PALANTIR PLATFORM: GOTHAM

SERVICE DEFINITION DOCUMENT

Prepared For: G-Cloud 14 Framework

palantir.com/uk

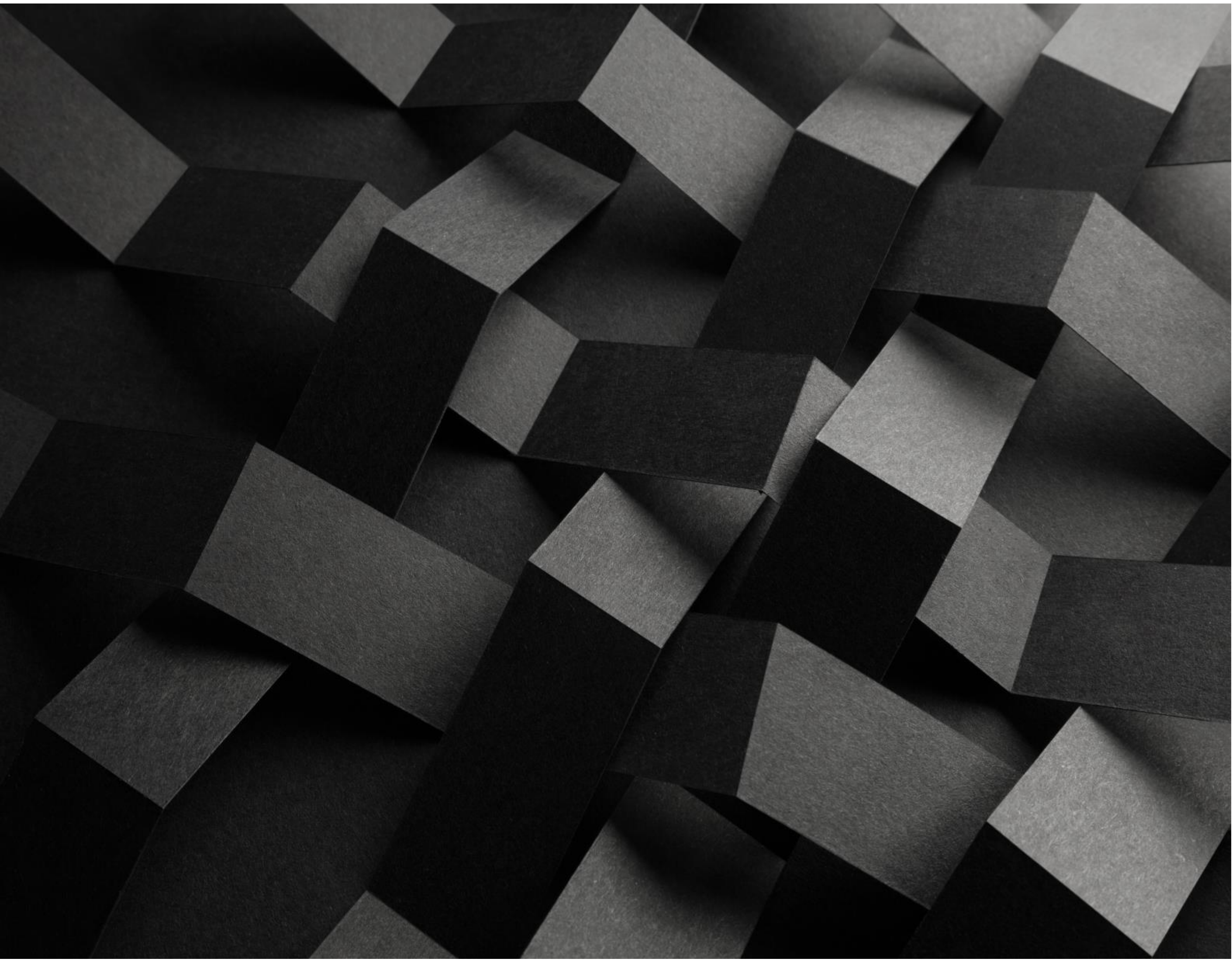


Table of Contents

1.0 PALANTIR GOTHAM SOFTWARE OVERVIEW

Useful Resources: Please visit our website and YouTube channel to access a variety of case studies, technical documentation, product demonstrations and additional information about the Palantir Platform.

1.1 Introduction

Palantir Gotham is a proven, end-to-end, commercial off-the-shelf ("COTS") platform for AI-enabled defence, intelligence, and law enforcement operations. It enables secure collaboration, intelligence analysis, and investigations to support front-line operations, specialised investigations, multi-jurisdictional strategic intelligence operations and strategic initiatives. It is the result of more than a decade of partnerships with military, intelligence, and law enforcement agencies. Palantir Gotham is operationally deployed in some of the world's most hostile threat environments for both international and national security across all Five Eyes ("FVEY") nations and coalition partners, NATO members, and some of the world's largest listed companies.

1.2 How Does It Work?

Palantir Gotham solves the problem of increasing data and threat complexity by bringing together data, users, and analysis into a single, cohesive platform. Rather than working in isolation with data siloed across disparate systems, authorised users from across an organisation can search, access, and analyse the same data foundation and share data with their peers under the platform's fine-grained security model. All platform application and features are backed by stringent, platform-wide security. In addition, the platform incorporates and leverages Palantir Foundry's capabilities, offering a suite of analytical and operational applications which can accommodate a wide range of workflows within a unified, interoperable solution.

The platform enables operational advantage and proactive deterrence for military, law enforcement, and intelligence agencies by providing a common operating picture ("COP") and common intelligence picture ("CIP"), and by supporting intelligence collection and production, investigative network analysis at scale, mission planning, targeting, execution, and after-action analysis. This lets commanders and staff visualise and analyse information from multiple systems in real time, and to work collaboratively and securely across the operating environment to achieve successful mission outcomes.
Palantir Gotham combines the following capabilities in a single, unified ecosystem:

- Enables the creation an integrated data asset which serves as a single source of truth for the entire organisation.
- Incorporates and leverages Palantir Foundry to import and export data to virtually any system, including existing applications and streaming sources. The platform can process data in any form, including audio and video.
- Allows users to conduct investigative workflows at scale, including link analysis, geospatial analysis, Call Detail Record (CDR) analysis, and object analysis, and to produce actionable intelligence from their full range of data.
- Lets teams share data, insights, and analyses with each other to grow their organisation's collective knowledge.
- Provides seamless and secure collaboration in classified and multi-level security environments, by leveraging a robust backend of federated access management.
- Enables multitasking, as users can open multiple instances of any application from within the same session.
- Features security and privacy tooling built to the strictest security, privacy and civil liberty standards, including granular Access Control Lists ("ACLs").

- Provides an extensible framework, which allows users to engage with in-house or third-party applications and models.
- Includes customisable interfaces, which lets users tailor their workspace to their use-cases and workflows.
- Has open APIs at every level, with access to raw, underlying data, to ensure openness, interoperability and extensibility.
- Frequently updated, ensuring that best-in-class status is maintained.
- Unifies operational and intelligence data and tooling to improve awareness of the operating environment.
- Provides consistent and traceable information to all levels of command, enabling more effective, higher-tempo cycles for decision making, planning, execution, and exploitation.
- Meets customer needs off-the-shelf, with the ability to be operational against these needs in support of live missions within weeks, and with minimal disruption of operations.

1.3 Platform Principles

Palantir Gotham serves as an organisation's knowledge base, containing the full record of an organisation's data, intelligence, and insights. It is built on the following principles:

Data Integration

Palantir Gotham efficiently integrates and models an organisation's data—regardless of format or volume—into a single, cohesive data asset that humans use to solve their toughest problems. Instead of rigid rows and columns, Palantir Gotham transforms structured and unstructured data into objects and associated properties that represent real concepts (such as people, organisations, places, documents, and events) and the relationships that connect them. This data model is called the "Ontology" is fully adaptable, changing in response to an organisation’s needs.

Unified Search and Discovery

Palantir Gotham offers a single point of search across internal and external data sources. During discovery, users can explore data in its original format, as well as in an enriched view only available in Palantir Gotham. The platform's federation capability seamlessly integrates external systems so they continue to add value to the data ecosystem. Users can promote external records to fuse them with the intelligence in Palantir Gotham, and relevant data is automatically surfaced to users for review, which simplifies analysis of large-scale data.

Secure Collaboration

Palantir Gotham makes organisation-wide collaboration possible through stringent, platform-wide security. Every piece of data is tethered to its original data source, where access restrictions can be applied at the level of the individual attributes that describe an object (e.g., a building's address, a vehicle's model). These permissions govern how people interact with data. All user and administrator interactions with the system and the use of information to which they have access are recorded in audit logs. These audit logs can additionally be configured to be tamper-evident. Security capabilities extend across the platform, so new data that users create is subject to the same standard of security, auditing, and history. By maintaining data security and integrity, Palantir Gotham supports insight sharing and collaborative intelligence across organisational boundaries; across security and data models; and across low-bandwidth, high-latency networks.

Openness, Extensibility and APIs

Palantir Gotham is a fundamentally extensible platform that maximises openness and control over the environment. Palantir Gotham interoperates smoothly with common programming languages, external systems, and software products through industry-standard REST APIs, while the platform's open APIs allow users to build new capabilities. All operations performed via APIs are subject to Palantir's security, audit logging, and safety checks, and all data can be exported in open formats for use in other frameworks. Palantir's open-source toolchain for HTTP/JSON APIs, generates client and server bindings in a variety of languages from a declarative API definition written in YAML. As technology evolves, Palantir Gotham is built to keep pace so that organisations have what they need to do their most important work.

1.4 Platform Features

Users can access and explore the Palantir Gotham's analytical functions through the Palantir Workspace - a cohesive, modern interface that connects the platform's applications and services. The Workspace is accessible from any modern browser or a lightweight desktop application.

Applications are the platform's core analytical tools, allowing users to visualise investigative and operational workflows, explore related objects, and engage with their data through intuitive interfaces. They also enable users to conduct large-scale analyses, securely collaborate in real-time, augment their work with machine learning capabilities, and utilise operational planning tools to unlock powerful new workflows and analytical outcomes.

All applications are backed by the same data asset and are fully integrated with one another. Users can move seamlessly between applications to view and analyse data in different ways. For example, a user might visualise a network of entities in the Graph application, then select and drag them into the Gaia application to view where the network's members have travelled, and finally move to the Dossier application to create an intelligence report that can be shared across multiple teams working on the same project.

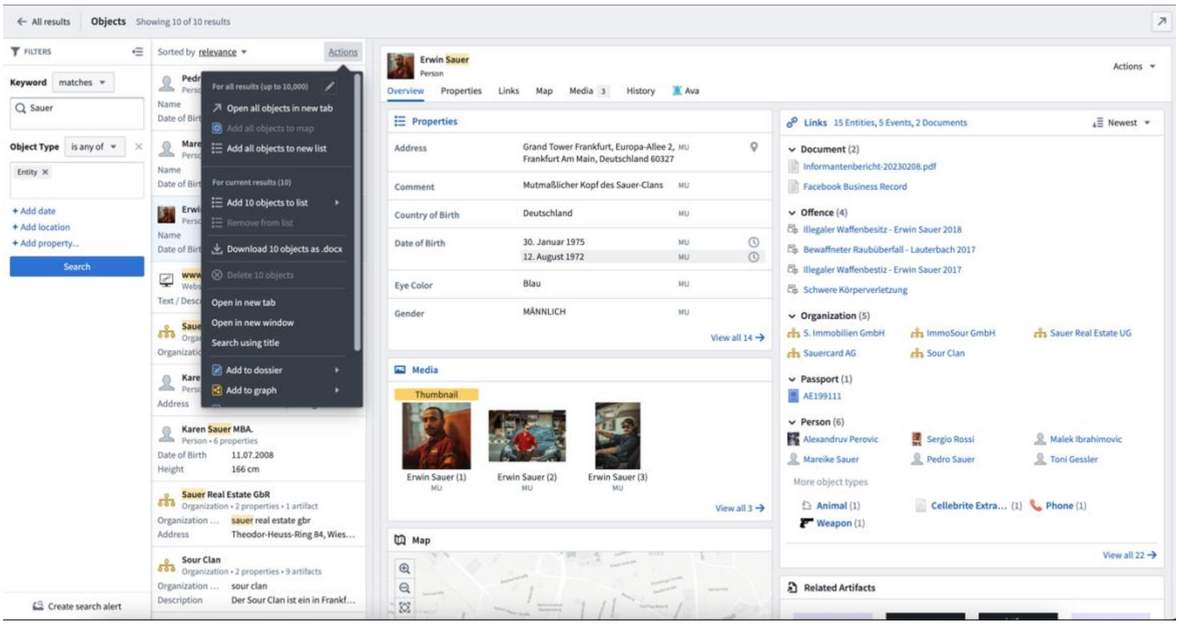
Please note, there are other applications which are used for more sensitive workflows, such as targeting, fires control and execution, ISR, and ISINT analysis which are not listed here. For more information on these capabilities, please contact Palantir directly.

Browser

Browser is an application that enables users to view and edit information related to specific objects or groups of objects within the platform's canonical data model (or "Ontology"). In Browser, users can view objects and entities, edit object properties, add notes, and view a history of changes that were made to the object. Browser can also be configured to support object-level workflows based on integration with third-party systems.

Browser gives users an overview of an entity's contacts and relationships. This includes additional details that are linked to the entity (such as attributes or other entities), as well as its associated metadata. For example, if an analyst wants to view information about an individual identified in a suspected criminal network using the Graph application, the analyst can double-click on the individual's icon in Graph. This will immediately open a view of the person entity in a new tab so that the analyst can review all data relating to the individual.

The application also includes expansive search capabilities which allow users to search all data in the platform with a single query that runs across integrated and federated data - regardless of source system, type of integration, or type of data. Summary results of user-dictated searches and aggregations are grouped in a single dashboard specifying the data source(s) for each hit. The platform's search and dashboard capabilities significantly reduce the time required to produce intelligence and improve the quality and depth of the information surfaced.



Keyword: matches — Sauer

Object Type: is any of — Entity

Karen Sauer MBA.
Person • 6 properties
Date of Birth 11.07.2008
Height 166 cm

Sauer Real Estate GbR
Organization • 2 properties • 1 artifact
Organization ... sauer real estate gbr
Address Theodor-Heuss-Ring 84, Wies...

Sour Clan
Organization • 2 properties • 9 artifacts
Organization ... sour clan
Description Der Sour Clan ist ein in Frankf...

Erwin Sauer
Person

Properties

Address	Grand Tower Frankfurt, Europa-Allee 2, Frankfurt Am Main, Deutschland 60327	MU
Comment	Mutmaßlicher Kopf des Sauer-Clans	MU
Country of Birth	Deutschland	MU
Date of Birth	30. Januar 1975 12. August 1972	MU MU
Eye Color	Blau	MU
Gender	MÄNNLICH	MU

Media: Erwin Sauer (1) MU; Erwin Sauer (2) MU; Erwin Sauer (3) MU

Links 15 Entities, 5 Events, 2 Documents

Document (2): Informantenbericht-20230208.pdf; Facebook Business Record

Offence (4): Illegaler Waffenbesitz - Erwin Sauer 2018; Bewaffneter Raubüberfall - Lauterbach 2017; Illegaler Waffenbestiz - Erwin Sauer 2017; Schwere Körperverletzung

Organization (5): S. Immobilien GmbH; ImmoSour GmbH; Sauer Real Estate UG; Sauercard AG; Sour Clan

Passport (1): AE199111

Person (6): Alexandruv Perovic; Sergio Rossi; Malek Ibrahimovic; Mareike Sauer; Pedro Sauer; Toni Gessler

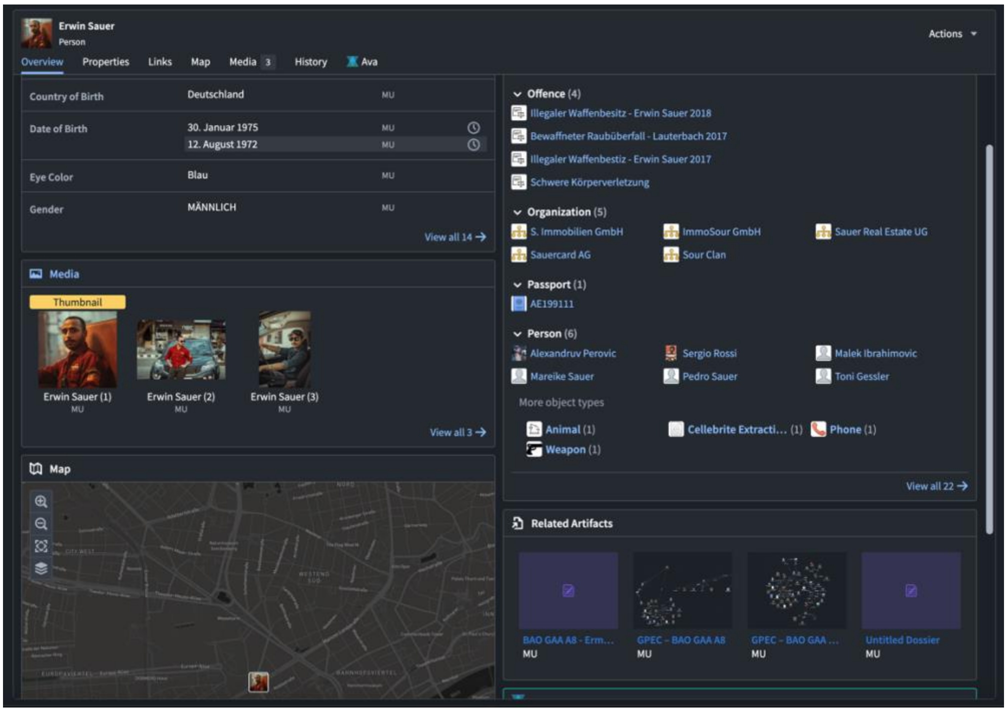
More object types: Animal (1); Cellebrite Extra... (1); Phone (1); Weapon (1)

Figure. *The Browser application enables users to search for objects, open folders and feeds, and search for documents.*

Custom Object Views

In Browser, users can create, view and interact with configurable dashboards called Custom Object Views (COVs). COVs enable individual users or teams to modify the standard object views that they access in Browser, allowing them to customise the way relevant information is presented in accordance with their needs. COVs can also be configured to display the same type of object differently for different teams.

COVs provides users with the ability to surface key insights in a flexible framework that can be adjusted as needs or workflows change. This includes organising standard summaries of operational data dashboards and dashboard summaries on user-dictated searches and aggregations.



Erwin Sauer
Person

Country of Birth	Deutschland	MU
Date of Birth	30. Januar 1975 12. August 1972	MU MU
Eye Color	Blau	MU
Gender	MÄNNLICH	MU

Media: Erwin Sauer (1) MU; Erwin Sauer (2) MU; Erwin Sauer (3) MU

Offence (4): Illegaler Waffenbesitz - Erwin Sauer 2018; Bewaffneter Raubüberfall - Lauterbach 2017; Illegaler Waffenbestiz - Erwin Sauer 2017; Schwere Körperverletzung

Organization (5): S. Immobilien GmbH; ImmoSour GmbH; Sauer Real Estate UG; Sauercard AG; Sour Clan

Passport (1): AE199111

Person (6): Alexandruv Perovic; Sergio Rossi; Malek Ibrahimovic; Mareike Sauer; Pedro Sauer; Toni Gessler

More object types: Animal (1); Cellebrite Extracti... (1); Phone (1); Weapon (1)

Related Artifacts: BAO GAA A8 - Erm... MU; GPEC – BAO GAA A8 MU; GPEC – BAO GAA ... MU; Untitled Dossier MU

Figure. *COVs show a user relevant information for any entity/object in Palantir Gotham. The widgets displayed can be customised according to the needs of the user without coding.*

COVs can be customised to highlight records, metadata, and other relevant pieces of data to visualise information specific to a user's workflows. COVs also support custom widgets or tabs that answer specific questions or display specific information. COV dashboards are interoperable with the platform's wider suite of applications, enabling users to pull customised data from across the entire platform ecosystem.

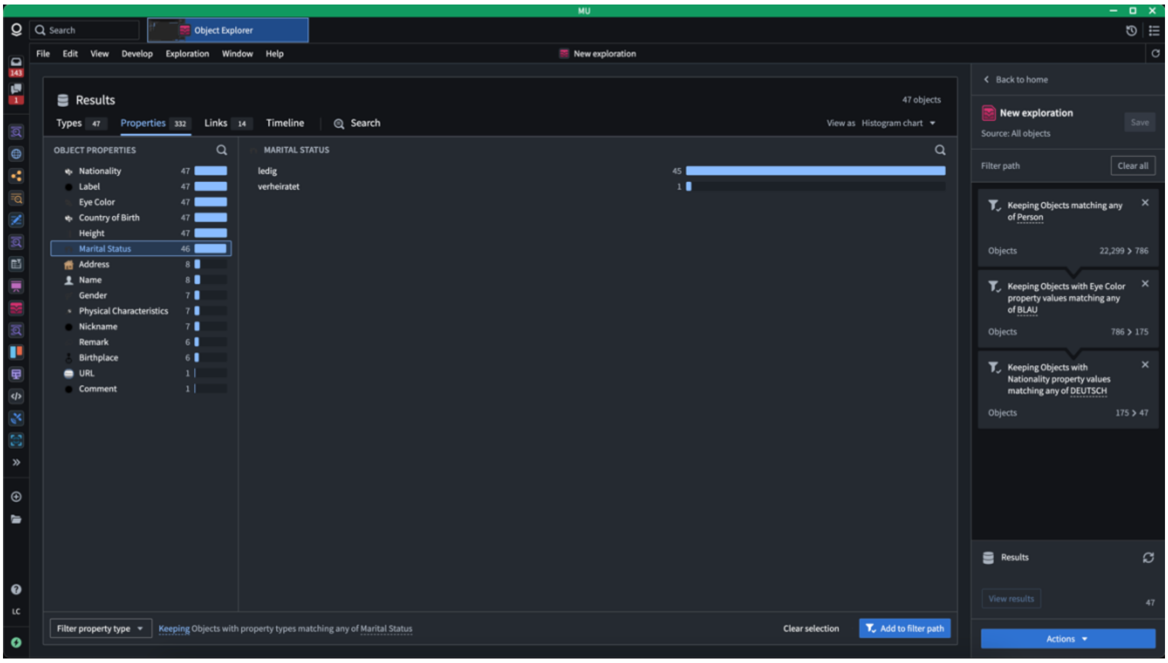
COVs organise information related to specific types of objects in terms of one or more tabs, each containing a different group of analytical and visualisation widgets to meet the needs of specific workflows or user groups. COVs can also be configured to display the same type of object differently for different teams. Information in different tabs can be locked down so that only users with the required permissions are able to see it.

Object Explorer

Object Explorer is Palantir Gotham's top-down analysis application, which offers users an intuitive, user-friendly way to analyse vast sets of data. Object Explorer enables users to find entities with similar characteristics and visualise their relationships, run analyses on millions of records at a time, and perform drill-down analyses on integrated data.

Within Object Explorer, users can quickly access embedded analysis tools, such as timelines and aggregation functions, to identify trends and patterns across large sets of data. This enables users to apply filters for sorting and drilling down into data, conduct time-based and trend analysis across all stored data, and define/apply logic to analyse data through filters. In addition, users can filter objects with similar characteristics and visualise their relationships using Object Explorer's graph tooling, which enables users to represent data as a bar chart, histogram, or pie chart. For example, an analyst can use Object Explorer to isolate financial transactions over a specified time period. The analyst can then use Object Explorer's Histogram tool to identify any trends or anomalies that require deeper analysis.

Users can also subscribe to real-time object alerts in Object Explorer to stay informed about changes to data that are relevant to specific workflows. Users can customise the conditions that trigger object alerts by defining rules or criteria that must be met e.g., when data is added to an object. Alerts can be configured to send notifications via email or directly to Inbox, the platform's alerting aggregation application.



OBJECT PROPERTIES	
Nationality	47
Label	47
Eye Color	47
Country of Birth	47
Height	47
Marital Status	46
Address	8
Name	8
Gender	7
Physical Characteristics	7
Nickname	7
Remark	6
Birthplace	6
URL	1
Comment	1

MARITAL STATUS	
ledig	45
verheiratet	1

Keeping Objects with property types matching any of Marital Status

Keeping Objects matching any of Person
Objects 22,299 > 786

Keeping Objects with Eye Color property values matching any of BLAU
Objects 786 > 175

Keeping Objects with Nationality property values matching any of DEUTSCH
Objects 175 > 47

Figure. *Users can drill down through data using the Object Explorer application.*

Chat

Chat is a communication application that enables users to securely send and receive messages, files, and data in a classification-controlled, hybrid network environment. With Chat, users can communicate directly in Palantir Gotham, eliminating the disruption or risk of third-party applications. Chat is fully integrated with the platform's suite of applications and is subject to its granular access controls and auditing framework.

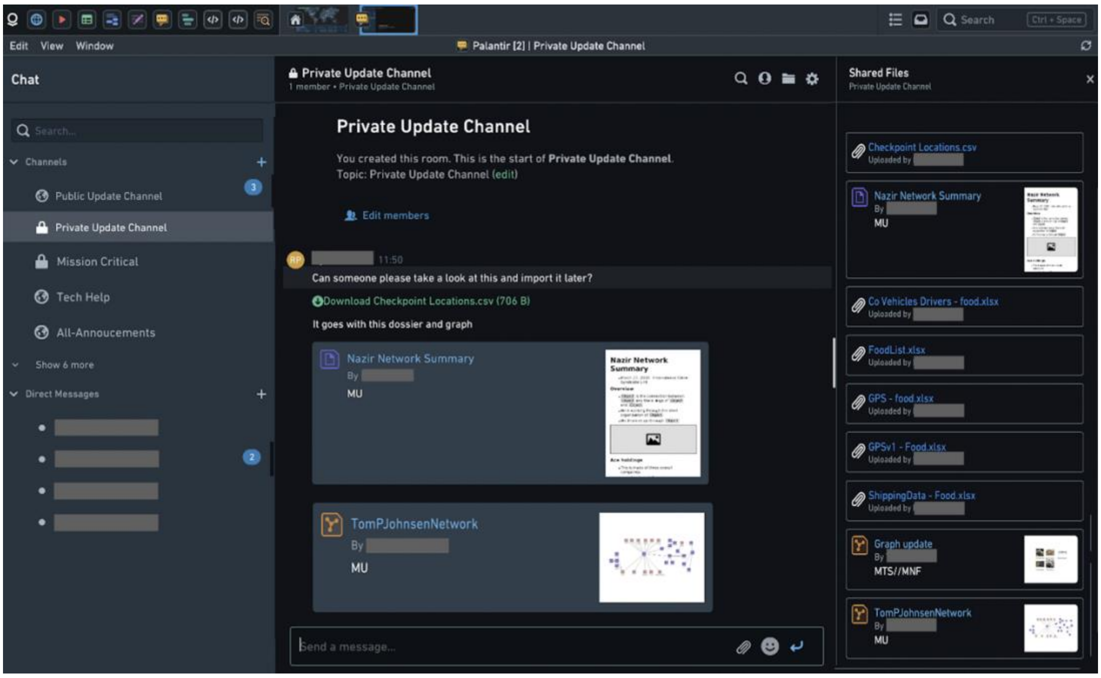
Chat is deployable in sensitive environments, including mission enclaves and partner networks. The application enables users to safely and securely access information and communicate with other authorised users in a range of settings, including across fixed installations and mobile units.

Chat's core capabilities include:

- **Collaboration:** Chat's modern instant messaging (IM) features allow users to securely exchange messages, files, objects, and artifacts either directly or via a private or public channel. To share findings generated in-platform, users can drag and drop objects or artefacts (e.g., reports) into chats to share them. All information shared is restricted with respect to the platform's fine-grained security model.

- **Security:** Chat's built-in security features preserve platform-wide classification levels and settings. This ensures that each member in a private or public channel will only be able to see information they are authorised to view. For example, an object shared in a channel may be marked as restricted. Only users authorised to access the object will be able to view it in the chat. Information is automatically redacted based on shared security permissions. In addition, users can set mandatory security levels on their channels, ensuring only users with certain security permissions can join.

- **Interoperability:** Chat seamlessly integrates with third-party messaging systems, allowing users to message teammates on external clients without leaving Palantir Gotham. This provides organisations with flexibility, as it enables Palantir users to communicate with non-Palantir users. Chat mirrors messages sent over connected systems, showing the same conversation in both the platform and alternate messaging clients.



Private Update Channel

You created this room. This is the start of **Private Update Channel**.
Topic: Private Update Channel (edit)

[redacted] 11:50
Can someone please take a look at this and import it later?
Download Checkpoint Locations.csv (706 B)
It goes with this dossier and graph

Nazir Network Summary
By [redacted]
MU

TomPJohnsenNetwork
By [redacted]
MU

Checkpoint Locations.csv
Uploaded by [redacted]

Nazir Network Summary
By [redacted]
MU

Co Vehicles Drivers - food.xlsx
Uploaded by [redacted]

FoodList.xlsx
Uploaded by [redacted]

GPS - food.xlsx
Uploaded by [redacted]

GPSv1 - Food.xlsx
Uploaded by [redacted]

ShippingData - Food.xlsx
Uploaded by [redacted]

Graph update
By [redacted]
MTS//MNF

TomPJohnsenNetwork
By [redacted]
MU

***Figure**. Chat enables users to securely chat, share material, and collaborate in a secure, classification-controlled environment.*

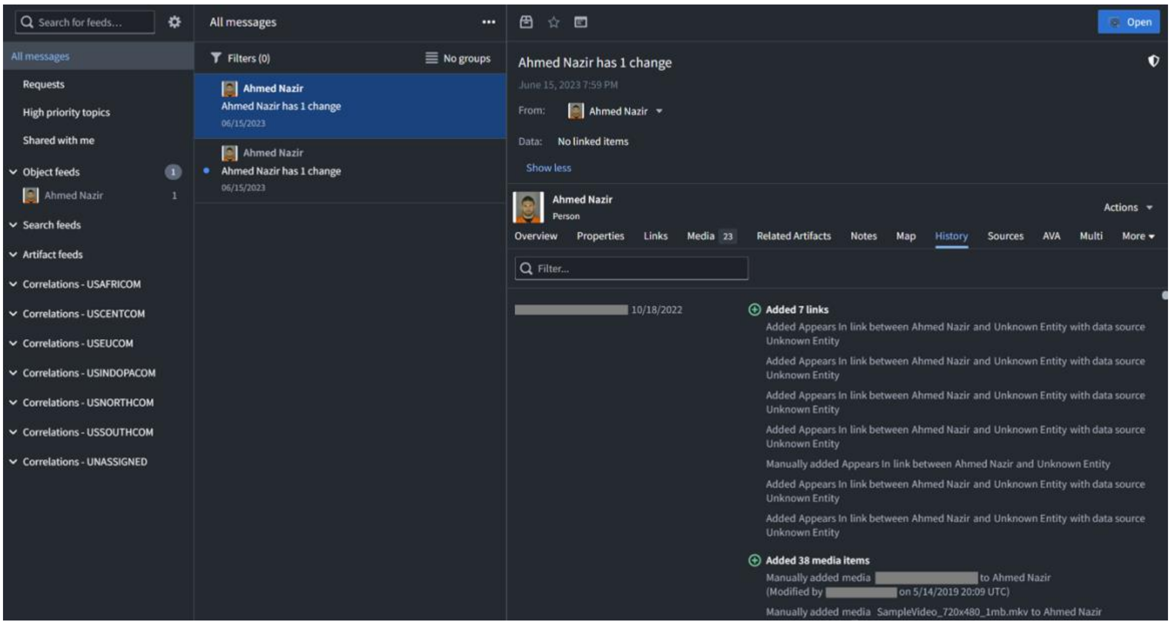
Inbox

Inbox centralises results, notifications, and alerts in an inbox-style interactive operational interface. With Inbox, users can view and triage alerts from across the platform in a single, unified view. Users are notified of alerts in Inbox through notifications. Notifications are only generated when a user subscribes to an alert, and they remain in Inbox unless a user manually archives the message. This subscription-based alerting system enables users to keep tabs on thousands of objects at a time and have confidence that no new information is lost.

Users can subscribe to a range of alert types, including, but not limited to:

- **Search feeds:** A user-defined alert, where a user defines the parameters of a search query run over the platform's data foundation. Users will receive notifications when there are new results that meet the criteria of the defined search.
- **Object watch feeds:** A user-defined alert, where a user subscribes to an object in Browser. Users will receive notifications when changes are made to the object.
- **Geofence alert:** A user-defined alert, where a user defines a "fence" on a map in Gaia and sets up alert criteria, for example, to be alerted if an object enters or exits the area.
- **Sharing alert:** Users receive a notification message if another user shares an artifact with them.

In Inbox, notifications are grouped into channels based on their alert type, and users can group their subscriptions into different channels from within the user interface. Alert behaviours and formats can be configured to suit specific workflows, or the preferences of individual users. Additionally, users can interact with and resolve alerts directly in the application. This includes viewing what actions need to take place to resolve an alert, as well as accessing a clear path to the relevant application to perform those actions.



Ahmed Nazir
Ahmed Nazir has 1 change
06/15/2023

Ahmed Nazir
Ahmed Nazir has 1 change
06/15/2023

Ahmed Nazir has 1 change
June 15, 2023 7:59 PM
From: Ahmed Nazir
Data: No linked items
Show less

Ahmed Nazir
Person

[redacted] 10/18/2022

Added 7 links
Added Appears In link between Ahmed Nazir and Unknown Entity with data source Unknown Entity
Added Appears In link between Ahmed Nazir and Unknown Entity with data source Unknown Entity
Added Appears In link between Ahmed Nazir and Unknown Entity with data source Unknown Entity
Added Appears In link between Ahmed Nazir and Unknown Entity with data source Unknown Entity
Manually added Appears In link between Ahmed Nazir and Unknown Entity
Added Appears In link between Ahmed Nazir and Unknown Entity with data source Unknown Entity
Added Appears In link between Ahmed Nazir and Unknown Entity with data source Unknown Entity

Added 38 media items
Manually added media [redacted] to Ahmed Nazir
(Modified by [redacted] on 5/14/2019 20:09 UTC)
Manually added media SampleVideo_720x480_1mb.mkv to Ahmed Nazir

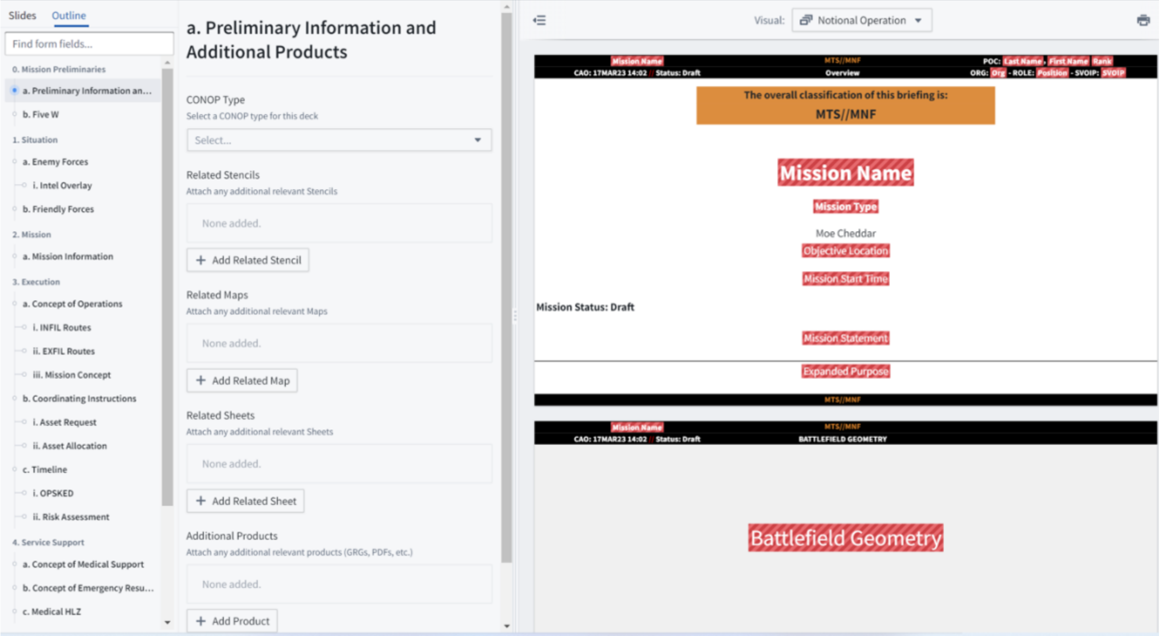
***Figure**. Viewing an alert for an object watch feed in Inbox. Object watch feeds notify subscribed users when a change has been made to a watched object.*

Slides

Slides is a data-centric briefing and presentation application. With Slides, information is fielded in real time and decks are backed by live data. Data used in Slides are maintained with a strict version control system that preserves all settings and classifications defined under Palantir Gotham's fine-grained security model. Users can quickly assemble new briefs based on templates customised to organisational requirements, ensuring all information is updated and protected automatically. Data and decks from Slides can be published to standard document formats (PPTX and PDF) for broader dissemination.

Slides' core capabilities include:

- **Collaborative Briefings:** Slides supports collaborative editing, allowing multiple users to work on the same deck. This reduces the need for teams to download and email static decks, as well as integrate multiple iterations of edits into a final version. Once a deck is complete, Slides' built in broadcasting ability allows users within Palantir to join a presentation as viewers. The broadcast feature also supports smooth transitions between multiple presenters across geographies, allowing any presenter to take over as needed.
- **Efficient Deck Creation:** Deck creation in Slides is designed to reduce the time and effort users spend creating decks. With template mode, presentations can be configured into reusable styles customised to organisational and doctrinal requirements. Intelligent fields auto-populate with existing data, and content is automatically styled - whether it be free text, uploaded media, or values pulled from other integrated data.
- **Application Interoperability:** Slides is interoperable with Palantir Gotham's wider suite of applications. Users can integrate data into presentations to enable interactive, cross-application briefings. For example, users can "clip" a subset of a network analysis produced in Graph and embed the clip in a deck produced in Slides. The embedded clip can then be opened in Graph to provide the rich Graph experience without having to leave the presentation.



a. Preliminary Information and Additional Products

CONOP Type
Select a CONOP type for this deck
Select...

Related Stencils
Attach any additional relevant Stencils
None added.

Related Maps
Attach any additional relevant Maps
None added.

Related Sheets
Attach any additional relevant Sheets
None added.

Additional Products
Attach any additional relevant products (GRGs, PDFs, etc.)
None added.

Mission Name MTS//MNF POC: Last Name, First Name Rank
CAO: 17MAR23 14:02 // Status: Draft Overview ORG: Org - ROLE: Position - SVOIP: SVOIP

The overall classification of this briefing is:
MTS//MNF

Mission Name
Mission Type
Moe Cheddar
Objective Location
Mission Start Time
Mission Status: Draft
Mission Statement
Expanded Purpose
MTS//MNF

Mission Name MTS//MNF
CAO: 17MAR23 14:02 // Status: Draft BATTLEFIELD GEOMETRY

Battlefield Geometry

Figure. *Slides can be used to collaboratively assemble mission briefings using an intuitive, drag-and-drop interface.*

Dossier

Dossier is a real-time collaborative text editor application that allows users to capture notes, annotate investigations, and compile custom profile sheets and summary reports. In Dossier, users create dynamic intelligence products, called dossiers. To assemble a dossier, users can write notes and drag-and-drop key entities and visualisations from other Palantir Gotham applications. All data inserted into dossiers retains a dynamic link back to its source, which updates to reflect any changes in the underlying data.

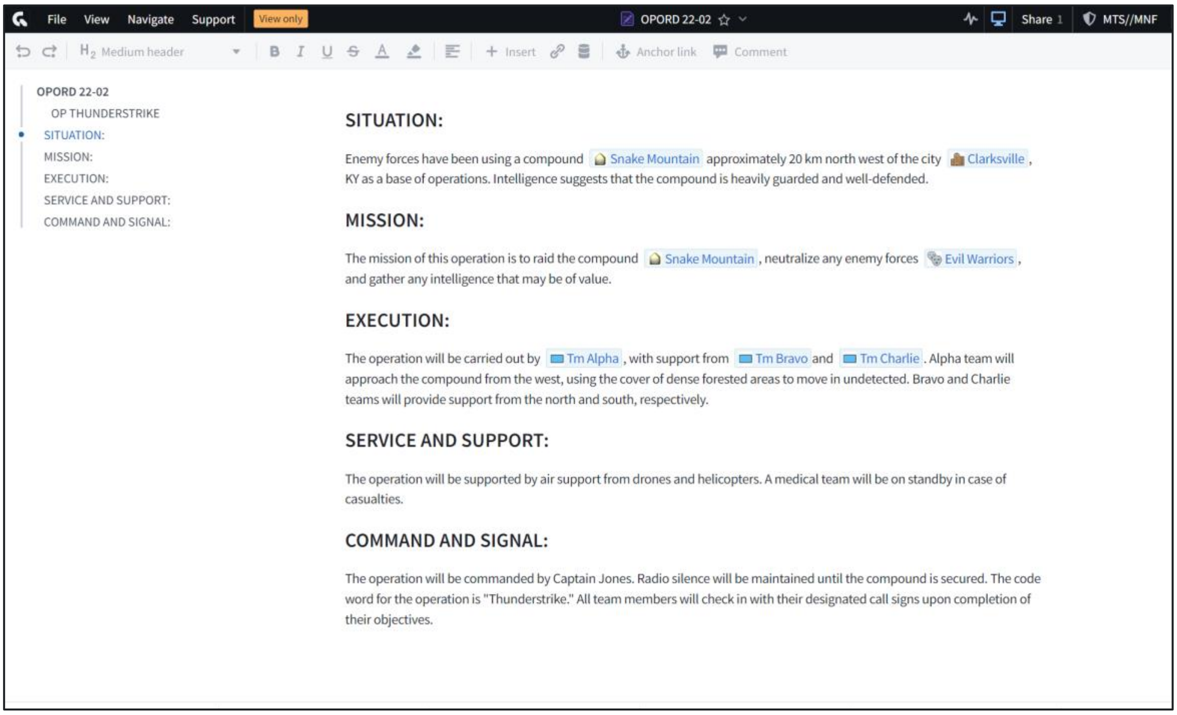
Users can embed the following into dossiers:

- Objects, including any person, place, event, or report from the platform's data foundation. By "mentioning" an object in a dossier, the object and the dossier are linked.
- Graphs and maps, which can be dragged over from the Graph and Map applications and annotated within the Dossier application.

- Snippets or excerpts from documents imported to Palantir Gotham, which retain document sourcing.
- Links to and previews of other dossiers, which create nested hierarchies of information.
- Additional attachments such as slide files, images, and URLs.

Dossier is a collaborative application. Multiple users can edit the same dossier at the same time, building on the analysis done by their colleagues. This creates a “white boarding”-type capability to allow contributions from across a team working together on a single case. Dossier can also function as a common environment for sharing, storing and updating findings as new information comes in. Critically, work is preserved even if one or more Dossier contributors switch out to focus on other tasks. Completed dossiers can be readily exported to Microsoft Word or PDF format for dissemination to partners or uploading to external report data foundation.

Dossier also allows users to create, save, and share reusable templates to automate the work of assembling dossiers. When creating a new report, users can select from an existing template, create a new template, or open an empty dossier. When creating a template, users can select from different types of headings, graphics, and placeholders, depending on their workflow. Meanwhile, Dossier also provides an overview of all templates available. Users can search for templates by name or author, and all Dossier templates can be shared across teams with respect to their access controls.



SITUATION:

Enemy forces have been using a compound Snake Mountain approximately 20 km north west of the city Clarksville, KY as a base of operations. Intelligence suggests that the compound is heavily guarded and well-defended.

MISSION:

The mission of this operation is to raid the compound Snake Mountain, neutralize any enemy forces Evil Warriors, and gather any intelligence that may be of value.

EXECUTION:

The operation will be carried out by Tm Alpha, with support from Tm Bravo and Tm Charlie. Alpha team will approach the compound from the west, using the cover of dense forested areas to move in undetected. Bravo and Charlie teams will provide support from the north and south, respectively.

SERVICE AND SUPPORT:

The operation will be supported by air support from drones and helicopters. A medical team will be on standby in case of casualties.

COMMAND AND SIGNAL:

The operation will be commanded by Captain Jones. Radio silence will be maintained until the compound is secured. The code word for the operation is "Thunderstrike." All team members will check in with their designated call signs upon completion of their objectives.

Figure. *Dossier enables users to embed existing objects into dossiers, which provides a dynamic link back to the object’s source.*

Graph

Graph is a network analysis application that allows users to create visual representations of networked data on a shared canvas. Graphs are backed by all the data within the Palantir Gotham’s data foundation, as well as data integrated from remote federated systems. In Graph, users can view aggregated property statistics to understand a network or make inferences about their data. In addition, users can organise, style, and annotate graphs as a part of a presentation or collaborative workflow.

Graph is interoperable with the platform’s wider suite of applications, enabling analysts to share and embed analyses produced in Graph as a part of their wider workflows. The application also enables collaboration, as users can concurrently work on analyses within Graph in real-time.

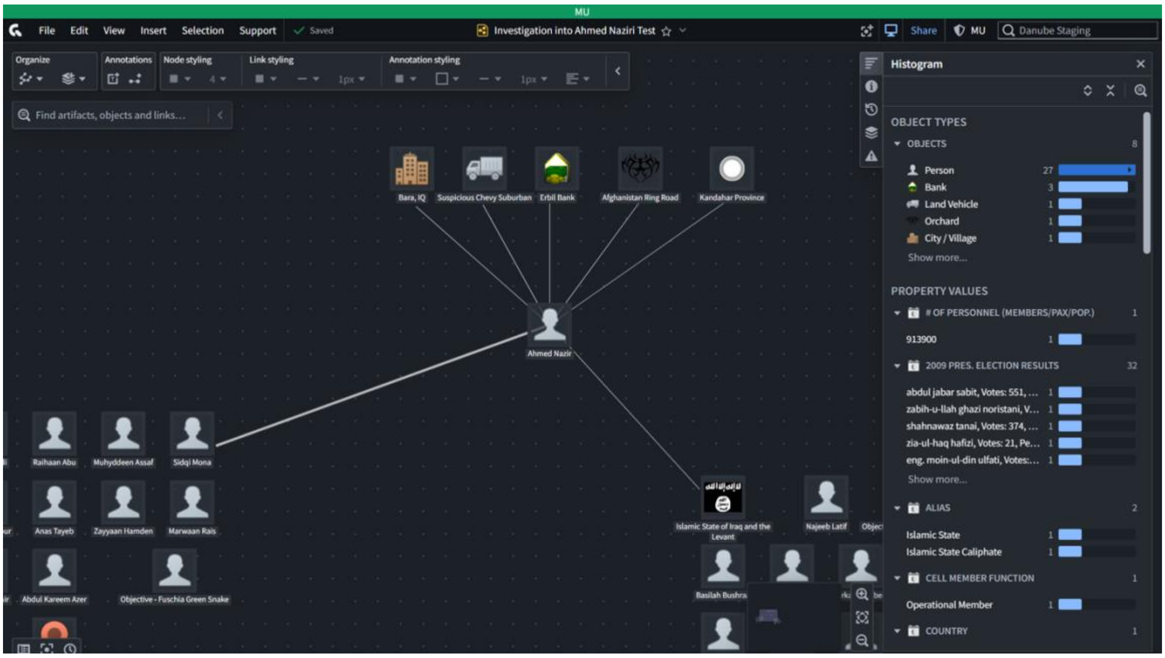


***Figure.** A notional example of how users can use Graph to create visual representations of networked data on a shared canvas.*

Graph is centred around the Canvas: a visual interface that allows users to display relevant artifacts, entities and links between them. Within Canvas, users can add data from Palantir Gotham's data foundation, as well as other sources (e.g., federated data sources), to their graphs. On the Canvas, the contents of a graph can be selected to make changes or view additional details for analysis using different helpers. Nodes and links can also be quickly rearranged spatially within the canvas to understand a network or make inferences about the data. In addition, users can organise, annotate, style, filter and search all objects on the Canvas.

From the canvas, users can utilise additional analytical tools (or "helpers") to surface insights that are not available solely by viewing a graph. These tools include the following:

- Histogram displays the frequency of occurrence for different buckets or groups: Object Types, Entity Properties, Event Properties, Entity Relationships, Events per Entity, Notes, Hints, and Tags.
- Selection is a miniature version of the Browser application that shows users details about selected objects and links. This enables users to quickly view details about data, without having to leave the Graph application.
- History enables users to view how the content and styling of a graph has changed over time, as well as which user performed the change. This enables teams to track the progress of cases/operations, which is especially useful for large-scale and complex projects.
- Table provides a tabular view of data on a graph. Tables can be exported to easily share any content produced using Graph.
- Search Around enables users to visually query data in the platform. From a graph's canvas, users can "search around" on selected objects to find links to other data. Searches are not limited to just single links and can also return complex graphs.
- Timeline can be used to visualise the time ranges of objects, properties, and links. Users can create time series visualisations of related behaviours and events. This enables them to analyse the time series to discover patterns and trends and forecast future activity.

Palantir Gotham also enables users to export a graph/chart from the Graph application in HTML format. This enables users to share analyses produced in Graph with partners, which can then be opened and interacted with in any modern web browser.

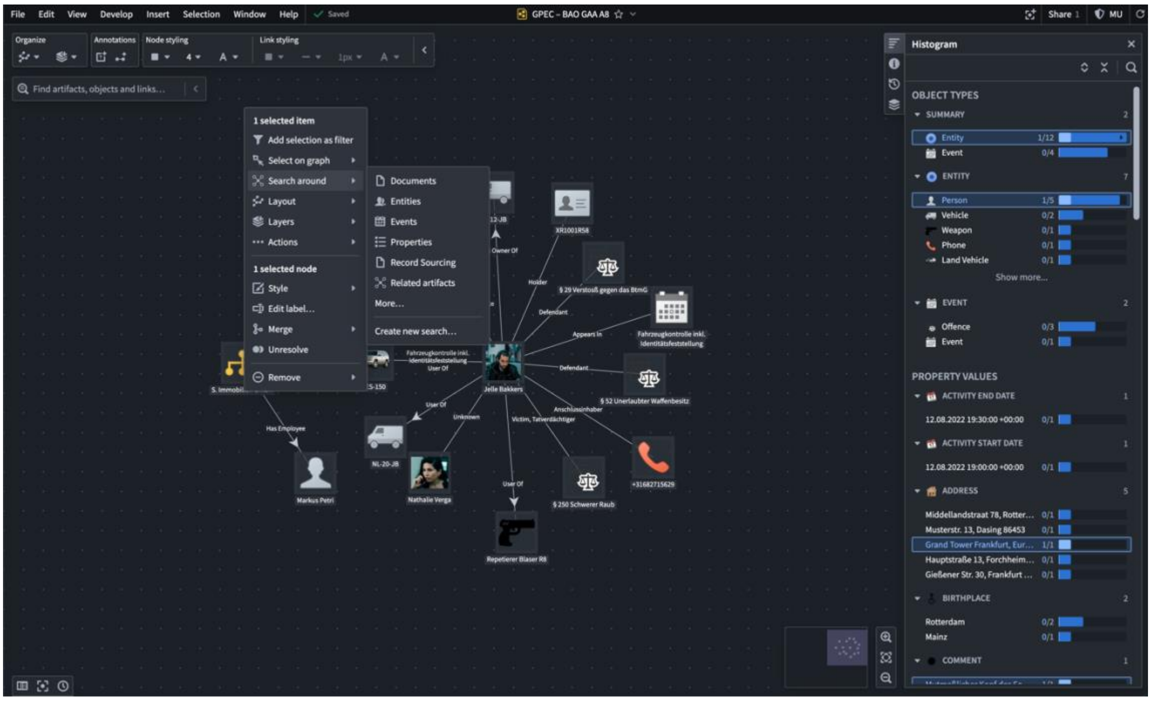


Figure. *Performing a "search around" query on a selected object in Graph.*

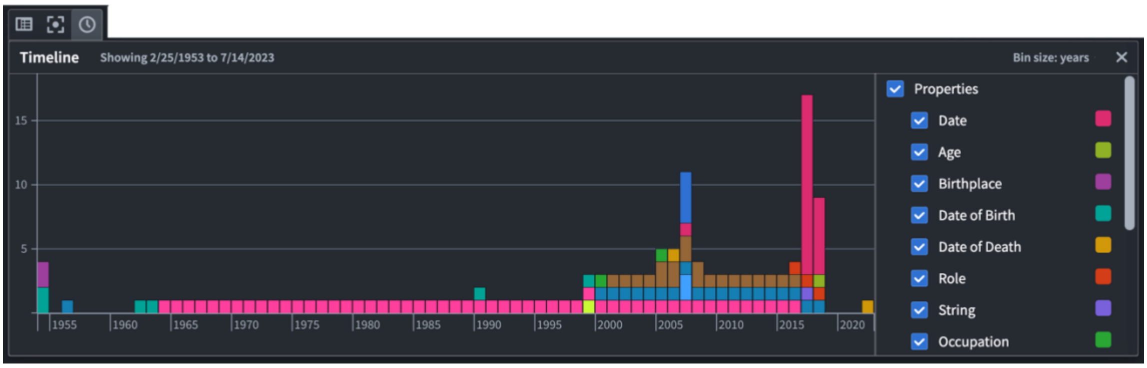


Figure. *Timeline enables users to visualise the time ranges of objects.*

Gaia

Gaia is a collaborative geospatial command and control application that facilitates operational intelligence integration of a battlefield or investigation in near real-time. Gaia enables users to integrate data from across Palantir Gotham into a cohesive map-based landscape, which can then be used to discover data trends, perform quick geographic searches, and create heatmap analyses. In addition, analysts can use Gaia to analyse an event, providing users with overview of what, where, and when an event occurred.

Gaia enables analysts to "geotag" objects (entities, events, or media, including images) and create geospatial metadata. An object that contains geospatial metadata — whether intrinsic or user-added — can be analysed geospatially and located via geo-searches (e.g., radius, route, polygon, temporal and by object type, property value or keyword). For example, an analyst can conduct a five-kilometer radius search for all individuals around the location of a known incident, to see who was close to the location of the incident over the course of a given time range. Objects that meet the search parameters are highlighted and can then be dragged-and-dropped into other applications for further analysis.

Gaia enables advanced Geospatial Information System (GIS) workflows and analyses, and supports custom tile sets, map layer formats, and geospatial overlays, including SHP, KMZ, KML and LYR files. Gaia can also integrate with various third-party platforms to deliver enriched visualisations customised for the organisation's specific needs (e.g. ATAK, WINTAK and MapBox).

Gaia is also interoperable with legacy systems, so users can quickly access all their data and intelligence associated with a geographic area to better inform operational planning and resource allocation. Users can then collaborate with teammates on an execution plan and track operation progress and outcomes on a shared map. Gaia leverages user-enriched data to allow the quick querying of historical and strategic datasets into a singular source of truth. Live data feeds can be integrated directly to provide users real-time situational awareness of rapidly evolving operations.

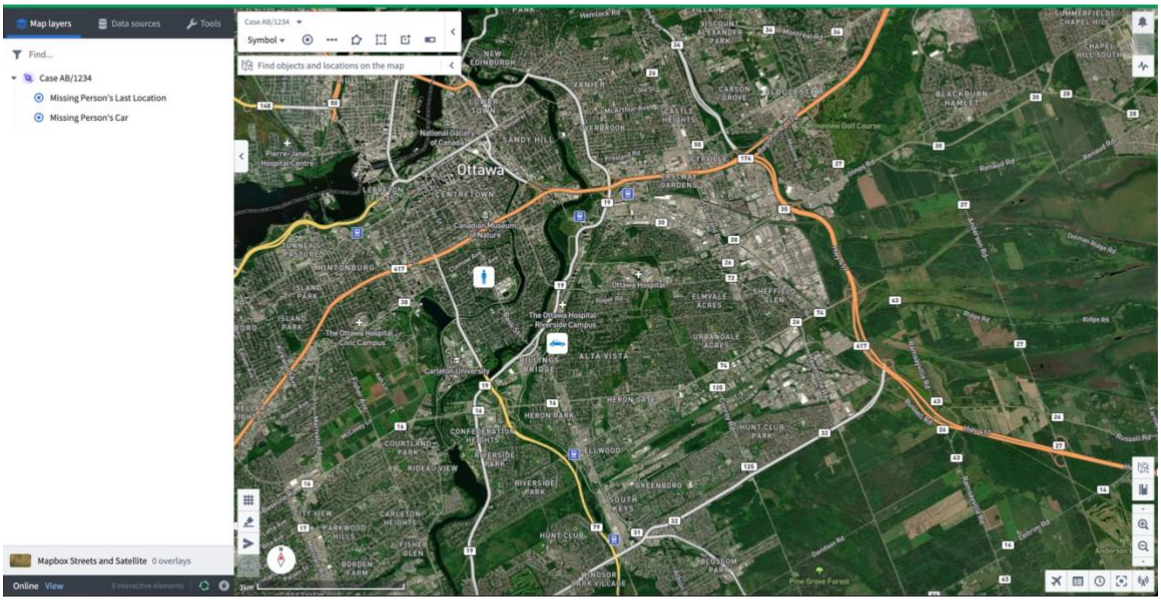


Figure. *Tracking a missing person's last location using Gaia.*

Video

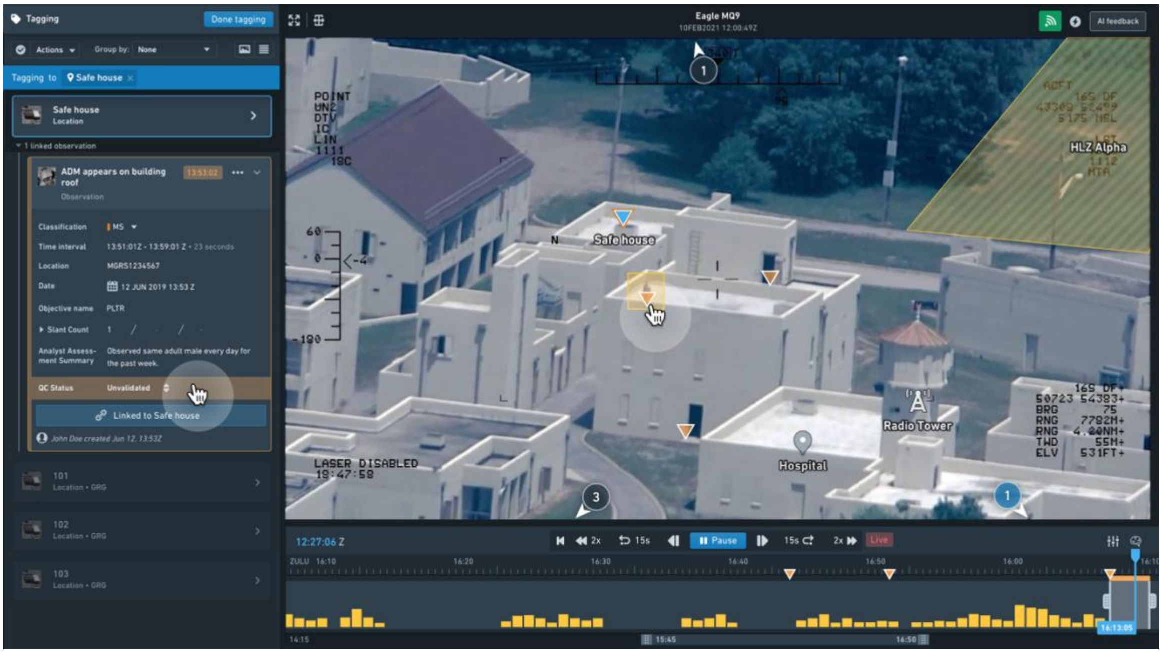
Video is an application that provides the ability to view, analyse, and enrich full motion video ("FMV") within Palantir Gotham. With Video, users can layer their institution's geospatial data on a live or archived video in real-time. They can then annotate videos and tag relevant entities to surface key insights pertinent to historical investigations or future mission planning. Annotations and tags are viewable to users as Augmented Reality (AR) overlays, which can be searched and filtered by authorised users. This enables analysts and operators to maximise their collective situational awareness and make complex decisions with confidence.

Video's core functionalities include:

- **Real-time analysis of enriched video streams.** All capabilities, features and tools can be layered onto live video while maintaining sub-second latency, ensuring users have the intelligence they need to make decisions in the moment. Users can view multiple streams simultaneously, allowing users to find key insights across a wider area.
- **AR overlays.** Users can utilise a variety of AR overlays - such as maps produced in Gaia, Blue Force Trackers (BFT/ATAK), prohibited or sensitive locations such No Strike Lists (NSLs), artificial intelligence (AI) detections, and other Palantir Gotham data sources - to contextualise streams and fix known locations onto each video frame.
- **Artificial intelligence (AI) models and machine learning (ML) integration.** Video provides open APIs and built-in analysis tools that enable users to leverage third-party AI/ML models. AI/ML models can be used to augment situational awareness by superimposing detections onto video streams in near-real time. Detections are surfaced to users for confirmation or dismissal, and users can provide live feedback to directly improve model accuracy.
- **Data enrichment/tagging.** Users can capture or highlight events on-the-fly by clicking on the interface as the stream plays live. For example, a user can tag an event, which automatically creates an object that becomes searchable for other users to build on. If an object already exists,

Video enables the user to search and merge objects when constructing tags, preventing duplication and improving collaboration across users.

- **Exports.** Users can export individual frames or full clips to their local system or other applications in Palantir Gothtam's ecosystem. All post-processed data added to the video (such as AI detections, AR overlays, and custom redaction/blur boxes) can be "burned" in, enabling as-seen exports while protecting sensitive content.
- **In-platform analytical tools.** Video includes tools that enable users to conduct second-order analyses based on automatic detections. For example, the Soak Tool can be used to generate heatmaps on aggregate detections in a given area over the course of a single stream, or to compare detections in the same area recorded at two different times.



Classification: MS
Time interval: 13:51:01Z - 13:59:01 Z • 23 seconds
Location: MGRS1234567
Date: 12 JUN 2019 13:53 Z
Objective name: PLTR
Slant Count: 1 / - / -
Analyst Assessment Summary: Observed same adult male every day for the past week.
QC Status: Unvalidated
Linked to Safe house
John Doe created Jun 12, 13:53Z

101
Location • GRG

102
Location • GRG

103
Location • GRG

Figure. *Tagging an observation flagged by an AI detection and linking it to a location in Video. Quality control steps can be applied to ensure the analyst's assessment of the detection and link validity are well-considered.*

2.0 PALANTIR GOTHAM SUPPORT OVERVIEW

2.1 Basic Summary

Palantir can provide support for Palantir Gotham, an enterprise platform which enables both technical and non-technical users to produce actionable intelligence based on a full ecosystem of available data. To help users learn to use Palantir Gotham and other Palantir platforms which utilise Palantir Gotham, Palantir can provide assistance with planning, set up and migration, security services, quality assurance and performance testing, training, and ongoing support.

2.2 Support Features

- Cloud software support; including public, private, community and hybrid clouds
- Migration and set up assistance
- Business analysis and cloud solution guidance
- User and service management
- End-to-end managed support
- Intuitive, easy to use interface
- Training on how to navigate the platform
- Helpdesk support

2.3 Support Benefits

- Ensure ease of use for technical and non-technical employees
- Enhanced strategic planning, reducing business risk and costs
- Rapid migration to chosen cloud service
- Fully managed migration process
- Optimised use of cloud software
- Flexible training delivery for varying user adoption rates and locations
- Multiple training modes; instructor-led, internet webinars and self-guided learning
- Bespoke, tailored training materials based on specific contract/project requirements

2.4 Additional Support

In addition to the support, training and documentation provided as part of our standard software licensing, Palantir can also provide supplementary support services and resources such as suitably qualified third-party Field Services Representatives (FSRs), who can provide a variety of project and use case support services. Please refer to our Lot 3: ‘Palantir Cloud Support Services’ offering for a description of supplementary support and implementation services.

3.0 PALANTIR SECURITY

Palantir believes data analysis software becomes a liability when it lacks robust, built-in access controls, and is firmly committed to protecting data security, privacy and civil liberties. As such, Palantir has made security its highest priority at every point in the development of Palantir, and it is why organisations in national security and global finance trust Palantir to safeguard their most important data assets. Palantir platforms are aligned with NIST 800-53 and NIST 800-171. Additionally, Palantir platforms annually complete a SOC 2, Type 2 audit (Security, Confidentiality, and Availability); are certified compliant with FedRAMP Moderate, U.S. DoD Impact Level 5, ISO 27001/27017/27018, and ISO 9001; hold cyber essentials and cyber essentials plus certificates; and perform an annual NHS Data Security Protection Toolkit assessment.

In addition, as a data processor, Palantir has extensive experience helping customers meet specific regulatory and industry requirements, including HIPAA, GxP, GDPR, CCPA, CJIS, and FISMA High.

Palantir operates in a broad variety of security environments with extremely diverse authentication requirements. In summary, Palantir's Security Model provides:

- Fine-grained access controls that secure every piece of data individually;
- Specific degrees of access including ownership, write, read, discovery and no access permissions;
- Collaboration with security;
- Secure data integration; and
- Full and immutable audit trail.

4.0 INFORMATION ASSURANCE

Our approach to information assurance takes all appropriate protective measures to establish administrative, technical and physical safeguards to assure information in all its forms.

Palantir platforms are aligned with NIST 800-53 and NIST 800-171. Additionally, Palantir platforms annually complete a SOC 2, Type 2 audit (Security, Confidentiality, and Availability); are certified compliant with FedRAMP Moderate, U.S. DoD Impact Level 5, ISO 27001/27017/27018, and ISO 9001; hold cyber essentials and cyber essentials plus certificates; and perform an annual NHS Data Security Protection Toolkit assessment.

Palantir services encompass threat mitigation, information security management, data traceability, access controls, encryption, systems development and maintenance, infrastructure security, and disaster recovery. Palantir platforms include built-in technical measures that protect and defend the system by ensuring its availability, integrity, authentication, confidentiality and non-repudiation. These measures were factored into the original software development process and continue to be priorities for current and future configuration.

Availability: Palantir platforms are designed for high availability and have been successfully deployed in environments with stringent uptime requirements. Palantir platforms provide several features that are designed to increase system availability, including redundant storage and a fault-tolerant architecture. Palantir will provide robust system patching on a frequent schedule, and all team members are experienced in regularly updating systems to minimise vulnerabilities. Palantir can conduct regular, incremental backups of all data in the system and provides the option to restore remotely.

Integrity: Palantir provides a high degree of system integrity by encrypting all data at rest and in transit and by regularly patching the operating system and all applications. Palantir platforms also include an audit log to ensure that all system activity and data usage is aligned with any governing rules or policies.

Authentication: Palantir platforms provide internal authentication and authorisation services that can store user groups and permissions and authenticate user credentials for the system. These services support Single Sign On (SSO), which allows for a single point of entry and access control. Palantir platforms can also integrate with third-party integration services such as Public Key Infrastructure (PKI) and Active Directory, and supports multi-factor authentication.

Confidentiality: Palantir utilises appropriate controls such as firewalls, password protection, encryption and digital certificates at all times to protect confidential information that is processed by, stored in or transmitted from the system. Palantir platforms include robust, granular access controls so that each individual piece of information can be marked with the appropriate classification. Palantir also ensures confidentiality by encrypting all data in transit and at rest.

Non-repudiation: Palantir offers non-repudiation by authenticating, monitoring and auditing all user activity in the system in protected access and activity logs.

5.0 ONBOARDING PROCESS

Palantir uses a multi-phase approach to the on-boarding process, which provides robust, agile and rapid approach to capability provision that has been tested, refined and proven across over hundreds of deployments with reliably excellent results. This multi-phase approach typically includes:

- Scoping and Clarification / Preparation Phase
- Infrastructure Setup Phase
- Implementation Phase
- Support & Maintenance Phase

5.1 AGILE METHODOLOGY

Palantir uses an Agile methodology to implement and configure our platforms. Structuring the implementation phase into Agile Sprints (time-bound periods of work, generally one (1) or two (2) weeks) gives customer stakeholders at all levels the opportunity to provide timely feedback, design input and updates on task prioritisation. Palantir then uses this information to inform Sprint planning, allowing them to quickly address changes in requirements with minimal disruption to the project schedule.

Unlike the Waterfall methodology, which can be linear or difficult to alter when project circumstances shift, Agile project plans are designed to incorporate the unexpected without disrupting the delivery of higher-level capabilities. In this way, an Agile approach will be better placed to build upon customer feedback on newly delivered capabilities, as well as to conduct any future unforeseen configuration work that may be required beyond the initial goals of this project. Further discussion and detail on Palantir's Agile methodology can be provided upon request.

6.0 TRAINING

Palantir designs and executes customer-specific training plans based on the user profiles, scale, workflows, and production timelines for each deployment of our software. Our approach to user training is flexible and aims to accommodate the different user groups of the relevant platform and their technical competencies to ensure all users become proficient at using the platform for their specific roles. Training can be delivered on site by Palantir, with expert support from Palantir's global engineering resources as needed, or via a variety of other self-guided methods.

The general types of training provided are:

- **In-person, instructor-led training**: Palantir can hold specific training sessions at customer locations, tailored according to user profile, specific contract requirements and project stage.
- **Internet webinars**: Webinars are available on a variety of topics, based on ongoing assessments of end user needs. Webinars allow flexibility scheduling, varying user adoption rates and location.
- **Self-guided learning**: Palantir also provides for self-paced training through our web-based video training application that includes features such as videos and documentation. Palantir have successfully used our web-based video training method at many engagements with diverse user bases.

7.0 SERVICE MANAGEMENT AND SUPPORT

7.1 Maintenance and Support Approach

Palantir's maintenance and support approach is designed to minimise system downtime and ensure that users have the access they require to perform mission-critical work. Support is accessible by phone or email. Our quality assurance measures ensure that support meets or exceeds industry best practices and is tailored to each individual organisation.

7.2 Support Services, including Service Desk Support

To ensure that users and system administrators are fully supported throughout the duration of the contract, Palantir can provide a combination of in-person and remote support services as needed. Help Desk support is handled by the Palantir's embedded engineering teams who provide prompt triage, response, and resolution of issues.

Palantir will implement, install, monitor, and test all parts of the platform for correct operation and can fully support the needs of the customer on an ongoing basis by providing maintenance services, including troubleshooting during critical periods and ongoing configuration work.

As a commercial product, our platforms also include an online support portal that provides authorised staff with immediate access to system information and help documents, including user guides, training manuals, frequently asked questions and troubleshooting documentation.

7.3 Incident Management

Our support model utilises Palantir's best practices for quality assurance and quality assurance surveillance. Palantir has a standard incident management process, annually updated, and approved by management, for security events and suspected security incidents that may affect the integrity, availability, or confidentiality of Palantir systems, such as data breaches. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation.

Palantir maintains both a process for manually reporting security incidents and an automatic alerting system of security events. Palantir employs activity and integrity monitoring tools with automated alerting and uses tools such as Jira and PagerDuty for triaging, notifying relevant parties, and tracking alerts and incidents. When the response teams receive a security alert, they tag the alert with a priority level and gather all relevant and precipitating details. Alerts are triaged on the basis of highest-priority alerts first.

High-severity alerts receive human action promptly. Other alerts receive a response based on predetermined SLAs. Alerts are categorised and tagged with relevant information for later review and analysis. If relevant, alerts are escalated to a Security Incident.

7.4 Change Management

Palantir's Change Management Policy sets standards for upgrading capabilities, responding to threats, adhering to laws/regulations, and complying with contract obligations, while limiting impact and ensuring adequate messaging. All changes to systems must be submitted as a "Change Request". The relevant teams review the request, prioritise, and develop a plan for implementation. Authorised users approve changes under Palantir policies and procedures, and customers are notified of any major changes per agreed upon processes.

The process typically includes:

- Change Tracking
- Testing
- Approval
- Communicating Changes
- Scheduled Maintenance
- Monitoring Changes
- Emergency Changes

7.5 Release Management and Preventive Maintenance

Palantir will perform release management and preventive maintenance on our platforms to ensure that they are kept in proper and reliable working order. Our maintenance structure is adaptive, providing regular and high-priority releases (as needed) and continually reprioritising work based on feedback and trends.

7.6 Feedback

Palantir constantly collects useful feedback from our users, monitors trends in incidents and new feature requests, and prioritises development work against what is observed in the field. Notable incidents are consolidated into internal tracking systems, where they are continually reviewed and analysed against other incidents received from across Palantir. Issues of wider concern are flagged to other engagement teams or to appropriate product developers for resolution in future product releases. Due to our rapid response times, Palantir have provided releases to customers in as little as one (1) hour for emergency fixes (e.g., for emergency security vulnerabilities).

8.0 SERVICE CONSTRAINTS AND LEVELS

Palantir recognises that each customer has different maintenance schedules and different service continuity needs. Palantir platforms are configurable to meet the specific needs of a customer's environment and Palantir teams can be flexible to meet the needs of a customer with respect to planned maintenance, service disruption and outages, and will ensure that any such events are appropriately communicated.

Wherever possible, planned maintenance will be carried out without affecting the service. This will generally be achieved by carrying out planned maintenance during periods of anticipated low traffic and by carrying out planned maintenance on part, not all, of the network at any one time. Where emergency maintenance is necessary and is likely to affect the service, Palantir will endeavour to inform the affected parties as soon as possible within the start of the emergency maintenance. Level of availability varies depending on the specific project.

Refer to the ‘Ongoing support’ and ‘User support’ sections of the ‘Palantir Platform: Gotham’ catalogue entry webpage for further information on Palantir’s Service Level Agreements (SLAs).

9.0 SERVICE TERMS

Please refer to the ‘Terms and Conditions document’ on the ‘Palantir Platform: Gotham’’ catalogue entry webpage.

10.0 BUSINESS CONTINUITY & DISASTER RECOVERY

10.1 Business Continuity

Palantir conducts a regular, and at least annual, risk assessment and business impact analysis to understand and mitigate risk of business disruption. Results of these assessments are used to update Palantir’s contingency policies and procedures. To ensure the reliability of plans in the event of an incident, contingency exercises are performed on representative environments at least annually and results are documented. Results of contingency exercises are then used to update the Continuity Plan.

Description of the Platform’s Business Continuity Configuration
Palantir has configured our platforms to be highly available and to take regular backups as part of its contingency planning. Palantir has minimised the need for downtime related to hardware failure or for maintenance to hardware or software products. Additionally, Palantir takes backups of the system to reduce the risk of data loss from corruption, accidental deletion, or to resolve disputes.

Highly Available Configuration
Palantir platforms are designed to be highly available. Customers are hosted in an active-active configuration; meaning that within a Region the fail-over status is Hot.

Data Centres
Palantir uses best in class cloud hosting providers such as Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) as the underlying cloud service providers for our platforms. The global infrastructure of these services is built around Regions and Availability Zones. A Region consists of multiple Availability Zones, physically separated and isolated, where offered by the underlying cloud service provider, which are connected with low-latency, high-throughput, and highly redundant networking. Cloud Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data centre infrastructures. Using this infrastructure, Palantir platforms are designed and operated such that failover between Availability Zones within a Region is executed automatically and without disruption to users (RPO/RTO: 0/0).

Data Stores
Palantir Foundry uses the underlying cloud providers' storage solutions, such as AWS S3, Azure Blob Storage, or Google Cloud Storage, as its primary customer data store. Palantir Foundry additionally uses Cassandra installed on the cloud providers' compute platform, such as AWS EC2 instances, Azure Virtual Machine hosts, or GCP Compute Engine, as its primary metadata and configuration data store.

Palantir Gotham uses Postgres or Oracle on the underlying cloud providers' storage solutions, such as AWS EC2 or RDS, Azure Virtual Machine hosts, or GCP Compute Engine, as its primary customer data store and metadata and configuration data store.

Additional computations may run on datasets within Palantir Foundry or Palantir Gotham to produce data transformations and may generate and store results or views in Elasticsearch or Postgres. Any computational index metadata, such as these, are considered secondary data stores and can be automatically rebuilt or rehydrated based on the Palantir platform’s primary data stores.

Palantir platforms leverage the underlying cloud service providers’ infrastructure to ensure all data, in primary or secondary stores, is replicated to multiple active hosts simultaneously, so that the platform is resilient to single points of failure and automatically restores redundancy after hardware faults are resolved. If an Availability Zone were to go down, no data will be lost permanently, and an RPO/RTO of 0/0 is achieved.

The SLAs of the underlying cloud service providers services are determined by the underlying cloud service provider and can be found on their respective websites.

10.2 Disaster Recovery

Backups
Palantir platform backups are archived sets of data used to restore the original after a data loss event. While a highly available configuration, as described above, mitigates risk resulting from a loss of a physical datacentre or other hardware outage, it does not mitigate the risk of data loss due to such things as accidental data deletion or corruption. To mitigate this risk, Palantir also takes regular backups of the system.

Upstream Customer Data Sources
Customers are responsible for the integrity and backups of data in customer managed source systems. The resilience of such data integrated into Palantir platforms are dependent on the customer's business continuity practices.

Platform Configuration Backups
Palantir leverages a system called Rescue to back up and restore the services that make up Palantir platforms. The backup cadence defaults to taking a backup snapshot every two (2) hours. Rescue stores these snapshots in an encrypted CSP storage bucket, such as AWS S3, Azure Blob Storage, or Google Cloud Storage. These snapshots can be used to restore the entire state of Palantir platform to a point in time. The default retention period for the Rescue backup is seven (7) days. Palantir continuously monitors Rescue to ensure the health of backups.

11. TECHNICAL REQUIREMENTS

Please refer to the ‘Using the service’ section of the’ Palantir Platform: Gotham’ catalogue entry webpage.

12. PRICING

Please refer to the ‘Pricing document’ on the ‘Palantir Platform: Gotham’ catalogue entry webpage.

13. OFF-BOARDING PROCESSES

Palantir platforms lay an integration layer on top of an organisation's disparate IT landscape, thereby serving as a single point of access to all data within an enterprise without requiring data duplication, data cleansing, or data warehousing. In this way, the cost, time and risk associated with implementation or cessation of service are minimised.

Palantir is an open platform with open, non-proprietary data and file formats, public APIs, a plug-in architecture, and numerous extensibility points. Once data is integrated into Palantir platforms, it is easy to export it in many different formats or otherwise make it accessible to other software systems. Such flexibility allows data to be exported in formats that are easily digestible by other tools as needed. Palantir can assist the customer with any data retention, archiving, transportation or destruction requirements.

14. DATA REMOVAL AND EXTRACTION

14.1 Data Removal

Palantir provides various capabilities for restricting and removing data from its platforms, including a hard delete capability, which involves a full purging of the specified data object and amounts to complete, irrecoverable removal of the underlying information and destruction of all traces thereof from the hardware. Palantir commits to purge and destroy customer data from any computers, storage devices and storage media that are to be retained by Palantir after the end of the contract period, and the subsequent extraction of customer data (if requested by the customer).

14.2 Data Extraction

If the customer wishes to extract their data when the contract ends, Palantir can export all existing data in the platforms into raw formats. Palantir's software platforms have been purposefully designed to prevent vendor lock-in. As such, they have an open, pluggable architecture with publicly documented APIs at every tier of the software. All data in the platforms can be securely exported in non-proprietary formats for use in other databases or systems. Palantir will work with the customer to determine the best export format(s) for customer datasets and their destination systems.

Palantir