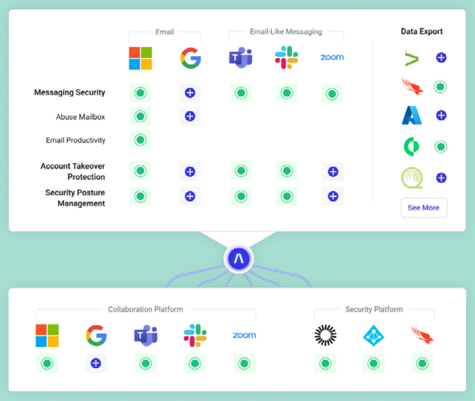
Abnormal

Abnormal API Integrations: Detect & Respond Faster

Integrate with your security tools to centralize insights and speed up remediation.



Both the volume and the sophistication of email attacks are increasing rapidly. This trend means security teams need to be able to detect, triage, and remediate threats more quickly.

Unfortunately for many organizations, detection and remediation often occur in different places. In fact, security teams consistently struggle to bridge data gaps and reduce silos, with 74% of organizations citing the lack of visibility into applications and data assets as an impediment to cyber resiliency. Security teams are further hindered by the growing cybersecurity skills gap, which increases the need for more integrated and automated workflows.

Abnormal is designed to break down email security silos and integrate seamlessly into existing workflows. The API-based architecture allows security teams to view email security data in the context of other security operations tools and extend Abnormal detection data to other critical platforms.

Leveraging a RESTful API, these integrations enable security teams to view, respond to, and report on Abnormal behavioral insights in existing workflows managed within other security and IT solutions.

3.4 Million workers constitute the current cybersecurity skills gap.

40% of security analysts' time is spent on automatable tasks.

20+ tools used to investigate and respond to incidents in 40% of organizations.

87% of security teams cite the inability to reduce silos as a barrier to cyber resiliency.

Abnormal provides the solution.

Connect Abnormal to other security platforms, including SIEM, SOAR, EDR/XDR, IAM, and ITSM solutions, via a RESTful API.

Connect the dots and monitor threats across your organization's entire attack surface.

Analyze Abnormal email threat detections within the context of other security events from across the organization.

Orchestrate and automate downstream workflows for incident management based on Abnormal insights.

Abnormal Behavioral Insights

Technology integrations enable security teams to easily query the Abnormal API and extract relevant data from various Abnormal categories, such as Threat Log or Abnormal Cases.

Details may include:

- Email attack type and vector
- Threat status and severity
- Impacted employees
- Sender attributes
- Remediation information

See Abnormal in Action. **Request a Demo.** abnormalsecurity.com ⟶

API Ingest

Cloud Email

Microsoft 365

Google

Cloud Collaboration

zoom

Microsoft Teams

slack

IAM

okta

Azure Active Directory

EDR/XDR

CROWDSTRIKE *

SOAR

splunk>

RAPID7

torq

Azure Sentinel

CORTEX XSOAR BY PALO ALTO NETWORKS

SIEM

splunk>

IBM

QRadar

Hunters.

sumo logic

revelstoke

Chronicle

ITSM

servicenow

* bi-directional integration

See Abnormal in Action. **Request a Demo.** abnormalsecurity.com ⟶