Palantir

Secure Collaboration

A Next Generation Collaboration Ecosystem

Palantir Technologies
→ palantir.com

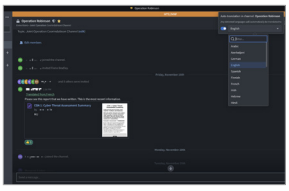
The Palantir platform offers users seamless and secure collaboration across mission enclaves and geographies in classified or multi-level security environments.

Palantir

Our solutions reflect nearly two decades of partnership with the Defense and Intelligence communities, helping empower end-users to make data-driven decisions across critical warfighting functions; users can securely collaborate on mission plans, create documents, slides, maps, and spreadsheets that update in real time with seamless synchronization. The Palantir platform's data-centric design enhances coordination and cooperation among DoD and mission partners by integrating previously stove-piped data sources and structuring mission data with a shared semantic layer that is security-aware. Furthermore, our solution offers additional protections to the networks and authoritative data sources involved by leveraging a robust backend of federated access management and control across role, echelon, and environment - even in disconnected, intermittent, and/or low bandwidth (DIL) environments.

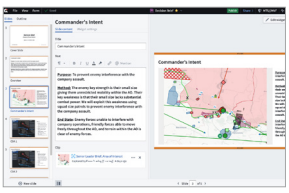
Mission Tools & Applications

With the Palantir platform, the U.S, Allies, and Communities of Interest (COIs) can leverage secure collaboration capabilities that are powered by intelligent security to seamlessly operate across security domains and mission enclaves.



Chat ↘

Users securely share direct messages, files, and data in a classification-controlled, cross-network chat application, with automatic translation, redaction, and mission data extraction. Palantir Chat interoperates with existing messaging systems, allowing users to collaborate live with any other chat clients users. Multi-user channels use access controls to manage membership, trace network access, and permissions of member users.



Briefings ↘

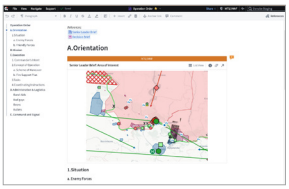
Enable collaborative slide development and live briefing with data-backed presentations. Users can drag and drop data and analysis from other applications to quickly build slides (e.g., embed dynamic maps within mission plans). Presentations built are both data and security-aware. Intelligent fields auto-populate where data already exists in the system and dynamically generate additional fields and options based on user input.

Gaia ↘

Securely integrate partners into all phases of an operation. Geospatial tooling enables analysts and operators to work within a shared map interface for intelligence preparation, digital mission planning, and live battle tracking on top of an integrated data asset. Users across mission enclaves and COIs can concurrently build a holistic operations plan with a shared understanding of both mission and operating environment.

Video ↘

Leverage AI-enabled video to power decisions. By tagging entities in the observed area, such as buildings, cars, or persons of interest, users can layer their institution's canonical geospatial data on live or archived video in real time. With automated insights from computer vision over full motion video, users can discover and decipher events as they evolve.



Dossier ↘

Capture, contextualize, and share data-driven insights and intelligence products. Users can create collaborative data-backed documents that update in real time and follow agency-defined business processes for document approval, dissemination, and archiving. Create new documents from scratch or via templates, and trace data back to the source with links that show provenance.

Security-First Software

At Palantir, we believe that agile and intelligent security is the differentiating factor for a truly collaborative experience. The complex range of current and anticipated worldwide operations that joint forces must be prepared to conduct require a solution that delivers capabilities for sharing mission data at SECRET/Releasable levels. To enable this, all applications are backed by a fine-grained security model. Security features like classification-based (CBAC), role-based (RBAC), and attribute-based (ABAC) access controls facilitate the seamless, secure sharing of artifacts and underlying data. Palantir's capabilities maintain rigorous, externally verified infrastructure and operations standards and are compliant with CNSSI 1253, ICD 503, and NIST SP 800-53 and has been accredited at the IL2, IL5, IL6, and TS/SCI levels.

Palantir

- → Coalition sharing and collaboration. Data replication across multiple servers at different enclaves allows data to be securely shared between partner nations. Users across warfighting functions, roles, and countries can make rapid operational decisions locally that are fully informed by a global dataset without jeopardizing the integrity or security of shared data.
- → A consistent user experience even in disconnected environments. Nexus Peering works even in low bandwidth conditions or disconnected environments. In those instances, data is queued for transmission when connection is reestablished. This ensures a consistent and reliable user experience regardless of connectivity.
- → Adaptable security levels. Artifacts like documents, slides, spreadsheets, and maps automatically update to the highest security level of their content. Alternatively, users have the option of redacting data down to a lower sensitivity level.
- → Robust classification and security permissions. Access Control Lists (ACLs) allow organizations to control data access based on mission sensitivity, personnel roles, data protection regulations, and other security considerations, ensuring that users can only view the information they are authorized to access. Controls can be placed on individual users, groups of users, individual pieces of data, and whole datasets.
- → Real-time data sharing without duplication or destruction. Nexus Peering combines data enriched by different users and teams without creating duplicate or conflicting copies of the data, thus improving situational awareness for all collaborators. Nexus Peering weaves together relevant information from other Palantir platform instances in the "mesh" to create an enterprise picture for shared workflows.

Real World Application

A U.S. defense organization uses the Palantir platform to power collaboration with mission partners and facilitate secure, classification-controlled information sharing across networks and security levels. As a result, this customer and the allies and partners it is responsible for coordinating with are able securely share information in real time. This timely contextual picture reduces risk and helps encourage stronger partnerships. The defense customer has powered collaboration in joint exercises which saw multiple partner nations to execute across warfighting functions via artifact/track sharing, track exportation to Joint Automated Deep Operations Coordination System (JADOCS), map sharing, internal and external chat, and translation.