Plandek

End-to-end metrics and analytics to deliver software better

Information security summary

March 2021

This short document accompanies the more detailed Infosec documentation available for review on request.

It considers the key considerations around Infosec and personal data protection when using Plandek.

It is designed to help new clients understand why Plandek is a trusted BI provider for enterprise clients in US, Canada and Europe.

Plandek approach to information security…

- Nature of data held and data encryption
- Systems architecture and data location
- Application and data security
- Infosec processes and procedures

Nature of data held and data encryption: Plandek is designed to collate and surface meta-data that does not contain sensitive client IP...

Data sources

Plandek data is sourced from the underlying tools used across the software delivery process. Key data sources are:

- Workflow management tools (e.g. Jira)
- Code repositories (e.g. Git)
- CI/CD tools (e.g. Jenkins)

Nature of data collected

Plandek only stores metadata about the software development process and **avoids storage of data which may hold sensitive IP (as such Plandek does NOT store data such as ticket descriptions, source code, commit messages, attachments or comments)**. Examples of metadata which Plandek may store includes information such as transitions of issues, the time of commits and pull requests and the person who performed the actions. For an exhaustive listing of data gathered, see data_stored_per_gatherer.docx in the folder.

Data encryption

All access to tools such as Jira, Github, Bitbucket and CircleCI are performed over encrypted connections. Plandek uses read-only accounts and will never change data in the source systems. Our analysis is performed on short-lived Kubernetes pods and the raw data is purged once analysis is complete. For customers with specific privacy requirements, the gathering stage of the process can be run on the customer side so your intellectual property is never on Plandek servers. All data that Plandek holds is encrypted at rest and in transit.

Protection of your access credentials

All **access credentials which are held are encrypted with Google Key Management Service**, giving us the ability to monitor decryptions, revoke and rotate keys regularly.

Enforcing privacy between customers

The Plandek cloud platform is multi-tenant and as a consequence, we devote considerable resources to ensuring that your data can only be accessed by your team. We employ a variety of technical measures to ensure this separation including fine-grained role based permissions which are a key focus of our annual penetration tests. To date, our penetration tests have not found any weaknesses in our separation between customers.

Systems architecture and data location: Plandek has been architected to offer cloud and on-premise data-gatherer solutions..

Plandek standard systems architecture summary

Data Tenancy
Plandek holds all data in the **Google Cloud Platform Belgium region**. Metric data is stored in **Elastic Cloud in the same Google Cloud region**.

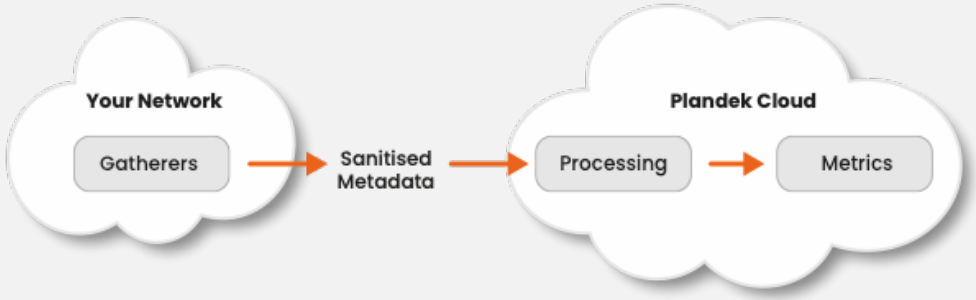
Gathering
Plandek's gatherers run on clients' servers and connect to the APIs exposed by client services. They fetch raw data, which is stripped down to the minimal amount of metadata required to power the product. This metadata is then sent encrypted to Plandek's API to be processed. This part of the system can run on-premise or in our cloud.

Processing
Processing runs on Plandek's servers and converts the metadata into events which are used to generate the metrics that power the Plandek Web Application.

Metrics
Metrics runs on Plandek's servers and consumes the processed data from processing and generates metric data based on it.

Web Application
Plandek's web application is built in React, over a high performance Node.js backend. We conduct an external white box penetration test and security audit on our infrastructure and externally accessible services at least annually.

Plandek on-premise data gatherer option



Plandek offers clients the option of an **on-premise data gatherer. This option ensures that sensitive data (received automatically via the connected APIs and not required by Plandek) are removed from the dataset before its encrypted export into the cloud - and therefore such data never leaves the client's network.**

The Plandek data collection process is separated into several stages to ensure that your source code does not leave your network and to put minimal strain on your services.

How it is deployed and managed
The on-premise gatherers are designed to run on a kubernetes cluster and are packaged as a docker container. This comprises of a long-running orchestrating component which communicates with Plandek's systems and launches short-lived gathering pods on the Kubernetes cluster.

Application and data security: Plandek is a highly secure environment...

Application Security

The Plandek platform is hosted on Google Cloud Platform in Belgium. Plandek follows Google's best practices for configuration and security. **The Plandek infrastructure and software is audited and pentested by Cure53** on a regular basis and any issues that are identified are rapidly resolved. To read more about Google Cloud's security see: https://cloud.google.com/security

Only the Plandek web application is exposed on the internet, all other resources are firewalled and only accessible via Google Cloud Identity-Aware Proxy or our VPN. The Plandek web application is only available via HTTPS, protected by TLS.

Data security

Plandek production database is Elasticsearch hosted by Elastic in Google Cloud Belgium. Elastic have an exemplary security model and we trust their ability to keep your data safe. See more about Elastic's security here: https://www.elastic.co/cloud/security
We store our metadata cache in Google Cloud Storage using customer supplied encryption keys and configuration in Postgres, encrypted at rest.
We never store or transmit data unencrypted.

Pentests and Vulnerability scanning

Plandek undertakes a white box source code audit and penetration test annually with Cure53. This covers our web applications and backend services and the underlying infrastructure. We also run automated vulnerability scans to identify risks and weaknesses in our systems on a continuous basis using intruder.io

Infosec processes and procedures: Plandek's business processes are built around the security requirements of our enterprise clients...

Employee access to customer data

- No Plandek employees access client data unless it is necessary to support the service or to resolve an incident. We also respect the privacy of our customers, so when it is necessary to access client data in Plandek, we will only view the minimum amount of data necessary to resolve the issue.
- Plandek limits the number of employees who have the ability to access customer data or production infrastructure to the minimum necessary to maintain and run the systems.
- Plandek requires that employees with access to customer data are based in the EEA. All employees are also vetted before employment commences, and all contracts contain confidentiality clauses.

Employee systems access

All access to internal systems and tools are only possible through either a VPN or Google Cloud Identity Aware Proxy and all employee devices are encrypted. We also mandate strong passwords and 2FA for employee accounts.

Authentication

Plandek supports authentication via Auth0, either with a username and password or via your own single sign on service. Our authentication system is built using Auth0. You can read more about Auth0's security here: https://auth0.com/security. Plandek supports fine grained role based authentication.

Protection of your access credentials

All access credentials which we hold are encrypted with Google Key Management Service.

Backups and Disaster Recovery

Plandek infrastructure covers multiple availability zones, and our databases are backed up and tested automatically daily.

Incident management

Plandek has a comprehensive and robust incident response plan for handling security incidents, from identification, to rapid mitigation to the post-mortem process.

Reporting an issue

If clients believe that they have identified a security issue, they contact security@plandek.com and the team will be in touch (within a tight SLA) to learn more about it and work with the client to reproduce and resolve the issue.

Plandek approach to GDPR and personal data security…

Plandek is GDPR compliant...

Plandek platform and data usage

- Plandek is a cloud-based analytics platform (European Google cloud) that is used by clients to analyse their end-to-end software delivery process
- Plandek works by mining data held in clients' underlying software delivery toolsets (e.g. Jira, Git, Jenkins) to surface delivery metrics in customisable dashboards used by the client to optimise their (internal) delivery process
- As such, Plandek only holds data already present in these underlying toolsets. This includes company employee names and email addresses and certain actions taken by the employees (e.g. completing a Pull Request, transitioning a ticket)
- The employee data is not shared with any third-party and is only used by the client teams themselves to improve their own performance over time
- Plandek allows analytical drill-down by workstream, team and individual (e.g. an individual's Completed Tickets). However, if desired, the collection of personally identifiable information and the ability to view individuals can be disabled, so data is only visible at a team level

Plandek use of personal data and GDPR compliance

- Under GDPR legislation, **Plandek is deemed the Data Processor and the client remains the Data Controller**
- As such, Plandek's use of personal data is fully GDPR compliant, as the client remains the Data Controller and under the terms of the Plandek T&Cs retains control of all data surfaced in the Plandek dashboards
- Any personal data is used for the client's own internal purposes only (and Plandek as Data Processor does not have the right to use the client data for its own purposes)
- When Plandek is used by the client:
  - a Personal Data Privacy Notice can be displayed to all users
  - all personal data is encrypted, securely held and not accessible to Plandek as Data Processor without client permission
  - only existing data held within company toolsets is collated and surfaced within the Plandek dashboards (no new personal data is collected)
  - the data is not shared outside the client company and is only used by the client employees themselves to self-improve their own performance in the workplace.