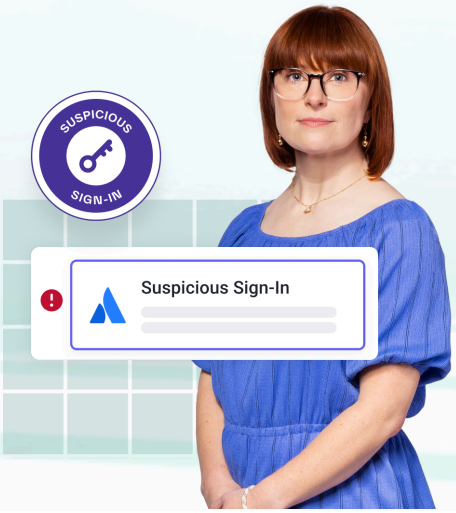
Atlassian Jira Account Takeover Protection

Analyze human behavior to secure your Jira projects.



Unauthorized access to Jira can be incredibly damaging

Tickets in Jira are likely to hold proprietary or otherwise confidential information about product enhancements, bugs, and new product development—presenting an attractive target for attackers to exploit.

Attackers continually target Atlassian

Nation-state threat groups have attempted to compromise Atlassian. Often, this is through credential compromise or social engineering tactics, with the goal of preying on human vulnerability to gain access to sensitive data.

Security teams lack visibility into Atlassian apps like Jira

While IT and security often have some amount of visibility into Atlassian, organizations note a lack of behavioral monitoring when it comes to who is accessing Atlassian apps such as Jira.

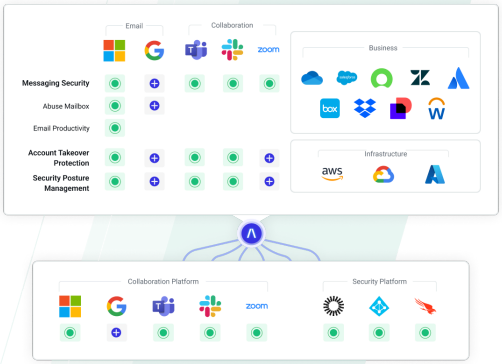
Extend Abnormal Protection Across All Platforms

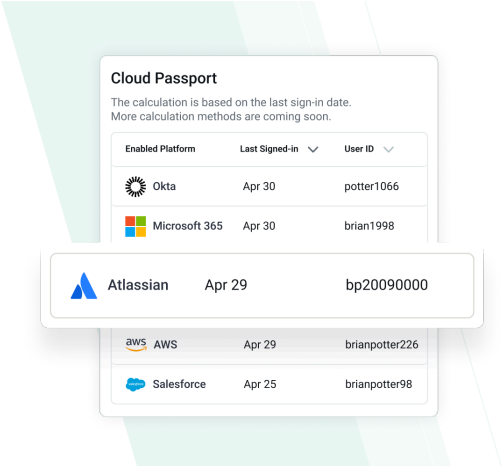
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. Of all the apps normally targeted in a breach, Atlassian's Jira has proven itself to be a regular target of sophisticated threat actors. This isn't surprising as Jira is typically the primary project management platform for proprietary software development. To stop these attacks, security teams need an extensible platform that provides consistent visibility and security automation across not only Jira but all cloud apps and services for holistic, higher fidelity detection. Abnormal provides that platform.

How Abnormal Secures Jira

Simple API Integration

Connect directly to Atlassian Access with Abnormal's cloud-native API architecture—automatically ingesting and normalizing sign-in signals related to every human in your organization that accesses the Jira platform.



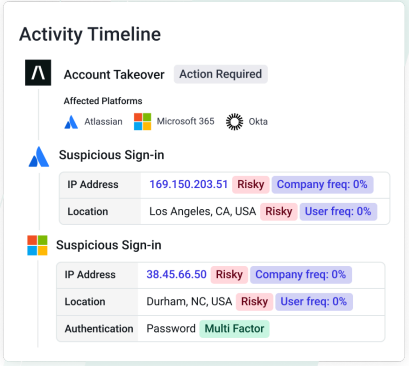


Continuous Monitoring of Human Behavior in Jira

Build dynamic behavioral profiles for every human accessing Jira, develop a behavioral baseline, then automatically detect and analyze anomalous deviations from that baseline.

AI Account Takeover and Response

When suspicious activity occurs, Abnormal Human Behavior AI automatically triggers the creation of a contextual Case populated with Jira activity. Each Case is scored based on detection confidence and continually enriched with new activity across all platforms integrated with Abnormal.



Try Abnormal Today

See how Abnormal can keep attacks out of your cloud email and connected platforms. Integrate in minutes via API.

abnormalsecurity.com/risk →

Abnormal