



## Trusted Computer Solutions – Product Overview

The TCS business model focuses on three key information technology areas: sales of commercial MLS products, system and network vulnerability assessment, and trusted systems software engineering services.

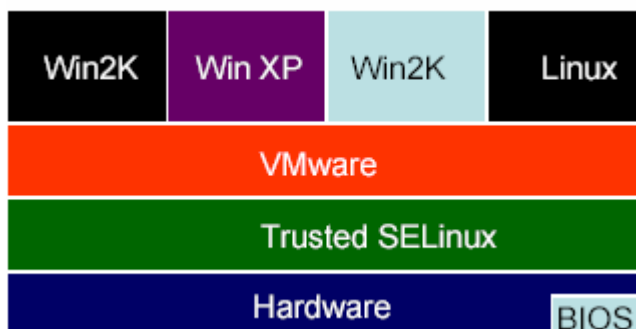
### **SecureOffice® Products Overview**

The TCS SecureOffice® suite of products provides a single point of access to multiple security domains through a single, high-assurance product. Such products enable connectivity from headquarters staff to remote offices, operating forces in the field, and even international coalition forces. Documentation and training address system installation and configuration; system administration; and user functions. All products are offered using Sun Microsystems Trusted Solaris™ 8 secure operating environment, purchased separately. TCS is currently undertaking the development of Trusted Linux which is a derivative of the NSA SE Linux solution. This is being evaluated to EAL4 under Common criteria. In the process all TCS products will be available on Trusted Linux as an alternative to Trusted Solaris 8.

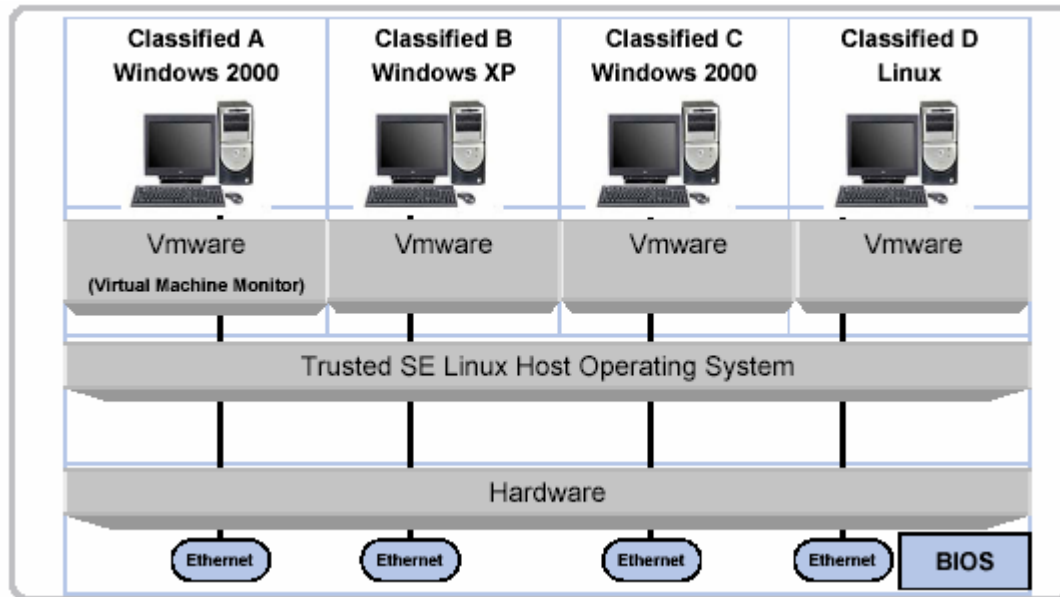
The Trusted Linux application environment will:-

- Use NSA SELinux as baseline, developing a commercial EAL-4 product that is functional (satisfy users) and accreditable (satisfy accreditors) with .
  - Labeled Security Protection Profile (LSPP)
  - Controlled Access Protection Profile (CAPP)
  - Role-Based Access Control Protection Profile (RBAC)
- Featuring (High Level)
  - Mandatory Access Controls (MAC) - MLS and TE
  - Label Encodings implementation compatible with current fielded systems
  - Least Privilege mechanism
  - Extended SELinux Role Based Access Control (RBAC)
  - Labeled Networking
  - (IPTABLES) Network Packet Filtering
  - Trusted X-Windows environment
  - Authorizations

NetTop is an emerging technology that allows multiple “virtual computers” to run on a single CPU/platform. Each virtual machine has its own OS and its own virtual hardware, The Trusted SE Linux operating system keeps the VMs separate and controls access to local resources, the host main OS provides the interface to the local peripherals



## NetOp network on a Desktop



## **SecureOffice® WebServer™**

SecureOffice® WebServer™ software allows organizations to maintain a common data set on a single World Wide Web (WWW) server that connects to multiple security domains/networks, alleviating the need to maintain separate servers and data sets for each domain or network. Using a single multi-level secure (MLS) Web server for all data eliminates the time and expense of maintaining a common and consistent data set on multiple disconnected servers. Using a secure operating system, information on the server can be segregated by categories, classification levels, or organizations. Individual users and groups can either be granted or denied access to this information based upon their authorization level or security clearance. Security is provided by Sun Microsystems Trusted Solaris 8 operating system and TCS SecureOffice® Foundation™ software. The standard Server supports up to 3 different networks at different classification levels. Additional classified networks can be optionally added. In the commercial world, WebServer provides an impenetrable barrier between the Internet and a corporate Intranet, while at the same time acting as the Web interface to the outside world. Outside browsers interact with the Web content offered up by WebServer, which then makes the determination of whether a request should be forwarded on to an internal server. All user data is strongly protected within WebServer by the mandatory access mechanisms of the Trusted Solaris 8 operating system.

## **SecureOffice® ContentManager™**

SecureOffice® ContentManager™ is a SecureOffice WebServer application that provides a secure mechanism for maintaining and disseminating documents and products at multiple security levels eg where users have access to a Content Management system on a Secret network and other users on a separate network need to browse or search for documents on the first network. Remote users can browse the document tree structure to view documents at their

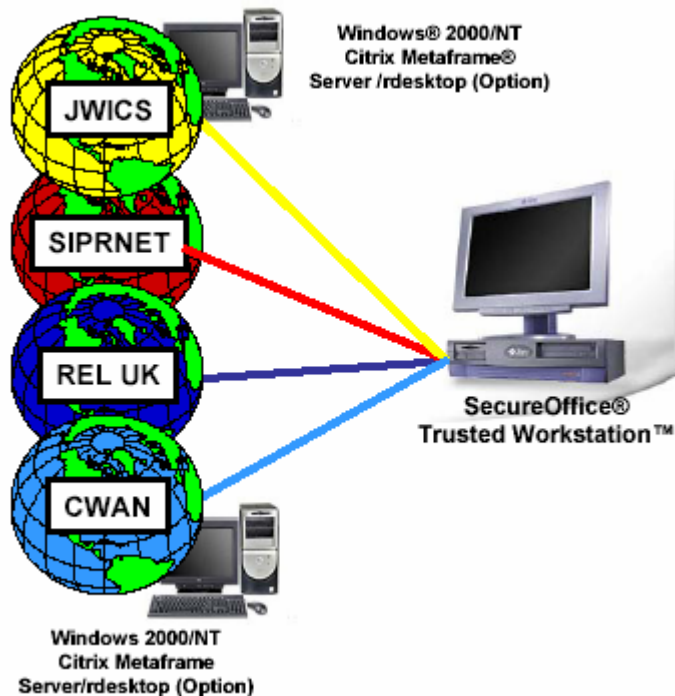
security level and below. Authorized users can post (write or upload) products/data to the server. With additional authorization, users can downgrade or re-label data on the server to make it available to other users at different security levels.

### **SecureOffice® DBConnect™**

SecureOffice® DBConnect™ contains all the features of SecureOffice WebServer, and adds multi-level relational Trusted Oracle Database functionality. NOTE: Does not include any Oracle products, which must be purchased separately. Security is provided by Sun Microsystems Trusted Solaris 8 operating system and TCS SecureOffice Foundation software.

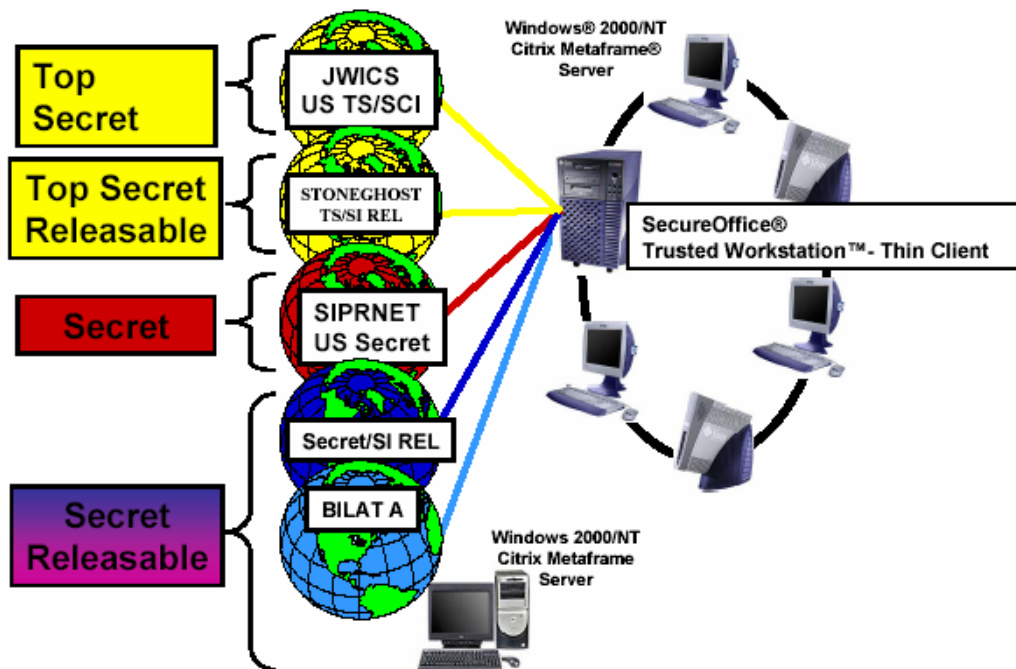
### **SecureOffice® Trusted Workstation™**

SecureOffice® Trusted Workstation™ software provides secure access to multiple Microsoft Windows® office automation applications running at different sensitivity levels, all from a single desktop. The system also allows individuals to retrieve, process, and disseminate information across networks operating at different security levels. The system provides a secure Microsoft Windows option, and information access and dissemination using Netscape for Web browsing and electronic mail. Security is provided by Sun Microsystems Trusted Solaris 8 operating system and TCS SecureOffice Foundation software. In addition to a number of standard security and functional features, the product features a robust and accredited Trusted Relabeler™ that allows authorized users to safely move appropriate information from one security level to another. The standard Workstation supports up to 2 different networks at different classification levels. Additional classified networks can be optionally added.



## **SecureOffice® Trusted Workstation™ (Thin Client)**

SecureOffice® Trusted Workstation™ Thin Client is a new and innovative concept which delivers all the functionality of the traditional SecureOffice Trusted Workstation product which is fielded around the world...but, in an ultra-thin client (appliance) environment. Like the traditional Trusted Workstation solution, Trusted Workstation Thin Client is designed to provide simultaneous secure access to both Microsoft Windows® applications and traditional UNIX® mission-critical applications running at different sensitivity levels...all from a single thin client. In conjunction with the Sun Microsystems SunRay Session Server™, the Trusted Workstation thin client allows users to retrieve, process, and disseminate information across networks operating at different security classifications/sensitivity levels. Trusted Workstation Thin Client provides a number of popular office automation and administrative applications. The system provides an optional Windows 2000/2003//NT environment that is fully application and network capable via Citrix MetaFrame® or Remote Desktop (RDP). Information access and dissemination is achieved using Netscape Navigator® for Web browsing and Netscape Messenger® for electronic mail in the UNIX environment and Internet Explorer and Microsoft Outlook® under Windows. Security is provided by Sun Microsystems Trusted Solaris 8 operating system and TCS SecureOffice Foundation software. In addition to a number of standard security and functional features, the product features a robust and accredited Trusted Relabeler that allows authorized users to safely move appropriate information from one security level to another. The standard Server supports up to 2 different networks at different classification levels. Additional classified networks can be optionally added.



## **SecureOffice® WebServices™**

SecureOffice® WebServices™ is a new family of network security products from TCS. Based upon a hardened version of the popular Apache Web Server, WebServices is the result of TCS' extensive experience working with its many customers in the U. S. Intelligence Community. This

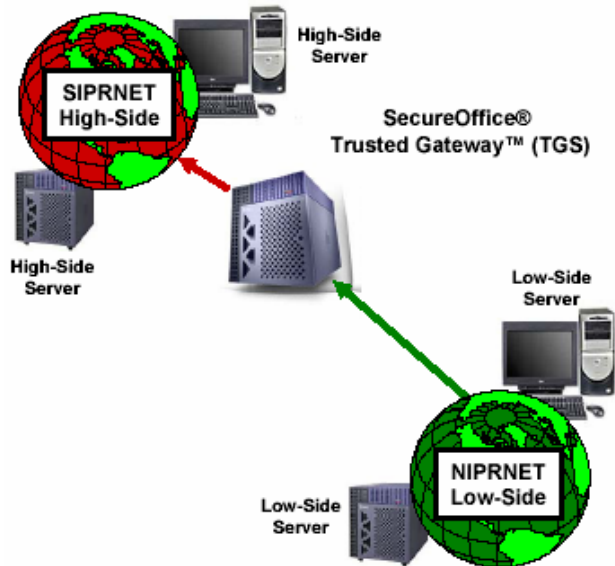
commercial product line is hosted on Sun Microsystems Trusted Solaris 8 operating system, a military-grade secure operating system that is now available and currently being used in the commercial world. WebServices has been enhanced to take advantage of all the additional security capabilities provided by Trusted Solaris such as Mandatory Access Controls (MAC), removal of the root "superuser" userid, data labeling and compartmentalization, increased auditing, plus much more. In addition, WebServices features support for SSL V3 encryption, X.509 digital certificates, and Apache Web Server features such as Host aliasing, and site mirroring. SecureOffice WebServices Configurations: As a "web firewall" or gateway that provides military grade protection of internal corporate Web servers. WebServices may be transparently inserted as a boundary device between the Internet and Intranet servers, allowing safe, secure EC or Internet Transactions without modification to internal servers. As a secure mail gateway capability that allows users on the Internet to securely access their corporate Microsoft Exchange or other web-enabled mail server. The interface to the mail server is via the user's standard web browser or Microsoft Outlook Express®. The look and feel of the mail client using a web browser is identical to Outlook Express. The Mail feature of WebServices eliminates the need for separate VPN software to ensure data privacy, using the browser's standard 128-bit encryption. In addition, long distance telephone charges can be avoided since the user only needs to access the Internet via a local ISP. User authentication can be via X.509 digital certificates, userid/password, or IP Address.

### **SecureOffice® Foundation™**

SecureOffice® Foundation™ is the underpinning upon which all TCS products are derived. This core set of TCS developed software components provides administrative and security enhancements to the Trusted Solaris 8 operating system. Foundation is ideal for customers who wish to develop customized solutions or enhance existing systems utilizing the Trusted Solaris operating system. Included in Foundation is a set of administrative and configuration tools for Trusted Solaris 8 that simplifies configuration and network (security, access, service level) policies. For example, the administration tools of Foundation easily adds or deletes network interfaces, workstations and servers. DNS, NIS+, NFS and print servers can all be easily configured. Foundation eliminates the need to edit security sensitive configuration files by hand. Changes via Foundation are propagated to similarly equipped TCS systems for ease of administration. Foundation also provides embedded kernel-level IP packet filtering for the desktop workstation or enterprise server. Foundation obviates the need for a separate filtering router.

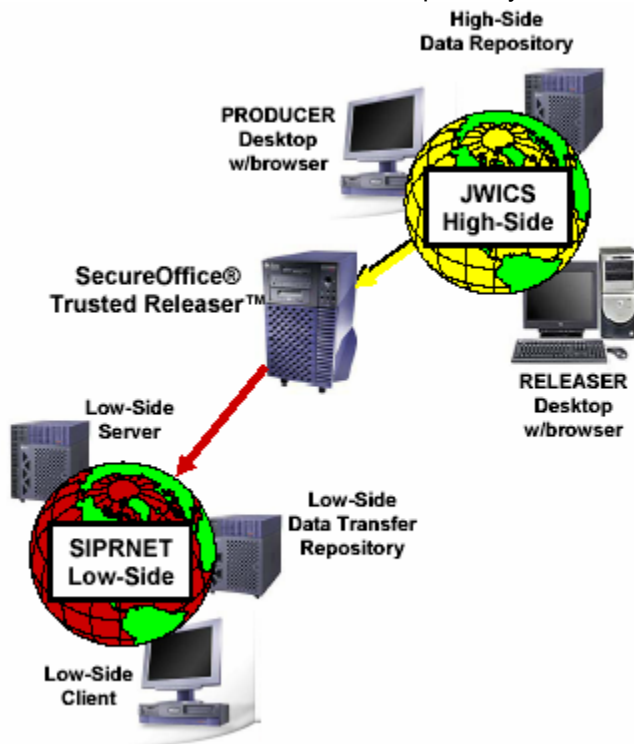
### **SecureOffice® Trusted Gateway™ (TGS™)**

SecureOffice® Trusted Gateway™ provides a secure one-way transfer of data from one network to another higher classified network. Using the TGS, an organization can move large quantities of data such as imagery, maps, and documents from one network to another with ease. Data of any format or type can be scanned for viruses and transferred using the TGS. Security is provided by Sun Microsystems Trusted Solaris 8 operating system and TCS SecureOffice Foundation software. The standard guard supports 2 networks (one high and one low). Additional low-level networks can be optionally added.



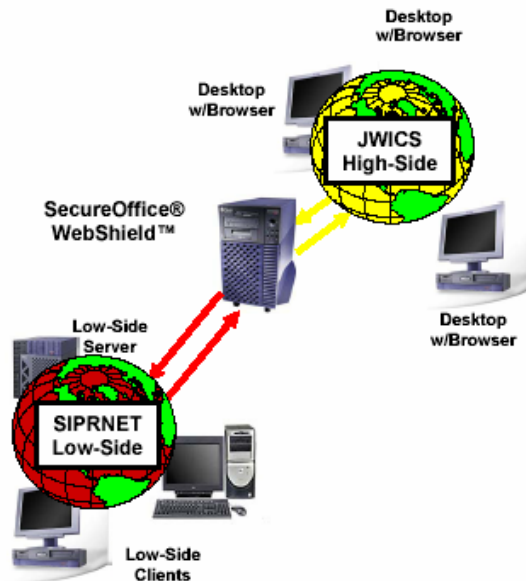
### **SecureOffice® Trusted Releaser™ (Requires TGS)**

SecureOffice® Trusted Releaser™ provides a means for automating the dissemination of sensitive data across security domains following the DoDIIS Inter Domain Transfer Policy of two-person review. The system addresses requirements to move sanitized data from a higher classified network to a lower network utilizing X.509 digital certificates to sign information to be downgraded. Includes configurable content filtering, audit and archiving functions to support site security policy. The standard guard supports 2 different networks at different classification levels. Additional classified networks can be optionally added.



## **SecureOffice® WebShield™**

SecureOffice® WebShield™ is a secure Web proxy that acts as a boundary device which allows secure Web browsing from one security domain to another. With WebShield, authorized users on a Top Secret network can browse designated Web servers on a Secret network. Alternately, authorized users on a Secret network can browse Coalition or Unclassified networks. WebShield uses network labeling and Mandatory Access Controls to compartmentalize and separate data at the different classification levels. Content filtering is extensive and fully configurable, including Dirty Word Scan of data (URLs, Form input, etc.) sent from browser to server, and filtering of Active content (Java, Active-X, etc.) and specified MIME types. Virus scanning of binaries sent from server to browser can be performed with the optional Virus Scanning Plug-in. Security is provided by Sun Microsystems Trusted Solaris 8 operating system and TCS SecureOffice Foundation software. In the commercial world, WebShield is a secure Web proxy that acts as a boundary device for preventing penetration into a corporate Intranet from the Internet, while allowing internal users to safely and securely browse the Internet.. Configurable security filters include the ability to filter any incoming and outgoing content, as well as virus



scanning any downloaded files .

## **SecureOffice® MailGateway™ (DoD – Based upon SecureOffice WebShield [Multi-level])**

SecureOffice® MailGateway™ is a secure gateway capability that allows users on different networks at different classification levels to share mail on a common Microsoft Exchange Mail Server. With SecureOffice MailGateway, users on JWICS, SIPRNET, and Coalition networks can all share a common Mail Server. The interface to the mail server is via the user's standard web browser or Microsoft Outlook Express®. The look and feel of the mail client using a web browser is identical to Outlook Express. MailGateway supports the browser's standard 128-bit encryption and user authentication can be via X.509 digital certificates, userid/password, or IP Address. Attachments in either direction can be supported depending upon the site's security policy.

## ***Virus Scanning Plug-in***

The TCS Virus Scanning Plug-In Option provides a means for automating the scanning and detection of viruses on TCS products. The option is available as a Plug-In to the SecureOffice product family (a SecureOffice product license is required for this Plug-In). Customer definable scanning options are available with maintenance plans to support the update of virus definitions.

## ***Training and Maintenance***

Trusted Computer Solutions, Inc. will provide training at a customer or TCS location for system installation and configuration, system administration, and end user tasks. Upon completion of installation and training, TCS will certify the system for proper functionality and clear it for secure operations. TCS recommends that customers purchase the Maintenance Option for all ordered software products. With the Maintenance Option, TCS will provide telephone support during standard US Eastern Timezone business hours. Bug fixes and upgrades for current software version levels are included in the Maintenance Option. There is no additional charge for services performed at a Government site within 50 miles of TCS headquarters in Herndon, VA. Outside the 50-mile radius, standard Government rates will apply for mileage and/or other travel expenses.

## ***Product Security Document Templates***

TCS will provide Certification & Accreditation (C&A) documentation templates in DITSCAP or DCID 6/3 format. The format and TCS product information will be correct, but site-specific content will not be included. In particular, the templates will not include updated C&A testing content (i.e., requirements matrices, technical tests, non-technical tests). Site-specific data and TCS updates to C&A testing content are available as a separate service.

### **About eB2Bcom**

eB2Bcom is an innovative Australian owned company specialising in the distribution, implementation and support of best-of-breed products for Identity Management, Security, MetaDirectory infrastructure & applications, Telecommunications, and ISP Messaging and solutions for Defence, Police, Intelligence & Enforcement.

An experienced team of software engineers are available for consulting in and around X.500/LDAP directories. These services including:-

- X.500, X.509 and LDAP architectural consulting and design of directory and security solutions.
- X.500 schema and basic access control design and implementation.
- Interface design and implementation for directory centric solutions



**Sydney:** +61-2-9779-1597  
**Melbourne:** +61-3 -9896-7800  
**Brisbane:** +61-7-3871-1440  
**Singapore:** +65-6841-7374  
**email:** [sales@eb2bcom.com](mailto:sales@eb2bcom.com)  
**Web:** [www.view500.com](http://www.view500.com) or [www.eb2bcom.com](http://www.eb2bcom.com)