Abnormal Security for Zoom

Analyze human behavior to protect Zoom conferencing.

Zoom Enables Remote Work but Invites Real Risk

Business gets done on Zoom, and often Zoom recordings and transcripts hold confidential conversations that look like gold to would-be threat actors.

Video-Based Attacks Are Making the News

While seemingly science fiction only a few years ago, deepfake attacks are a present danger. Recently, attackers are using deepfake audio and video to commit fraud and attempt to steal information.

Security Lacks Visibility Into Zoom 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 Zoom and gain excess privileges without triggering a security response.

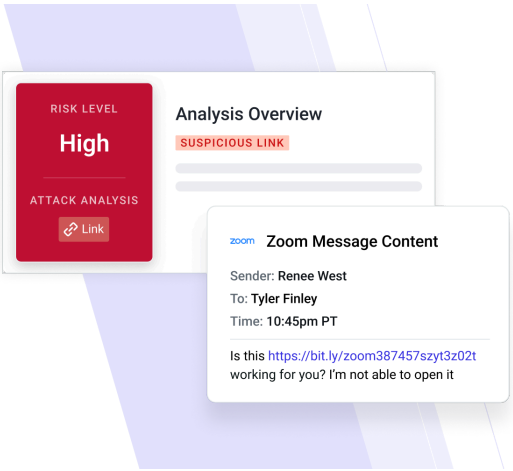
Extend Abnormal Protection Across All Platforms

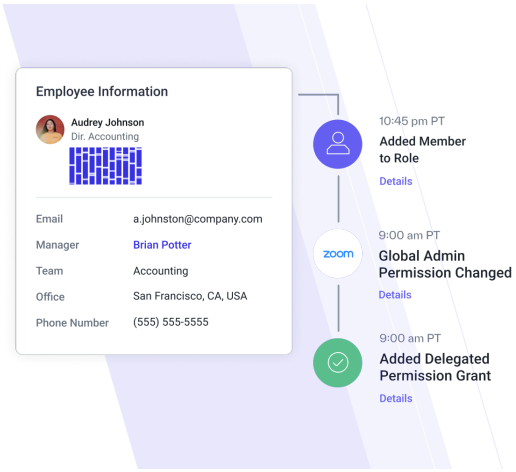
Humans are the biggest vulnerability for any organization, and while email is the primary way those humans are targeted, collaboration apps like Zoom present significant risk. Zoom has been a target of amateur and sophisticated threat actors alike since it became a cornerstone of remote working culture—and breaches involving conferencing tools like Zoom continue to proliferate. To stop Zoom attacks, security teams need an extensible platform that provides consistent visibility and security automation across not only Zoom but all cloud applications and infrastructure services for holistic, higher fidelity detection. Abnormal provides that platform.

How Abnormal Secures Zoom

Detect Malicious Messages

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



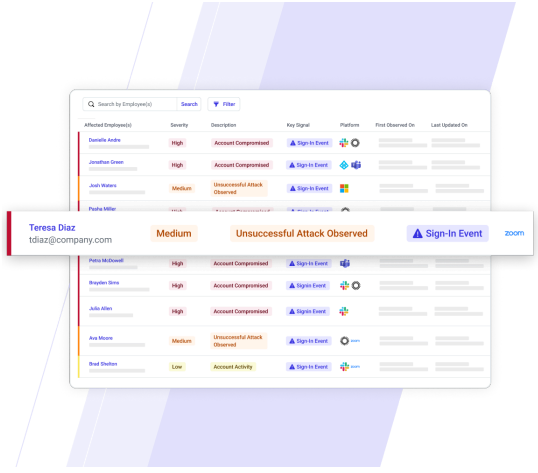


Continuous Monitoring of Zoom Privileges and Human Behavior

Automatically learn and dynamically monitor how humans in your organization are accessing Zoom and when user privileges change. Abnormal builds a behavioral baseline for every human in Zoom, 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 Zoom 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