



DYNAMIC SYSTEMS INC.®



YOUR DATA IS OUR BUSINESS

CROSS DOMAIN SECURITY SOLUTIONS

Controlling access to different levels of classified data has traditionally been accomplished through the use of isolated networks and stand-alone machines. Such architectures, however, severely limit functionality, increase acquisition and overall life cycle costs, and substantially increase footprint size. The answer is Cross Domain Solutions that leverage Common Criteria certified technologies into accredited multilevel security (MLS) architectures. DYNAMIC SYSTEMS, Inc. has partnered with leading companies to provide complete, packaged security solutions which bridge separate security enclaves to improve network interoperability without increasing security risks or costs.

The Combined Enterprise Regional Information Exchange System (CENTRIXS) is supported with innovative technologies for secure information sharing and collaboration. CENTRIXS is a secure wide area network that provides the U.S. and more than 30 coalition nations with capabilities for selectively sharing intelligence and operational information. Key technologies provided which are crucial to the success of the CENTRIXS platform include:

- Multilevel Thin Client (MLTC)
- Trusted Application Layer Interface (TALI)
- Cross Enclave Search Tool (CEST)

These same capabilities have also been fielded as part of the Joint Cross Domain eXchange (JCDEX) platform. Dynamic Systems and Maxim Systems, Inc. provide systems engineering and program management support for this intelligence and target tracking environment, which handles security at the operating system level, significantly reducing software development costs.

Multilevel Thin Client (MLTC)

The MLTC is a Secret and Below Interoperability (SABI) accredited Trusted Solaris Ultra Thin Client workstation capable of displaying data from multiple independent networks at different classification levels, based on the clearance level of the user. The small footprint of these terminals replaces traditional standalone PCs, previously dedicated to separate networks, and lower system costs by more than 50% through use of a server centric architecture. All system maintenance, software and access control is handled at the server level, which also increases security by limiting media removal and storage to a single location. The MLTC allows session mobility through the use of 'smart cards', including Common Access Cards, that allows users to start a session, then move between workstations, inserting their card to bring up their same

secure network connections at a different location. More than 100 MLTC terminals were used as part of the US Joint Forces Command (USJFCOM) Combined Joint Task Force (CJTTFEX) 04-2-Operation Blinding Storm in June 2004, coordinating operations between US, British and other coalition forces, comprising more than 28,000 participants. The MLTC deployment includes Navy Command and Control ships and Joint Command Centers. The system is also now in use at the US Army Joint Operations Center in Afghanistan supporting Operation Enduring Freedom. Additionally the MLTC is currently in the process of attaining the Top Secret and Below Interoperability (TSABI) accreditation.

Trusted Application Layer Interface (TALI)

The TALI enhances cross domain capabilities by allowing most any network or Web-based application to work with a multilevel secure Trusted Operating System (TOS) through integration of a specialized Java component. This software technology, which is part of the **Dynamic Systems, Inc.** Trusted Data Sharing Solution® (TDSS), allows proprietary and legacy applications previously developed for secure standalone networks to share data in ways never before possible. The TALI creates an interface to a trusted information broker permitting applications to 'inherit' the security functionality of an underlying TOS, even if the programs themselves were not written with security in mind. This capability allows interagency, interstate and international coalition data sharing critical to coordinated efforts in modern war fighting and emergency response. The technology also has numerous uses in the commercial world for any industry that demands high system and data integrity assurance, such as e-Commerce, Financial Services, Healthcare and Communication Services.

Combining Technologies and Capabilities

- All applications run from back end servers so thin client workstations consist only of a monitor, keyboard and mouse. This results in space, weight, and power reduction, providing a more manageable workspace.
- System costs are reduced by more than 50% through use of a server centric architecture.
- Ease of Certification and Accreditation. MLTC has been evaluated and accredited through the NSA SABI penetration testing and is the only current SABI accredited multilevel network solution in operation today. The ILS is currently being evaluated for EAL7+ certification.
- Mandatory Access Controls ensure the secure separation of data at each classification level.
- Constant preservation of the integrity of sensitive data without restriction of the connectivity required to do business.
- Encourages productivity by providing simultaneous accessibility to both secure and general-purpose networks from the same workstation for rapid task performance and data distribution. MLTC provides concurrent access to both Microsoft Windows programs and traditional UNIX mission-critical applications running at different classification levels.
- Allows hot desk session mobility between thin clients through the use of 'smart cards'.
- Allows the use of All-source multilevel data feeds on a single box.
- Permits the use of tools and applications traditionally available on only a single security classification level, allowing greater collaboration.
- Low → High security level data upgrade and transfer capabilities.
- Despite tight controls, CENTRIXS technologies allow full functionality and user scalability, equivalent to a traditional PC environment.
- Hardware rather than software-based security that, by its nature, cannot be hacked or compromised. This eliminates the possibility of human error typically associated with configuration and means that no rule sets or filters need to be maintained, which significantly lowers the cost and complexity of administration.
- Supports multiple protocols, thereby eliminating the need to write specialized code to maintain data integrity and ensuring greater flexibility for system and network integration.
- Incorporates Quality of Service content filtering features that guarantee bandwidth allocation and resilience to denial-of-service attacks.
- Ease of deployment as it 'clips on' with standard commercial off-the-shelf equipment and connections, integrating with multiple computer exchanges or thin clients.

MLTC Customers

Operational Sites

USS Mt. Whitney
USS Blue Ridge
HQ Pacific Command
Joint Operations Center (JOC) Baghram, Afghanistan
US Army Tactical Support Vehicle (TSV) Ship

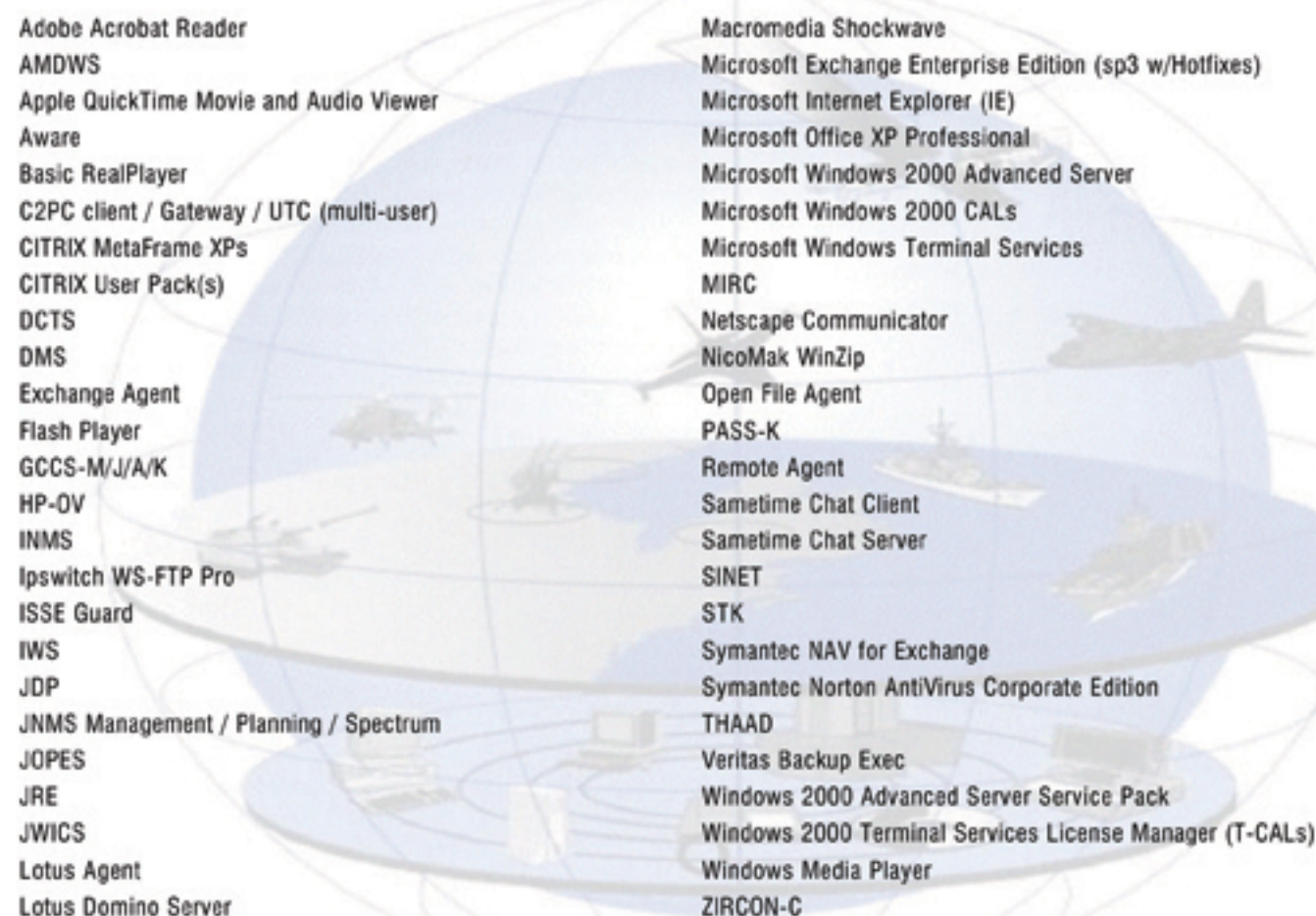
Test Sites

Deployable Joint Command and Control (DJC2) Panama City, FL
Program Executive Office (PEO), Command, Control and Communications - Tactical (C3T), Ft. Monmouth, NJ
Space and Naval Warfare Systems Center, San Diego (SSC-SD)
Navy Research Lab, Charleston, NC

Future Deployment Sites

USS Cole
Joint Force Fires Coordinator (JFFC), Ballistic Missile Defense Operations Center (BMD OC), Colorado Springs, CO

Cross Domain Solutions and the MLTC work with nearly any application or external system. Today, the MLTC has been proven with the following:



CROSS DOMAIN SOLUTIONS

Cross Enclave Search Tool (CEST)

CEST further enhances cross domain computing by providing the capability to allow search and retrieval of documents and database records across different networks and across security levels. Designed to work like current Web-based search portals, CEST permits US and coalition users access to data at or below their security clearance level. The system is capable of providing records at multiple security levels and searches local shared folders, repositories, and websites as well as Microsoft Exchange and Lotus Domino servers. User authentication and data labeling is tightly controlled by a multilevel secure TOS, ensuring individuals only receive search results they are authorized to view.

Joint Cross Domain eXchange (JCDX)

JCDX is a Global Command and Control System-Maritime (GCCS-M) compliant intelligence and tracking environment for both ashore and afloat, fixed and mobile targets. The system is a near-real time, MLS Sensitive Compartmented Information (SCI) level, C4ISR tracking environment that creates multi-source intelligence reports detailing

foreignforce activities and potential threats. Dynamic Systems provides system engineering, software development, program management, and maintenance services. JCDX has been installed at 22 land-based intelligence centers in the US, UK, Bahrain, Japan, Australia, and the Republic of Korea as well as on two afloat operational platforms. To date, the company has trained more than 1,100 users and system administrators on the system.

**Call the experts at
Dynamic Systems, Inc.
today to see how a
Sun Ray™ MLS Solution
can help secure your data.
(310) 337-4400.
www.DynamicSystemsInc.com**

