ISG Intelligence Systems Group

Privacy & Security

- **Does Graphus has access to my emails (Does Graphus read my company emails)?**

Graphus personnel does not have access to your email or your Graphus Portal unless you have subscribed to Managed SOC plan that explicitly tasks Graphus to provide you monitoring, investigation and incident response service. Graphus processes inbound and outbound emails in-memory to identify threats to your business. It does not store emails outside of your cloud office platform (e.g. G Suite). Graphus extracts and stores meta attributes in Graphus Cloud. These attributes are accessible to only your authorized personnel (e.g. G Suite admins) for viewing and are used for investigating suspicious activities and in incident response to detected threats.

How is customer data (e.g. meta attributes) secured in the Graphus Cloud?

Graphus Cloud uses Amazon Relational Database Service (RDS) for encrypting and storing customer data (customer emails are not stored in Graphus Cloud). Amazon RDS uses cutting edge security and encryption technology. Google Apps customer use Google Single Sign On (SSO) to access Graphus Portal. Two factor authentication is supported for customers using username & password. Password is secured using PBKDF2 for hashing that uses salt unique for each user with 1000 iterations of hashing. Graphus Portal uses Secure Transport Layer (HTTPS) for securing data in motion when accessed by customers using web browsers.

What is the data retention policy after trial or paid subscription is over?

Once the Trial or Subscription expires, customer data is purged from the Graphus Cloud. During Trial or Subscription period, data older than 7-days is automatically purged on a regular basis.

ISG Intelligence Systems Group

Who has access to My Graphus Portal?

For Professional & Enterprise subscriptions, only G Suite (Google Apps) admins of your domain have access to the Graphus Portal. For Managed Service subscription, Graphus SOC (security operations center) has access to the Graphus Portal to provide full range of managed services (Monitoring, Investigations, and Incident Response) as part of the Managed SOC subscription.

Subscription Plans

- **Can you pick and choose users for monitoring for a paid subscription plan?**

The purpose of Graphus is to protect the entire business from cyber criminals. The detection technology works best when all users within an organization are monitored. For this reason all users with an active inbox must be monitored.

Can I upgrade my subscription plan?

Yes, you can upgrade your subscription plan at anytime to any of the higher plans.

Miscellaneous

What threats does Graphus protect against?

1. Social Engineering Threats (phishing, spearphishing, cyber-scams).
2. Account Compromise
3. Malicious Attachments
4. Malicious URLs Security

ISG Intelligence Systems Group

Can you adjust frequency of Alerts?

Graphus Customer Portal is updated as soon as a suspicious activity is identified. Email Alerts to registered admin accounts are generated every hour. At this time the frequency of Alerts can't be adjusted.

Does Graphus protect Google Drive?

At this time Graphus doesn't provide security functionality pertaining to Google Drive. There is an add-on functionality planned on the roadmap that will provide visibility into usage and security policy compliance for Google Drive.

Does Graphus protect Office 365?

Graphus for Office 365 is planned for late 2017. Customers can sign up for early beta by sending email to info@contact-isg.com