Palantir

Target Workbench

Collaborate across the target lifecycle.

Palantir Technologies
→ palantir.com

At Palantir, we build next generation software to help solve some of the world's most critical problems. Over the course of 20+ years, we have developed a set of core capabilities that connect our intelligence and defense partners' most sensitive data and analytic capabilities to help power operational execution.

Overview ↘

Palantir Target Workbench is a modern solution for efficient and responsible target management. Users can centrally manage intelligence gathering and target identification, leveraging a shared and access-controlled common intelligence, operating, and targeting picture to visualize order of battle. Built on top of the Palantir platform's robust and security-aware architecture, users across intelligence and operations are able to collaborate securely and seamlessly across the entire target lifecycle. Below are the core Palantir platform pillars which underpin the capability:

- Data-Centric. Integrates and visualizes models and data, regardless of type or volume.
- Secure. Drives organization-wide collaboration with stringent, platform-wide security.
- Interoperable. Offers federated data systems, extensibility, and data export.

Features ↘

Target Workbench aims to provide a flexible, process-oriented scaffolding that allows users from across the target lifecycle to collaborate securely, responsibly, and effectively. Integrating learnings from the field, Target Workbench manages the targeting decision framework, including assignment authority, objectives, selected cycles, control measures, risk thresholds, and resource assignment. Agile and tactical, Target Workbench can be deployed to different environments, and supports ingest and export of multiple message types to communicate with systems at the edge.

Palantir's human-in-the-loop approach to product means Target Workbench supports adherence to doctrinal targeting lifecycle standards, while permitting for maximal allowed customization. In accommodating the variance, users are empowered to dynamically change the loop when, for example, initial assumptions and ground truth diverge. To accelerate and improve the decision-making ability of users, AI-generated insights surface key supporting intelligence, fostering comprehensive, responsible targeting lifecycle – from identification to execution and evaluation. In integrating AI enablement into the baseline of the product, users can reduce the total time to decision-making.

Collaborative.

Palantir Target Workbench supports secure collaboration to empower the range of users required for effective and responsible management throughout the target lifecycle, across echelons. Directorates can centrally manage intelligence gathering and target identification with a shared and access controlled common intelligence picture to visualize order of battle backed by authoritative multi-INT

Palantir

Palantir Technologies
→ palantir.com

sources. Once a potential target has been identified, operators can move them through the authorized approval processes to track status and push secure messages commensurate with the guidance and objectives of the targeting authority. In platform, multiple users can collaborate in real-time on the same targets for improved understanding and situational awareness. Target Workbench supports attaching intelligence, either from in-platform insights or external sources, to help users make maximally informed decisions.

Configurable.

Palantir Target Workbench enables authorized users to bring targets from the identification to execution and evaluation. Anchored around a Kanban board-like interface, Target Workbench maps to the targeting stages, customizable to organization-specific targeting workflow nomenclature. Correctly permissioned users can enable workflow-centric "collection" with the ability to flexibly sort and group targets, configure columns, select actions, and issue warnings. Operators – wether they are configuring or actioning targets – are maximally empowered by the technology required to complete these critical workflows. Additionally, Target Workbench allows for the integration of multiple Effector Pairing solutions so that users can select and and action targets, with decisions captured for continuous evaluation of the Fires process.

Below are configurable elements that Target Workbench integrates into its workflow-centric approach:

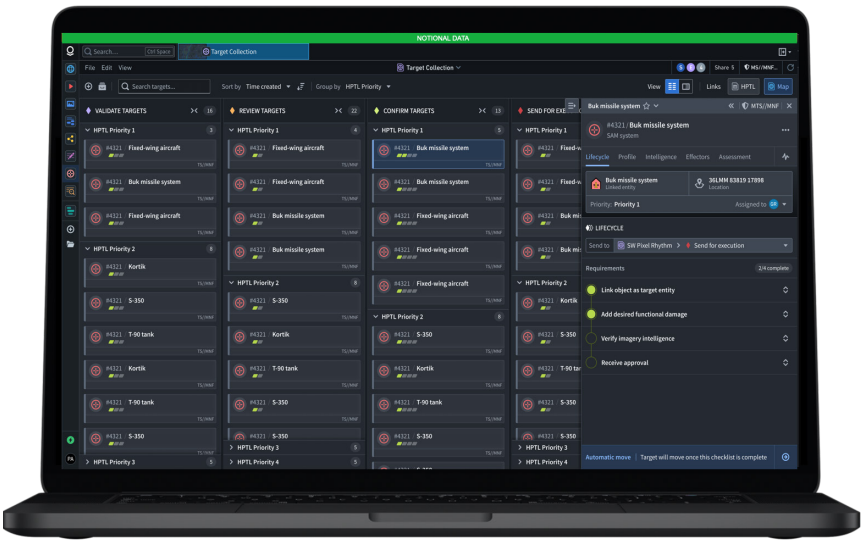
- Lifecycle. Authorized users are able to define what stage of the lifecycle the target is at (e.g., target identification, target execution, BDA).
- Approvals. Sets the approvals required for action to be taken on sensitive targets or in sensitive contexts, in line with the application's purpose to enable users to conduct responsible decision-making.
- Activities. Activities tracks the list of changes that have been made to the target (e.g., moving columns, BDA fields) to promote transparency in decision-making across the application.
- Profile. Users can attach more information about the target under this tab.
- Location. Users are able to set or edit a location to a link object's live location.
- Intelligence. Users can attach detections, information, and media to the target. This includes photographs and documents, which enable users to create a comprehensive view of the target.

Palantir

Palantir Technologies
→ palantir.com

Secure.

Like all Palantir solutions, Target Workbench is backed by platform-wide privacy and security models: role, classification, and attribute-based access controls provides nuanced management over user interactions with data and platform resources. Palantir's granular security markings ensure that only the stages of the targeting process that a user is authorized to see are surfaced. For example, a user with 'imagery analyst' permissions would only see the columns relevant to their workflow (e.g., 'In Investigation' and 'Sent for Approval'). Furthermore, the current status of a given target is visible alongside the corresponding security marking.



Operator Centric.

Partially automated, this baseline capability gives time back to operators in time-sensitive and constrained decision-making environments, surfacing results to target location queries and enabling prioritization of targets. Users can quickly understand critical questions such as: 'Where should I be searching for targets? Of things that are targets, the priority of those things?' Target Workbench leverages HPTL infrastructure to quickly define to users what they can add to the Kanban board and adds warnings or alerts that flag areas of interest, the decay time of intelligence, and more. The platform also supports No-Strike List (NSL) integrations to ensure users have a complete picture of a potential target's environment, including available resources, the recency of the intelligence, and NSL entities.

Example Workflow ↘

Within a unified, AI-enabled and security-aware single pane of glass view, users can manage the entire targeting decision framework.

1 Tasking	Outcome Enabled: Timely, on-demand commercial overhead collection driven by the user community's evolving needs.
2 Exploitation	Outcome Enabled: Build mission critical intelligence and nominate targets from any type of overhead imagery.
3 Target	Outcome Enabled: Full, doctrine-based lifecycle management and custody of targets at scale.
4 Execute	Outcome Enabled: View all targets on a fused, multi-INT map to apply the Military Decision-Making Process (MDMP) in a single, intuitive platform.
5 Battle Damage Assessment (BDA)	Outcome Enabled: Accelerate the BDA process by tasking overhead collection to quickly receive relevant imagery.

A Verified Solution ↘

With Palantir's modern Software-as-a-Service (SaaS) solutions, organizations are addressing data modernization challenges and increasingly harnessing massive-scale data for accurate insights and data-driven operations and decision-making at all levels. The Palantir platform is a rapidly-deployable product designed to enable adhere to the strictest of Privacy and Civil Liberty standards and built on the principles of Zero-Trust security. Palantir has deployed solutions in the cloud on NIPR, SIPR, and JWICS; these capabilities are delivered on AWS GovCloud, SC2S, and C2S, respectively. Palantir's capabilities maintain rigorous, externally verified infrastructure and operations standards and are compliant with GDPR, CNSSI 1253, ICD 503, and NIST SP 800-53 and has been accredited at the IL2, IL5, IL6, and TS/SCI levels.