Abnormal Security Product Privacy Guide

What services does Abnormal Security provide?

Abnormal Security 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 take over (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 Security 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.

© 2021 Abnormal Security Corporation. All rights reserved.

Abnormal Security 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 are 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 are used only for the purpose of delivering the Service to each customer.

Certain components of the Service, are delivered to Abnormal Security's customers in a federated model so that these collective intelligence and data sets can enhance protection for all Abnormal Security customers. Data collected and processed to create the Service's Vendor and Threat Intelligence Data feeds are produced from attacker signals which 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, anonymized, or aggregated 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 email 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.

Data Type	Description	Processing & Purpose	Storage & Limitation
Email Metadata	Data assigned by email clients, servers, and Message Transfer Agent (MTA) during email transit such as: **Email Headers:** • Recipients • Subject • X-headers • SMTP • IPs • Mail path • Auth results	The Service processes email metadata to perform SPF/DMARC/DKIM analysis and to check against typical account activity. For example, the Service may review and confirm the login IP of a given session matches a recognized pattern.	The Service stores malicious email metadata to infer long term suspicious patterns. For example, does authentication usually succeed, and does the authentication follow usual IP patterns. Email metadata are stored by the Service for 180 days by default.

© 2021 Abnormal Security Corporation. All rights reserved.

Data Type	Description	Processing & Purpose	Storage & Limitation
BCC Email Address Information	Blind Carbon Copy (BCC) address information is not contained in email headers addressee information but contains information that canhelp identify additional recipients of the message.	The Service processes BCC email address information to perform analysis to identify additional techniques used by threat actors in attacks. Some attack techniques leverage BCC recipients and as such it is useful to process such information.	The BCC email address information is stored by the Service in the same manner as the email metadata (180 days) by default.
Email Body Content	Email body content is the written content within an email, including any images and/or hyperlinks contained within the email body content.	The Service processes email body content to extract, determine, or identify hyperlinks, topics IDs, indications of urgency, and writing patterns. For example, the email body content may indicate an urgent financial request, a known malicious hyperlink, or contain an unusual mail signature.	The Service ***does not store*** email body content for emails the Service identifies as non-malicious. The Service ***does store*** email body content for emails the Service identifies as malicious. Malicious email body content is stored by the Service for 180 days by default.
Email Attachments	Email attachments are files attached by a sender to an email.	The Service processes email attachments to identify malware and ransomware contained within an attachment, process topic IDs, and to analyze hyperlinks contained within attachments. For example, a PDF attached to an email may include a hyperlink that leads to a malicious website, or a .jar file may contain malicious code such as a virus or ransomware.	The Service ***does not store*** email attachments for emails the Service identifies as non-malicious. The Service ***does store*** email attachments the Service identifies as malicious. Malicious email attachments are stored by the Service for 180 days by default.
Email System Metadata	Email system metadata are identifiers assigned by the customer's email system service provider (i.e., Microsoft or Google). These identifiers enable email message retrieval with email system credentials such as: • Tokenized user ID • Message ID	The Service processes email system metadata to enable the Service to interact with the customer's email system APIs to the extent necessary to provide the Service.	The Service stores email system metadata to ensure the Service can invoke the customer's email system APIs for normal operation of the Service. Email system metadata are stored by the Service for 180 days by default.

© 2021 Abnormal Security Corporation. All rights reserved.

Data Type	Description	Processing & Purpose	Storage & Limitation
Abnormal Metadata	Abnormal metadata are data about an email message derived, calculated, or otherwise generated by the Service in the course of its normal operation such as: • Topic ID • Risk score • Top level domain of contained links • Number of links in email body • Number of attachments • Size(s) of attachment(s)	The Service generates and processes Abnormal metadata to perform the Service's designed functions and analysis. For example, the Service may generate and process Abnormal metadata to perform topic analysis that results in inferences of suspicious content, or to conduct analysis of possible financial or data requests and/or malicious attachments associated with a particular email message.	The Service stores Abnormal metadata to enable the Service to understand normal communication patterns and topics from a given email sender. Abnormal metadata are stored by the Service for a maximum of 180 days by default.

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 to allow a user of the API (in this case the Service) the ability 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 for the processing and storage activities detailed in the table above.

Abnormal Security 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. For example, Abnormal Security regularly executes the Standard Contractual Clauses (commonly referred to as EU Model Clauses) with customers.

How Long Does the Service Retain Data?

The Service retains the data types that it stores for the applicable default retention time indicated in the table above. During infrequent occurrences where an email requires additional analysis by the by the Service or an Abnormal Security researcher, personal information may be stored temporarily by the Service until the malicious indicators identified by the Service within the message are validated, which is designed to occur within three hours of receiving such message.

© 2021 Abnormal Security Corporation. All rights reserved.

Can the Service Delete and/or Rectify Data?

Yes. Customers can email support@abnormalsecurity.com to make specific data deletion and/or rectification requests, either for personal data or for other data types processed by the Service. Abnormal Security 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 those data are in transit and at rest. While data are in- transit, the Service leverages industry standard secure data transmission protocols with session authentication and encryption; all data in transit are 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 Security'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 Security maintains an Information Security Program (ISP) addressing the Service and Abnormal Security's general business practices to ensure a secure environment for personnel, customers, systems, and data.

To demonstrate the design and effectiveness of Abnormal Security's control environment, an independent third-party audit is conducted on an annual basis. Abnormal Security 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.

© 2021 Abnormal Security Corporation. All rights reserved.

Some key features of the ISP are outlined below:

Email Account Compromise Detection

Abnormal Security 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 function are implemented for systems access. Systems access for all personnel is issued on an as-needed basis, regularly reviewed by management, and is revoked in accordance with company policy and following termination of employment with Abnormal Security. Physical access to Abnormal Security'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 Security 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 are utilized for network firewall protection. Subnet-separated VPCs provide separation and connectivity between different systems controlled by Abnormal Security.

Credential and Key Management

Abnormal Security stores critical encryption keys (i.e., O365 secrets and cipher keys) in AWS Key Management Service (KMS). AWS KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules for data protection.

Security Practices & Policies

Abnormal Security 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 Security 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 Security's internal policies.

Are third parties involved when the Service processes data?

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

www.abnormalsecurity.com/trust →

© 2021 Abnormal Security Corporation. All rights reserved.