Solution Brief

SpyCloud

Simplify NIST Password Guidelines with Active Directory Guardian

SpyCloud

Solution Brief Overview

It's inevitable: people reuse passwords. Faced with complicated password requirements and hundreds of online accounts to keep track of, it's no wonder that 70% of users exposed in 2021 breaches were reusing previously compromised passwords and either knew and haven't updated or don't know and don't understand the risk that's associated with compromised passwords. To remember their login information, many users rotate through a familiar set of passwords or change them by just a few characters to squeak by complexity requirements.

Attackers count on these bad habits. As soon as criminals gain access to a set of credentials through a data breach, they begin testing stolen passwords against other accounts to see what they can exploit. Advanced crimeware has made it easy for even unsophisticated threat actors to engage in credential stuffing and password spraying attacks at scale.

To help organizations mitigate the risk posed by users' bad password habits, the National Institute of Standards and Technology (NIST) designed a set of password guidelines with human behavior in mind. While most of NIST's password guidelines can be enforced directly within directory services like Active Directory, there's a critical exception: banning "commonly-used, expected, or compromised" passwords.

SpyCloud simplifies NIST password guidelines by enabling you to check your employee passwords against the largest database of stolen credentials in the world. With SpyCloud Active Directory Guardian you can prevent, identify and reset breached Active Directory passwords automatically, dramatically reducing the time, cost, and resources required to align with NIST guidelines.

Password Guidelines in NIST Special Publication 800-63B

In NIST Special Publication 800-63B section 5.1.1.2, 'Memorized Secret Verifiers,' NIST lays out password guidelines designed to encourage users to choose strong passwords, along with strategies to help enterprises mitigate the risk posed by human behavior.

- Previous breach exposures
- Less than 8 characters
- Context-specific words
- Dictionary words
- Repetitive characters
- Password hints

SpyCloud

To account for users' tendency to rely on weak and reused passwords, NIST calls for organizations to check credentials against a list of "commonly-used, expected, or compromised" passwords, including dictionary words, repetitive characters, and previous breach exposures.

Unlike most of the NIST password guidelines, which can be automated using out-of-the-box controls in directory systems like Microsoft Active Directory, checking for weak or exposed passwords requires additional support. In particular, identifying passwords found in previous breaches poses a burden for security teams without the time or resources to keep up with the latest breach data on their own, let alone apply that information to their own user credentials.

Using SpyCloud to Align with NIST Guidelines

SpyCloud maintains the largest repository of recaptured data in the world, growing by a billion assets per month, with a focus on maintaining a high volume of plaintext passwords. With **SpyCloud Active Directory Guardian**, you can operationalize that data to automatically detect and reset Active Directory passwords NIST would classify as "commonly-used, expected, or compromised," dramatically reducing the time your security team needs to spend researching new breaches, remediating exposed passwords, and investigating potentially compromised accounts.

Active Directory Guardian can help you align with NIST guidelines by detecting, resetting, and reporting on:

- Exact employee credentials exposed in a third-party breach
- "Fuzzy" credential matches, meaning a compromised password that has been reused with trivial changes
- Any password that has appeared in the SpyCloud breach database, regardless of username
- Dictionary words
- Repetitive characters
- Context-specific terms

SpyCloud maintains the largest repository of stolen credentials in the world:

170+ Billion
Recaptured Assets

30+ Billion
Email Addresses

25+ Billion
Total Passwords

...and growing by a billion assets per month.

SpyCloud

Key Features & Benefits

Reduce your team's workload with "set it and forget it" automation

NIST guidelines put the onus on the enterprise to identify when user credentials have been exposed in third-party data breaches. Unfortunately, new breaches happen constantly, which creates a challenge for organizations. Researching, parsing, normalizing, and matching breach data to Active Directory passwords takes time that busy security teams don't have to spare, not to mention the cost of remediating compromised accounts. Instead of hiring additional resources to try to keep up, you can get peace of mind by automating that process with SpyCloud Active Directory Guardian.

SpyCloud typically ingests a billion new breach assets per month, helping you stay on top of new breaches without performing research on your own. Active Directory Guardian operationalizes that data for you, giving you the ability to prevent employees from setting bad passwords, scan your Active Directory for new exposures, and reset compromised credentials automatically.

Stay ahead of criminals with early access to breach data

When a new breach occurs, the clock starts. For the first 18 to 24 months after a breach, criminals keep the data within a close circle of trusted associates while they assess what kind of data they have, crack passwords, and experiment with the most effective methods of monetizing it. This is the most lucrative time for a criminal to have access to stolen credentials, and the most dangerous time for enterprises. Only after the original criminal group has extracted as much value as possible from the breach data do they allow it to trickle onto deep and dark web forums where anyone can access it. By that point, the worst damage has already been done.

With Active Directory Guardian, you can prevent the use of bad passwords and remediate compromised accounts early in the breach cycle, before criminals have a chance to use them.

Criminals use sophisticated crimeware to automate credential stuffing and password spraying attacks. With Active Directory Guardian, you can automate your defenses to match.

SpyCloud

SpyCloud researchers infiltrate criminal communities to uncover breaches from the underground well before they make public headlines. In some cases, we're even the first to inform the affected victim organizations through our responsible disclosure process. We typically recapture breach data before the criminals who stole it have had a chance to crack the passwords, so we crack the passwords at scale to make them actionable for our customers, enabling you to identify matches within your Active Directory logins right away.

Protect your organization from account takeover attacks

Imagine: One of your senior executives signs up for a Fantasy Football account using their work email address...and their Active Directory password. When attackers breach Fantasy Football and steal those login credentials, criminals have everything they need to take over that Active Directory account and compromise financial accounts, customer data, intellectual property, and anything else your executive has access to.

Active Directory Guardian helps you identify and react quickly to situations like this by alerting you to credentials in your Active Directory that have been exposed in a new data breach, including exact credential matches and "fuzzy" variations. Though users often think that adding a few characters or replacing letters with numbers in the style of "leet speak" adds a layer of security, criminals can easily identify these fuzzy variations of exposed passwords with automated account checker tools. Active Directory Guardian helps you stay one step ahead.

When you come across a compromised credential, NIST recommends resetting the user's password. Active Directory Guardian makes that easy by providing the option to reset exposed passwords automatically. You can also view a report of exposures to help you reset passwords manually or reach out to users for individual security education.

Employees often reuse Active Directory credentials on third party sites, putting your organization at risk when those sites are breached. With Active Directory Guardian, you can detect and reset exposed passwords automatically.

SpyCloud

Identify employee password reuse across work and personal accounts

Employee personal accounts represent a major blind spot for security practitioners, who typically have no way of knowing whether an employee has reused their Active Directory password in combination with different usernames. Meanwhile, it's trivial for an attacker to connect the dots between an executive's personal account, john.smith@example.com, and their work alias, john.smith@employer.com.

SpyCloud Active Directory Guardian enables you to check your Active Directory passwords against our entire database of plaintext passwords, helping you detect whether those passwords have ever been exposed in a data breach.

Ban common or expected passwords that can put your organization at risk

Given the choice, users will select memorable passwords rather than secure ones. To help mitigate that risk, NIST recommends banning common or expected passwords, including dictionary words, repetitive characters, and context-specific terms.

Active Directory Guardian checks your employees' credentials against our pre-populated list of banned passwords, which includes passwords the SpyCloud research team has determined are the most commonly-used. You can easily add to the list to include context-specific words such as your company name.

More importantly, **Active Directory Guardian also enables you to search the entire SpyCloud database** to identify whether the passwords have ever been exposed in a breach, even if your users weren't involved. Unlike a dictionary tool or other type of static list, this database covers billions of unique combinations created by human minds and stays up-to-date as SpyCloud researchers identify new breach exposures.

When an employee reuses the same password with different usernames, it's hard for security practitioners to detect — but trivial for an attacker to connect the dots. Active Directory Guardian makes it easy to check for any password exposure, regardless of username.

SpyCloud

Built for Security

SpyCloud takes precautions to keep your data secure. Active Directory Guardian code goes through internal and third-party security reviews upon every major release.

Because of the sensitivity of running on the domain controller, the password filter is designed to "fail open" to ensure that its impact on your environment remains minimal. In other words, if the password filter fails for any reason, it will allow users to create unchecked passwords rather than locking them out. SpyCloud's scanner provides a backup for checking skipped passwords, as well as identifying newly-exposed credentials.

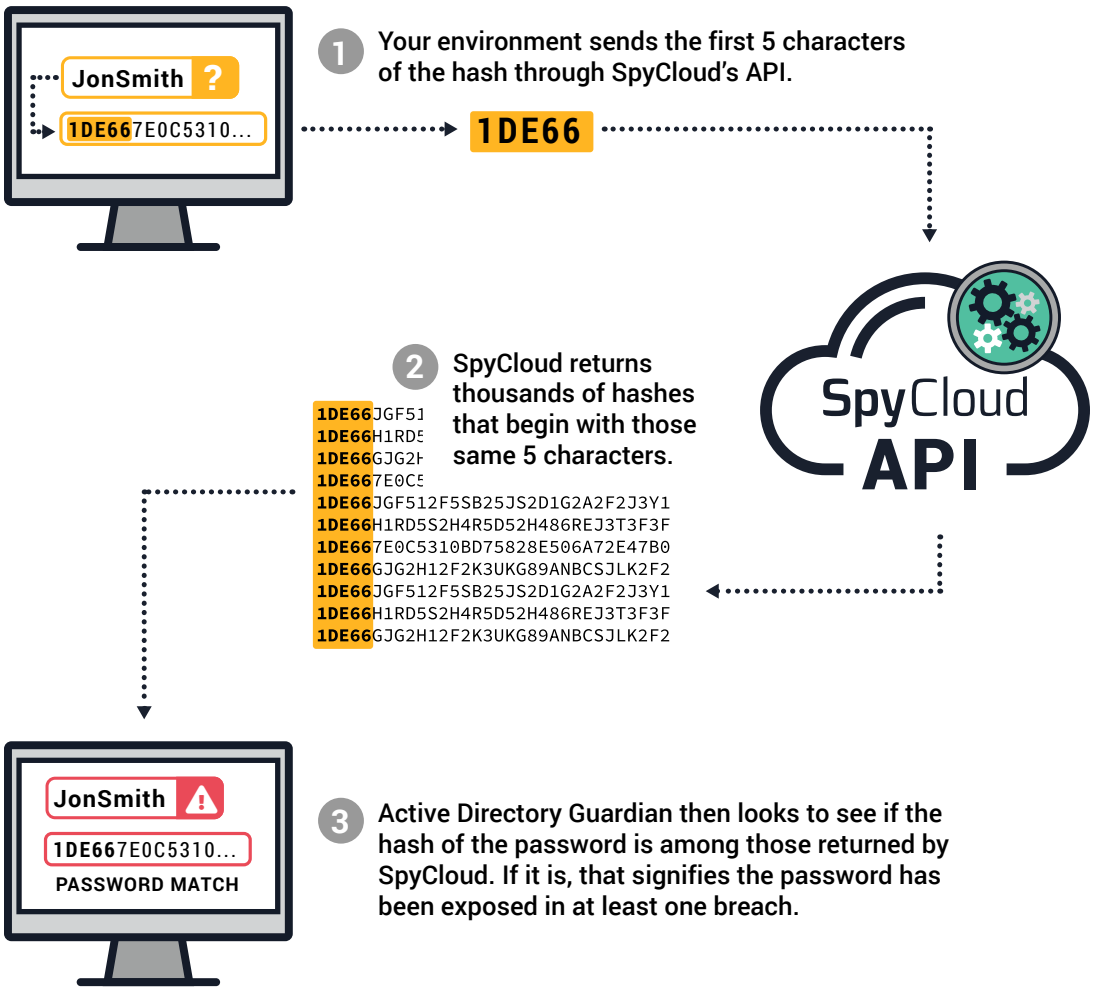
During the scanner's comparison process, data downloaded from the SpyCloud API and NTLM hashes pulled from Active Directory are held in ephemeral memory storage, not cached or stored on disc. The data is encrypted in memory, meaning that if someone were able to access your system while the data was still in memory, they would still need to decrypt the data.

By default, Active Directory Guardian does not push data back to SpyCloud. The single exception is when you select the option to check your users' passwords against the entire SpyCloud database to see if they have ever been exposed in a breach, even if it wasn't your users who were affected. In this case, Active Directory Guardian uses an approach called **k-anonymity,** which means that only the first 5 characters of each password hash are sent over the network—never the user's actual plaintext password. This method ensures that if the traffic were intercepted, it would be useless to an attacker.

With Active Directory Guardian's k-anonymity approach, SpyCloud's API service will only receive the first five hash characters of a password. We never send or receive a user's actual plaintext password. This ensures that if the traffic were intercepted, it would be useless to an attacker.

SpyCloud

Here's how k-anonymity works:



As shown in the above graphic, let's look at one user's password: **fluffybunny.** The NTLM hash of fluffybunny is 1DE667E0C5310BD75828E506A72E47B0. ADG would query SpyCloud's API with the first 5 characters of the hash (1DE66) to see all passwords that may match in our database. Keep in mind that SpyCloud's API service will only receive those first five hash characters (never the user's actual plaintext password). The response from our API is several thousand full NTLM hashes that begin with the same 5 hash characters (1DE66) for exposed passwords.

ADG then looks locally at all of the returned responses to determine if 1DE667E0C5310BD75828E506A72E47B0 exists in it. If it does, this signifies that the password has appeared in at least one breach.

SpyCloud

How It Works

SpyCloud Active Directory Guardian includes two components that can be installed together or separately: a password filter and a scanner. While they can be used independently, installing both components provides the most comprehensive protection for employee accounts.

Option 1: Check at Password Creation – SpyCloud's password filter is installed on the domain controller and enables SpyCloud to check the contents of employee passwords as they are created - preventing employees from choosing weak or compromised passwords in the first place.

Whenever a user chooses a new Active Directory password, the password is automatically checked for:

- Repeated Characters (aaa, 111)
- Sequential Characters (123, abc)
- Banned passwords in a custom dictionary of up to 50,000 entries
- Any password that has appeared in the SpyCloud breach database, regardless of username

If the password filter detects a match, the risky password is blocked and the user is prompted to make a new selection. You can ingest logs from the password filter into your SIEM or other log management system.

Option 2: Scan for New Compromised Credentials – SpyCloud Active Directory Guardian is a browser-based application that installs as a service and runs locally in your environment. When you run a manual or automated scan to check for compromised passwords, Active Directory Guardian uses native Microsoft calls to pull data from the SpyCloud API and compares it locally to NTLM hashes of your Active Directory passwords. Because Active Directory does not log into any user accounts, there is no risk of locking out users through brute force attempts. It does not need to run on the domain controller.

The password filter prevents employees from setting weak or compromised passwords in the first place, and the scanner detects and resets additional exposures as new breaches occur over time.

SpyCloud Active Directory Guardian helps you secure your employees' passwords from the moment they're created, and monitor them over time for new exposures.

About SpyCloud

SpyCloud transforms recaptured data to protect businesses from cyberattacks. Its products leverage a proprietary engine that collects, curates, enriches and analyzes data from the criminal underground, driving action so enterprises can proactively prevent account takeover and ransomware, and protect their business and consumers from online fraud. 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 over 150 cybersecurity experts who aim to make the internet a safer place.

SpyCloud

Summary Aligning to NIST Password Guidelines with SpyCloud Active Directory Guardian

NIST Guideline	How SpyCloud Helps
Identify and avoid: "Passwords obtained from previous breach corpuses."	SpyCloud maintains the largest repository of data breach data in the world, gathered early in the breach timeline to help your organization stay ahead of criminals. With Active Directory Guardian, you can prevent employees from choosing Active Directory passwords that have appeared in the SpyCloud database before, and automatically monitor your AD passwords against our entire database to detect the use of compromised passwords. As we collect additional breach data and users recycle passwords, you'll be alerted to new exposures automatically.
Identify and avoid: "Dictionary words."	The Active Directory Guardian password filter automatically blocks passwords containing repeated or sequential letters, in addition to previously-exposed passwords. You can also upload a Banned Password List containing up to 30,000 entries, including dictionary words. On an ongoing basis, organizations also have the option to check Active Directory passwords against the entire SpyCloud basis for new exposures, independent of username. Unlike a static dictionary, SpyCloud's database reflects the ways people commonly put dictionary words, slang, names, easy-to-type characters, and common phrases together to form passwords.
Identify and avoid: "Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')."	
Identify and avoid: "Context-specific words, such as the name of the service, the username, and derivatives thereof."	Security practitioners can easily add to Active Directory Guardian's banned password list to include any context-specific words relevant to your organization.
Remediate compromised passwords: "If the chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret, SHALL provide the reason for rejection, and SHALL require the subscriber to choose a different value."	The password filter prevents users from creating bad passwords in the first place. When you scan passwords in Active Directory Guardian to check for new exposures, you have the option to reset exposed passwords automatically. You can also use clean, easy-to-read reports of exposed credentials to remediate manually or reach out to users for security education.