



# THE TRUSTED SOLARIS™ 8 OPERATING ENVIRONMENT

## PROVEN SECURITY, RELIABILITY, AND SCALABILITY

When separation of information and individuals is of prime importance, the Trusted Solaris™ 8 Operating Environment is the platform of choice. It is an extension of the Solaris™ 8 Operating Environment, the established OS leader for security, reliability, and scalability in the Internet age.

As you might expect, Trusted Solaris 8 software is compatible with the Solaris 8 Operating Environment. That means administrators who have used Solaris software will also be familiar with most Trusted Solaris administration tools.

### SECURITY EXTENSIONS

Over the past few decades, computer systems have become corporate-wide resources, essential for day-to-day operations. A wide range of information on new products, employee compensation, health records, marketing and sales plans, and other sensitive data is often stored on these systems. Considerable cost, damage, and loss can be caused by hostile or unauthorized access and use of this information.

To control external access, firewalls and other access control methods are often used as gatekeepers. With the Trusted Solaris 8 Operating Environment, the software provides extensive internal protection against intruders and misuse by enabling administrators to:

- *Limit access to system data and resources.* Controls may be set on all potential interactions with programs, file access, and utilities on a user-by-user basis.
- *Eliminate super user.* Dividing super-user functions into multiple roles makes penetration far more difficult.

- *Independent evaluation authority.* An independent third party evaluates the operating system to validate that its security functions are working correctly.
- *Prevent “eavesdropping” in the window environment.* In conventional UNIX® environments, an intruding program can capture keystrokes typed in other windows. Trusted Solaris software provides a “trusted” path that protects entered data. This is particularly important for passwords, which may also be protected by requiring password changes or generating random passwords.
- *Augment security auditing.* Actions that may affect security or sensitive files can be monitored. To detect suspicious actions, administrators may generate reports of usage by user, file, data, and time.
- *Prevent spoofing programs.* Trojan horses, such as programs to intercept passwords or other sensitive data, are prevented by a graphical user interface and protocol. A trusted graphic displayed in a reserved area provides continuous, visible feedback of session integrity.
- *Protect local devices against unauthorized users.* Authorized users may control access to local devices.

In many cases, misuse by authorized users is the main source of security violations. Trusted Solaris software helps stop these violations by enabling administrators to implement a security policy that controls the access and handling of information, including system administration, operation, and monitoring tools.

### HIGHLIGHTS

- |  |  |  |
|--|--|--|
| <ul style="list-style-type: none"> <li>• Based on the leading UNIX operating environment, combining power, stability, and predictability with backwards compatibility</li> <li>• Offers new Java™ technology-based administration tools that support enhanced features for comprehensive and easy-to-use remote management</li> <li>• Simplifies software installation and setup, and offers comprehensive integration capabilities</li> </ul> | <ul style="list-style-type: none"> <li>• Supports client naming services including NIS and NIS+</li> <li>• Assures superior availability through a small, stable kernel design and load balancing across multiple processors</li> <li>• Scales to handle heavy traffic, huge data sets, and compute-intensive problems in a highly secure environment</li> </ul> | <ul style="list-style-type: none"> <li>• Supports the latest networking protocols and adheres to all major industry standards</li> <li>• Provides additional assurance through an independent EAL4 Common Criteria evaluation (currently in progress)</li> </ul> |
|--|--|--|

## SECURITY FEATURES

### MANDATORY ACCESS CONTROLS (MAC)

Every organization has at least two levels of information. The first is available to everyone, while the second is available only to authorized users. A MAC label access control feature allows information to be processed at multiple sensitivity levels.

MAC hierarchical and compartmentalized labels correspond to the sensitivity of information that must be kept separate, even when it is stored on a single system. Because information labeling happens automatically, MAC is mandatory. Ordinary users cannot change labels unless the system administrator gives them special authorization. In fact, users with labels in separate compartments are not allowed to share information.

---

*By enhancing and extending security mechanisms, Trusted Solaris 8 software provides additional protection for servers and desktop systems that process highly sensitive information.*

---

Publicly distributed information can be assigned a label of PUBLIC, while information that is distributed only within an organization's intranet may be labelled PRIVATE. A label with a compartment, such as PRIVATE-ENGINEERING, may be used for information that is available only to certain members of an organization, such as the engineering team.

### LABELS

Trusted Solaris 8 software provides two types of labels: sensitivity and clearances. Sensitivity labels are assigned to files, devices, windows, hosts, networks, and all other system objects accessed by users. Clearances set an upper and lower sensitivity boundary where a user can work. System administrators assign clearances to indicate the level of trust or job responsibility required by those accessing the system. Additionally, user accounts can be configured to provide visible window labels in a banner across the top. Each label is displayed in a unique color for ease of recognition.

### DISCRETIONARY ACCESS CONTROLS (DAC)

DAC uses file permissions and optional access control lists (ACLs) to restrict access to information based on a user's identity or group membership. It is discretionary because permissions may be changed by the file's owner. Unlike Solaris software, ROOT (super user) is not exempt from DAC restrictions. DAC is used along with MAC to control all access to system files.

### PRIVILEGES

Trusted Solaris 8 software enforces the *least privilege* security principle. This divides the unlimited power of a program running as ROOT into many distinct privileges that can be tightly controlled, mitigating the risk that occurs in standard operating systems when programs running as ROOT are exempt from all policy controls.

Using privileges, an administrator can give a program the power to bypass some aspect of the security policy, such as DAC restrictions, without providing more power than it needs. Additionally, administrators can restrict the use of privileged programs to people who can be trusted to use the privileges appropriately.

### ROLE-BASED ACCESS CONTROL (RBAC)

Another aspect of least privilege is applied to system management. Trusted Solaris 8 software divides administrative tasks among a number of roles that are functionally constrained to grant only necessary and sufficient powers.

Administrators must log in and authenticate as standard users, then assume a particular role through a second authentication process. This ensures that administrative activities, which can all be audited, are traceable back to a specific, authenticated individual.

### AUTHORIZATIONS

The final piece of the least privilege puzzle is user authorizations. Authorizations are to users what privileges are to programs. They are expressed hierarchically to provide greater flexibility, and are checked by trusted applications to restrict access.

**RIGHTS PROFILES**

Trusted Solaris 8 software maintains a database of functionally-related procedures known as Rights Profiles. Authorizations required to use these rights, as well as the specific Solaris software commands and their required security attributes—including graphical CDE actions—are enumerated in each profile. To construct more powerful rights from narrowly focused ones, Rights Profiles can be combined hierarchically. Rights hierarchies may be assigned to users or administrative roles through the User and Administrative Roles Manager tool.

The security attributes associated with commands and actions are not globally applied; they are available only to authenticated users and roles. For Solaris 8 software, supported attributes are the real and effective user and group IDs that are applied at execution. Trusted Solaris 8 software extends these attributes to include the specific privileges, labels, and clearances for each command and action.

To handle tasks that must be performed by multiple users, the Rights Manager tool allows administrators to modify existing profiles or create new ones. By modifying a default set of profiles, an organization can redistribute responsibilities among as many administrators and users as necessary. Using rights, administrators can give users the power to bypass some aspect of the security policy, without giving them more power than they actually need to perform their jobs.

**COMMON DESKTOP ENVIRONMENT (CDE)**

Trusted Solaris 8 software users and administrators work within a trusted X11 window environment. In an intuitive manner, this extends the standard CDE environment to transparently separate data at multiple sensitivity levels. Along with the trusted path menu, actions assigned to a user or role account are accessed through the front panel. Roles are protected from interference by other applications via special CDE workspaces, which are protected by enforcing MAC, DAC, and trusted path policies.

**SELECTION CONFIRMATION**

Authorized users may cut and paste or drag and drop text, binary data, and graphics between windows. Before confirming a transfer, a trusted

selection confirmation tool makes sure users view the selected data during a cut and paste. Authorized users may upgrade or downgrade the label during the transfer. The trusted windowing system prevents unauthorized transfers and enables auditing of successful and failed transfers.

**TRUSTED NETWORKING AND INTERCONNECTIVITY**

Hosts running Trusted Solaris 8 software can share information with hosts running other trusted and standard operating systems while enforcing access controls on all communications. To do this, administrators specify security attributes for each host and network. Trusted Solaris 8 networking also uses the specified attributes when enforcing security policy. Default security measures may be used for hosts and networks that do not understand security or support these attributes.

**TRANSPARENT ACCESS TO REMOTE FILES**

Trusted Solaris 8 software uses Sun's distributed network file system, NFS, to provide transparent access to remote files while fully enforcing the MAC and DAC features of the system. Diskless clients are also supported.

**LABELED PRINTING**

Administrators may restrict the sensitivity levels of information sent to individual printers. MAC compares the sensitivity label of the job to the printer's label range. Listing of print queues is restricted, so users see only their own print jobs if MAC checks are passed. Printer output has mandatory banner and trailer pages with label information and handling instructions.

**TRUSTED PATH**

The trusted path ensures that users are not tricked by a hostile program into supplying information that might be used to penetrate the system. Through the trusted path menu, users perform security-sensitive tasks such as changing their passwords or working labels, and authorized users authenticate themselves when assuming administrative roles.

A distinctive stripe along the bottom of the monitor assures users that they are communicating with the trusted path. The screen stripe also provides continuous feedback about the labels of the currently active window and input from the keyboard.

**DEVICE ALLOCATION**

Authorized users may employ allocatable media devices for importing or exporting information. When a device has a specific sensitivity label, the owner is the only one who can access the information on it.

**PLUGGABLE AUTHENTICATION MODULE**

Trusted Solaris 8 software uses pluggable authentication modules (PAMs) to provide failed-login account locking, trusted-path checking, and machine-generated passwords. Custom password encryption/generation algorithms are implemented by a shared library. This replaces the standard Trusted Solaris 8 software algorithms, with no code changes required.

**NAME SERVICE SUPPORT**

Supported name services include NIS and NIS+. In addition to the distributed databases in Solaris 8 software, additional trusted networking databases are provided. Remote administration is provided for all services.

**TRUSTED MAIL**

Users are notified about incoming e-mail through the Mail subpanel on the front panel. When the recipient clicks on a mail icon, a mail reader is displayed at the sensitivity label of the incoming message, irrespective of the current workspace's sensitivity label.

Mail can be received by an account only if the message is within the account's clearance. Mail can be sent to a host only if the message is within the host's sensitivity label range.

**SCALABLE SECURITY FEATURES**

Most off-the-shelf applications designed for the Solaris Operating Environment run without modification in a Trusted Solaris 8 environment. By enabling or disabling various security features, organizations can configure their operating environments to satisfy a wide variety of policies.

**ASSURANCE**

In a trusted systems evaluation, product features must meet a specified set of criteria. Over the years, Sun products have successfully passed many government-sponsored evaluation programs. Trusted Solaris 8 software is currently in evaluation against the Common Criteria at the EAL4 level with the Labeled Security Protection Profile (LSPP—equivalent to the Orange Book—TCSEC—B1 class).

**STANDARDS**

Trusted Solaris 8 software meets the following government and industry standards:

- X11R6.4 window system, CDE 1.3
- ToolTalk™ 1.2
- IEEE Standard 1003.1-1998 (POSIX)
- FIPS 151-1, 151-2
- Open Group (TOG) UNIX 98, 95
- System V Interface Definition Issue 2, Vol 1-3
- ABI compatibility with SPARC™ Compliance Definition 1.1, X86/Intel
- Trusted Standards Interoperability Group standards (TSIX [RE]) 1.1
- Year 2000 Compliance: Follows X/Open® guidelines
- Interface Standards: X/Open UNIX 98
- Graphics Standards: X11, PostScript™, Display PostScript™, OpenGL®
- Desktop Standards: CDE (Common Desktop Environment), Motif

- Object Standards: Java™ IDL
- Connectivity Standards: ONC™, ONC+™, NFS, WebNFS™
- Internet Standards: HTTP, FTP, Telnet, DNS, IMAP4, SMTP, IPv6, IPSec

**SYSTEM REQUIREMENTS**

- SPARC (32-/64-bit) or Intel Architecture (32-bit) platforms
- Disk Space: 1 Gbyte for desktops; 2 Gbytes for servers
- Memory: 128 Mbytes minimum

**FOR MORE INFORMATION**

To find out more about Trusted Solaris 8 software, please visit Sun's Web site at [www.sun.com/trusted-solaris](http://www.sun.com/trusted-solaris).

For more information on the Solaris 8 Operating Environment please visit [www.sun.com/solaris](http://www.sun.com/solaris).

**HEADQUARTERS** SUN MICROSYSTEMS, INC., 901 SAN ANTONIO ROAD, PALO ALTO, CA 94303-4900 USA  
PHONE: 800 786-7683 INTERNET: [www.sun.com/software/](http://www.sun.com/software/)



© 2000 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, ONC, ONC+, Solaris, Trusted Solaris, ToolTalk, WebNFS, and We're the dot in .com are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Products bearing SPARC trademarks are based on an architecture developed by Sun Microsystems, Inc. OpenGL is a registered trademark of Silicon Graphics, Inc. PostScript and Display PostScript are trademarks or registered trademarks of Adobe Systems, Incorporated. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. X/Open is a registered trademark of X/Open Company Ltd. Information subject to change without notice.