Zendesk Account Takeover Protection

Analyze human behavior to secure customer engagement in Zendesk.

Helpdesk platforms considered a Top 5 concern

In a recent survey, when asked which platforms security leaders were most concerned would become targets in a breach attempt, CRMs and Helpdesk platforms like Zendesk were noted in the top 5.

Sensitive data in Zendesk is attractive to attackers

Risks to customer engagement platforms like Zendesk aren't hypothetical. Sophisticated threat groups attempt to compromise and expose customer data in these platforms with advanced social engineering and phishing techniques.

Security teams lack visibility into platforms like Zendesk

As the Zendesk platform is normally owned by the customer support organization, security teams often lack the necessary visibility and access to effectively monitor and protect the platform.

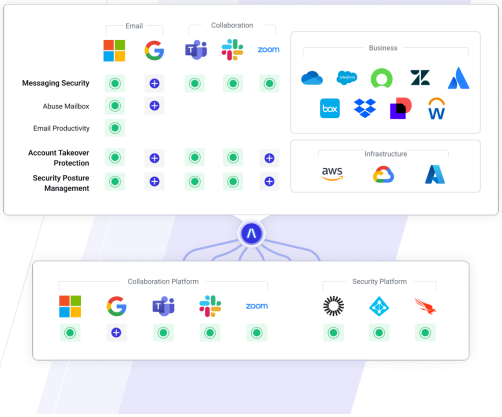
Extend Abnormal Protection Across All Platforms

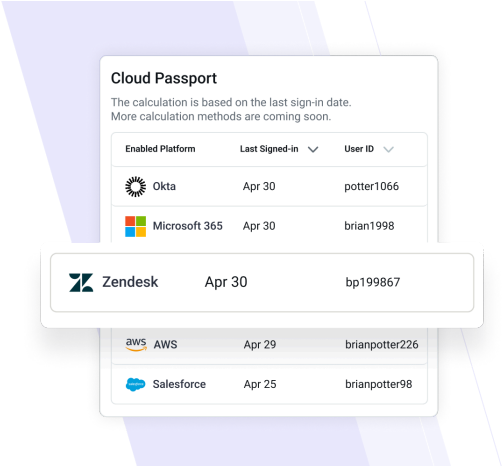
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. Customer data is some of the most critical to protect as any breach that impacts customer privacy can cause financial *and* reputational damage. To stop attackers from breaching customer support platforms like Zendesk, security teams need an extensible platform that provides consistent visibility and security automation across not only the Zendesk platform but all cloud apps and services for holistic, higher fidelity detection. Abnormal provides that platform.

How Abnormal Secures Zendesk

Simple API Integration

Connect directly to Zendesk with Abnormal's cloud-native API architecture—automatically ingesting and normalizing sign-in telemetry for every human in your organization who is accessing Zendesk.



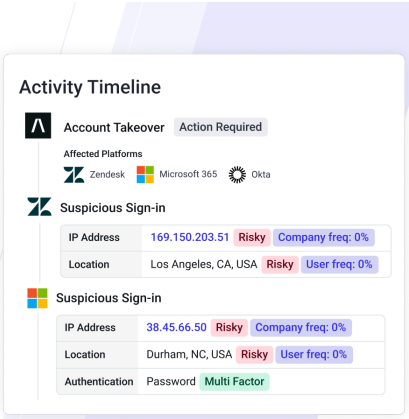


Continuous Monitoring of Human Behavior in Zendesk

Build dynamic behavioral profiles for every human in your organization that uses Zendesk, develop a behavioral baseline and automatically detect anomalous activities that deviate from that baseline for further analysis.

AI Account Takeover and Response

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