

Solaris™ 10 Operating System and Security

Advanced Features Enable Secure Systems



Highlights

- Verifies the integrity of your system using file verification features
- Reduces risk by granting only the privileges needed using User and Process Rights Management
- Defends your system against attack through the Secure By Default networking profile, Solaris IP Filter Firewall, and TCP Wrappers.
- Simplifies administration by using open, standards-based Solaris Cryptographic and Solaris Key Management frameworks for encryption
- Controls access to data based on its sensitivity through Solaris Trusted Extensions labeled security technology
- Evaluated against some of the most stringent independent testing profiles available

> Security is built in, not bolted on

Security is more than a mix of technologies — it's an ongoing discipline. At Sun, we're reinforcing our more than 20-year commitment to building security into the Solaris™ Operating System with the release of the Solaris 10 OS — our most security-enabled OS yet.

File integrity

System administrators can detect possible attacks on their systems by monitoring for changes to file information. In the Solaris 10 OS, binaries are digitally signed, so administrators can track changes easily. All patches or enhancements are embedded with digital signatures, eliminating the false positives associated with upgrading or patching file integrity-checking software. The Solaris 10 OS also provides the Basic Audit and Reporting Tool (BART) for integrity checking of customer files. In addition, the Solaris Fingerprint Database project, hosted by Sun on the SunSolveSM Web site, provides free online file integrity verification utilities for many generations of the Solaris OS.

User and Process Rights Management

Hackers often attempt to exploit root accounts because those accounts are empowered with complete access to UNIX® systems. The Solaris 10 OS offers unique User and Process Rights Management technology to reduce risks by granting users and applications only the minimum capabilities needed to perform their duties. Unlike other solutions, the Solaris 10 OS requires no application changes to take advantage of these security enhancements.

Solaris applications, running on 64-bit SPARC®, AMD™, and Intel processors, also are automatically protected from a form of intrusion known as “stack smashing” by a nonexecutable stack feature. No application changes or performance degradation are required.

In addition, the Solaris 10 OS offers an extensive system event audit-trail facility. Access to files, devices, roles, system services, and applications are recorded. This audit trail is exportable into an open XML format or can be automatically transported to another system.

Network service protection

The Solaris 10 OS provides protection against inappropriate use of network resources through its Secure By Default networking configuration, which disables many unused network services to reduce exposure to attack. With Secure by Default, an administrator can enable or disable individual network services or change how they listen for network connections.

The Solaris 10 OS also ships with Solaris IP Filter Firewall software preinstalled. This integrated firewall can reduce the number of network services that are exposed to attack and provides protection against maliciously crafted networking packets. Starting with the Solaris 10 OS 8/07, the Solaris IP Filter Firewall can also filter traffic flowing between Solaris Containers when it's configured in the Global Zone. In addition, TCP Wrappers are integrated into the Solaris 10 OS, limiting access to service-based allowed domains or partner sites.

Cryptographic services and encrypted communication

For high-performance, systemwide cryptographic routines, the Solaris Cryptographic Framework adds a standards-based, common API that provides a single point of administration for cryptographic routines and digital

certificate lifecycle management. The Solaris Key Management Framework provides a single set of administrative commands for digital certificate creation requests, manipulation, and loading. These pluggable frameworks balance loads across hardware accelerators and software implementations, increasing encrypted network traffic throughput. They're available to applications written to use the PKCS #11, Sun Java™ Enterprise System (NSS), OpenSSL, and Java Cryptographic Extension APIs.

The Solaris 10 OS also provides protection against theft of sensitive material by encrypting communications using Solaris IPsec/IKE and Solaris Secure Shell protocols. Solaris IPsec/IKE complies with industry standards to provide data encryption between two or more systems over the network, without any application modification. The Solaris Secure Shell protocol is a specific set of utilities modified to allow for encrypted remote access and file transfer between two systems.

Flexible enterprise authentication

The Solaris 10 OS delivers a number of flexible authentication features, including support for the Pluggable Authentication Mechanism (PAM), which makes it possible to add authentication services to the OS dynamically. Sun and third-party vendors provide many PAM modules and customers can create their own to meet specific security needs.

The Solaris Kerberos Service delivers Kerberos-enabled remote applications such as rsh, rcp, telnet, Solaris Secure Shell, and NFS file sharing. Kerberos-based protocols allow for standards-based enterprise single sign-on (SSO), authorization, and encrypted communication. Lightweight Directory Access Protocol (LDAP)

client-side authentication and interoperability enhancements enable enterprise-wide, secure, standards-based access to your servers and applications. To enable easier integration with existing environments, the Solaris 10 OS provides NIS and NIS+ to LDAP gateways. All Solaris User and Process Rights Management information can also be stored and managed centrally using LDAP-based directory server software.

System-specific userIDs now have strong password encryption options, including MD5 and Blowfish, as well as account lockout, password history and complexity checking, long password format, and a banned passwords list.

Repeatable security hardening and monitoring

New features in the Solaris 10 OS make it easier than ever to minimize and harden a system. The Reduced Networking Metacluster install option creates a minimized Solaris OS image, ready for administrators to add functionality and services in direct support of their system's purpose.

And the Secure By Default networking configuration disables many unused network services, while configuring all other services for local system-only communications. The Solaris Service Manager can be used to control exactly which services run, who can manage those services, and what privileges those services run with.

What's more, the freely available Solaris Security Toolkit assists in the process of installing and maintaining a minimized and hardened operating system security configuration. The toolkit integrates with the Solaris JumpStart™ installation process for repeatable secure installations, or it can be used to harden an existing system

Learn More

For more information about Solaris 10 OS security, visit the Solaris Security Learning Center at sun.com/solaris/secure/.

The Solaris Trusted Extensions data sheet is available at sun.com/software/solaris/ds/trusted_extensions.jsp. And the Solaris Security Toolkit can be found at sun.com/blueprints/tools/.

according to a site-defined security profile. The toolkit also includes an audit mechanism to compare a running system configuration against a site-specified hardening profile.

Mandatory access control, labeling, and security certification

Solaris Trusted Extensions solve the problem of controlling access to sensitive data by implementing sensitivity labels for access control to files, printers, networks, windows, applications, and devices. Solaris Trusted Extensions is the only labeled OS feature to support full enterprise-class solutions, giving customers multi-level desktops through the GNOME-based Java Desktop System or CDE, simple deployment, and centralized userID management.

The Solaris 10 OS 11/06 is currently in evaluation at EAL4+, one of the highest level of Common Criteria Certification, with three Protection Profiles: Labeled Security Protection Profile (LSPP), Controlled Access Protection Profile (CAPP), and Role-Based Access Control Protection Profile (RBACPP). In addition, Solaris 10 OS 3/05 has completed evaluation at EAL4+ with CAPP and RBACPP.