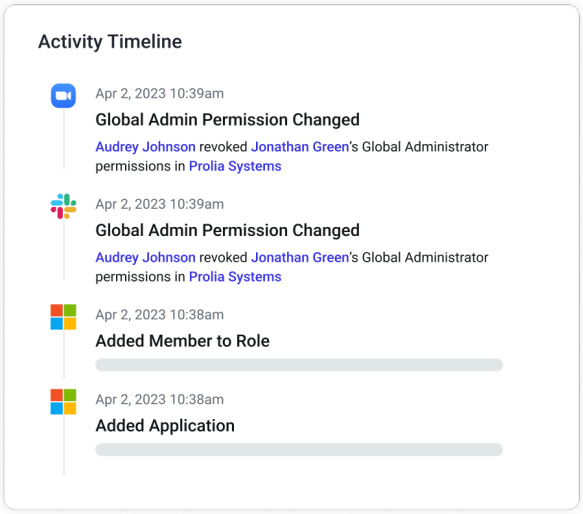
Abnormal

SaaS Security Posture Management

Available as an Add-On to Abnormal Inbound Email Security
Monitor high-impact changes to user privileges across SaaS applications.

Security teams lack visibility into user privileges across SaaS applications. Who has admin access on Slack? Who can see all of the recordings in Zoom?

These blindspots open the door for attackers looking to compromise privileged accounts and use them to move laterally throughout the organization. Beyond outright threats, privilege misconfiguration that unintentionally gives users excessive permissions and access could lead to privacy and compliance risks.



SaaS Security Posture Management helps you understand user privileges across your SaaS applications.

Dynamically monitors for user privilege changes across Slack and Zoom, including timestamps and users involved—determining which changes may present a risk and need further investigation.

Provides a before-and-after view of each change—giving insight into what the normal state looked like and how a given application has been affected. The platform includes links to the PeopleBase profiles for users involved and next steps to aid in investigation.

Supports remediation with a simple workflow to acknowledge each change for cross-team accountability. Admins can also schedule email notifications and export events to the SIEM so that high-risk changes can be actioned quickly.

The Abnormal Advantage at a Glance

Enables expansive visibility. By dynamically monitoring for and surfacing new privilege changes across all SaaS apps and email platforms, Abnormal gives greater visibility into configuration risks across your inter-connected cloud communications ecosystem.

Gives contextual insights. Abnormal helps to cut down on notification noise—not only by surfacing high-impact changes, but also by helping security practitioners understand the implications of the change.

Provides remediation support. Boost security collaboration through a shared acknowledgment workflow and ensure events are shared with the SIEM to enrich ongoing investigations with contextualized privilege change insights.