Coalition Working for Intelligence Partners with MindLink:

A Customer Success Story

Introduction

MindLink are specialists in real-time collaboration systems for highly-secure, mission-critical operations. Our platform is designed for the highest levels of classified communication for government agencies and partner nations. It enables accurate and expedient decision making across mission theatres, in some of the most secure environments in the world.

Since 2018 MindLink has significantly grown its chat services with the Five Eyes (FVEY) Top Secret (TS) and Sensitive Compartmented Information (SCI) National Service providers in the United States and the United Kingdom.

MindLink is the go-to multinational, multi-tenant, coalition chat tool on the TS/SCI fabric. As one of few tools capable of meeting stringent security requirements it is the only known Int. B and Int. C accredited chat service for exceptionally controlled information (ECI) approved by data owners.

An estimate of MindLink's current deployments, at the TS/SCI-level, include instantiations in 30+ individual FVEY and U.S. intelligence and defense communities; dozens of multilateral and bilateral chat services between 1st, 2nd, and 3rd parties; and is the collaboration chat service of choice across the UK's intelligence and defense communities.

The key driver for the adoption of MindLink is that it enables inter-organizational collaboration with full Attribute-Based Access Controls (ABAC) and Enterprise End-to-End Encryption (EE2EE) capabilities. On a single infrastructure instantiation, it allows multiple tenant organizations on the system to collaborate with approved coalition partners. To ensure the privacy of coalitions and their members, MindLink introduces a strict, deep, attribute and classification/clearance-based ethical wall using a secure communities architecture. In effect, it separates tenants that are not permitted to know about, or interact with each other, on the same MindLink instantiation.

To strengthen the use case of MindLink for intelligence and defense, it has been field-tested in low-bandwidth, high network interruption environments. In these constrained network scenarios, MindLink has proven to be a light-weight commercial-off-the-shelf (COTS) chat service. As a result, MindLink is currently deployed with a variety of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) fixed sites to provide near real-time mission awareness and chat history to operations teams.

The purpose of this case study is to highlight the unique problem-solution areas addressed by MindLink for the global intelligence and defense community while also drawing a path for the future. Read on to find out what MindLink can do for your mission.

Problem Definition

With the sweeping changes of digital transformation taking place in every industry across the globe, defense and intelligence organizations are no stranger to modernization, and the need to replace legacy systems to meet the demands of future missions. The current state of collaboration and the systems used between coalition and mission components is disjointed, inflexible and insecure. As a result, this removes the ability to stand up quick and effective collaboration between ever-changing coalition partnerships.

Since the introduction of chat tools, they have been adopted as means for mass collaboration by the global defense and intelligence community. Though chat tools have not outright replaced more traditional means of communication or collaboration, it is certainly the preferred method for partners to share intelligence securely across mission and coalition partners. As quoted from an insider familiar with mission collaboration systems “you can’t have a tel-co [teleconference call] with thousands of members, let alone know who is actually on the call and if they’re meant to be there”.

On the other end of the spectrum, a medium like email might have the ability to reach larger audiences but does not facilitate real-time collaboration and less secure. Due to the real-time and persistent nature of chat and chatrooms, it is a proven medium for collaboration across the mission theatre. From an IT security perspective, chat is inherently more securable, in contrast to other media as chatrooms act as secure data containers, managed by the organization.

Partner nations within a coalition or isolated mission components recognize the use of disparate systems and chat services that cannot communicate with each other as one of the primary barriers for effective mission collaboration. The use of collaboration systems deployed across coalitions, by each mission component, is fragmented and presents significant challenges for interoperability. Consequently, observing the dynamic nature of an evolving coalition, this limits flexibility by not being able to connect with and onboard coalition partners.

Even in scenarios where multi-national mission components can collaborate using a legacy system, security is another major concern as legacy platforms are often not equipped or maintained to protect against emerging cybersecurity threats. A chat system, specifically the data contained within, is a high-value mission asset and, without up-to-date protection, is vulnerable to compromise. A cybersecurity incident could expose entire cross-sections of the mission with a high potential for devastating consequences.

In the realm of government-off-the-shelf (GOTS) collaboration systems this problem is exacerbated as much of the systems and features are developed in-house and systems approach end-of-life due to orphaned technical support.

Finally, unlike commercially available systems, the older GOTS systems in use do not incorporate modern user experience (UX) design tailored for external collaboration with mission partners in an ever-changing coalition landscape.

In summary, the coalition mission theatre requires a secure, coherent, and adaptable solution for collaboration between partner nations which current systems cannot serve.

Additional Constraints

Building on the complexity of an already intricate problem, additional constraints arising from the global intelligence community introduce significant new challenges that require a novel approach towards solution architecture. Layered on top of the need to securely connect mission elements across organizational and international boundaries the system must also deliver on industry-specific best practices, strict security and data-handling requirements and usability in remote/forward deployed scenarios.

Protecting against the Insider Threat

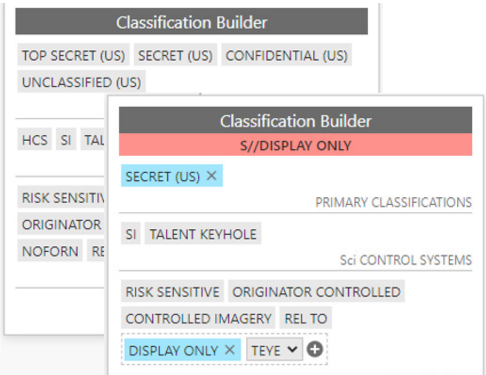
Some of the most prominent security threats originate from inside the organization. Ranging from mild to severe, the insider threat includes incidents involving the 'accidental user' up to more nefarious cases with rogue administrators. Observing the most infamous cases of the last decade, the largest disclosure of classified data occurred through leaks from within the organization rather than the efforts of an external, bad actor. Whereas modern collaboration systems address the insider threat to some extent, systems dating from an earlier era are often solely designed to mitigate external security threats and leave the organization exposed.

Governed Encryption

Encryption isn’t a foreign concept to mission systems and has already gained traction in consumer spaces in the likes of mobile messaging apps. More recently the notion of end-to-end encryption has also become mainstream. The challenge here is not in implementing end-to-end encryption for a mission collaboration system but rather, it is about preserving security while allowing central governance of the encryption keys. The goal is to enable secure collaboration with organizational oversight.

Delegated Authentication and Access Control

To mitigate against insider threat and to support custom authentication methods the mission collaboration system’s authentication and access controls need to be decoupled from the system. Delegating these controls to an external system protects the underlying collaboration estate and reduces the attack surface for the insider threat. More specifically, pertaining to bad actors with security clearance and administrative privileges.



Classification Labelling

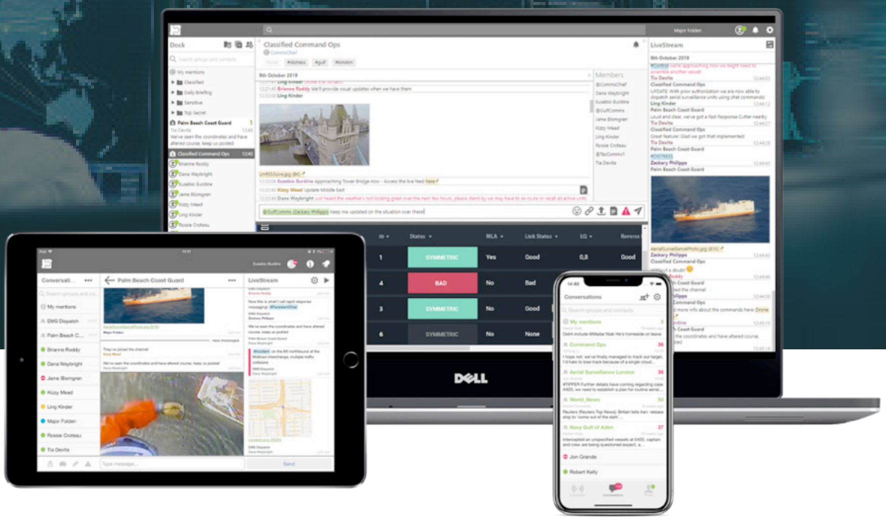
All data shared between mission partners on the system must adhere to classification techniques which have been developed by the intelligence community over multiple decades. The techniques ensure that highly sensitive data is handled correctly. As such, it is necessary to classify and label all data according to security classification standards, for example, CAPCO (US) or GCSP (UK). Like the classification markings on physical documents or emails, any message, conversation, or group must also contain a security classification marking. The marking is both displayed to the user and machine-readable to enforce access rights based on security clearance.

Low Bandwidth Consumption

Forward deployed personnel often face poor network conditions which permits intermittent connectivity with other mission components, at best. Operating in these condition’s restricts the range of tools available for mission collaboration to lightweight applications with a low network footprint as opposed to extensive, cloud-based, software suites.

Secure Community Support

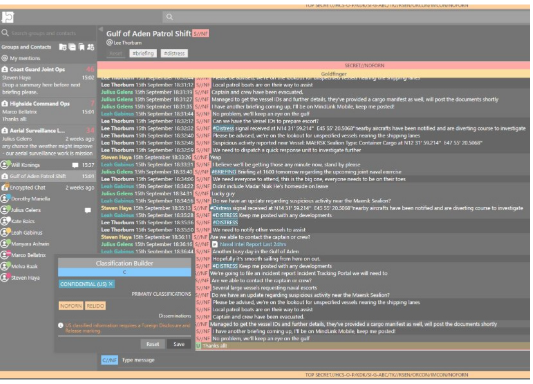
Following industry best practices, collaboration takes place in secure enclaves known as communities of interest (COIs). This practice is designed to quickly stand-up effective collaboration on specific topics that is restricted to relevant parties based on 'the need to know' – which is modelled using a multitude of security attributes, one of which being security clearance. To facilitate this practice, a modern collaboration system will need to integrate such capabilities as a first-class feature.



Solution Design & Implementation

Following the paradigm of persistent chat, a chat system connects thousands of users to disseminate mission-critical information in real-time and is a high-value asset for collaboration across the mission theatre. But to do so securely with the additional, nuanced technology and policy constraints stemming from industry requirements creates a complex problem demanding an equally complex solution.

It was evident that designing a solution would require specialist expertise. With a strong pedigree in engineering collaboration solutions, specifically persistent group chat, and having developed an extensible, next-generation chat engine, MindLink was the right solution partner.



TOP SECRET//HCS-O-P/KDK/SI-G-ABC/TK//RSEN/ORCON/IMCON/NOFORN

Coast Guard Joint Ops 46
Steven Haya 15:02
Drop a summary here before next briefing please.

Highside Command Ops 7
Marco Bellatrix 15:01
Thanks all!

Aerial Surveillance L... 34
Julius Gelens 2 weeks ago
any chance the weather might improve - our aerial surveillance work is mission

Will Konings 15:37
Gulf of Aden Patrol Shift 15:01
Encrypted Chat 2 weeks ago
Dorothy Mariella
Julius Gelens
Kate Baics
Leah Gabinus
Manyara Ashwin
Marco Bellatrix
Melva Baak
Steven Haya

Gulf of Aden Patrol Shift S//NF
@ Lee Thorburn
Reset #briefing #distress

SECRET//NOFORN
Goldfinger

Lee Thorburn 15th September 18:31:12 S//NF Local patrol boats are on their way to assist
Julius Gelens 15th September 18:31:19 S//NF Captain and crew have been evacuated.
Julius Gelens 15th September 18:31:27 S//NF Managed to get the vessel IDs and further details, they've provided a cargo manifest as well, will post the documents shortly
Julius Gelens 15th September 18:31:35 S//NF I have another briefing coming up, I'll be on MindLink Mobile, keep me posted!
Leah Gabinus 15th September 18:31:44 S//NF No problem, we'll keep an eye on the gulf
Lee Thorburn 15th September 18:32:12 S//NF Can we have the Vessel IDs to prepare escort?
Lee Thorburn 15th September 18:32:32 S//NF #Distress signal received at N14 31' 59.214" E45 55' 20.5068"nearby aircrafts have been notified and are diverting course to investigate
Lee Thorburn 15th September 18:32:40 S//NF Please be advised, we're on the lookout for unspecified vessels nearing the shipping lanes
Lee Thorburn 15th September 18:32:46 S//NF Suspicious activity reported near Vessel: MAERSK Sealion Type: Container Cargo at N12 31' 59.214" E47 55' 20.5068"
Lee Thorburn 15th September 18:32:59 S//NF We need to dispatch a quick response unit to investigate further
Steven Haya 15th September 18:33:26 S//NF Yeap
Leah Gabinus 15th September 18:33:31 S//NF I believe we'll be getting those any minute now, stand by please
Julius Gelens 15th September 18:33:40 S//NF #BRIEFING Briefing at 1600 tomorrow regarding the upcoming joint naval exercise
Lee Thorburn 15th September 18:34:06 S//NF We need everyone to attend, this is the big one, everyone needs to be on their toes
Leah Gabinus 15th September 18:34:22 S//NF Didnt include Madar Niak He's homeside on leave
Julius Gelens 15th September 18:34:31 S//NF Lucky guy
Leah Gabinus 15th September 18:34:56 S//NF Do we have an update regarding suspicious activity near the Maersk Sealion?
Steven Haya 15th September 18:35:13 S//NF #Distress signal received at N14 31' 59.214" E45 55' 20.5068"nearby aircrafts have been notified and are diverting course to investigate
Leah Gabinus 15th September 18:35:28 S//NF #DISTRESS Keep me posted with any developments
Lee Thorburn 15th September 18:35:36 S//NF #DISTRESS
Lee Thorburn 15th September 18:35:50 S//NF We need to notify other vessels to assist
Steven Haya 15th September 18:36:11 S//NF Are we able to contact the captain or crew?
Julius Gelens 15th September 18:36:16 S//NF Naval Intel Report Last 24hrs
Leah Gabinus 15th September 18:36:44 S//NF Another busy day in the Gulf of Aden
S//NF Hopefully it's smooth sailing from here on out.
S//NF #DISTRESS Keep me posted with any developments
S//NF We're going to file an incident report Incident Tracking Portal we will need to
S//NF Are we able to contact the captain or crew?
S//NF Several large vessels requesting naval escorts
S//NF Do we have an update regarding suspicious activity near the Maersk Sealion?
S//NF Please be advised, we're on the lookout for unspecified vessels nearing the shipping lanes
S//NF Local patrol boats are on their way to assist
S//NF Captain and crew have been evacuated.
S//NF Managed to get the vessel IDs and further details, they've provided a cargo manifest as well, will post the documents shortly
S//NF I have another briefing coming up, I'll be on MindLink Mobile, keep me posted!
S//NF No problem, we'll keep an eye on the gulf
U Thanks all!

Classification Builder
C
CONFIDENTIAL (US) ×
PRIMARY CLASSIFICATIONS
NOFORN RELIDO
Disseminations
US classified information requires a Foreign Disclosure and Release marking.

C//NF Type message

TOP SECRET//HCS-O-P/KDK/SI-G-ABC/TK//RSEN/ORCON/IMCON/NOFORN

MindLink Chat Engine and MindLink Anywhere

The MindLink Chat Engine (MCE) forms the foundation of the solution architecture. It acts as a secure collaboration backbone built on the fundamentals of persistent chat by enabling real-time, high-volume, persistent group chat and advanced file sharing capabilities. Due to its extensible architecture the platform was augmented to meet the demands of mission usability and security.

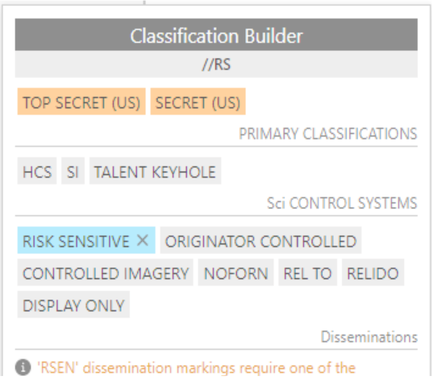
Where MCE operates as the persistent chat back-end, MindLink Anywhere (MLA) is the front-end designed to harness the real-time, high-volume collaboration capabilities and deliver a mission-focused user experience. Together they form the solution set for secure, inter-organizational collaboration.

Secure By Design

Security is undoubtedly the most significant solution area but should not come at the expense of delivering frictionless, real-time collaboration. To address the security requirements MCE and MLA have been extended with unique, highly secure controls to ensure data is protected and still deliver real-time collaboration.

Attribute-Based Access Control

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 permission rules, using secret attributes and security clearances sourced from trusted third-party directories. This encourages information flow across the mission theatre though autonomous and devolved management of chat rooms, whilst ensuring Exceptional Controlled Information (ECI) level protections.



'RSEN' dissemination markings require one of the

Classification Labelling

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 and 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 real time.

Community of Interest Support

Communities of Interest (COIs) is a key, operative paradigm in the global intelligence community for disseminating information to approved parties based on the "need to know". In practice this creates additional access parameters to sensitive information beyond, but not excluding, traditional security clearance levels.

With MCE and MLA we have applied COIs as a first-class concept to our chat system, as part of the security engine as wells as the user experience. In effect, COIs segregate 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 intelligence community by ensuring data is organized and shared only with those with a "need to know".

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 and developed in collaboration with cryptography experts from the FVEYs. It leverages the "Communities of Interest" pattern to protect and exchange encryption keys whilst preserving both organizational governance and the scalability required for effective mass-participation, real-time 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.

Coalition-Ready

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 bi-lateral and multi-lateral intelligence dissemination.

Mission-Focused UX

The MindLink solution set, MCE and MLA, is specifically designed to support critical use cases and ways of working across the modern mission theatre. By developing this in collaboration with mission end-users, it natively supports mission scenarios such as real-time coordination, watch-based teamwork, 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 real-time.

Support and Development Services

As a critical service of international importance, MindLink's professional services and enterprise support team assist and support in the maintenance of their deployments in both development and production environments. This ranges from the enabling of experimental features to test; to priority 1, 24/7 enterprise support; to assistance with user onboarding and new. Following MindLink's immediate product roadmap and key delivery milestones, the FVEY introduce new features to their user base following a regular software release cadence.

Using close working knowledge of their use case, environments, and the extensible nature of the MindLink Chat Engine and MindLink Anywhere, MindLink works closely with the intelligence community for continuous innovation in the complex world of coalition collaboration.

Outcomes Achieved

Since the first deployment in 2018 within the intelligence community, user uptake continues to tick upwards and current deployments are rising to over 30 instantiations across various partner nations and organizations. With an increasing footprint in the FVEY Partners' collaboration estate MindLink have successfully delivered the first of many milestones to improve coalition collaboration across the mission theatre. Besides all-round improvements to collaboration, improved Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), IT security posture and agile IT are also included among the observed outcomes.

Improved Collaboration across the Mission Theatre

With MCE acting as a centralized hub service for secure collaboration across national and organizational boundaries, the collaborative sphere becomes much larger in comparison to using legacy systems. In turn, this enables more frequent and closer communication between all allied partner nations and organizations within the coalition without compromising security. In real terms, it has empowered dozens of nations, agencies and mission components to collaborate in a threat intensive environment.

Strengthened C4ISR Posture

Designed to serve as a high-volume, real-time collaboration backbone for the modern mission theatre, MCE has directly contributed to strengthening the coalition's C4ISR posture. Leveraging the concept of multi-tenancy and deeply integrated mission features, MCE directly facilitates the secure, real-time sharing of mission-critical intelligence across coalition partners. As a result, mission components benefit from heightened situational awareness, shortened response times and increased knowledge of the environment and adversaries.

Improved IT Security Posture

From the ground up MCE is secure by design to mitigate and protect against external and internal threats. MCE natively integrates security capabilities that were previously bolted on to legacy systems to reduce dependency and vulnerability. MCE also introduces new capabilities aimed at secure multi-tenancy to compartmentalize collaboration on the system into containers, based on 'the need to know'.

Agile IT – faster adoption, onboarding, activity

As a central multi-tenant collaboration service, new partners and their users are swiftly onboarded to the system. With highly intuitive interface and resources to facilitate user adoption, users get up to speed quickly and begin collaborating with mission partners.

Conclusion

The MindLink solution set has proven to deliver the intended results of secure, real-time collaboration between mission and coalition partners all while conforming to strict industry practices and security requirements. Accounting for all outcomes achieved, the MindLink solution set extends far beyond the scope of replacing legacy systems with a more modern solution but delivers total digital transformation for the coalition/mission theatre, serving as a next-generation, extensible foundation for the mission collaboration needs of the future.

Customer Testimonial

> *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 real-time and brings focus to mission execution.*

MindLink

Facts & Figures

We note a growing MindLink footprint within Intelligence and Defense to address the increasing need for secure collaboration between coalition partners with stronger mitigation against data breaches, particularly insider threat.

Main Data Breach Causes

Frequency by Initial Attack Vector[1]

19% Stolen or compromised credentials

15% Cloud misconfiguration

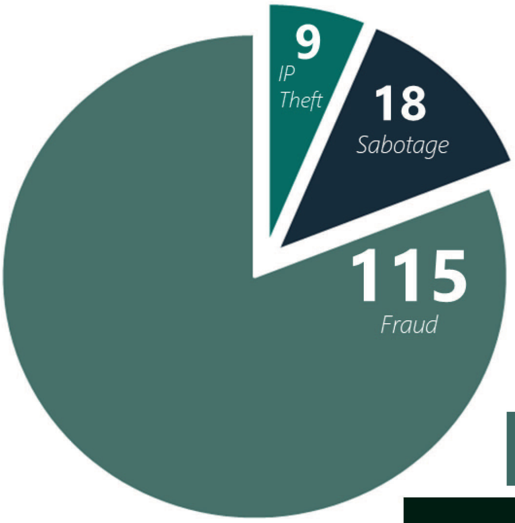
16% Phishing

19% Compromise at a partner

12% Malicious insider

142 Insider Threat Incidents in 2018

At US Local and Federal Government resulting in Intellectual Property Theft, Sabotage or Fraud[2]



$4.35m

Average US data breach cost per incident 2022[1]

0 MindLink-related Data Breach Incidents

34+ MindLink Chat Engine Deployments

500+ Missions Served

20,000+ Licensed Users in the Intelligence Community

Sources:

[1] *Data Breach Causes & Cost per Incident, IBM Cost of a Data Breach Report 2022, https://www.ibm.com/downloads/cas/3R8N1DZJ*

[2] *Insider Threat Incidents 2018, CISA.gov, https://www.cisa.gov/sites/default/files/publications/Insider%20Threats%20101%20What%20You%20Need%20to%20Know_508.pdf*