Abnormal Security for Slack

Analyze human behavior to secure Slack collaboration.

Slack enables collaboration but invites risk

Slack boasts 10M+ active users. The amount of sensitive and confidential data shared between those users is incalculable and often in public company channels.

Slack is used as an entry point by attackers

Threat actors are targeting enterprise Slack tenants as either an entry point—often via session hijacking—or as a means to move laterally via social engineering messages sent to IT to escalate privileges or reset passwords.

Security lacks visibility into Slack sign-ins and settings

1 in 3 security practitioners note that they lack visibility into SaaS security settings. This creates a blindspot wherein an attacker can access Slack and gain excess privileges without triggering a security response.

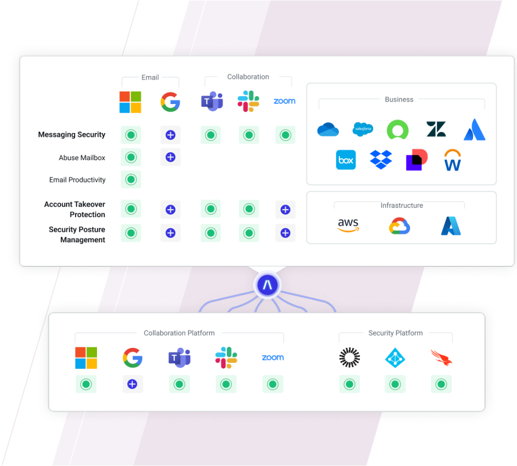
Extend Abnormal Protection Across All Platforms

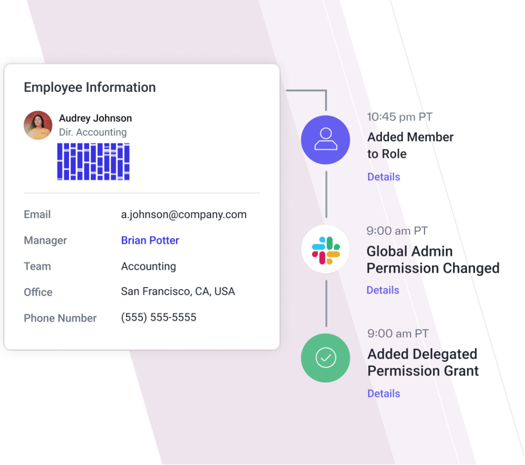
Humans are the biggest vulnerability for any organization, and while email is the primary way those humans are targeted, collaboration apps like Slack present significant risk. Slack has been a centerpiece in many of the most recent and highest profile cloud breaches, being used as the entry point, a way to execute chat phishing attacks, as a means to move laterally, or in some cases, a way to taunt the victim's organization. To stop would-be Slack hacks, security teams need an extensible platform that provides consistent visibility and security automation across not only Slack but all cloud applications and infrastructure services for holistic, higher fidelity threat detection. Abnormal provides that platform.

How Abnormal Secures Slack

Simple API Integration to Stop Malicious Messages

Connect directly to Slack with Abnormal's cloud-native API architecture—automatically ingesting and normalizing access, privilege, and messaging data. Abnormal analyzes all Slack messages for malicious URLs and immediately notifies the SOC team once detected.





Employee Information

Audrey Johnson
Dir. Accounting

Email	a.johnson@company.com
Manager	Brian Potter
Team	Accounting
Office	San Francisco, CA, USA
Phone Number	(555) 555-5555

10:45 pm PT
Added Member to Role
Details

9:00 am PT
Global Admin Permission Changed
Details

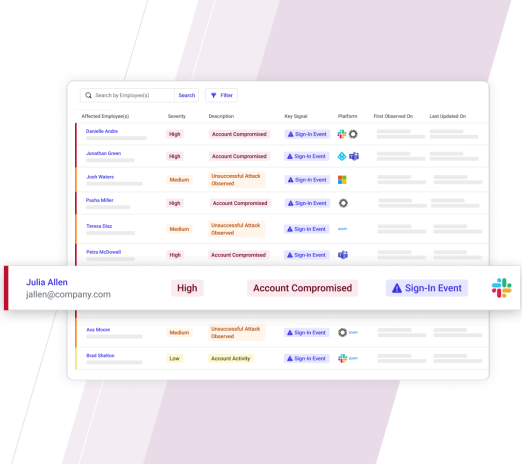
9:00 am PT
Added Delegated Permission Grant
Details

Continuous Monitoring of Slack Privileges and Human Behavior

Automatically learn and dynamically monitor Slack access patterns and user privileges. Abnormal builds a behavioral baseline for every human in Slack, notifying administrators when anomalous activity occurs or when user privileges are suddenly elevated.

AI Account Takeover and Response

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



Search by Employee(s) | Search | Filter

Affected Employee(s)	Severity	Description	Key Signal	Platform	First Observed On	Last Updated On
Danielle Andre	High	Account Compromised	Sign-In Event			
Jonathan Green	High	Account Compromised	Sign-In Event			
Josh Waters	Medium	Unsuccessful Attack Observed	Sign-In Event			
Pasha Miller	High	Account Compromised	Sign-In Event			
Teresa Diaz	Medium	Unsuccessful Attack Observed	Sign-In Event	zoom		
Petra McDowell	High	Account Compromised	Sign-In Event			
Julia Allen jallen@company.com	High	Account Compromised	Sign-In Event			
Ava Moore	Medium	Unsuccessful Attack Observed	Sign-In Event	zoom		
Brad Shelton	Low	Account Activity	Sign-In Event	zoom		

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