DATASHEET

SpyCloud

ENTRA ID GUARDIAN

AUTOMATE COMPROMISED PASSWORD REMEDIATION & PROTECT YOUR ENTERPRISE FROM ACCOUNT TAKEOVER

A criminal who gains access to your users' Entra ID credentials through a third-party breach, malware infection, or successful phishing attack can easily log into your corporate network – accessing business critical services, applications, and data. Protect your enterprise by taking swift action to automate remediation of exposed credentials.

PRODUCT OVERVIEW

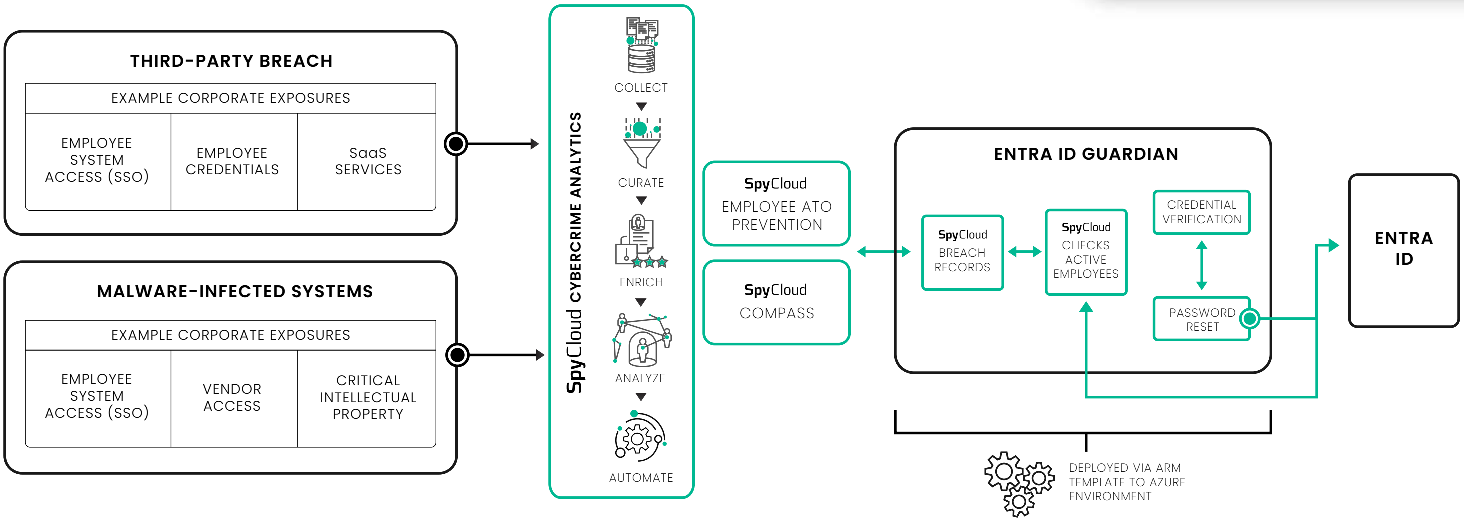
SpyCloud checks your users' Entra ID credentials against billions of recaptured darknet assets to see if any of your corporate logins are available to cybercriminals. With SpyCloud Entra ID Guardian, you can automatically reset exposed passwords – keeping your corporate assets secure. Entra ID Guardian makes it easy to identify reuse of compromised credentials, check for prior exposure, and mitigate new exposures to maintain account security.

BENEFITS AT A GLANCE

Stay Ahead of Criminals ▪
With proactive monitoring of Entra ID for exposed employee credentials

Reduce Your Team's Workload ▪
With automated detection and remediation of exposed passwords

Lock Out Bad Actors ▪
By making sure your assets are protected from passwords that criminals have stolen from breaches, malware infections, and successful phishes


THIRD-PARTY BREACH
EXAMPLE CORPORATE EXPOSURES
EMPLOYEE SYSTEM ACCESS (SSO)
EMPLOYEE CREDENTIALS
SaaS SERVICES
MALWARE-INFECTED SYSTEMS
EXAMPLE CORPORATE EXPOSURES
EMPLOYEE SYSTEM ACCESS (SSO)
VENDOR ACCESS
CRITICAL INTELLECTUAL PROPERTY
SpyCloud CYBERCRIME ANALYTICS
COLLECT
CURATE
ENRICH
ANALYZE
AUTOMATE
SpyCloud EMPLOYEE ATO PREVENTION
SpyCloud COMPASS
ENTRA ID GUARDIAN
SpyCloud BREACH RECORDS
SpyCloud CHECKS ACTIVE EMPLOYEES
CREDENTIAL VERIFICATION
PASSWORD RESET
ENTRA ID
DEPLOYED VIA ARM TEMPLATE TO AZURE ENVIRONMENT

HOW IT WORKS

THE SET UP

- Entra ID Guardian will be deployed via an ARM Template into a customer's Azure environment.
- Entra ID Guardian will be configured through specifying a SpyCloud Enterprise API Key, connection details for Entra ID connectivity and SMTP connectivity.
- Users of Entra ID Guardian will need to have specific roles granted in order to login and view the application. Entra ID Guardian will scan Entra ID accounts for password exposures using newly released breach and malware data as it's made available.

DELIVERY

The Entra ID Guardian will be deployed through an ARM Template as an Azure Container Instance (ACI.) The deployment as an ACI will allow customers to deploy without requiring a VM or server to be provisioned, simplifying the deployment and upgrade over the lifetime of the product.

SUPPORTED CAPABILITIES

COMPLETE CREDENTIAL SCANNING

- Scan all accounts in Entra ID to detect whether the account is active, and if active, testing any credentials for compromise that are available within SpyCloud
- Support for exact password match scanning only

SCANNING STATISTICS REPORTING

- A dashboard screen providing summary scanning statistics reporting for the last 24 hours, last 7 days, or last 30 days for:
  - **Accounts Scanned**: The number of accounts scanned, whether there is a match or not
  - **Passwords Checked**: The number of passwords checked for all scanned accounts
  - **Passwords Matched**: The number of matched accounts
  - **Passwords Reset**: The number of password reset operations performed
  - **Emails Sent**: The number of emails sent to end users, excluding administrators

REMEDIATION OPTIONS

- Adjust User Risk *(choose High, Medium, Low)*
- Password Reset
- Log Password Match
  - Account name / email
  - Source ID
  - Breach or malware title
  - Partial password (masked)
- Email to User via Default Template
- Email to Administrator via Canned Email
- Delayed Password Reset Option
  - Notify the user via email and then reset the password within a specified number of hours

TECHNICAL REQUIREMENTS

- Azure Environment
- Office 365 License or equivalent SMTP based email support
- Entra ID License
- SpyCloud Enterprise License with API Key (configured without IP Allow Listing)

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 more than half 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**.