MindLink Chat Engine

MindLink Chat Engine (MCE) is an ultra-secure and mission-focused collaboration platform designed for classified communications at above TOP SECRET. MCE protects mission data, enables mission-critical use cases, delivers frictionless and safe sharing of highly sensitive information in realtime.

Designed for mission scenarios, MCE meets strict security requirements in key areas such as data classification (above Top Secret), enterprise end-to-end encryption, and communities of interest. Through MCE, we deliver unparalleled, secure, realtime collaboration capabilities for the modern mission theatre.

Classification & Control

MCE data classification is the unique adaptation of military-grade labelling and access control techniques to chat rooms and messages using sophisticated national classification systems such as CAPCO as GSCP.

Mission-focused UX

MCE natively supports mission scenarios such as realtime coordination, watch-based teamwork, incident management, and is engineered for use from remote or forward-deployed positions.

Communities of Interest

The MCE security architecture is rooted in the novel "Communities of Interest" paradigm advocated by the Intelligence Community based on 'the Need to Know' and Coalition Working.

Enterprise End-to-End Encryption

MCE's end-to-end encryption is an innovative approach to zero-trust architecture using specialized information security paradigms adopted by the Intelligence Community.

MindLink

Chat and Collaboration with a Mission Focus:

Realtime, High Volume

MCE is a next-generation ultra-secure persistent chat server engineered for high volumes of messages, chat rooms, and active users.

It acts as frictionless communication backbone for the demanding, dynamic, and data-intensive modern mission, whilst organizing and safeguarding highly-sensitive data.

This delivers faster, more accurate, and more intelligent decision-making towards better mission outcomes, whilst simulaneously mitigating increasingly prevalent threats to success.

Mission Features

The MCE platform is specifically designed to support critical use cases and ways of working across the modern mission theatre.

It natively supports mission scenarios such as realime coordination, watch-based teamwork, and incident management, and is engineered for use from remote or forward-deployed positions.

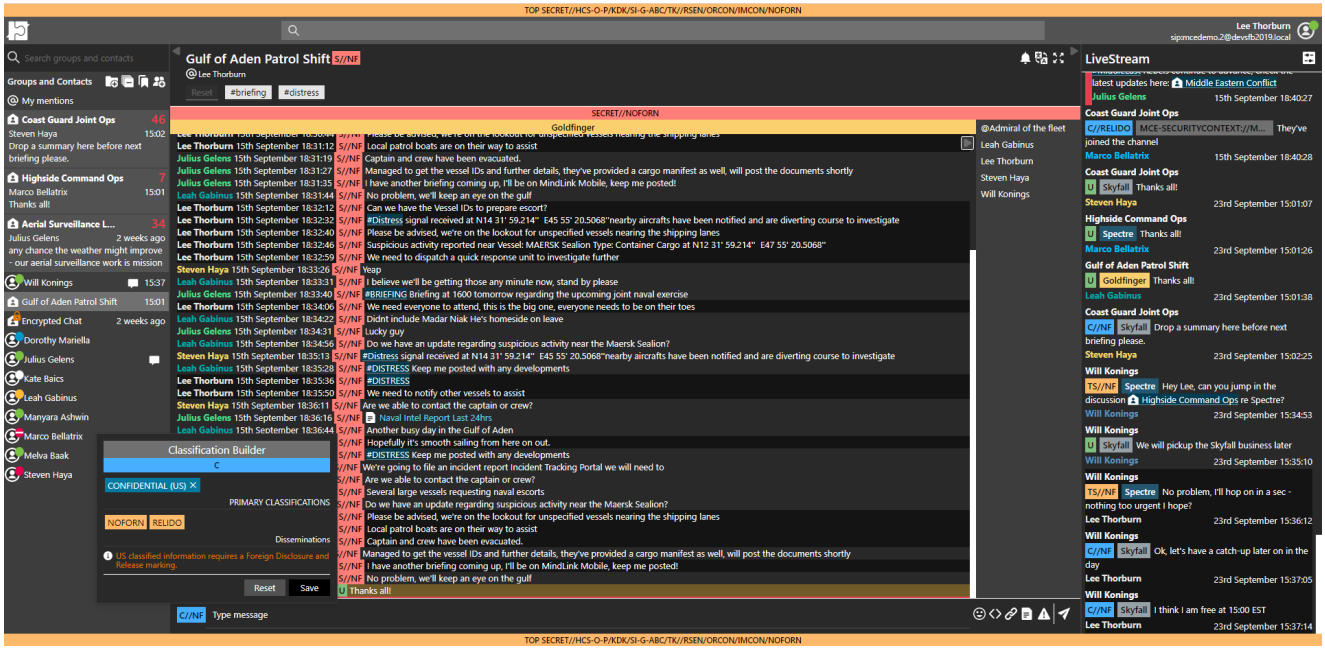
This maximizes operational efficiency through purpose-built tooling by empowering users to focus on mission activities, events, and outcomes, in realtime.

Access Control

The MCE security engine is a sophisticated and multi-layered access control system based on military-grade practices of secret attributes, roles, and security clearances.

It allows chat room access rights to be configured at multiple levels of privilege and granularity through expressive and role-based permissioning rules, using secret attributes and security clearances sourced from trusted third-party directories.

This encourages information flow across the mission theatre through autonomous and devolved management of chat rooms, whilst ensuring that the governance and confidentiality of such highly-sensitive data is maintained.



Secure collaboration using MCE and MindLink Anywhere

MindLink

Next-generation Security Ecosystem:

Communities of Interest

The MCE security architecture is rooted in the novel "Communities of Interest" paradigm advocated by the Intelligence Community.

It segregates all aspects of the system - such as chat rooms, users, and content - into secure compartments to enforce strong access-control boundaries, define explicit data handling procedures, and mitigate spillage risks.

This protects highly-sensitive information using best-practice techniques from the IC by ensuring data is organized and shared only with those with a "need to know".

Data Classification

MCE data classification is the unique adaptation of military-grade labelling and access control techniques to chat rooms and messages using sophisticated national classification systems such as CAPCO as GSCP.

It treats secure chat rooms as dynamically classified documents, performing message and room labelling, classification banner-rollup, and security clearance authorization.

This secures classified data using government-mandated information management practices as first-class chat system constructs, whilst allowing the data to be shared frictionlessly in realtime.

End-to-End Encryption

MCE's end-to-end encryption is an innovative approach to zero-trust architecture using specialized information security paradigms adopted by the intelligence community.

It leverages the "Communities of Interest" pattern to protect and exchange encryption keys whilst preserving both organizational governance and the scalibility required for effective mass-participation, realtime collaboration.

This mitigates prevalent insider threat against the vast attack surface of a typical chat system without compromising the capability of the system to support the modern mission.

Why the FVEY nations choose MindLink

"MindLink Chat Engine enables our internal users and external coalition partners to collaborate effectively and securely in active mission scenarios. By enforcing data classification and end-to-end encryption we minimize the risk of data spillage to better protect the mission. MindLink not only increases our data security posture but directly impacts our ability to make critical decisions in realtime and brings focus to mission execution."

- Government Technology Consultant for US IC

MindLink

Forward-thinking Design & Flexible Deployment:

Secure Multitenancy

MCE multitenancy is the ability to define deep ethical walling mechanisms, trust models, and data management controls to securely partition users and chat rooms on a single MCE instance.

It enables MindLink to be hosted as a centralized hub service for users from allied organizations, agencies, or countries whilst maintaining granular levels of trust, segregation, and secrecy as necessary.

This facilitates the rapid onboarding of multiple coalition partners across the mission arena whilst proactively controlling the risks associated with multi-party intelligence dissemination.

Self-Hosted

MCE is a self-contained system designed to be run on any Windows compute hardware.

It supports a flexible deployment model for on-premises, sovereign cloud, or public cloud, including isolated or forward-deployed networks.

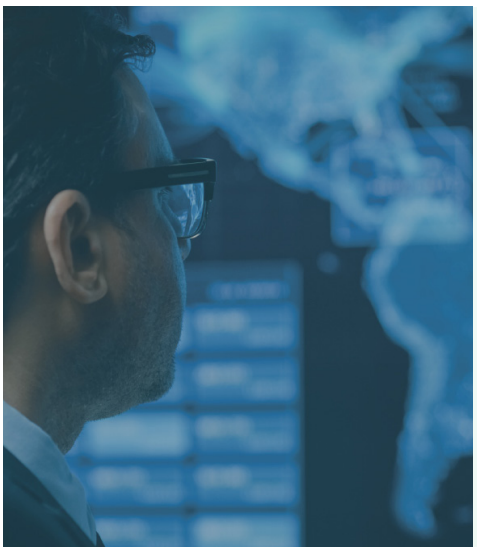
This delivers realtime collaboration capabilities that meet the most demanding of technology, security, and mission needs.

Architecture

MCE is built using a cutting edge event-driven, distributed, and self-healing architecture.

It treats all interactions on the system as immutable data streams, balancing and processing the work across a highly available server cluster.

This achieves reliable, scalable support for large-scale mission operations whilst being inherently compliant and auditable against insider threat.



Advanced Integration Options

MCE is designed to integrate with both existing enterprise infrastructure and third-party collaboration systems.

It synchronizes users and secret attributes from enterprise directories and trusted attribute servers and alagamates third-party complementary modalities (e.g. instant messaging and voice) towards a unified end-user experience.

This provides a low-barrier onboarding and adoption path, implicit compatibility with overarching compliance, security and governance ecosystems, and a seamless end-user collaboration experience.

Find out what MindLink can do for your Mission

Visit MindLinkSoft.com