Asana Account Takeover Protection

Analyze human behavior to protect your projects and plans.

Project management apps house proprietary data

Platforms like Asana often contain links to sensitive sales and marketing documents. Administration and protection of these platforms are typically handled by go-to-market operations, not the security team.

Third-party access invites extra, often unseen risks

Project management platforms allow third-party access to enable collaboration with a variety of partners. While this boosts productivity and creativity, it invites risks in the event a partner becomes compromised.

Asana security is strong but is only one layer

Asana takes an active role in detecting malicious activity on its platform. However, if a user appears legitimate in Asana but exhibits suspicious activity elsewhere, cross-platform visibility is required to detect this.

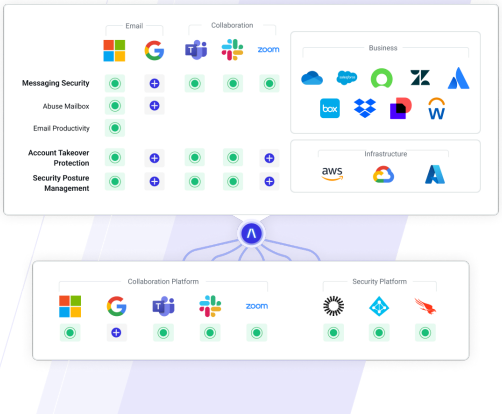
Extend Abnormal Protection Across All Platforms

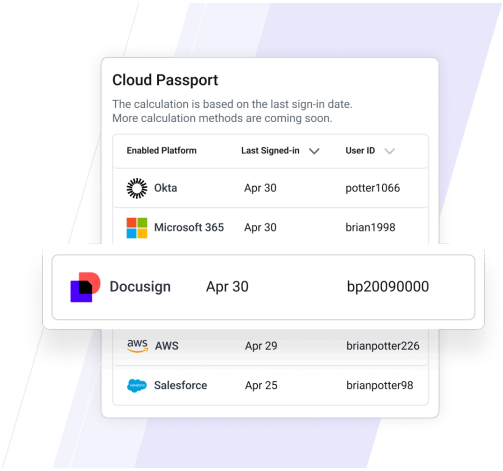
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for security teams. Project management platforms like Asana are prime targets, as attackers can easily blend in amongst internal and external collaborators with access to the platform. To detect these attackers, security teams need an extensible platform that provides consistent visibility and security automation across not only Asana but all cloud apps for holistic, higher-fidelity detection. Abnormal provides that platform.

How Abnormal Secures Asana

Simple API Integration

Connect directly to Asana with Abnormal's cloud-native API architecture. Integrate in minutes to gain visibility into every human accessing and collaborating in Asana.



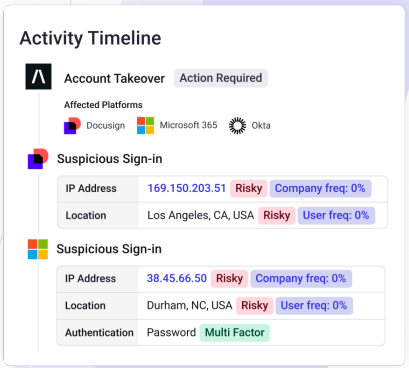


Continuous Monitoring of Human Behavior in Asana

Automatically learn normal Asana access behavior, develop a behavioral baseline, and detect anomalous events indicative of account compromise.

AI Account Takeover and Response

When suspicious activity occurs, Abnormal's Human Behavior AI automatically triggers the creation of a contextual Case populated with Asana 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