

SpyCloud

ACTIVE DIRECTORY GUARDIAN

AUTOMATE ATO PREVENTION AND REMEDIATE COMPROMISED IDENTITIES **WITHIN 5 MINUTES**

THE PROBLEM

Your employee's Active Directory (AD) credentials could be exposed in many ways: third-party breaches, malware infections, or successful phishing attacks. More concerning, exposed credentials tied to their personal identity – beyond your organization's visibility – can also be used by criminals to gain access into your corporate network. Protect your enterprise by automatically scanning and remediating all exposed credentials tied to employee identities to prevent targeted attacks.

PRODUCT OVERVIEW

SpyCloud Active Directory Guardian amplifies your identity protection efforts to safeguard employee identities by checking AD credentials against billions of recaptured darknet assets to see if any of your corporate logins are available to cybercriminals – automatically remediating exposed passwords **within five minutes from discovery**. Using the world's largest repository of recaptured identity data and SpyCloud's proprietary IDLink analytics, Active Directory Guardian also prevents employees from choosing weak or exposed Active Directory passwords that overlap across their personal and professional identities. As new incidents occur, you can automatically reset exposed passwords and disable high-risk employee accounts – keeping your corporate assets secure.

BENEFITS AT A GLANCE

Holistic Identity Matching

with IDLink analytics uncover hidden exposures linked to breaches, malware infections, and successful phishing attacks

Stay Ahead of Criminals

with rapid remediation of newly compromised Active Directory accounts to prevent criminals from targeted employee ATO attacks

Prevent Password Reuse

by detecting exposed credentials used by employees in corporate and personal accounts, with privacy by design

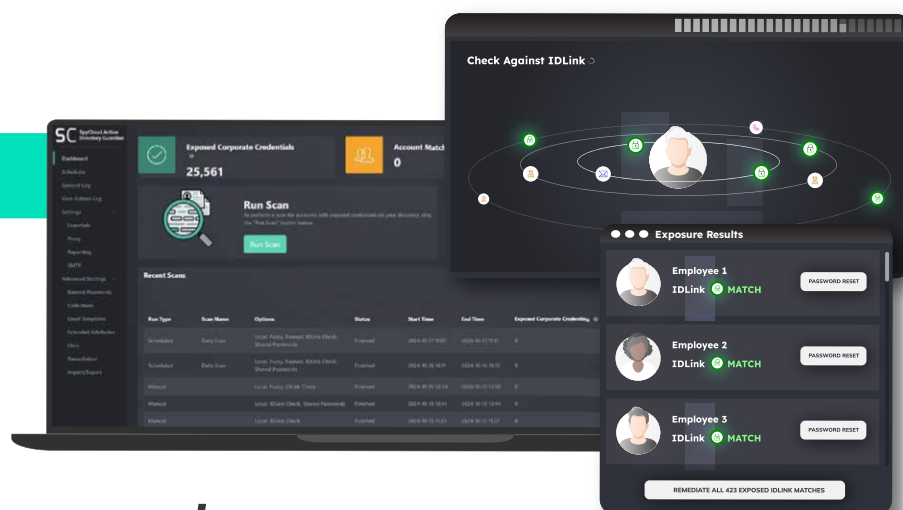
KNOW MORE. DO LESS.

WITH SPYCLOUD HOLISTIC IDENTITY MATCHING

Scan AD with IDLink analytics to find hidden exposures within your workforce, some of which are outside your visibility. Automatically detect exposed credentials and reset within 5 minutes.

Find up to 14x more passwords per user

SPYCLOUD ACTIVE DIRECTORY GUARDIAN



HOW IT WORKS

SpyCloud Active Directory Guardian includes two components that can be implemented together or separately: a browser-based application that installs as a service and runs locally, and a password filter that runs on your domain controllers.

MULTIPLE SCANNING OPTIONS

AUTOMATIC SCANS

Automatically look for exact matches of exposed Active Directory credentials in SpyCloud's database, for around the clock ATO protection.

DEEPER DAILY SCANS

Configure rules for timing and scans that match your workforce's behavior, combining fuzzy variations (checking **1,000 common variations** of employee credentials), password-only matches, banned passwords, shared passwords, and compromised passwords found by IDLink analytics shared between your employee's personal and professional identities.

REMEDIATION OPTIONS

Decide when and how to remediate based on a scan criteria and inform your AD users utilizing our SMTP functionality. Minimize employee disruption by automating workflows and improving employee password hygiene.

KNOW MORE WITH IDLINK ANALYTICS

Seamlessly built into Active Directory Guardian, SpyCloud's proprietary IDLink analytics expand your ATO prevention strategy by exposing the overlap of your employee's personal and professional identity, scanning for hidden credentials in the hands of criminals. IDLink looks for connections on everything that makes up a digital identity – from matching emails, to usernames, passwords, and more – and returns compromised credentials that match your employee's AD password.

IDLink scans can find up to 14x more passwords per user – compared to exact matches.

1

Active Directory Guardian uses native Microsoft calls to replicate data related to users in your AD environment including NTLM hashes of your AD passwords.



2

Active Directory Guardian pulls exposed credentials matching your SpyCloud watchlist domain via the SpyCloud API and runs analytics locally.



3

Active Directory Guardian checks your AD users' passwords, including "fuzzy" variations, to ensure they haven't been exposed from third-party breaches, malware, or successful phishing attacks.



4

Scanning with IDLink automatically returns any compromised passwords found in SpyCloud's database that are correlated to your employee's holistic identity.



5

If the user's credentials match, you can automatically reset the password through AD.

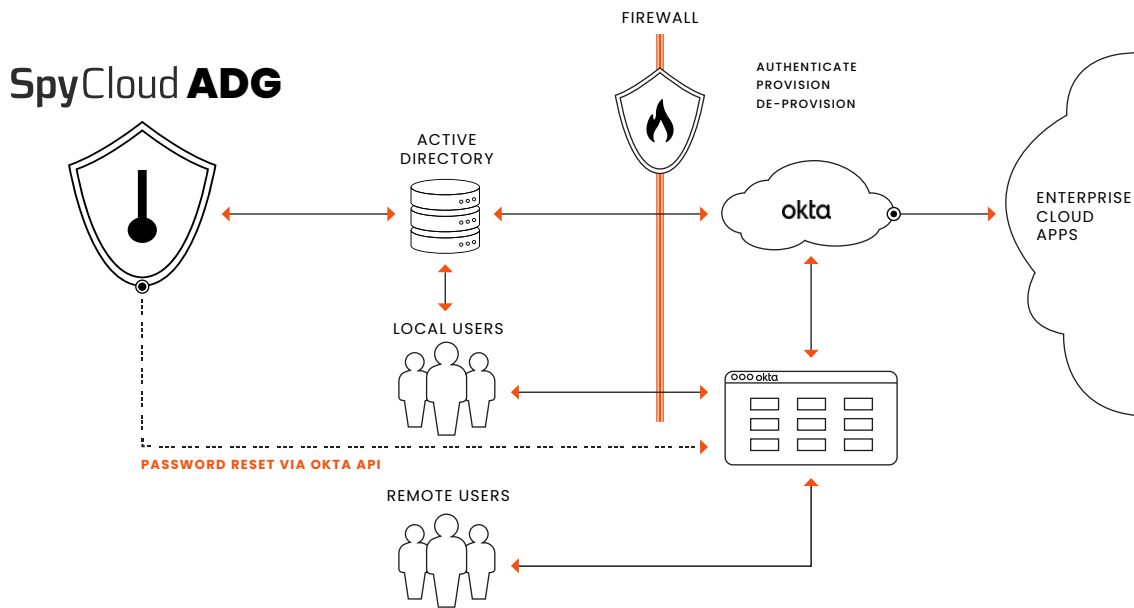


6









Other options include disabling the account, alerting the security team, or notifying the user when a password reset is required.

ACTIVE DIRECTORY GUARDIAN + OKTA REMEDIATION WORKFLOW

Active Directory Guardian + Okta Remediation Workflow: This is an example of a customer’s environment using Okta with authentication provided by AD. Active Directory Guardian is configured to directly connect to Okta using the Okta API.



PRODUCT CAPABILITIES

- 
AUTOMATIC SCANNING
 Continuously detect any new compromised credentials in SpyCloud’s database to remediate exact-match scans within 5 minutes of discovery
- 
AUTOMATED IDENTITY ANALYTICS
 Scan with IDLink analytics to identify sharing and reuse of personal and professional passwords to remediate hidden compromise
- 
BANNED PASSWORDS
 Block employees from using specific passwords, such as company name, industry terms, team names, and keywords related to current events
- 
SCHEDULED SCANNING
 Scan at your preferred cadence with reports delivered directly to your inbox to catch exposures or the reuse of compromised passwords
- 
CUSTOM REMEDIATION POLICIES
 Notify users with custom emails sent from a known internal address, disable user, or reset passwords
- 
REMEDIATE SHARED PASSWORDS
 Gain visibility of internal password reuse via regularly cadenced scans and apply remediation policies to users
- 
NIST COMPLIANCE
 Align to NIST password guidelines by preventing employees from setting weak or compromised passwords and automatically filtering out bad passwords
- 
SECURE DIRECTORY CONNECTIONS
 Enforces explicit LDAPS-only or LDAP-only modes with immediate validation, eliminating insecure protocol fallback and reducing misconfigurations

PASSWORD FILTER

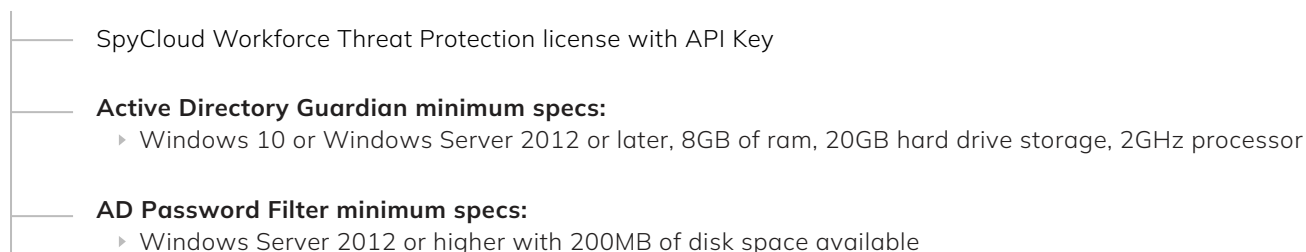
Secure your employees' passwords from the moment they're created, and monitor them over time for new exposures. Check Active Directory passwords as they are created and reject weak or exposed passwords.

Whenever a user chooses a new Active Directory password, SpyCloud checks the password for:



If the Active Directory Guardian password filter detects a match, the risky password is blocked and the user is prompted to make a new selection. Each possible outcome can be ingested into your SIEM for analysis.

TECHNICAL REQUIREMENTS



Using a different directory store? Learn more about our other Identity Guardian offerings including [Entra ID Guardian](#) or [Okta Workforce Guardian](#).

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, 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.