



LOCKHEED MARTIN
We never forget who we're working for™

Trusted Manager (TMAN)

Secure, Trusted Information Sharing

For more information or demonstrations contact:

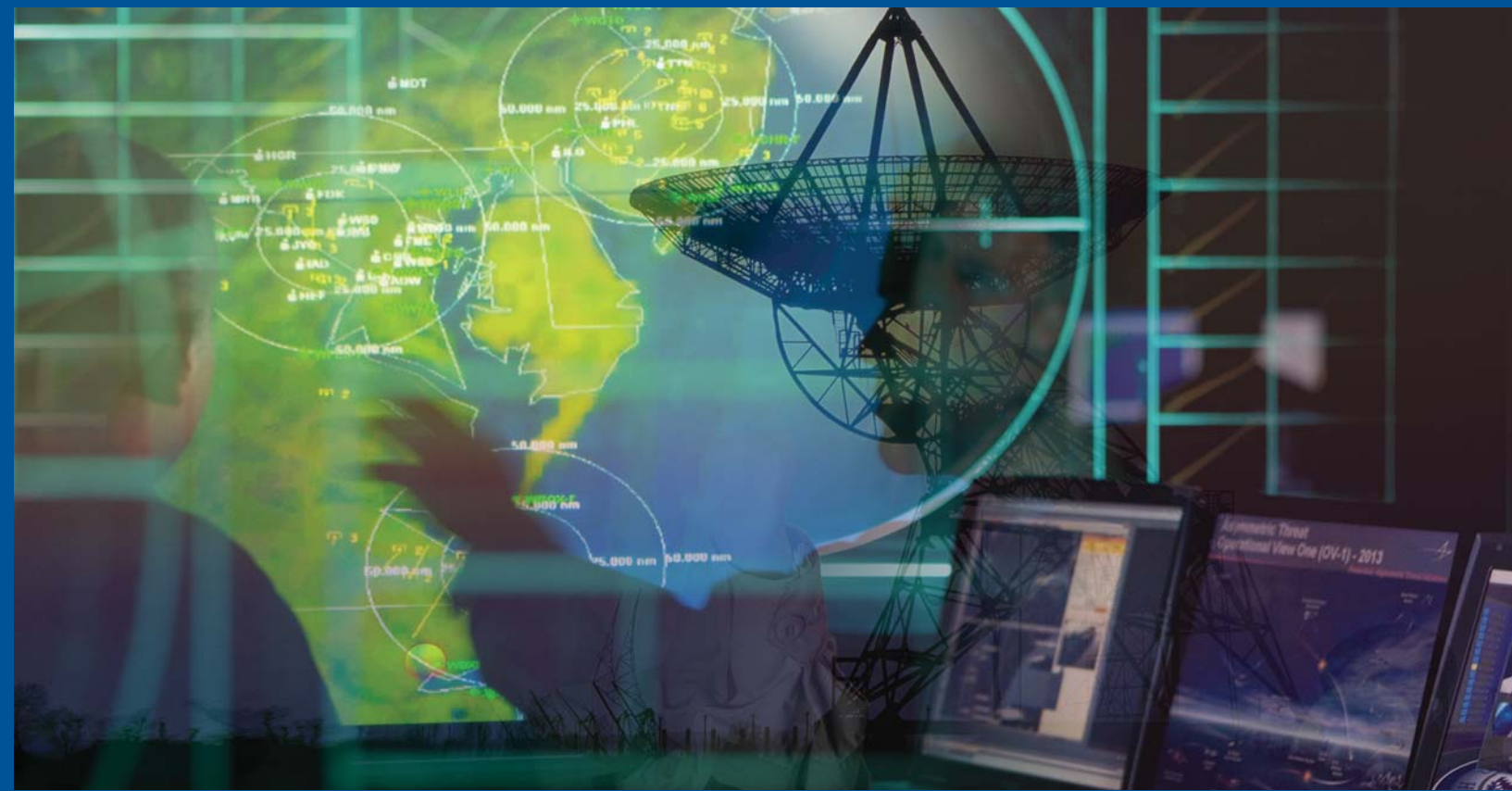
Lockheed Martin
 Telephone: 866-500-TMAN
www.lmtrustedmanager.com

Lockheed Martin is an Equal Opportunity Employer.

©2009 Lockheed Martin Corporation

LOCKHEED MARTIN, LOCKHEED and the STAR DESIGN [and any other marks used in the body of this document] are either registered marks in the U.S. Patent and Trademark Office and/or other countries throughout the world, or are trademarks and servicemarks of Lockheed Martin Corporation in the U.S. and /or other countries.

Printed in the United States of America 08/09. All Rights Reserved.



Trusted Manager (TMAN)

The Challenge: Secure Data Sharing Across Intelligence Networks

Today's global terrorist threat is real. In order to discover and inhibit the source of that threat, decision makers need a way to quickly access multiple sources of data through secure channels. Often, intelligence sharing introduces a variety of classification, compartmentalization, and need-to-know access criteria. In these types of environments, the process of gathering and consolidating vital intelligence may be impaired when mismatched schemes of data protection force potential partners to work in mutual isolation. To bridge the gap in intelligence sharing, Lockheed Martin has developed the product that protects intelligence data while enabling dissemination across organizational boundaries: Trusted Manager (TMAN).



The Solution: Trusted Manager

Accredited by the Defense Intelligence Agency, Lockheed Martin's Trusted Manager (TMAN) fosters secure data sharing by bridging the gaps between information assets of dissimilar classification or ownership. TMAN secures data exchange among attached entities by applying rule-sets based on classification hierarchies, sender and receiver identities, transfer protocols, data types, message formats, and individual content items. Originally developed as a multi-level secure guard for tactical imagery, TMAN is currently deployed as a core element at many customer sites.

The system is completely transparent in operation when processing data approved for automatic upgrade/downgrade. TMAN is simply embedded in the connection media and renders the network transparent to policy-consistent exchanges and opaque to all others. TMAN's mediation is coercive but non-intrusive. Supported systems initiate data transfers by ordinary means, such as file transfer protocol (FTP) invocation, whereupon TMAN's own highly-specialized FTP implementation transparently intervenes to secure the transaction.

TMAN is the guard of the present and future in that both its hardware and software are designed for extensibility. New message and data types are easily incorporated into the architecture by means of pluggable parser modularity and an infinitely expandable rule-set. The hardware platform is adjustable based on user needs and fully compliant with government standards, such as Director of Central Intelligence Directive (DCID) 6/3.

TMAN: Capable and Scalable

True Multi-Level Capability	While many competing designs bridge assets of only two classifications, a single TMAN instance safely administers as many discrete enclaves as its physical backplane can accommodate. Current installations typically support four or five levels with room to spare.
Outstanding Speed	TMAN's operation is non-blocking and non-serializing, in that TMAN achieves high aggregate throughput by supporting multiple concurrent transactions. TMAN supports up to 10Gbps channels.
Designed for Continuous Growth	TMAN's internal architecture maintains a high degree of separation between its core security functions and the data analysis engine. That principle of modular independence makes TMAN readily extensible to new exchange protocols, media, and formats without affecting the secure core or the considerable investment in its validation and accreditation.
Three Dimensions of Scalability	TMAN configurations span wide ranges of performance, degree, and function: Performance - TMAN can be installed on any platform running Sun® Solaris™ 10 with Trusted Extensions Operating System. Options range from laptops to high-end SPARC/X86 servers. Complete installations range in size from 19-inch racks to 1/2 ATR ruggedized ground and airborne chassis. Degree - Current TMAN deployments administer environments ranging from two to five discrete enclaves. Function - TMAN is easily configurable for operation in any combination of its principal transfer modes, with or without a human reviewer.
Proven Performance	TMAN has a long record of successful deployments and a history of agency accreditations. TMAN's numerous customers and growing baseline support a wide range of customer interaction.

Principle Modes of Operation

Upgrade: TMAN supports data upgrades while retaining the transparency and reliability of familiar transfer protocols as no hardware-only or "data-diode" solution can. TMAN also inspects payload data in order to curtail the exposure of high-value assets to errant or malicious fragments.

Automated Downgrade (Restricted): TMAN supports automated downgrade in restricted instances where data verification can be established without human review. This mode of operation is often appropriate for highly-formatted alphanumeric products or where data sensitivity can be positively ascertained via digital signatures or other administrative means.

Human Reliable Review (General): In the case of semantically rich data, e.g., free text and imagery, only human judgment can determine its suitability for downgrade. In this mode of operation, TMAN's human reliable review engine interacts with a human operator to enforce a highly structured and meticulously audited process of review and adjudication.

