DATASHEET

SpyCloud

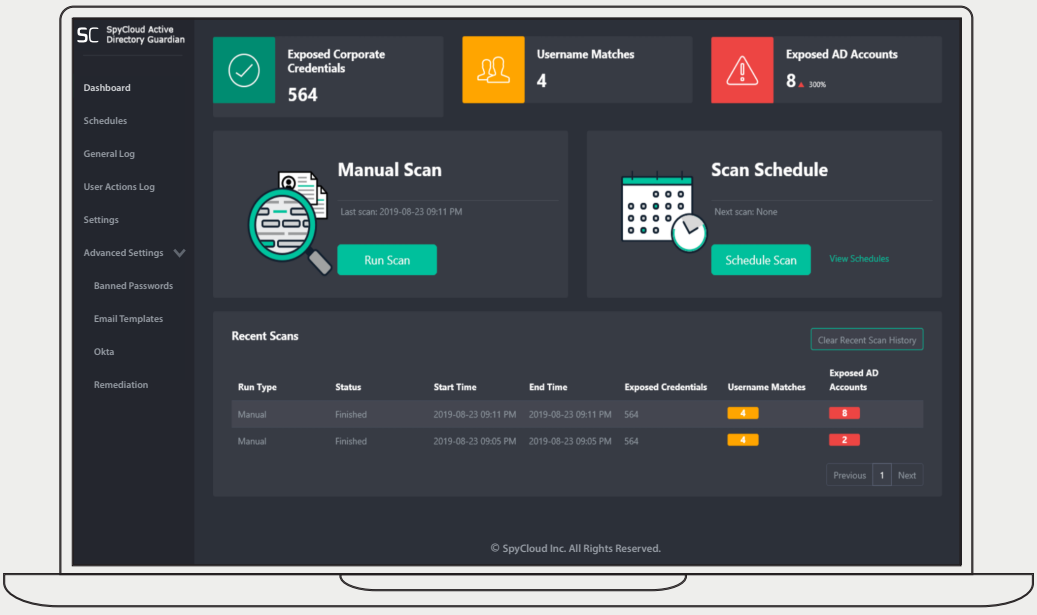
ACTIVE DIRECTORY GUARDIAN

AUTOMATE COMPROMISED PASSWORD REMEDIATION

A criminal who gains access to your users' Active Directory (AD) credentials through a third-party breach or malware infection can easily log into your network – accessing business critical services. To protect your enterprise, you need to take action quickly.

PRODUCT OVERVIEW

SpyCloud checks your users' Active Directory credentials against billions of recaptured darknet assets to see if any of your corporate logins are available to cybercriminals. With **SpyCloud Active Directory Guardian**, you can prevent employees from choosing weak or exposed Active Directory passwords using the largest repository of recaptured credential data in the world. As new incidents occur, you can automatically detect and reset exposed passwords and disable high-risk employee accounts – keeping your corporate assets secure. Active Directory Guardian makes it easy to identify reuse of compromised credentials, scan for "fuzzy" variations and off-limits passwords, and check for prior exposure.



Active Directory Guardian: At-a-glance view of your Active Directory status. Run a manual scan of all credentials, schedule scans, and view results of previous scans for username matches, exposed credentials, and exposed AD accounts.

BENEFITS AT A GLANCE

STAY AHEAD OF CRIMINALS
with proactive monitoring of your Active Directory 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 by strong passwords from day one

REDUCE EFFORT
identifying, investigating, and remediating potential account takeovers by automatically enforcing corporate password policies

SpyCloud

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. When your users create passwords, you can prevent them from using dictionary words, sequential characters, or previously-breached passwords. To mitigate new exposures, proactively monitor your AD using a variety of scan options to include exact credential matches, “fuzzy” variations, password-only matches, banned passwords, and shared passwords.

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

1

Active Directory Guardian uses native Microsoft calls to pull 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 email domain via the SpyCloud API and runs analytics locally.

3

When aligning with NIST password guidance, **Active Directory Guardian** checks each of your AD users' passwords, including "fuzzy" variations, to ensure these passwords have not been seen in a breach or malware logs that exist anywhere in SpyCloud's database.

4

If the user's credentials match, you can automate remediation for password reset through **AD**, including environments where Okta is used for SSO.

5

AD remediation includes the option to disable the user, blocking account takeover attempts using the compromised credentials. Or you can configure notifications to inform the user when a forced password reset is required.

When scanning for previously compromised passwords across the entire SpyCloud dataset to align with NIST password guidance, Active Directory Guardian uses **k-anonymity** to check passwords, where the first five characters of each password hash are sent over the network — never the user's actual plaintext password. This method checks if there has ever been a match in the SpyCloud database, while not letting attackers have access to actual passwords.

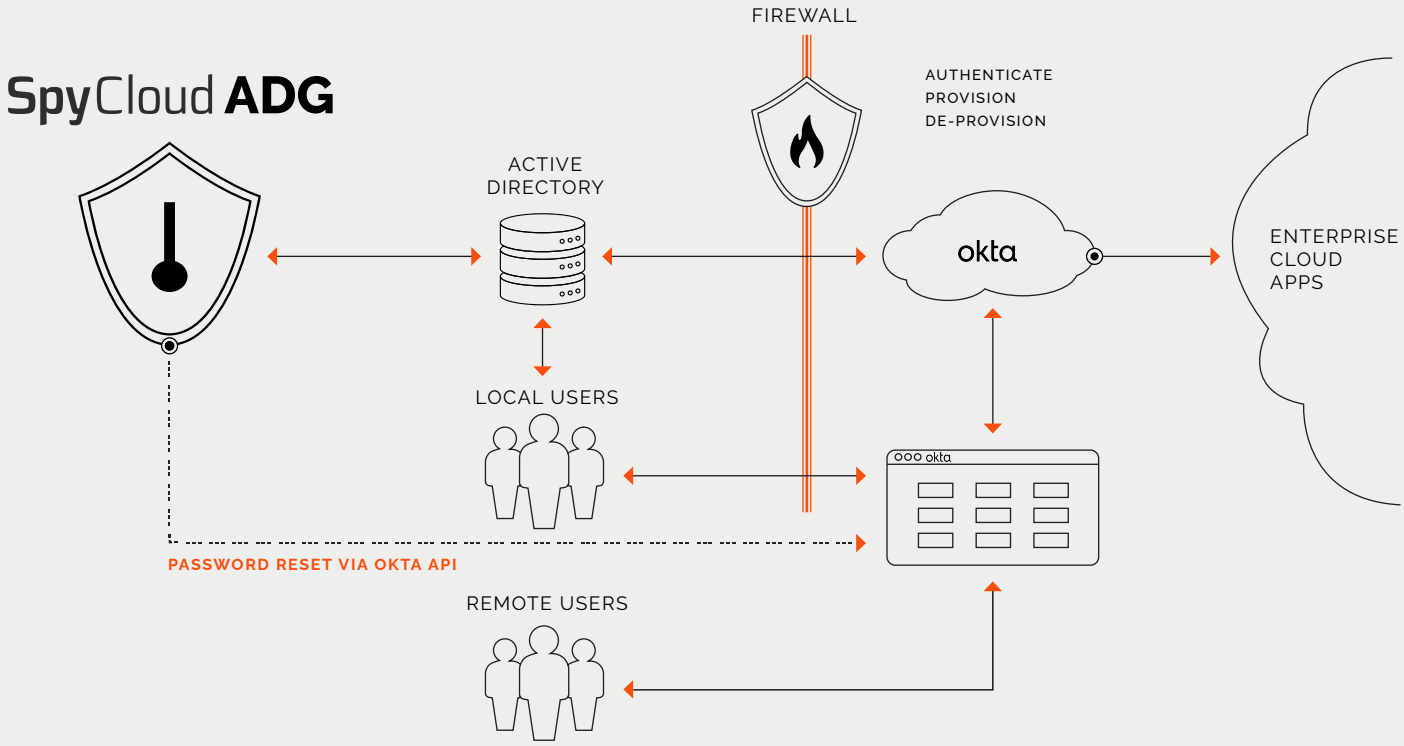
NOTE: The user and AD hash data is held in ephemeral memory storage, not cached or stored on disk.

SpyCloud

AUTOMATICALLY RESET COMPROMISED PASSWORDS

EASY OKTA INTEGRATION

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

USER NOTIFICATIONS

Inform users when a forced password reset is required and create workflows to mitigate exposures

CUSTOM REMEDIATION POLICIES

Options include notifying users with custom emails sent from a known internal address, and multiple remediation options including disabling users or applying to users based on role type

BANNED PASSWORDS

Block 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

REPORT ON SHARED PASSWORDS

Gain visibility of internal password reuse via regularly cadenced scans

NIST COMPLIANCE

Align to NIST password guidelines by preventing employees from setting weak or compromised passwords and automatically filtering out bad passwords

SpyCloud

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:

- Repeated characters
- Sequential characters
- Banned passwords
- Previously-exposed passwords
- Required length
- Containing a user login
- Matching the minimum threshold

If the ADG 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.

SYSTEM REQUIREMENTS

- Active Directory Guardian requires an active SpyCloud Employee ATO Prevention license
- Active Directory Guardian includes two separate components: a browser-based application that installs as a service and runs locally, and a password filter that runs on you domain controllers
- **Active Directory Guardian minimum specs:**
  - Windows 10 or Windows Server 2012 or higher, 8GB of ram, 20GB hard drive storage, 2GHz processor
- **Password Filter minimum specs:**
  - Windows Server 2012 or higher with 200MB of disk space available
- For the best experience, SpyCloud recommends locally hosted Active Directory (on-premise or VMs in a data center) and hybrid Azure hosted setups

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 half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to nearly 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.