SpyCloud

Case Study

Global Professional Services Firm Automates Account Takeover Prevention for 6,000+ Users with SpyCloud Active Directory Guardian

Overview

This global professional services firm has over 6,000 employees spread across more than 60 office locations. The organization offers consulting services that cover multiple service lines, including business restructuring, tax, mergers and acquisitions, disputes and investigations, and performance improvement.

Challenge

When the firm first encountered SpyCloud a number of years ago, they had a problem: many of their employees were using compromised passwords.

Solution

SpyCloud Active Directory Guardian's automated AD scans and password resets enabled the organization to detect and respond to compromised employee credentials at scale, providing a strong foundation for their now-robust employee ATO prevention program.

Result

With SpyCloud, the firm protects 6,000+ user accounts around the world from ATO and maintains compliance with both GDPR and CCPA. Automated password resets give them confidence during audits – plus, they've boosted their score with cybersecurity insurance providers.

SpyCloud

Automating Account Takeover Prevention

This global professional services firm uses SpyCloud to monitor the credentials of employees at all of the company's global offices, as well as service providers enrolled in their Active Directory.

Multiple times a day, the organization 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.

"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 the firm's senior director of IT operations.

"Capturing the issues before they become a problem is significant," the senior director of IT operations 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.

> **"Active Directory Guardian protects our whole organization no matter where they are in the world. Everybody's protected."**
>
> **- SENIOR DIRECTOR OF IT OPERATIONS, GLOBAL PROFESSIONAL SERVICES FIRM**

"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," the senior director of IT operations 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 the firm, 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 the firm 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 the senior director of IT operations.

SpyCloud

"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, 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 the senior director of IT operations, 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, or maybe their consciousness around security," the senior director of IT operations 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."

> **"Without the visibility SpyCloud provides, we would have been at a very big risk of compromise."**
>
> **- SENIOR DIRECTOR OF IT OPERATIONS, GLOBAL PROFESSIONAL SERVICES FIRM**

Protection For Years to Come

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

"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."