Abnormal

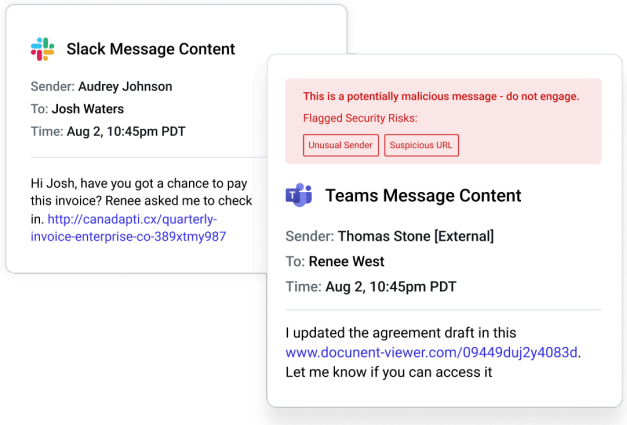
Messaging Security

Available as an Add-On to Abnormal Inbound Email Security

Detect malicious message content across collaboration apps with autonomous AI.

Use of collaboration apps is on the rise as employees use them to work and communicate in a remote-first world. Attackers are taking advantage, moving laterally from email to these alternative communication methods to run their scams.

Unfortunately, many of these enterprise platforms do not come equipped with threat detection—particularly the ability to detect malicious message content. This means a compromised internal user or external collaborator with access can execute a phishing attack via chat that is hard to detect and even harder to stop.



Messaging Security prevents the spread of malicious content.

Uses autonomous AI to inspect every message on Slack, Microsoft Teams, and Zoom, scanning for malicious URLs in threads, groups, channels, and chats. Once surfaced, security teams can take action to mitigate the threat and investigate the account that originated the message.

Bolsters investigation into advanced attacks across platforms by logging malicious collaboration app messages and email attacks in the same Threat Log. This enables a greater understanding of the attack scope and a more comprehensive overview of the impact to your cloud communications.

Scans messages from external collaborators with access to workspaces and meeting rooms to uncover cases of potential partner and vendor compromise and protect platforms against third-party risk.

The Abnormal Advantage at a Glance

Gives expansive visibility. Compromised email credentials often mean compromised collaboration app credentials as well. Abnormal provides visibility into malicious messages across the spectrum of platforms to keep all communications secure.

Deepens threat investigation. By combining suspicious emails and malicious messages in one Threat Log, security teams can follow the pathway of a specific attacker or uncover the impact of an account takeover detected by Account Takeover Protection.

Stops insider and external threats. Abnormal protects against internal phishing attempts through chat apps from both malicious insiders and compromised external accounts. This protects your employees, your partners, and your vendors by quickly detecting when a user has been compromised.

See Abnormal in Action. **Request a Demo.**

abnormalsecurity.com →