ORACLE DATA SHEET

Oracle Solaris 11 Engineered for Security, Designed for Compliance

Oracle Solaris 11 is a complete, integrated, and open platform engineered for secure and compliant enterprise cloud environments. Oracle Solaris combines the power of industry-standard security features, unique security and anti-malware capabilities, and compliance management tools for low-risk application deployments and cloud infrastructure.

KEY FEATURES

- No-compromise virtualization with Oracle Solaris Zones and the Kernel Zones feature of Oracle Solaris
- Integrated compliance monitoring and reporting
- Cryptography is FIPS 140-2 validated
- Common Criteria evaluated for OSPP at EAL4

KEY BENEFITS

- Reduce the cost and effort of meeting compliance regulations
- Prevent malware from collecting and leaking sensitive data
- Protect your environment from business-damaging attacks

RELATED PRODUCTS

Oracle recommends the use of the following products alongside Oracle Solaris:

- Oracle Solaris Cluster for High Availability
- Oracle Enterprise Manager – Ops Center Management Suite
- Oracle Solaris Studio Development Tools

A More Secure Enterprise Cloud

Oracle Solaris 11 includes a full distribution of OpenStack, the popular open source project that provides cloud management infrastructure, as a standard, supported part of the platform. Oracle Solaris enhances the OpenStack security posture by automatically sandboxing the infrastructure services and limiting allowed behavior; providing seamless methods to administer, delegate, and record administrative actions across hardware, software infrastructure, and application tiers; and building on Oracle Solaris, which is designed, developed, and tested to be secure.

A More Secure Application Lifecycle

Oracle Solaris 11 includes an archive format called Unified Archives, which enables rapid cloning of application environments across virtualization and bare metal through the development, test, and production lifecycle.

This integrated workflow is designed to ensure businesses stay secure and compliant from an initial install, which establishes a verified, compliant, secured application environment, to destruction. The cryptographically verified application environment has a consistent security posture throughout the development, test, certification, and deployment processes. In addition to standard security features, application weaknesses and misuse can be prevented by centrally managing the read/write access for either an entire virtual machine (Immutable Zones, a feature of Oracle Solaris) or application sandboxing protecting against multistage attacks.

A More Compliant Infrastructure

Compliance management and reporting is a low-value activity that doesn't transform business. Oracle Solaris lowers the cost and effort of compliance management by designing security features to easily meet worldwide compliance obligations; documenting and mapping technical security controls for common requirements like PCI-DSS to Oracle Solaris technologies with a simple-to-use tool that provides not only

reporting but also simple instructions on how to mitigate any compliance test failures; and providing compliance report templates. The compliance system is standards based (XML) and built on the SCAP ecosystem (XCCDF, OVAL, and SCE), which easily integrates with enterprise wide compliance management programs. The graphic below represents a detailed compliance check, which is part of a 200-check PCI-DSS report template.

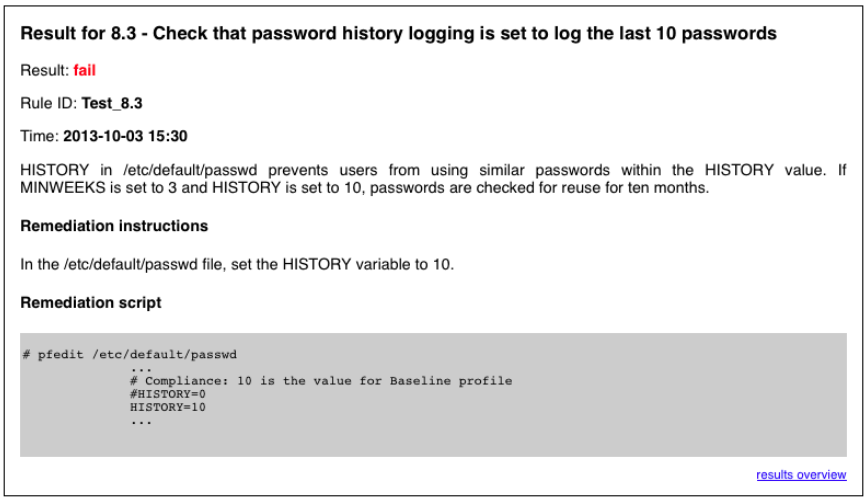


Figure 1. Integrated compliance reporting with Oracle Solaris 11

A More Secure Application

Application weaknesses not only compromise the confidentiality and integrity of the application, but also can be used to collect private information or stage additional attacks. Oracle Solaris improves application security by wrapping the application in layers of security controls inside the virtual machine that can be centrally managed outside the application environment. Oracle Solaris security features are engineered together to reduce risk with a low administrative burden.

Applications, when deployed on Oracle Solaris, are automatically or easily protected against common security exploits by the anti-malware system, a collection of hardware (ADI, ASLR, DEP, and NX) and software technologies (verified boot, signed packaged, and software integrity checking) that build upon each other to ensure the integrity of both infrastructure and applications. Application Data Integrity (ADI), new in the M7 processor, enhances the anti-malware system by protecting memory from a wide variety of data access attacks including buffer overflow and over-reads.

Applications can cryptographically protect data with low-overhead hardware encryption by using one of these solutions: the OASIS PKCS#11 API-based cryptographic framework (used by many commercial programs), OpenSSL, or Java JCE programmatic interfaces. Applications or infrastructure components provided by Oracle Solaris (such as SSH, IPsec, and Kerberos) are automatically accelerated and optimized for extreme performance.

Application data at rest can be cryptographically protected on local disk, iSCSI, or Fibre Channel using ZFS encryption. ZFS disk encryption complements application encryption

RELATED SERVICES

The following services support Oracle Solaris:

- Oracle Premier Support for Systems
- Oracle Premier Support for Operating Systems
- Oracle Solaris Premier Subscription for Non-Oracle Hardware

by protecting data outside the application such as configuration files, application logs, backups, etc. ZFS encryption is at the dataset level and allows flexibility in deployment models for cross-organizational and shared systems. ZFS encryption keys can be stored locally, over the network, or via Oracle Key Manager.

Oracle Database takes advantage of Oracle Solaris plus Oracle's SPARC hardware acceleration to increase database transparent data encryption speeds (almost 5X faster than competing platforms). Oracle Solaris complements this high-performance relational encryption by adding ZFS encryption that protects Oracle Database files (log, journal, etc.) and by applying additional controls such as encrypted swap. Together, these create a full-stack encrypted system that is able to meet many encryption compliance requirements.

A More Secure Infrastructure

Applications and cloud infrastructure can be logically isolated using non-global Oracle Solaris Zones, the fully isolated Oracle Solaris Kernel Zones feature, or fine-grained behavior sandboxing. The sandboxing system (Oracle Solaris with role-based access control) can be used to limit application behavior at runtime without code changes by modifying the startup manifest. The sandboxing system is easy to configure and centrally manage via LDAP. For example, the sandboxing system can be a compensating security control by wrapping legacy apps in additional protections (for example, only allow to bind to port 443 but not 80), or it can be used to impose central IT compliance policies on independently managed lines of business, or to limit the risk surfaces.

Immutability is a special sandboxing mode that can protect either the application machine/zone or the Oracle Solaris global zone in which system configuration is locked while applications run as normal. This is easy to configure and is enabled/disabled with a simple reboot. Logical separation is not unique to the compute layer, but it is extended to traditional networking as well as to application-driven software defined networking functionality. Oracle Solaris provides network virtualization, which emulates complex multitier applications in software. Virtual networking works in conjunction with an industry-standard firewall that integrates with the application starter and fine-grained network sandboxing. Virtual networks and multi tier applications also can be defined by creating secure tunnels using IPsec.

Oracle Solaris logs application messages via a standard system log collector and records system activity via a kernel-controlled auditing system. Audit provides evidence-quality information that integrates with the remote audit collector, while both logs and audits can be securely integrated with enterprise security event analysis systems.

An Assured Platform

Oracle Solaris and integrated third-party source code follow 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.

This assurance program is supported by external security evaluations. Oracle Solaris 11 was evaluated under Common Criteria for the OSPP protection profile at EAL4 along with FIPS 140-2 for both the Oracle Solaris Cryptographic Framework and OpenSSL. More information on these evaluations can be found at:

http://www.oracle.com/us/support/assurance/evaluations/index.html

More Information

For more information about Oracle Solaris 11.3, visit oracle.com/solaris.

CONTACT US

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

CONNECT WITH US

blogs.oracle.com/solaris

facebook.com/oraclesolaris

twitter.com/orcl_solaris

oracle.com/solaris

Integrated Cloud Applications & Platform Services

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0715

Oracle is committed to developing practices and products that help protect the environment