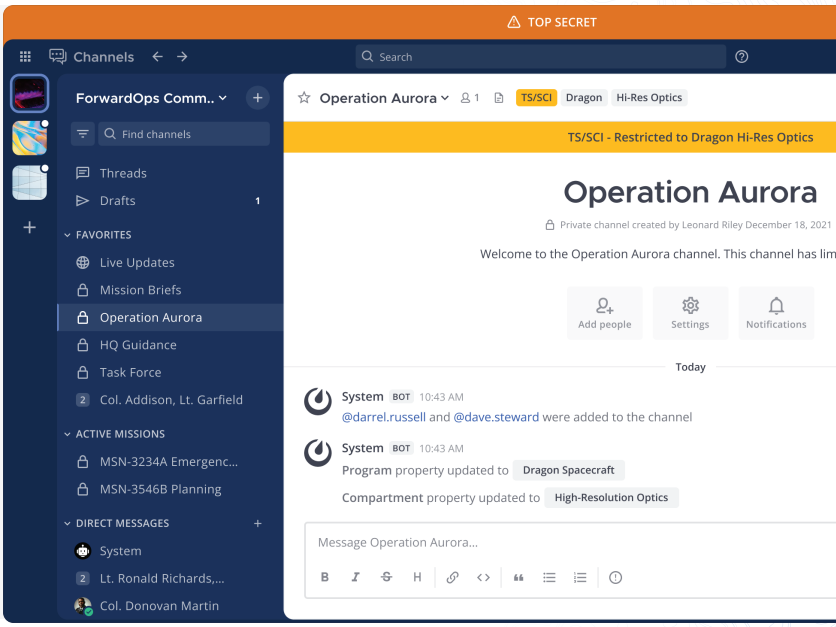
Mattermost

About Mattermost

Sovereign collaboration and workflow automation for multi-domain secure operations

Mattermost Enterprise Advanced is purpose-built for multi-domain secure operations at scale. Dynamic Zero Trust access controls enforce data segmentation across classified environments, while data spillage handling and burn-on-read messaging protect the most sensitive workloads.

Scale to 200,000 concurrent users across air-gapped and DDIL architectures, with **automatic channel translation** and **mission partner environment support for seamless cross-domain collaboration.**



Zero Trust by Design

Attribute-based access control (ABAC), identity-centric access management (ICAM), and policy segmentation enforce trusted data separation across classified environments, with dynamic policy enforcement from user authoritative sources.

Sovereign Data Protection

Channel classifications, data spillage handling, and burn-on-read messaging safeguard classified and sensitive workloads with stringent protection controls.

Ultra-High Resilience

Scale to 200,000 concurrent users across high-availability architectures with zero-downtime upgrades. Shared channels keep mission-critical teams connected across air-gapped, DDIL, and mission partner environments.

Contact Us: mattermost.com/contact-sales/

Key Capabilities

Zero Trust Access Controls

Dynamic attribute-based access controls enforce zero trust policies across channels, files, and messages based on clearance level, programme affiliation, device type, and location. Policies are configured via Common Expression Language (CEL) or a simple GUI, with attributes synchronised from ICAM platforms or a user authoritative source, aligning with DoD and allied Zero Trust frameworks.

Burn-on-Read Messaging

Set visibility time limits on messages so they are automatically removed from endpoints after a defined period. Ideal for exchanging sensitive information such as one-time passwords, personally identifiable data, or during time-sensitive operations at the edge, minimising exposure windows for classified communications.

Mission Partner Environments on the Edge

Support cross-domain collaboration with automatic channel translation for real-time multilingual communication across global and coalition environments. Shared channels synchronise messages and files between separate Mattermost servers, enabling federated operations even across isolated networks on the edge.

Environmental Attribute-Based Controls

Synchronise environmental attributes from third-party endpoint security, network management, ICAM, and security tools to enforce dynamic zero trust policies. Policies incorporate device state, network segmentation, endpoint security posture, and other environmental attributes to maintain control of classified and sensitive information.

Channel Banners & Data Spillage Handling

Channel banners display classification markings (CUI, U, S, TS) visible at all times. Any user can quarantine potential data leakage for review; reported content is immediately hidden and a designated security team is notified with full context, including a list of users who may have seen the data. After security review, posts can be cleared or permanently deleted from the system.

Security-Optimised Mobility

Advanced mobile protection without requiring MDM: OS-level data-at-rest encryption, biometric authentication, jailbreak/root detection, screenshot and recording prevention, and a secure file viewer that allows documents viewing without local download. Intune MAM enforces policy-based controls and prevents data leakage between personal and work mobile devices.

Ultra-High Resilience in Air-Gapped and DDIL

Scale to 200,000 concurrent users with high-availability architecture, dedicated write-through caching, and zero-downtime upgrades. Shared channels ensure operational continuity across air-gapped, DDIL, and degraded network conditions, enabling joint and coalition operations.

Everything in Enterprise

Enterprise Advanced includes all Enterprise capabilities: sovereign AI automation, workflow automation with collaborative playbooks, critical infrastructure hardening (FIPS 140-3, STIG), high availability and resilience, eDiscovery and legal hold, AD/LDAP synchronisation, federated communications, and 24/7 support with a four-hour SLA.

Ready for multi-domain secure operations?

Contact us today at mattermost.com/contact-sales

Mattermost