SpyCloud

Case Study

Atlassian Protects Its Enterprise And Its Customers While Saving Time With Automated ATO Prevention From SpyCloud

Overview

Atlassian's team collaboration and productivity software helps teams organize, discuss, and complete shared work. Teams at more than 225,000 customers, across large and small organizations – including Bank of America, Redfin, NASA, Verizon, and Dropbox – use Atlassian's project tracking, content creation and sharing, and service management products to work better together and deliver quality results on time.

Challenge

Due to the increasing number of industry breaches, Atlassian sought a more efficient and proactive approach to addressing potential future incidents, without the burden of collecting, curating and validating exposed data on their own.

Solution

The company selected SpyCloud Employee ATO Prevention to proactively protect their 7,000 employees from the consequences of ATO, as well as SpyCloud Consumer ATO Prevention to detect potentially compromised customer accounts.

Result

Atlassian protects its employees and customers from cyberattacks with SpyCloud's solutions, reducing resource hours spent researching Atlassian's potential involvement in public breaches and securing its brand reputation.

Software Company Atlassian Protects Hundreds of Thousands of Corporate and Customer Accounts from ATO

Previously, Atlassian lacked visibility of the exposed credentials of their employees. Given the challenge of staying ahead of the ever-evolving threat landscape, they realized the need to proactively protect themselves against potential account takeover (ATO) attacks involving data stolen in third-party breaches. Atlassian prioritizes security and sought a reliable, scalable solution, allowing them to provide customers with the confidence that their corporate resources are secure.

Initially, Atlassian took a manual approach to addressing public third-party data breaches. For example, when an industry breach was made public, members of the security team would have to comb through the breach data to see if Atlassian was involved and would pre-process the dataset to make it actionable, then contact any impacted employees to remedy the issue. This manual process would take four or more hours per breach, and with breaches being made public seemingly every day, the team was spending too much time trying to keep up.

“We had to do everything manually before, and the whole process took a lot of time,” said Niels Heijmans, Principal Security Intelligence Analyst at Atlassian.

They knew there had to be a better way and started looking into different options to help address their challenge. During their search, Atlassian evaluated vendors and found that many vendors were opaque in their data sources and collection time; it wasn’t clear where the data came from, or how old it was, or if the data set had already been actioned by Atlassian’s security team.

Transparency, the ability to quickly recapture data within days of a breach or malware infection occurring, and automated solutions made SpyCloud stand out from the competition. SpyCloud’s cyber analytics engine that transforms recaptured data from the criminal underground to make it truly actionable, coupled with its ability to recapture breached data earlier in the attack timeline, helped Atlassian solidify its decision to implement SpyCloud’s Employee ATO Prevention solution.

It took Atlassian a mere two weeks to fully automate the credential collection, verification and rotation process with SpyCloud’s API for both employees and customers, and the solution’s automation resulted in zero maintenance time. Atlassian is now alerted of any corporate credentials exposed in third-party breaches, and that notification triggers an automated ticket through their security operations center to action the issue, prompting the employee to reset their password.

In addition to monitoring the use of exposed credentials, SpyCloud’s solutions help Atlassian identify when employees or suppliers accessing Atlassian services on personal devices are infected with malware, an incredibly difficult cyber threat to detect on devices outside of corporate control. The security team is then able to reach out to the infected user and help them remedy the issue by providing the infection source information and steps to remove the malware.

“It puts your organization at risk if a personal device is being used to log in with corporate credentials,” Niels said. “To combat this, SpyCloud offers unique data richness and transparency that goes beyond just finding compromised credentials. SpyCloud can tell you what user is infected with malware and for how long, which makes a difference in your incident response.”

With the success of protecting employee accounts, Atlassian looked to fulfill their customer-focused corporate values by also protecting customer accounts with SpyCloud Consumer ATO Prevention. Many of Atlassian's customers use their software to enable mission-critical tools, so a disruption or attack could have significant impacts, such as halting financial transactions or delaying critical medical decisions. Malicious actors gaining access to these types of business processes could have detrimental results, and Atlassian doesn't stand for that. Protecting customers is at the core of how Atlassian operates.

Results

Automated Solution Protects Employees and Enables Time Savings

Atlassian no longer spends hours manually processing public breaches. SpyCloud's API allows Atlassian to quickly detect compromised credentials and remediate them automatically with SpyCloud's fresh, actionable breach data and malware bot logs at their fingertips.

"Because the solution is fully automated, we are able to process 14,000 unique credentials per month. This scalability allows us to use our resources efficiently," Niels said.

Extending ATO Prevention to Malware-Infected Users

Once Atlassian saw the results of how they were able to protect employee accounts and prevent ATO, they decided to explore how SpyCloud could help them support their corporate value to honor their customers. SpyCloud identified credentials from Atlassian users who had logged into their accounts using malware-infected personal devices. Atlassian tested 55,000 of these recovered logins against their consumer database over a three-month period and discovered that 70% matched their current Atlassian passwords. They were able to reset passwords for these users and secure their accounts.

Today, Atlassian uses SpyCloud data to protect accounts for teams at over 225,000 customers and secure their mission-critical business processes.

> “Because the solution is fully automated, we are able to process 14,000 unique credentials per month. This scalability allows us to use our resources efficiently.”
>
> - Niels Heijmans,
> Principal Security Intelligence Analyst

Ease of Integration for Automation

Atlassian was able to easily integrate SpyCloud's solutions into its security framework to maximize the value of its cybersecurity investments. SpyCloud's solutions are integrated with AWS Lambdas, Jira, Splunk, and Atlassian's security, orchestration, automation, and response (SOAR) solution to enable fully automated workflows that protect employee and customer accounts.

Ongoing Support Enhances Vendor Relationship

SpyCloud's dedicated customer success team ensures Atlassian's satisfaction with its solutions and maintains an open communication cadence to support their needs. Whenever Atlassian requests feature updates or additional recently-recaptured data, SpyCloud's team is quick to go the extra mile.

"Whenever I have questions or feedback, the SpyCloud team is always willing to help," Niels shared. "They're happy to have discussions about the products because we're investing in them and finding value in them. And when I have ideas on improvements, there's always someone from SpyCloud who will listen and help us."

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.

Enterprise Protection

Prevent account takeover that can lead to ransomware.

Learn More

Consumer Protection

Combat account takeover and online fraud.

Learn More

Investigations

Unmask criminals attempting to harm your business.

Learn More

Data Partnerships

Enhance your solution with SpyCloud's data.

Learn More

Learn more at spycloud.com