Alvarez & Marsal Automates Account Takeover Prevention for 6,000+ Users with SpyCloud Active Directory Guardian

About the Customer

Alvarez & Marsal is a global professional services firm with over 6,000 employees spread across 54 office locations. With employees and customers around the world, Alvarez & Marsal is subject to a variety of regulations, such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This case study explores how the company uses SpyCloud to automate account takeover prevention for their workforce.

Automating Account Takeover Prevention

Alvarez & Marsal uses SpyCloud to monitor the credentials of employees at all 54 of the company's global offices, as well as service providers enrolled in their Active Directory.

Multiple times a day, Alvarez & Marsal runs SpyCloud Active Directory Guardian to find out if any of their 6,000+ users' credentials have been exposed on the criminal underground, checking against billions of compromised credentials in SpyCloud's database that have been recovered from third-party breaches. Active Directory Guardian automatically forces password resets for users whose login information has been compromised.

> " Active Directory Guardian protects our whole organization no matter where they are in the world. Everybody's protected.

"What SpyCloud's Active Directory Guardian does for us is invaluable. To be able to search through billions of data points — it's impossible for us to do. But Active Directory Guardian picks out issues instantly," said Alvarez & Marsal Global Senior Director of IT Operations, Dan Holland.

"Capturing the issues before they become a problem is significant," Holland said; it's one key reason why the company has never experienced a breach.

Automation makes it possible for his team to close the gaps left by employees' bad password hygiene, which evolves constantly. They've found that the biggest risk is presented by employees who reuse passwords from their personal life to protect their work accounts.
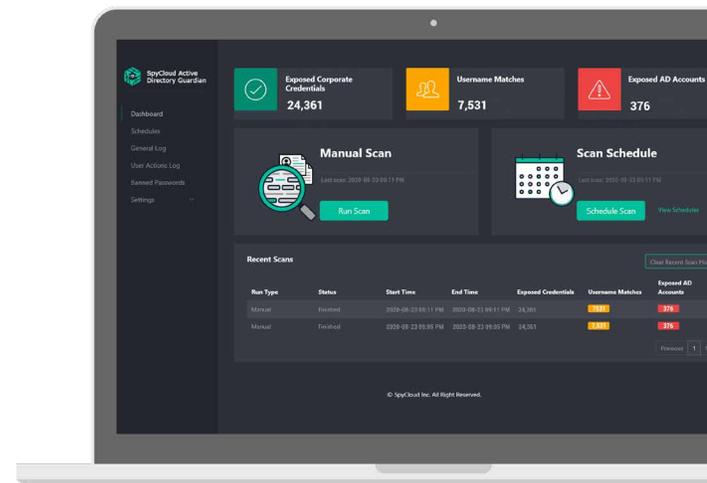
SpyCloud Active Directory Guardian scans Alvarez & Marsal's 6,000+ user accounts multiple times per day.

"We have seen people cycle through passwords that have normally been quite good, run out of ideas, and then go back to an old LinkedIn password," Holland explained. "Active Directory Guardian needs to be run regularly because we have a lot of people looking at what we do and looking for possible routes in. Our SOC team is a very busy group."

For Alvarez & Marsal, SpyCloud plays an important role in a robust security program.

"Even though we have other layers of protection, we still see password reuse. So we know that if it wasn't for Active Directory Guardian, people's behavior would put us into a position of weakness."

Preparing to Meet Global Compliance Regulations

Adopting Active Directory Guardian has made it easier for Alvarez & Marsal to prepare to meet the wide variety of compliance regulations they are subject to as a global company, such as Europe's General Data Protection Regulation (GDPR), and set the company up for success with the California Consumer Privacy Act (CCPA).

"Because we're global, we're subject to everyone's regulations. So we have to treat everything at that top level and address accordingly," explained Holland.

"SpyCloud plays a part in helping us understand our security posture. We can say we're Cyber Essentials Plus certified, we can discuss what processes we have in place with Active Directory Guardian to protect us in case a password is leaked. There's a gap that SpyCloud's Active Directory Guardian fills for us, and lots of people don't have that addressed. We think that gives us a little bit of an edge on any queries that go down that particular path."

Specifically, Holland said, using SpyCloud to support their preparation for GDPR set them up for success with CCPA.

"GDPR is comprehensive, and CCPA follows a very similar ethos. Being prepared for GDPR and having our answers ready and that toolset that we use, which includes SpyCloud, puts us in a very good position to be able to address CCPA."

For Holland, using SpyCloud to detect and reset compromised passwords automatically provides peace of mind when auditors reach out. He feels confident in his ability to answer their questions and satisfy requirements related to account security.

"SpyCloud often comes into the picture during an audit, either to make a statement on our posture, or to talk about what happens if a password is discovered. Active Directory Guardian reports in, we have tickets created, and we can track what's discovered and when.

And it also will give us an indication of particular user habits, of maybe their consciousness around security," Holland explained. "I see a lot of audit requests from banks, customers, etc. We're asked, how quickly can you react to something? With Active Directory Guardian running on a daily basis, as soon as there's a hit, the password is reset. I'm not sure you can do much better than that."

Compliance aside, the ability to address these types of concerns with SpyCloud has provided other unexpected benefits.

"As a byproduct, SpyCloud has also given us a better score with our insurance companies. I remember six months ago being brought into a meeting with our cyber insurance providers and they told us that we were the lowest-risk company that they had seen. That's due to the stack we've implemented, and obviously SpyCloud is part of that stack."

Protection For Years to Come

When Alvarez & Marsal first started using Active Directory Guardian a number of years ago, they were just beginning to roll out a multi-factor authentication program. SpyCloud data provided powerful evidence of password reuse that helped accelerate MFA adoption across the business. Today, Active Directory Guardian is a central piece of a larger toolset the company has built to protect employee accounts from account takeover.

"This is a product that we've purchased or renewed year on year. So there's the value of it. Every year, it's automatically renewed—no questions asked. That's quite a powerful statement really, especially when there are a lot of options in different areas in the marketplace and sometimes budgets are difficult. SpyCloud seems to be one of the first that gets ticked off the list."

Without the visibility SpyCloud provides, we would have been at a very big risk of compromise.

The SpyCloud Difference

Current, Relevant, Truly Actionable Data

With SpyCloud Active Directory Guardian, you can detect and reset compromised Active Directory passwords automatically using the largest database of compromised credentials in the world.

Whether you choose to run a manual or automated scans, SpyCloud checks your users' Active Directory credentials against billions of recovered breach assets to see if any of your corporate logins are available to cybercriminals. You can identify if your employees have reused exact breached credentials, "fuzzy" variations that are easy for criminals to detect, off-limits passwords like your company name, or any password that has ever appeared in the SpyCloud database.

138+ B
Recovered
Breach Assets

24+ B
Total
Passwords

29+ B
Email
Addresses

150+ PII
Data
Types

SpyCloud

Request a Demo at spycloud.com