SpyCloud

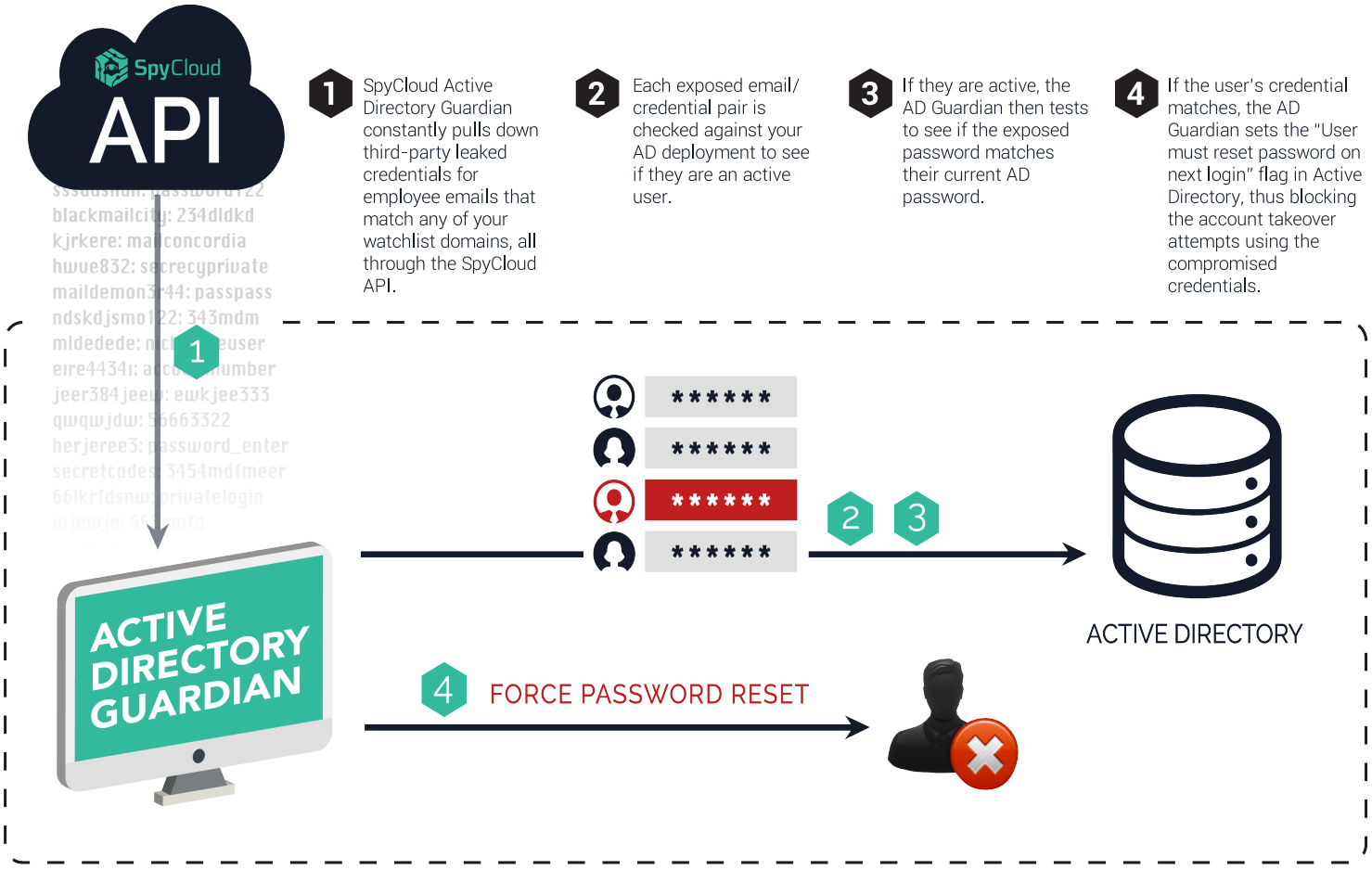
Active Directory Guardian

Protect Employees. Protect the Enterprise.

Of the 53,000 security incidents included in the 2018 Verizon Breach Report,[1] a whopping **48 percent involved stolen credentials**. A criminal who finds your employee's Active Directory password through a third-party data breach can easily log into your network or access services like remote file shares, Microsoft Exchange email servers, or SharePoint enterprise collaboration tools. For a busy security team, identifying, investigating, and remediating potentially compromised accounts poses a major challenge.

With SpyCloud Active Directory Guardian, you can:

- Automatically monitor your Active Directory for compromised employee credentials
- Remediate compromised passwords automatically or with the click of a button
- Simplify compliance with NIST password guidelines checks
- Stay ahead of criminals with early notification of new exposures using the largest database of stolen credentials in the world



1. SpyCloud Active Directory Guardian constantly pulls down third-party leaked credentials for employee emails that match any of your watchlist domains, all through the SpyCloud API.
2. Each exposed email/credential pair is checked against your AD deployment to see if they are an active user.
3. If they are active, the AD Guardian then tests to see if the exposed password matches their current AD password.
4. If the user's credential matches, the AD Guardian sets the "User must reset password on next login" flag in Active Directory, thus blocking the account takeover attempts using the compromised credentials.

[1]https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

SpyCloud Active Directory Guardian

Leaked credentials are the number one risk to account takeover. For multiple reasons, including password reuse and weak passwords, employees expose their credentials and therefore AD, often without their knowledge. Without a proactive solution, the enterprise is in constant danger for an attack that begins with one person but escalates rapidly. **SpyCloud protects on-prem Active Directory and/or cloud-based Azure exposure with Active Directory Guardian, a comprehensive AD protection solution.**

Integrate

SpyCloud Active Directory Guardian integrates into on-prem AD and/or Azure AD domains via the SpyCloud API, pulling in robust exposure data from the SpyCloud database and comparing new stolen credentials to your Windows domain users. The flexibility of the SpyCloud API also makes integrating into other enterprise internal systems, such as Splunk, easy and results can be exported in a CSV. Leverage the SpyCloud API with your own tools or SpyCloud's to protect employees and the enterprise 24/7/365.

Monitor

SpyCloud Active Directory Guardian runs locally and constantly compares new stolen credentials against every active Windows domain user. The dashboard displays how many employees have exposures, who those employees are, the exposed password and if the password was reused from other accounts. SpyCloud discovers exact matches as well as similar "fuzzy" matches for breached passwords, giving the enterprise security team instant access to the organization's vulnerability stance with reports that answer the who, what, when and where so action can be taken.

Respond

Only SpyCloud provides remediation tools when exposed credentials are discovered in Active Directory. If the SpyCloud exposure data matches that of an employee's credential, SpyCloud Active Directory Guardian automatically forces the exposed user to proactively reset their password. The employee is prevented from logging in with exposed credentials, thus avoiding account takeover.

SpyCloud

Web: spycloud.com
Phone: +1 (800) 513-2502
Sales Inquiries: sales@spycloud.com

No other solution provides the same level of monitoring with proactive, automated resolution. Protect your enterprise by fortifying Active Directory with SpyCloud Active Directory Guardian. **Request a demo today.**