRODUCT OVERVIEW

The SpyCloud Enterprise Protection for Elastic Integration enables organizations to seamlessly incorporate SpyCloud's extensive breach and malware records into their Elastic SIEM environment. This integration empowers enterprises to enhance their security operations by utilizing existing security tools for alerting and automated analysis, driving efficiency and improving identity exposure remediation.



Visualize SpyCloud's recaptured data within Elastic's security environment

BENEFITS AT A GLANCE

NATIVE INTEGRATION
Directly integrate SpyCloud breach and malware data into Elastic Security

ENHANCED SECURITY POSTURE
Leverage comprehensive breach intelligence for improved employee exposure detection and response

OPERATIONAL EFFICIENCY
Utilize Elastic capabilities for alerting and analysis, responding to SpyCloud records directly and pushing to your SOAR

CUSTOMIZABLE DASHBOARDS
Gain insights with high-level dashboard statistics confirming data ingestion and showcasing data

HOW IT WORKS

SpyCloud Enterprise Protection for Elastic performs a daily ingest of the latest breach and malware-exfiltrated data published by SpyCloud. This cleaned, normalized data, free of noise and duplicates, is saved into Elastic. Customers can configure alerts and automated workflows to leverage SpyCloud's breach and malware records, all within your Elastic environment. This integration allows enriched data to be passed to SOAR platforms for automated incident response.

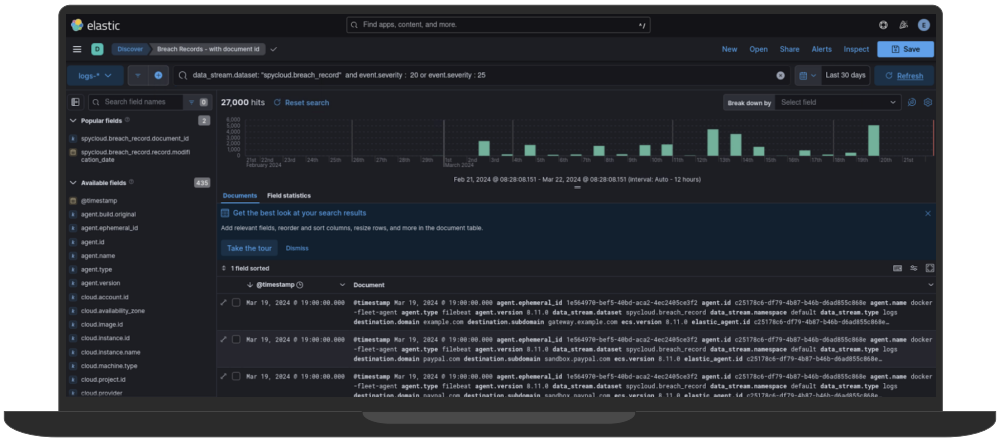
SpyCloud

KEY CAPABILITIES

COMPREHENSIVE DATA INGESTION | Pull breach and malware records from SpyCloud to identify breadth of exposed identities and unauthorized access to applications.

ADVANCED ALERTING | Configure alerts for breach records, malware detections, and infected assets directly within Elastic Security. Enable security teams to quickly identify and respond to threats.

DASHBOARDING AND VISUALIZATION | Access pre-configured dashboards to monitor data ingestion status and visualize breach and malware data and customize to highlight key metrics relevant to your organization.



Search within Elastic to find relevant SpyCloud breach and malware records

ALERTING ON BREACH RECORDS

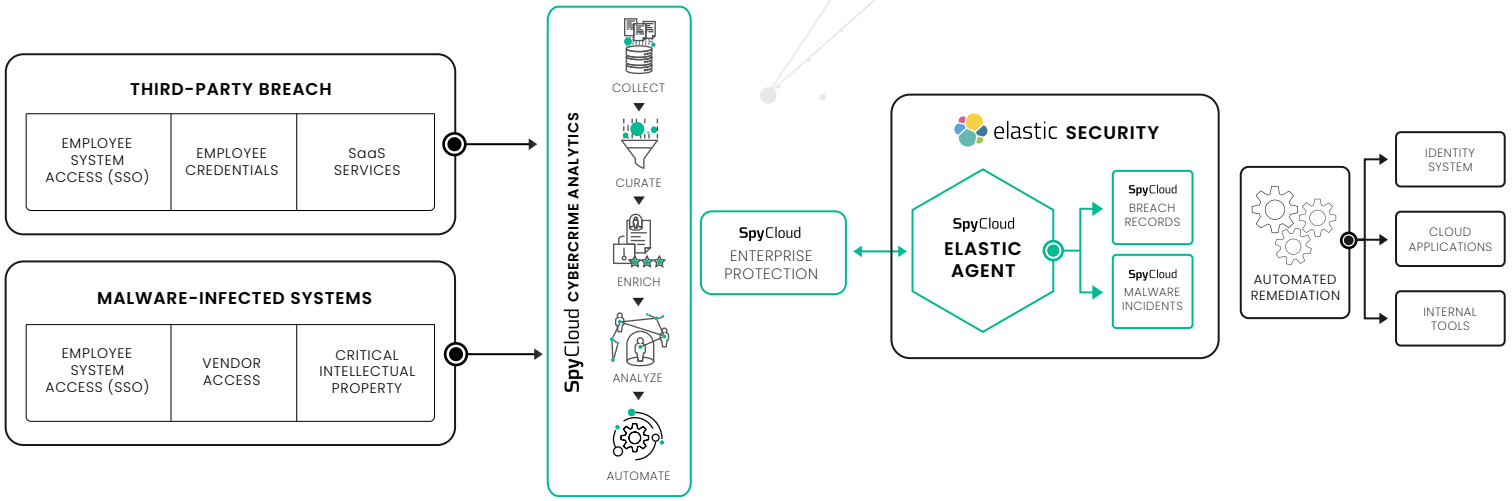
Alerting to SpyCloud breach records begins with the daily ingestion, which includes compromised credentials and high-value PII. This data is saved into custom indices within Elastic, enabling real-time detection of exposed credentials. When a breach record is identified, Elastic generates an alert, allowing security teams to proactively respond to prevent targeted account takeover.

RESPONDING TO MALWARE RECORDS

SpyCloud ingests malware records from infected devices to visualize the amount of exposed credentials to corporate applications, even those hosted outside your managed domain*. This data is integrated into custom indices within Elastic, enabling the identification and alerting of malware activity. When malware infections are detected, Elastic generates alerts that allow security teams to track and mitigate risks effectively. These alerts can be integrated with SOAR platforms, automating the response to detected threats.

**Requires SpyCloud Compass license*

SpyCloud



SpyCloud Enterprise Protection for Elastic streamlines your analysis and response for compromised credentials

TECHNICAL REQUIREMENTS

- SpyCloud Enterprise Protection for Elastic requires an active ELK License with an Elastic Agent installed
- Analyzing SpyCloud breach or malware data requires a **SpyCloud Employee ATO Prevention** license, 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 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 more than half of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 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**.