Solaris™ Trusted Extensions

Labeled Security for Absolute Protection

Control access according to data sensitivity

At Sun, we're reinforcing our more than 20-year commitment to security by integrating labeled security into the Solaris™ 10 Operating System. Called Solaris Trusted Extensions, this advanced security feature implements labels to protect your data and applications based on their sensitivity level, not just on who owns or runs them. Credit card information, classified data, and personal records remain secure, and they can't be accessed by or written to unauthorized sources.

Highlights

- Solaris Trusted Extensions enhance existing Solaris security, preserve application investment, and provide for IT flexibility
- Mandatory access control enforces policy-based access to data
- Labeled desktops include the Trusted CDE and Trusted Sun Java Desktop System
- Labeled device access prevents malicious moving of data into the wrong hands
- Labeled networking provides a secure way to scale your system to the network

Extends Solaris OS security

Solaris Trusted Extensions is an extension to the proven Solaris 10 security model. It utilizes User and Process Rights Management, Solaris Containers, file systems, and networking and doesn't require a new or separate kernel. Best of all, it doesn't require ISVs to requalify their applications to run them with sensitivity labels. And because it's an extension to the Solaris 10 OS's security policy, Solaris Trusted Extensions technology is flexible and quick to deploy: You can add new applications, new users, and more, very quickly, without extensive analysis of each application — and without the need to write complex, error-prone security policies that require a system reboot.

Mandatory access control

Solaris Trusted Extensions mandatory access control policy (MAC) adds sensitivity labels to all aspects of the Solaris 10 OS. Labeled objects have an explicit relationship with each other, and an application can't usually see or access data with a different security label — applications are allowed read-only access to data, or to write to that data, if they have appropriate authorizations. The MAC policy applies to all aspects of the operating system, including file, print, networking, window management, and device access, and even system administrators can't violate the policy inadvertently. Solaris User Rights Management provides a role-based access control mechanism for delegating administration tasks and enforcing separation of duties among administrators, security officers, auditors, and users.

Labeled desktops

With Solaris Trusted Extensions, users who are authorized to view data at multiple classification levels can do so on a single desktop, with separation of information still strictly enforced. Competitors' products force users to repeatedly logout of one level to login to another level.

Sun enforces the MAC policy through two labeled desktop interfaces, the Trusted CDE desktop and the Trusted Sun Java™ Desktop System. Trusted CDE preserves a look and feel familiar to former Trusted Solaris 8 OS customers, while Trusted Java Desktop System introduces the world's first labeled interface based on the GNOME open source desktop standard. Each window is labeled with a stripe that alerts you at a glance as to a document's security classification. The interface doesn't allow your users to drag-and-drop or copy files between windows with different security labels unless they have authorization. Users can have multiple Web browsers, email windows, or other applications open on the same desktop, each displaying just the data that application is cleared to view.

Labeled device access

With Solaris Trusted Extensions, devices on the system — including files systems, terminals, disk drives, USB thumb drives, CD-ROMs, printers, audio devices, and network interfaces — have labels associated with them. Security administrators can determine what types of data can be accessed by any given device, so sensitive information can't be written to devices that might be compromised or that might broadcast sensitive information to unauthorized users. Credit card data, banking records, and other classified documents can be labeled to prevent their transmission over the Internet or from being copied to a floppy or CD.

Labeled networking

Solaris Trusted Extensions uses the CIPSO labeled-networking standard for exchanging data among multiple systems. CIPSO allows several systems to preserve label security when sharing data via NFS or other networking protocols, without requiring application modification. Solaris Trusted Extensions also has the unique ability to create multilevel ports for any application, allowing you to use existing applications in a labeled security environment, while preserving existing investments in software and allowing for greater flexibility as application needs change.

Certified, integrated and easy to use

With the Solaris 10 3/05 release, Sun has also achieved Common Criteria independent security certification against the Controlled Access and Role Based Access Control Protection Profiles at Evaluation Assurance Level 4+ (CAPP & RBACPP @ EAL 4+). We will achieve the same results with Solaris 10 11/06 by August 2007, and expect to complete Labeled Security Protection Profile (LSPP @ EAL 4+) for Solaris 10 11/06, using the Solaris Trusted Extensions feature, by December 2007.

Learn More
To learn how to safeguard your Web servers, visit sun.com/solaris/teachme.

For additional information on Solaris Trusted Extensions and other Solaris OS security features, go to sun.com/solaris/features.

Because Solaris Trusted Extensions is a feature of the Solaris 10 OS, it runs on all hardware platforms that the Solaris 10 OS does, including SPARC, x64, and x86 architectures. And that means your administrators can become familiar with Solaris Trusted Extensions naturally, as they learn and use other Solaris 10 OS security features. It also means that you can add new security levels, applications and devices without the need to create long, error prone security policy files.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com