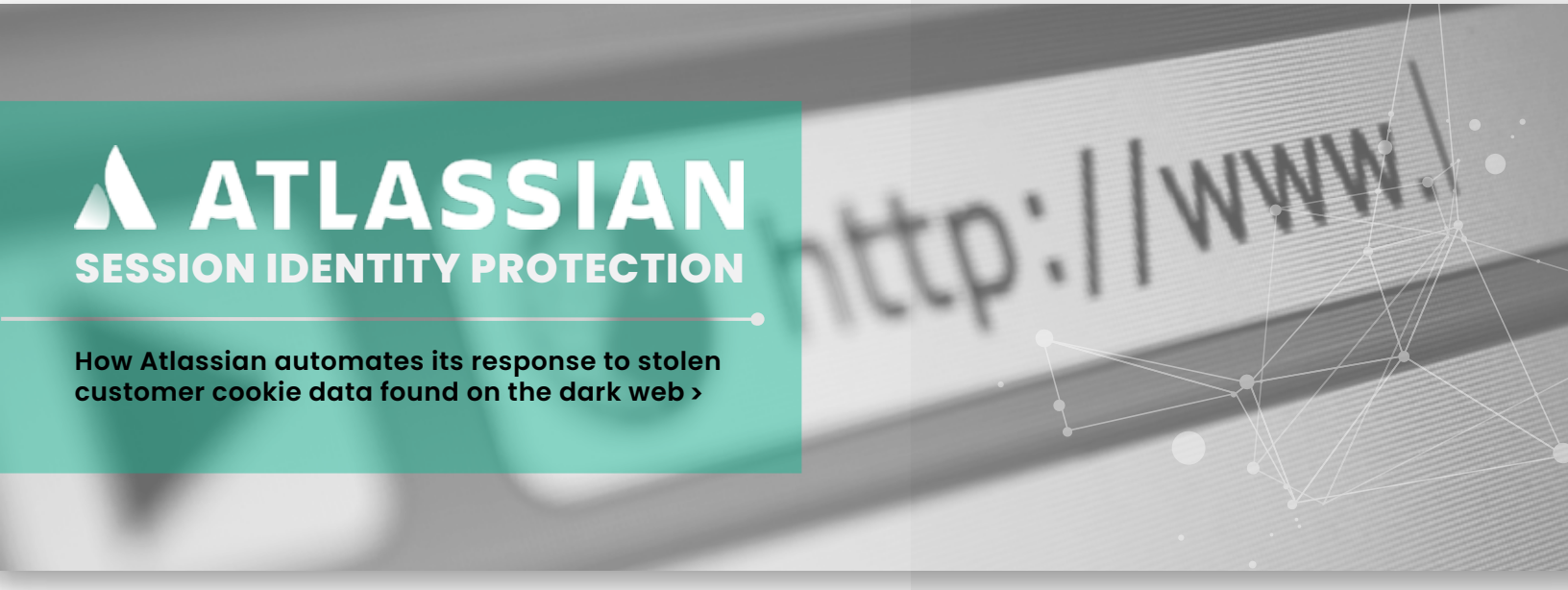
SpyCloud

CASE STUDY



ATLASSIAN
SESSION IDENTITY PROTECTION

How Atlassian automates its response to stolen customer cookie data found on the dark web ›

Atlassian's team collaboration and productivity software, which includes Jira, Confluence, and Trello, helps teams around the globe get work done. More than 250,000 customers across large and small organizations – including Bank of America, Redfin, NASA, Verizon, and Dropbox – use Atlassian's products.

With so many customers accessing its tools daily, how does a company like Atlassian stay ahead of evolving threats that can impact their business? For Niels Heijmans, Principal Security Intelligence Analyst, his approach to consumer risk protection took a happy turn three years ago when he came across SpyCloud's account takeover prevention solutions.

The Atlassian team started by implementing SpyCloud **Customer Account Takeover Prevention** to gain visibility into their customers' breach exposure and stolen credentials to protect against traditional account takeover. Now, a few years later, they're tackling the next generation of attacks, too, by adopting SpyCloud's **Session Identity Protection** to identify exposed session cookies and invalidate them before criminals can use them for session hijacking.

THE CHALLENGE

Today, malware-infected customers pose one of the highest risks to businesses – and businesses often have the least visibility into this particular problem. As cybercriminals increasingly leverage stolen cookie data exfiltrated by malware, Atlassian needed a scalable way to identify exposures and automatically invalidate compromised sessions to protect its customers.

THE SOLUTION

With **Session Identity Protection**, Atlassian now protects its more than 250K cloud customer accounts from session hijacking, automatically, with zero operational overhead.

SpyCloud

CASE STUDY

ADDRESSING THE NEXT BIG THREAT:
SESSION HIJACKING WITH STOLEN CUSTOMER COOKIES

A **stolen cookie from a web session**, when put in the wrong hands, can allow bad actors to bypass all forms of authentication – from passwords to multi-factor authentication (MFA) and even passkeys – to assume the access of an authenticated user. Session hijacking originates from the takeover (or "hijack") of an active browser or application session using a stolen, still-valid authentication cookie where the criminal appears as a verified clone of a legitimate customer.

Criminals leverage these active sessions to gain access to customer accounts and steal sensitive data. Last year alone, SpyCloud researchers recaptured 22 billion stolen cookies from malware records, which indicates criminals are increasingly stealing, buying, and trading fresh cookie data that comes with a high likelihood of account takeover success.

"Almost everyone is aware that bad actors are stealing passwords. But I don't think a lot of people realize that MFA alone isn't enough to protect users against account takeovers. Session hijacking is still very new – but for Atlassian, it's become high on our radars. As long as a cookie stays valid, the gate to that consumer's account remains wide open."

Today, **39%** of organizations don't terminate session cookies at the sign of exposure. Atlassian, with the help of Session Identity Protection, is ahead of the curve. Niels has already gone to work, leveraging automation to invalidate 41,000 stolen authentication session cookies to proactively protect almost 38,000+ customer accounts in 2023.

"Our customers are everything to us. We have a core value around protecting them at all costs. So by adding Session Identity Protection to the rest of our SpyCloud instance, we basically get rid of the threat of account takeover, whatever the source – which means our customers and their data are safe."

ATLASSIAN'S OUTCOMES WITH SPYCLOUD
BY THE NUMBERS

Customer organizations identified as having **exposed session cookies**	**8.5k**
Authentication cookies **invalidated**	**41k**
Individual user accounts **protected from follow-on attacks**	**38k**
Saved per month due to **detection and response efficiencies**	**160 hours**

**data represents an 11-month time period*

EARLY STOLEN COOKIE DETECTION MEANS NO MORE PANIC, NO MORE FIRE DRILLS

Because its user base is so large, the Atlassian security team is used to frequent notifications and alerts about data exposure concerns. In the past, they didn't always have answers, and the team had to manually verify problems, do lengthy investigations, and then determine an appropriate response. The team was expending extra resources in repetitive detection and response work. With SpyCloud, Atlassian's analysts save 160 hours per month of repetitive work – no longer needing to manually parse, validate, and deactivate sessions due to higher-fidelity alerts and automation workflows.

Additionally, because SpyCloud continuously ingests and analyzes stolen cookie data from the deepest layers of the darknet daily, all that data is recaptured very early in the attack timeline. The fresh data insights are made available to Atlassian through Session Identity Protection. Niels says, ***"Now, when we're notified of a concern by another team or tool internally, it's just a quick check for us. And odds are, we already acted on that data three months ago, when SpyCloud found it for us first."***

HOW IT ALL WORKS

Atlassian integrated SpyCloud with their existing tool stack to create an automated workflow for invalidating stolen session cookies. Says Niels, ***"SpyCloud is actually the benchmark of success for all of our third-party integrations. The integrations with our SIEM platform and ticketing tools are so seamless that we use them as a comparison point across our entire tool stack."***

For Atlassian, the setup and integration process was simple to deploy, and is serverless with zero required maintenance. It's very much a 'set it and forget it' scenario for Niels' team. Here's what it looks like:

1. Pull enriched Session Identity Protection data via SpyCloud's API into existing service.
2. Atlassian's automated workflow automatically revokes all active sessions on every device for an identified, exposed user.
3. Get back to other work, with the confidence that customers are being continuously protected.

Atlassian invalidates all known compromised sessions for impacted users on the back-end automatically, but they've also given their customers **added visibility into the problem** and offer additional countermeasures directly via their in-app Credential Invalidator functionality. Now, when Atlassian customers reset a forgotten password or proactively change a password, they also automatically get logged out of the active session used to change the password. Customers who have admin credentials can also configure the idle session timeout or reset all sessions for a configured authentication policy.

SpyCloud

CASE STUDY

FAST PROTECTION FOR THREAT VECTORS, NEW AND OLD

As cybercriminals evolve their account takeover tactics beyond traditional use of credentials, Atlassian has peace of mind knowing they are keeping pace with the next generation of threats. By leveraging SpyCloud Session Identity Protection, Niels feels confident that they are sticking to their core company value of protecting their customers.

"With Session Identity Protection, we're protecting our customers as proactively as possible in today's threat landscape. SpyCloud gives us the speed we need to act fast – before an attacker has the chance to abuse stolen cookies. The impact has been huge for us."

ABOUT SPYCLOUD SESSION IDENTITY PROTECTION

SpyCloud identifies infected consumers and monitors malware logs for compromised session cookies tied to your application that can be used for session hijacking – alerting your business so you can act quickly to protect these high-risk accounts.

Learn more at spycloud.com.

KEY BENEFITS

- Real-time, high-fidelity alerts
- Definitive evidence of exposures
- Automated workflows
- Easy integrations with existing tools
- Significant resource and time savings