WHITEPAPER

Considerations for Choosing an Enterprise Account Takeover (ATO) Prevention Solution

SpyCloud

SpyCloud

Table of Contents

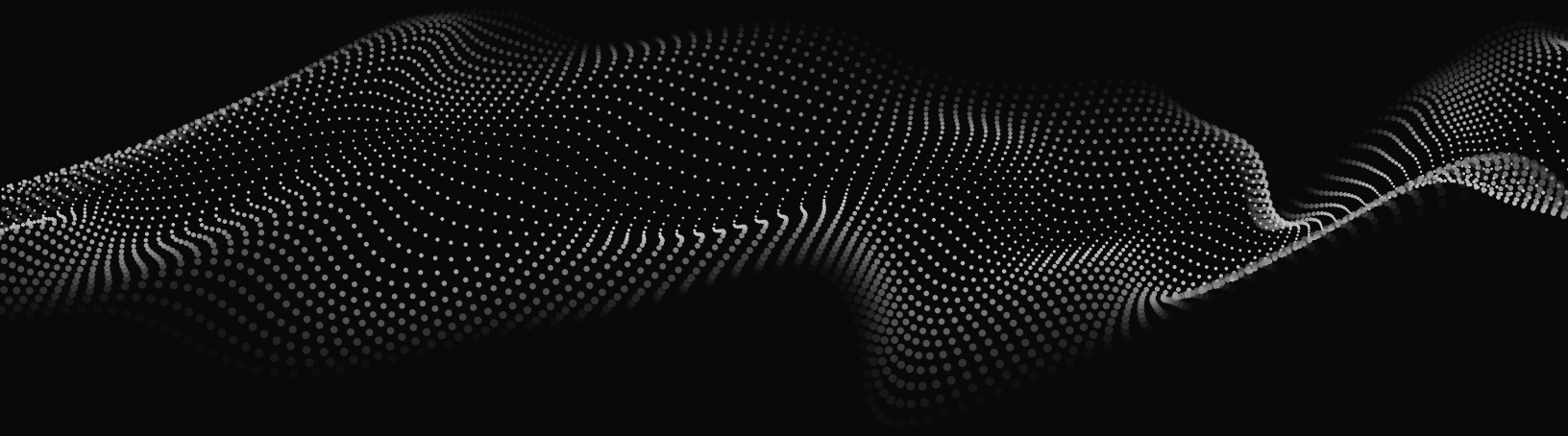
Overview 03

Key Considerations when Evaluating ATO Prevention Solutions and Vendors 03

- Data Collection 03
- Malware Data 04
- Early Detection 04
- Data Cleansing, Curation, and Enrichment 05
- Automation 05
- Proof of Concept 06
- Support 06
- NIST Compliance 06

Employee ATO Prevention Solution Checklist 07

Take Action Against ATO with SpyCloud 08



SpyCloud

Overview

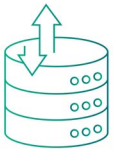
Account takeover (ATO) attacks are on the rise, increasing **307%** over the last 3 years and costing organizations billions of dollars – a whopping **$11.4 billion** in 2021 alone. As the most desirable data that criminals can steal, credentials continue to be the **top entry point** into organizations and the leading cause of breaches because they allow bad actors to appear as legitimate users in your system.

With millions of usernames and passwords stolen each year, ATOs are more common than ever. Last year, SpyCloud recaptured **1.7 billion credential pairs** (email address/user name + password combinations), which continue to be the most highly sought after and lucrative asset in the criminal underground to not only perpetrate attacks like ATO, but also follow-on attacks including **ransomware**. For example, the high-profile Colonial Pipeline incident involved criminals gaining access to the pipeline's system using compromised credentials and launching a ransomware attack. This stolen data can provide entry points into the network and specific applications, where customer data, financial information, intellectual property and other sensitive data is housed.

To prevent these cyberattacks, organizations must find ways to detect and reset compromised credentials. However, each of these only addresses one aspect of the problem. To be effective, an ATO prevention solution must take into account what can be considered the "next generation of ATO prevention," which focuses on not only addressing ATO via stolen credentials, but also malware-stolen session cookies as criminals evolve their tactics to include hijacking web sessions.

Consider the following best practices and guidelines for evaluating how a proper ATO prevention solution can save your organization time and resources spent to reduce risk.

Key Considerations When Evaluating ATO Prevention Solutions and Vendors



Data Collection

Data collection at the scale you need to stay on top of threats is impossible for most enterprises. Organizations simply can't get ahead of the constant onslaught of compromised data that needs to be found, curated, and matched to users with the speed necessary to act before it's used to cause harm to your business.

Many ATO prevention tools lack comprehensive data collection from all levels of the darknet. While many solutions collect commodity and medium-value data available on open and vetted forums on the criminal underground, ideally an ATO prevention solution will devote human intelligence resources to the lower and core layers of the darknet, where high-value data is traded and sold in closed and offline groups. This specialization goes beyond basic threat intelligence to collect data early in the breach timeline for the fastest identification and remediation of compromised employee, partner, and supplier accounts before they can be used to harm the business.

The solution's data repository should be both comprehensive and constantly refreshed. In addition, the company should be able to present a year's worth of the following metrics that you would find meaningful for remediation and reporting, including:

- The count of unique data collected from third-party data breaches, such as email addresses, usernames, passwords, and personally identifiable information (PII)
- The count of unique data collected from malware victim logs, including credentials, PII, IP addresses, and web session cookies
- The number of plaintext/cracked passwords
- The above data, specific to your company's domain(s)

At the same time, the vendor should be willing and able to prove that it adheres to ethical standards in data collection.

Malware Data

Malware-infected devices present a high risk to the enterprise because they enable threat actors to siphon employee credentials and web session cookies (even for third-party applications like from SSO and VPN instances), and other data that helps them infiltrate your business via ATO or session hijacking. Using stolen authentication data in stolen credentials and session cookies on **anti-detect browsers**, adversaries can log into an employee's accounts like a legitimate user, even bypassing multi-factor authentication (MFA).

To protect against this threat, a comprehensive ATO prevention solution will include insights into employees' managed and even unmanaged malware-infected devices accessing your network so compromised passwords can be reset and stolen web sessions can be invalidated as soon as possible, thus locking out bad actors before they can launch ATO or ransomware attacks.

Early Detection

After a breach takes place, attackers typically keep stolen data contained within a small group of trusted associates while they monetize it, often before the breached organization realizes there's been an incident. By the time the data leaks beyond these closed groups and the public becomes aware of the breach, stolen data has typically already been exposed for 18 to 24 months.

Therefore, the ability to detect the exposure of user credentials and cookies as early as possible in the breach timeline is a core functionality for an ATO prevention solution. Truly stopping ATO requires identifying compromised accounts early, before criminals have time to use the stolen credentials, test them against other accounts, or sell/trade them on the darknet. The only way to do that is to have access to a comprehensive, constantly updated, real-time database of breach and malware data.

Data Cleansing, Curation, and Enrichment

Collecting data from the darknet is simply not enough when it comes to preventing account takeover. Threat intelligence solutions that collect and distribute public breach data are reactive and don't provide the actionable data needed to stop additional data breaches and account takeovers, or get ahead of ransomware attacks. Enterprises require actionable data that is properly cleansed and enriched in order to get ahead of these threats.

Data from the darknet doesn't come packaged nicely – it is typically recaptured in messy and unstructured formats. Your ATO prevention solution should be underpinned by a cleansing and curation process to parse and normalize the data, remove the noise, and get to what is truly relevant and actionable. Ensure the solution has the capability to eliminate unnecessary alerts by removing files that don't contain passwords or highly valuable PII. This process should also identify duplicate records, including how many times they've been seen in breaches and combo lists so you know the scale of particular employees' risk in the criminal underground.

Data enrichment offers contextual insights including the source, breach description, and the actual breached plaintext password to increase its actionability. A vendor's ability to crack collected passwords allows you to determine whether exposed credentials exactly match the in-use credentials for your employees.

Solutions that only offer data collection and put the burden of actionability on the enterprise don't add value to your security posture. Data quality and actionability are critical when it comes to preventing ATO and follow-on ransomware attacks. Having access to high-quality data that is clean, enriched, and analyzed enables you to correlate it to individual users across their multiple online personas to determine their true risk to your enterprise.

Automation

According to **The CISOs Report**, 41% of CISOs consider automation to be one of their top three security goals. Automated solutions prove valuable to security teams as they allow for predetermined actions to be approved or denied with a proactive lens on prevention and protection while minimizing the impact on busy teams.

With so much data available in the criminal underground, it's next to impossible for organizations to stay ahead of threats if their security teams are spending hours manually searching for, filtering, and sorting public breach data. Having the ability to automatically query data in a well-documented, standardized format is desirable because it saves internal teams time and effort, while ensuring protection from ATO.

Ideally, the solution should also offer integrations into existing workflows and applications, including directory services, SIEMs and other internal detection tools, allowing enterprises to automate password resets and make sure the right teams are armed to remediate malware-infected devices effectively.

Automating actions like alerts and password resets are the best way an ATO prevention solution can minimize delays. Ultimately, the faster an ATO prevention solution can detect compromised credentials, the faster the organization can take action.

Proof of Concept

To evaluate the quality and actionability of their data, you should request a "match rate test" and a proof of concept (POC) of the ATO prevention solution. Each vendor should be able to prove its results by sharing what data exists in their system (all time and collected over the last 12 months) matching your active users including overall match rate, actual credential matches, and plaintext passwords.

In these types of tests, it's easiest to narrow the field by choosing the vendor who provides the most results of the broadest variety and highest quality.

Support

An organization wanting enterprise-grade data security should not settle for anything less than enterprise-class support from its ATO prevention solution vendor. The vendor's customer support team should be available live during regular working hours and 24/7/365 for critical items, as well as offer rapid resolution and concise communication. Further, their customer success team should work in partnership with you, building a long-term relationship and ensuring positive experiences with the vendor and the solution.

In addition to dedicated customer support and success teams, the vendor should have service-level agreements (SLAs) in place that include a maximum of one business day to turn around high-priority requests, and 99.9% uptime for any hosted APIs or portals.

NIST Compliance

Enterprises face an ever-increasing list of regulatory **compliance** obligations, and the level of compliance can vary by industry. Your ATO prevention solution should help you meet the growing regulatory compliance needs of your organization, including National Institute of Standards and Technology (NIST) password guidelines that emphasize strong policies that reduce the risk of ATO:

- Ban "commonly-used, expected, or compromised" passwords, including passwords included in a previous breach corpus
- Require 8+ character minimum passwords
- Don't force arbitrary password resets because it leads to password reuse and rotation
- Limit the number of failed password attempts

SpyCloud

Employee ATO Prevention Solution Checklist

When evaluating ATO prevention solutions, use this quick guide to make sure the solution checks all the boxes:

Data Collection

- ☐ The solution incorporates both breach data and malware data.
- ☐ The solution monitors for compromised accounts for employees, partners, and suppliers.
- ☐ The vendor's data is constantly refreshed.
- ☐ The vendor adheres to ethical standards for data collection.

Malware Data

- ☐ The solution identifies managed and unmonitored malware-infected devices that are accessing your corporate network.
- ☐ The solution includes information siphoned from malware-infected machines, including compromised credentials and stolen web session cookies.
- ☐ The solution offers visibility into compromised third-party applications (i.e. SSO, VPN), providing a comprehensive post-infection remediation plan to negate entry points for ransomware.

Early Detection

- ☐ The solution identifies compromised credentials and stolen cookies early in the attack lifecycle.

Data Cleansing, Curation, and Enrichment

- ☐ The solution offers more than just a raw data feed.
- ☐ The vendor cleanses and curates the data to ensure it's relevant and actionable to power the solution.
- ☐ The vendor enriches the data with source information to provide more contextual insights.
- ☐ The vendor invests heavily in password cracking, making the data actionable and avoiding extraneous alerts.

Automation

- ☐ The solution automates exposed password alerts and reset capabilities.
- ☐ The solution integrates with other tools in your security framework.

Proof of Concept

- ☐ The vendor allows you to test data to ensure quality results.

Support

- ☐ The vendor offers comprehensive support through a dedicated team.
- ☐ The vendor's customer support team offers rapid resolution and concise communication.
- ☐ The support team is available for live support and also handles critical items 24/7/365.
- ☐ The vendor goes beyond customer support with a customer success team to ensure you see long-term value with the vendor and solution.

Compliance

- ☐ The solution helps meet government and industry regulatory standards and practices.

SpyCloud

Take Action Against ATO with SpyCloud

To truly protect against ATO that can lead to follow-on cyberattacks like ransomware, threat intelligence solutions simply aren't enough. With attacks stemming from criminals and also accidental or unwitting insider threats, ATO prevention solutions must be more comprehensive to include monitoring for compromised credentials and web session cookies.

SpyCloud's enterprise ATO prevention helps reduce your risk of a data breach by alerting you when your employees' credentials appear on the criminal underground, which in turn reduces entry points for criminals to deliver ransomware to your network.

By checking your employees' credentials and web session cookies against the largest repository of recaptured data in the industry, you can reset compromised authentication data before criminals have a chance to use it.

SpyCloud's enterprise solution checks all the boxes for ATO prevention:

- Take control of your human attack surface
- Shorten your exposure window with early notification of new exposures
- Prevent, detect, and reset compromised employee passwords
- Identify employees infected with infostealer malware
- Identify third-party vendors and suppliers with breach and malware exposures
- Protect board members and high-profile executives from account takeover
- Help meet regulatory compliance
- Enhance existing workflows for employee account takeover prevention

Why SpyCloud?

SpyCloud exists to disrupt the cycle of cybercrime, including account takeover, ransomware, and online fraud. Our solutions are powered by Cybercrime Analytics based upon the world's largest and most actionable collection of recaptured breach and malware data.

As a trusted partner to B2B organizations and consumer brands around the globe, including half of the Fortune 10, SpyCloud protects more than 3 billion accounts from cyberattacks perpetrated using stolen data. Hear from some of our happy customers:

> *We process 14,000 unique credentials obtained by SpyCloud per month – those are probably somewhere on the dark web or being shared across malware developers that are sharing the data sets or selling it.*
>
> – Atlassian Principal Security Intelligence Analyst, Niels Heijmans

> *Having a certain level of automation is important. It's super flexible, efficient and easy, so it gives our team the opportunity to spend time on other priorities rather than manual tasks related to monitoring for and remediating compromised credentials.*
>
> – EUROCONTROL Cyber Security Program Manager, Patrick Mana

> *The SpyCloud data is more specific and actionable than any other solution we've found, giving us employee, account-level and source detail we need to mitigate the threat and take immediate action.*
>
> – Chemical Company Director of Global IT Infrastructure

Learn how to protect employees, partners, and VIPs from ATO at **spycloud.com.**

SpyCloud