MITIGATE RISKS WITH INTELLIGENT SECURITY CONTROLS

KEY FEATURES

• Security in Silicon: Hardware-integrated cryptographic acceleration to protect both data and network.
• Reduce Exposure: Hardened by default to limit network exposure and networked services.
• Automatic Protection: Anti-exploit techniques coupled with integrated best practice security controls increase resilience and reduce complexity.
• Multi-tenant: Isolate applications and workloads on shared hardware. Reduce costs and management.
• Secure Virtualized Applications: Reduce misbehaving applications and contain malware with application security policies ranging from network port to entire virtual machine.
• Control Administrators: Isolate administrative roles to prevent data loss and delegate administrative responsibilities.
• Compliance Reporting: Report on configuration management for internal and regulatory security policies.
• Simplified Operations: Security features are integrated with each other and core technologies such as Oracle Solaris ZFS, Image Packaging System, and Oracle Solaris Networking.
• Assured Deployment Platform: Oracle Software Security Assurance Process reduces weakness present in both Oracle Solaris and third-party code.
• Government Security: Trusted Extensions, a feature of Oracle Solaris, provide a modern multilevel environment for high security environments.

REDUCE RISK WITH ORACLE SOLARIS 11

Oracle Solaris 11 provides granular and flexible layers of security controls that work together to reduce the likelihood and impact of security incidents, protecting your organization from loss of good reputation and fiscal harm. Advanced security features protect data, isolate applications, limit user actions, and report on system activities to meet even the strictest security policies.

Holistic Security Architecture

Oracle Solaris 11 engineers rejected the ad-hoc security practices and features used by other operating systems by instead focusing on engineering security into the core of the operating system and integrating security features seamlessly into each layer.

Access Control

Security administrators can apply fine grained security policies at the application and user level using simple tools that restrict or grant specific system behaviors (like program execution, file access, and network port control). The same underlying mechanism, generally referred to as the role-based access control (RBAC) framework, is used to delegate administrative functions, restrict user access, implement administrative hierarchies, allow job role assumption without re-logging in, contain applications to specific actions, isolate zones from each other, elevate administrative capabilities, set software restriction policies, and to restrict applications to be immutable and read-only. The isolation of administrative functions into grantable profiles removes the need for and high risk of anonymous and too powerful root access. Oracle Solaris access controls ensure applications run with the minimum access permissions needed to accomplish their tasks, limiting misbehaving applications or malware from impacting other applications on the system.

Authentication

Security policies can be enforced across an entire network of systems by integrating with an LDAP directory service such as Oracle Directory Server Enterprise Edition. Kerberos is not a bolted-on application, but it is integrated with auditing, cryptography, and user management functions to provide strong enforcement of enterprise authentication policies and secure the Kerberos-enabled Oracle Solaris applications.

Pluggable Authentication Modules (PAM) was originally developed on Oracle Solaris to provide authentication flexibility, such as adding two-factor authentication. Oracle Solaris extends basic PAM capabilities of other operating systems by allowing per user/role authentication stacks and uses PAM to set cryptographic keys for encrypting Oracle Solaris ZFS home directories. PAM is the authentication mechanism for the RBAC framework, providing control for initial and subsequent authentication.
File Access

The RBAC principles of least privilege and rights delegation are further refined in ZFS. Specific administrative actions can be delegated to users for each dataset. For example, users can be granted permission to make snapshots and clones of their home directories. The RBAC framework works in conjunction with the NFSv4 access control lists (ACLs) to define who can and cannot access to a file both locally and when shared over NFSv3 or NFSv4, CIFS, SCP, and SFTP. These file-sharing mechanisms are managed by the Service Management Framework (SMF) which are secure by default and take advantage of hardware-assisted cryptography.

Security in Silicon — Cryptography

Modern processors such as Oracle’s SPARC T4 are designed to deliver high performance cryptography by integrating cryptographic operations into the processor instruction set. This software in silicon cryptographic engine is used throughout Oracle Solaris 11 to accelerate Oracle and third-party applications, Java, and Oracle Fusion Middleware, and the Oracle Database to seamlessly encrypt and protect confidentiality of data at rest and in transport.

Cryptographic Providers

Oracle Solaris 11 provides two building blocks for accelerated cryptography, the Oracle Solaris Cryptographic Framework and OpenSSL. The cryptographic framework is a pluggable system that implements the RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) v2.20 that are used to match cryptographic requirements of applications to underlying hardware- or software-implemented cryptography modules. The cryptographic framework is used when encryption key management is important or the application has complex cryptography needs. Hardware and software cryptography is optimized at the machine code level to ensure the highest performance for these applications.

OpenSSL is provided for applications that typically do not have complex key management requirements. OpenSSL is typically used by open source applications and is the preferred library for secure HTTP traffic. OpenSSL can take advantage of hardware cryptography either through the cryptographic framework or directly using an optimized encryption engine.

Oracle Solaris components such as Secure Shell (SSH), ZFS, Kerberos, and Internet Key Exchange Protocol (IKE) use the cryptographic framework by default with no additional configuration needed to take advantage of high-performance cryptography on both SPARC and Intel Xeon platforms.

Java, Oracle Database, and Oracle Fusion Middleware are all automatically accelerated on Oracle Solaris by indirectly or directly using the cryptographic framework, the Oracle Solaris database cryptographic pathway, or compiled to use SPARC T4 instructions natively.

Disk and Network Data Protection

Organizations cannot afford data loss; personally identifiable information (PII) and proprietary business information being lost or accidentally divulged are not acceptable to customers, regulators, or management. The Oracle Solaris 11 RBAC framework protects against unauthenticated access or administrative misuse of critical data, but doesn’t protect against the physical loss or incorrect management of a dataset.

Oracle Solaris ZFS encrypts at the file system level, which can be used to encrypt a home directory, an entire disk, remote storage (Fiber Channel or iSCSI), or a local disk pool.
Management of encryption keys using Oracle Key Manager enforces correct use of a dataset by providing separation of duties (and access to data) driven by policies as opposed to “always available.”

Oracle Solaris ZFS encryption is complementary to cryptography at other layers of the application stack. For example, Transparent Data Encryption, a feature of Oracle Database, protects database content, but leaves some utility files unencrypted on disk. Use of both Oracle Solaris ZFS encryption and Oracle Database encryption provides comprehensive protection.

Software Security Defined Networking
The ability to encrypt network traffic with no performance impact provides the ability to simplify network architectures. Currently a mesh of routers, switches, physical firewalls, network cables, and virtual LANs is used to create multitier applications (such as an ERP system). Hardware-assisted secure tunnels built using IPsec can be used to reduce complexity by defining point-to-point tunnels where needed, mimicking the traditional multitier environment in a flat physical network. These secure tunnels are defined using typical Oracle Solaris mechanisms and can take advantage of all the Oracle Solaris capabilities (such as network virtualization and firewall) and features such as SMF, etc.

Organizational Security and Compliance
Security is expanding from primarily technical issues (such as changing telnet to SSH) to organizational issues (do we meet PCI requirements?). Oracle Solaris eases the burden of organizational security by providing an assured base platform supported by an ecosystem that supports higher-level security goals such as compliance enforcement and reporting.

Secure by Default
Oracle Solaris 11 is installed with the default Oracle Solaris security policy, a policy based on industry best practices that has the following features:

- Administrative user — Accessed via the RBAC system administrator role, can use sudo and su
- Limited network exposure, SSH is the only network service enabled
- Limited installation of packages
- Limited auditing is enabled (logon, privilege escalation, logoff)

This policy is a security baseline appropriate for many types of environments with limited modification. Additional guidance can be found in the Oracle Solaris 11 Security Guidelines and the Center for Information Security Solaris 11 benchmark to develop organizational best
Anti-Malware + Anti-Exploitation + Integrity Validation

Attackers have generally moved on from attacking operating systems and instead are focusing the majority of their energy in compromising applications that are easier targets. Multistage compound attacks build upon a single exploitation that is then used to subsequently find weakness across the network.

It is critical to limit damage of malware or misbehaving applications. On Oracle Solaris this can be accomplished using a combination of:

- Application security policies
- Immutable zones, a mechanism where zones have limited access to the local file system. Designed for web applications that connect to remote databases and logging server.
- Address space layout randomization to protect against application buffer overflow exploits
- Cryptographically signed executables ensuring Oracle Solaris provided utilities are provided by Oracle
- Package integrity validation where files and executables obtained via the packaging system match what is installed on disk

Assured Platform

Oracle Solaris and integrated third-party source code follow the Oracle Software Security Assurance, a program that encompasses every phase of the product development lifecycle. Oracle Software Security Assurance is Oracle's methodology for building security into the design, build, testing, and maintenance of its products. Oracle's goal is to ensure that Oracle's products, as well as the customer systems that leverage those products, remain as secure as possible. See http://www.oracle.com/us/support/assurance/index.html for more information.

This assurance program is supported by external security evaluations; currently Oracle Solaris 11 is being evaluated under Common Criteria for the OSPP protection profile at EAL4 along with FIPS 140-2 for both the cryptographic framework and OpenSSL. More information on these evaluations can be found at: http://www.oracle.com/us/support/assurance/evaluations/index.html

Understanding and Reporting on Risk and Compliance

Security decisions are generally driven by either compliance requirements or by risk analysis. Risk is defined as likelihood multiplied by the impact of a security event. Understanding and reporting on risks saves money by selecting the correct set of security controls to address potential risks.

Auditing and Logging

Comprehensive auditing and reporting on an environment can help detect unusual behavior before an event occurs. Understanding the status of a running system can reduce the risk of a data theft event. Traditional UNIX logging (syslog) is a debugging tool. Records generated are application-defined and report on what applications developers decide to log. It is not appropriate to treat logs as fully trusted sources of data. A compromised application will
change generated log events, but logs can be used as a very helpful diagnostic step.

Instead, analysis of risk should be performed using tamper-proof auditing data that is administrator-controlled and kernel mediated. By default auditing is enabled on Oracle Solaris for key events (login, privilege escalation, etc.). However, there are many classes of audit data available to record. Audit events should be transported to another Oracle Solaris system using the remote audit collection capabilities and analyzed for attack signatures or anomaly detection either using the basic analysis facilities in Oracle Solaris or a third-party Security Information and Event Management (SIEM) system.

A unique capability of Oracle Solaris is the ability to tag administrative files and record any changes in the audit log. This administrative edit command is a simple mechanism to record any privileged configuration edits.

Compliance Reporting

Compliance reporting itself does not increase security or reduce risk, but it is an administrate mechanism designed to reduce risk and ensure that internal or external security and privacy requirements are being met. All the effort required to produce compliance reports could be better spent in doing activities that do make a functional difference. Oracle Solaris 11 is trying to reduce the burden of compliance reporting activities by embracing the U.S. Department of Defense Security Content Automation Protocol SCAP ecosystem, a collection of interrelated standards for security reporting and configuration automation, and utilizing those tools to report on system configuration compliance objectives for both the public sector space and for the enterprise market. The OpenSCAP framework has been added to Oracle Solaris 11.1 with reporting templates to follow.

Conclusion

Protecting your organization from reputation or fiscal harm requires advanced platform security features to protect data, isolate applications, limit user actions, and report on system activities. The holistic security architecture in Oracle Solaris 11 is engineered with core operating system and SPARC features to minimize costs and meet the strictest security requirements.

Contact Us

For more information about Oracle Solaris, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.