Abnormal

Abnormal AI Product Privacy Guide

What Service Does Abnormal Provide?

Abnormal helps our customers protect their Microsoft Office 365 and Google Workspace environments with a cloud-native software-as-a-service email security platform (the Service). The Service uses traditional email security approaches paired with AI/ML detection techniques to identify and remediate targeted phishing attacks and Business Email Compromise (BEC), and offers three core capabilities:

Email Protection

The Service's protection capability addresses BEC attacks as well as the full range of targeted and socially engineered email attacks with an AI/ML decision engine that secures customers' business communications.

Email Account Compromise Detection

The email account compromise detection feature set is designed to enable customers to detect account takeover (ATO) attacks by leveraging the Service's AI/ML signal analysis engine to augment traditional detection methods.

Incident Response Automation

The incident response automation functionality supported by the Service enables security operation teams to respond quickly and proactively to the attacks the Service detects by leveraging automation

Personal Data Processing

Similar to traditional email security solutions such as the "secure email gateway" or "SEG", Abnormal AI processes multiple data elements within a customer's email system to provide the Service. Because the Service addresses corporate email security issues like BEC and ATO, and because people communicate via those email systems, the Service processes personal data.

Abnormal follows key privacy and data protection principles of data minimization and processing purpose limitations, as well as maintenance of security, integrity, and confidentiality to ensure personal data is appropriately protected in alignment with global privacy frameworks. The Service is designed to process only the personal data necessary to enable the Service to perform its functions, and the personal data is used only to deliver the Service to each customer.

Certain components of the Service are delivered to Abnormal AI's customers in a federated model so that these collective intelligence and data sets can enhance protection for all Abnormal AI customers. Data collected and processed to create the Service's Vendor and Threat Intelligence Data feeds are produced from attacker signals that contain limited amounts of personal data. Because attackers send malicious emails to customers, these feeds are produced with appropriate privacy-by-design processing methods to ensure that any customer-identifying personal information is removed, de-identified to the extent possible when used for such purposes.

What Data Types Does the Service Process and Why?

The Service processes and stores only the minimum amount of data, including personal data, necessary to enable the Service to perform its functions. The Service does not store, persist, or retain the contents of or attachments to emails that the Service identifies as non-malicious using its AI/ML models; rather, only email content and attachments (if any) that the Service identifies as malicious are transferred to the Service's cloud-based servers for further processing and analysis.

For a comprehensive breakdown of the data types processed by each product and their associated retention periods, please refer to our Privacy Data Sheet, available in the Security Hub (under NDA).

How Does the Service Process Data?

The Service interacts with the customer's email system through the email provider's Application Programming Interface (API). Microsoft and Google publish APIs that allow a user of the API (in this case, the Service) to process the data types listed and described above directly within the customer's cloud email tenant. The data types stored by the Service, as indicated in the table above, are transferred from the customer's email system to the Service's infrastructure located in the United States or the EU (depending on deployment) for processing and storage.

Abnormal works collaboratively with all customers to ensure that personal data transfers made as a result of the Service's operation are conducted in accordance with applicable laws. Abnormal regularly executes the Standard Contractual Clauses (commonly referred to as EU Model Clauses) with customers.

Are Third Parties Involved When the Service Processes Data?

Yes, Abnormal engages third-party service providers to help provide the Service. An up-to-date list is available here.

Can the Service Delete and/or Rectify Data?

Yes. Customers can email privacy@abnormal.ai to make specific data deletion and/ or rectification requests, either for personal data or for other data types processed by the Service. Abnormal reviews each request and engages with the customer to collaboratively and appropriately address the request without undue delay.

Does the Service Encrypt Data It Processes?

Yes. The Service encrypts the data it processes while that data is in transit and at rest. While data is in transit, the Service leverages industry-standard secure data transmission protocols with session authentication and encryption; all data in transit is encrypted using TLS 1.2 sessions with a 2048-bit RSA asymmetric key, and HTTPS is required for all traffic. The Service employs industry-standard AES 256 encryption protocol and multi-factor encryption technologies on all data stores, including production databases, big data files used for data processing, database backups, read-replicas, and snapshots.

Does the Service Process Data Securely?

Abnormal's Security, Engineering, Infrastructure, and Product Management teams work together to ensure that appropriately designed and industry-standard technical and organizational security measures are applied to the Service.

Abnormal maintains an Information Security Program (ISP) addressing the Service and Abnormal's general business practices to ensure a secure environment for personnel, customers, systems, and data.

To demonstrate the design and effectiveness of Abnormal AI's control environment, an independent third-party audit is conducted on an annual basis. Abnormal maintains a SOC 2 Type 2 report as a result of this regular audit activity and, on request can share the most recent SOC 2 report under a non-disclosure agreement.

Some key features of the ISP are outlined below:

AI

Please see our AI information in our Security Hub.

Email Account Compromise Detection

Abnormal requires strong access controls for any system that processes or stores customer data, including personal data. Such controls include multi-factor authentication,

leveraging biometric fingerprint verification where practical, to access company systems and customer data. Role-based access practices and controls grounded by the principle of least privilege and required job functions are implemented for systems access. Systems access for all personnel is issued on an as-needed basis, regularly reviewed by management, and revoked in accordance with company policy and following termination of employment with Abnormal. Physical access to Abnormal AI's offices is controlled by unique card key access and is monitored 24/7 by CCTV. No customer data is stored on-premises.

Network and Cloud Security

Abnormal utilizes Amazon Web Services (AWS) Virtual Private Cloud (VPC) to isolate and protect systems it controls, including those that support the Service. A combination of VPC and AWS Security Groups is utilized for network firewall protection. Subnet-separated VPCs provide separation and connectivity between different systems controlled by Abnormal.

Security Practices & Policies

Abnormal uses industry-standard Software Development Lifecycle processes to ensure all production code is peer-reviewed and deployed via approved deployments. Role-based data access is granted to employees on a per-need basis only. Abnormal applications and systems, including the Service, are monitored for indications of compromise and unauthorized access using a defense-in-depth approach and actively investigated 24/7. Patches are identified, reviewed, and applied within an appropriate timeline determined by Abnormal's internal policies.

All sections in this document apply to the products listed on Abnormal's website.