DATASHEET

SpyCloud

OKTA WORKFORCE GUARDIAN

AUTOMATE COMPROMISED PASSWORD REMEDIATION & PROTECT YOUR ENTERPRISE FROM ACCOUNT TAKEOVER

A criminal who gains access to your users' Okta Workforce 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. Secure your enterprise with automated remediation of exposed Okta Workforce credentials and prevent account takeover and MFA overloading.

BENEFITS AT A GLANCE

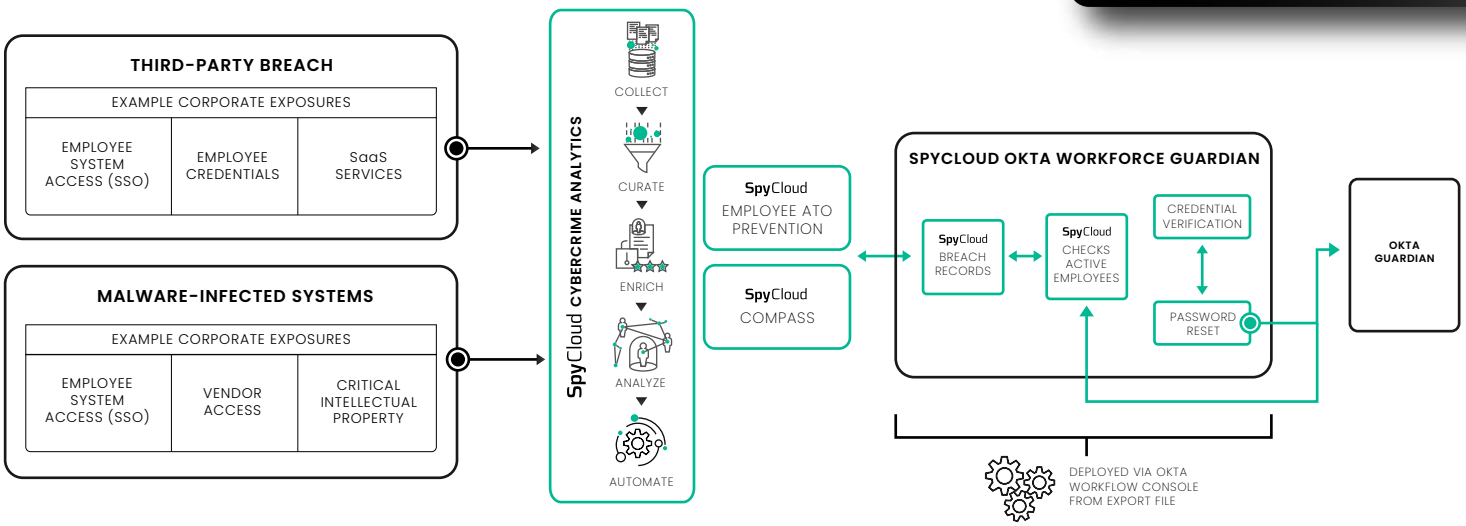
Stay Ahead of Criminals
With proactive monitoring of Okta Workforce for exposed employee credentials

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

PRODUCT OVERVIEW

SpyCloud checks your users' Okta Workforce credentials against billions of recaptured darknet assets to see if any of your corporate logins are available to cybercriminals. With SpyCloud Okta Workforce Guardian, you can automate password reset for exposed accounts and disable high-risk employee accounts – keeping your corporate assets secure. Okta Workforce Guardian makes it easy to identify reuse of compromised credentials, check for prior exposure, and mitigate new exposures to maintain account security.



HOW IT WORKS

FUNCTION & DELIVERY

This product uses Okta Workflows to compare exposed passwords from a customer's SpyCloud Enterprise Protection API against live Okta Workforce users' passwords. The distribution model for Okta Workforce Guardian will be an export file downloaded from SpyCloud, which is then configured in your Okta Workforce workflow environment.

SUPPORTED CAPABILITIES

SpyCloud doesn't just change the risk level for every time an employee email randomly gets mentioned in a forum or data post, but instead actively validates that exposed passwords aren't being used. When an exposed password is in use, SpyCloud's Okta Workforce Guardian can remediate that exposure.

- Check passwords against all users in your Okta Directory
- Use the Watchlist as guidance for select password checks

REMEDIATION OPTIONS

- Notify exposed users
- Perform password resets
- Change user group to apply additional login requirements
  - Step-up authentication
  - MFA
- Deny access

TECHNICAL REQUIREMENTS

- 20 available Okta Workforce Workflows
- Super Administrator access to the organization

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**.