Oracle Solaris 11 and PCI DSS
Meeting PCI DSS Compliance with Oracle Solaris 11

April 4, 2013

Matt Getzelman  PCI Practice Director, Coalfire
# Oracle Solaris 11 and PCI DSS Compliance

## Table of Contents

- Executive Summary ...................................................................................................................... 3
- Introduction ........................................................................................................................................ 3
- Oracle Solaris 11 and Key Features for PCI DSS Compliance ................................................................. 5
  - PCI DSS Segmentation Solutions within Oracle Solaris 11 ................................................................. 6
  - System Software Management ......................................................................................................... 8
  - “Secure by Default” and Service Management ............................................................................... 9
  - Compliance Reporting and External Evaluation .................................................................................. 10
- Conclusion ........................................................................................................................................ 11
- Mapping PCI DSS Requirements to Oracle Solaris 11 ......................................................................... 12
- References & Resources ..................................................................................................................... 31
- About Oracle .................................................................................................................................... 32
- About Coalfire .................................................................................................................................. 32
- Acknowledgments ............................................................................................................................... 32
- About the Author ............................................................................................................................... 33
Executive Summary

This paper provides guidance to IT professionals who are implementing Oracle Solaris 11 within their Cardholder Data Environment (CDE) and to the Qualified Security Assessor (QSA) assessing those environments. The Payment Card Industry Data Security Standard (PCI DSS) applies to all organizations that store, process, or transmit cardholder data. This includes entities such as merchants, service providers, payment gateways, data centers, and outsourced service providers.

This guidance is not intended as an in-depth technical assessment of Oracle Solaris 11 or an installation guide, but rather an analysis of its ability to meet and support the PCI DSS requirements. In evaluation of Oracle Solaris 11 and its security capabilities, Coalfire has determined that it is fully capable of supporting PCI DSS compliance.

The Oracle Solaris 11 features highlighted within this document specifically address PCI DSS compliance; however, the same basic tenets can be used for meeting other regulatory environment standards such as the Gramm–Leach–Bliley Act (GLBA), Sarbanes Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA).

Introduction

This guidance highlights the security features of the Oracle Solaris 11 operating system and its supporting technologies as an ideal platform for hosting PCI DSS applications. This paper makes the following assumptions:

- The reader is familiar with the Payment Card Industry Data Security Standard (PCI DSS)
- The reader has some familiarity with the basics of the Oracle Solaris 11 operating system
The PCI DSS applies to all organizations that store, process or transmit cardholder data. With rapidly changing security compliance expectations, how can systems administrators possibly ensure that the environments they manage are secure and meet all applicable compliance standards?

Achieving and maintaining PCI DSS compliance is not a trivial task; however, Oracle continues to work closely with industry security organizations to ensure its offerings provide solutions to the many compliance challenges facing organizations today. Oracle Solaris 11 is an excellent example of an architecture solution that allows users to easily meet and maintain PCI DSS requirements.

IT professionals who are considering implementing, or have already implemented Oracle Solaris 11 within their cardholder data environment can use this paper as a reference guide for meeting and maintaining PCI DSS compliance. The guidance is organized into the following sections:

**I. Oracle Solaris 11 and Key Features for PCI DSS Compliance:**
An overview of the security features offered by Oracle Solaris 11 and how they help IT professionals efficiently deploy and maintain PCI DSS compliant systems. This area highlights the following security features:

- PCI DSS Segmentation Solutions within Oracle Solaris 11
- System Software Management
- System Configuration with the Service Management Facility (SMF)
Oracle Solaris 11 and PCI DSS Compliance

d. Compliance Reporting and External Evaluation

II. - Conclusion: Summarizes the Coalfire evaluation of Oracle Solaris 11 and its ability to meet and/or exceed PCI DSS requirements.

III. - Mapping PCI DSS Requirements to Oracle Solaris 11: This section provides the critical details on the specific PCI DSS requirements that must be met by Oracle Solaris 11 for deployment in a PCI DSS compliant environment. In addition, the appendix identifies the additional PCI DSS requirements that would benefit from the Oracle Solaris 11 features detailed in this guidance.

IV. - References and Resources: Links and references to materials identified in this document and any additional information that is available on Oracle’s website.

Oracle Solaris 11 and Key Features for PCI DSS Compliance

Oracle Solaris 11 delivers groundbreaking features for fast, secure and reliable deployments within large-scale cloud environments and enterprise data centers. When deployed within an in-scope PCI DSS environment, Oracle Solaris 11 must meet all directly applicable PCI DSS requirements. This guidance shows how Oracle Solaris 11 has been evaluated to meet all directly applicable control objectives. In addition, this guidance outlines several Oracle Solaris 11 supporting features that help address PCI DSS requirements that are not directly related to operating system implementations. Coalfire’s opinion is that the following key features of Oracle Solaris 11 best support PCI DSS compliance:

PCI - DSS Segmentation Solutions within Oracle Solaris 11: Information on multiple virtualization and segmentation technologies available to Oracle Solaris 11 users and how these features support PCI DSS compliance.

System Software Management: The process of updating and maintaining an Oracle Solaris environment has been improved in
Oracle Solaris 11 and PCI DSS Compliance

Oracle Solaris 11. This section provides information on the Image Packaging System and how it directly supports compliance with PCI DSS section six (Develop and Maintain Secure Systems and Applications).

System Configuration with the Service Management Facility (SMF): Information on the Oracle principle of “Secure by Default” and how this supports compliance across multiple PCI DSS sections and requirements.

For additional information on Oracle Solaris 11 Technologies, please visit:


PCI DSS Segmentation Solutions within Oracle Solaris 11

Proper understanding of PCI DSS scope is essential when designing and implementing the architecture of a CDE. The scope of an organization’s PCI DSS assessment must include all system components that store, transmit or process cardholder data. To reduce the scope of PCI DSS compliance, an organization can segment its network and systems in order to isolate components that store, transmit or process cardholder data from the rest of the corporate infrastructure. This removes systems that are unrelated to payment card handling from the overall PCI DSS scope.

There are a number of inherent features within Oracle Solaris 11 that support different methods of network segmentation and customers have the added benefit of not being confined to the traditional segmentation method of hardware firewalls.

This flexibility ensures that their environments can continue to evolve to address emerging business opportunities and security challenges without adversely affecting an organization’s overall PCI DSS scope. In Coalfire’s opinion, it is Oracle’s ability to offer different virtualization technologies on the Oracle Solaris 11 platform that offer end users the most flexibility in configuring an architecture that is scalable and easily manageable. Three key segmentation technologies to highlight are:

- Logical Domains (hardware virtualization)
Oracle Solaris Zones (software virtualization)

Network Virtualization (virtual NICs and VLANs)

**Tip:** Oracle Solaris Zones can be stacked on top of logical domains so that the hardware is broken into isolated virtual machines with independent operating system kernels and then further subdivided by zones to further segment applications or operating system functions.

**Logical Domains (LDOMS):** The traditional hardware-virtualization technology that allows users to segment a server into separate logical domains running on a hypervisor. This technology allows for up to 128 separate virtual machines on one system and offers true kernel space separation.

**Oracle Solaris Zones:** Oracle Solaris Zones are a featherweight virtualization utility built into Oracle Solaris 11 Operating Systems (available on both SPARC and x86 platforms). Oracle Solaris Zones provide isolated process trees based on a common OS kernel foundation and can provide fine grained access to system resources.
Note: Oracle Solaris Zones and Logical Domains are not exclusive technologies; they can be used in a complementary fashion when designing a network infrastructure. Oracle Solaris Zones can be stacked on top of logical domains so that the hardware is broken into isolated virtual machines with independent operating system kernels, and then further subdivided by Oracle Solaris Zones to segment applications or operating system functions.

Network Virtualization: Virtual NICs and VLANs can easily be created inside a single instance of Oracle Solaris 11, allowing for additional segmentation options. As part of the powerful network stack architecture, these tools can be utilized to create application-specific virtual networks than can assist with PCI DSS segmentation.

For additional information on Oracle virtualization technologies please visit the following links:


System Software Management

Oracle Solaris 11 utilizes a new network-based package management system called the Image Packaging System (IPS). This feature simplifies the process of updating and maintaining an Oracle Solaris 11 environment and allows administrators to ensure and verify the integrity of their systems. IPS helps system administrators meet the challenges and requirements outlined in section six of the PCI DSS with regard to change and patch management. For detailed information on PCI DSS requirement six and how Oracle Solaris 11 can solve associated compliance challenges, please review the “Mapping PCI DSS Requirements to Oracle Solaris 11” section below on page 12.
In Oracle Solaris 11, the UNIX root account has been set up as a role, and remote access to the root account is disabled. The Oracle Solaris Role-Based Access Control (RBAC) features make it easy for administrators to meet the controls detailed in PCI DSS section eight.

IPS is integrated with both Oracle Solaris Zones and the native Oracle ZFS file system. Administrators can now easily update their systems and any associated virtual environments through IPS, which improves upon the system update process in previous versions of Oracle Solaris. When a system is updated in IPS, all Oracle Solaris Zones are updated in lockstep so that system integrity is always maintained.

IPS will apply all updates and changes to a clone created from the current ZFS file system with full automatic dependency checking. If anything unexpected occurs during the package update process, administrators can roll back to before the change quickly without any modifications.

The IPS features allow Oracle Solaris 11 customers to address several PCI DSS requirement areas around configuration, change control and patch management. For additional information on IPS and ZFS technologies please visit the following links:


“Secure by Default” and Service Management

Oracle has made significant changes to the initial configuration of Oracle Solaris 11 to ensure it is inherently “Secure by Default”. “Secure by Default” is a system posture that exposes a minimized network-facing attack surface by disabling all non-essential network services. There are no inbound network services listening by default other than SSH; this means that out-of-the-box, an Oracle Solaris 11 installation meets industry security best practices and all directly applicable PCI DSS requirements.

The Service Management Facility (SMF) is an important part of the system configuration and software package installation architecture. The SMF repository in Oracle Solaris 11 supports PCI DSS compliance in a variety of ways including:
Oracle Solaris 11 and PCI DSS Compliance

- Increased control over administrative customizations for service and system configuration
- Configuration preservation during system updates
- Improved auditing of system state changes

Together the “Secure by Default” configuration, the supporting features of Oracle Solaris 11, and the available SMF utilities make setting up and maintaining a secure PCI DSS environment much easier for system administrators. The increased audit and alert functions allow changes to critical system components to be easily tracked and alerted on. For additional information on the SMF technologies, please visit:

**Compliance Reporting and External Evaluation**

Compliance reporting in itself does not improve security or reduce risk; however, it is an administrative mechanism designed to ensure that security and privacy requirements are being met. Oracle is helping to reduce the burden of compliance reporting activities by embracing the U.S. Department of Defense Security Content Automation Protocol (SCAP) ecosystem. SCAP is a collection of interrelated standards for security reporting and configuration automation, and Oracle utilizes 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 (with update 11.1) and reporting templates are soon to follow.

Oracle Solaris and integrated third-party source code follow the Oracle Software Security Assurance (OSSA), a program that encompasses every phase of the product development lifecycle. Oracle Software Security Assurance builds security into the design, build, testing, and maintenance of its products.

Additionally, Oracle Solaris 11 is currently being evaluated under Common Criteria for the Operating System Protection Profile (OSPP) protection profile at Evaluation Assurance Level (EAL) 4 along with FIPS 140-2 for the Oracle Cryptographic Framework.
Conclusion

The information presented in this guidance document shows how Oracle Solaris 11 can meet all applicable PCI DSS requirements.

System administrators can ensure that the environments they manage are secure and meet all applicable compliance standards (such as PCI DSS). With Oracle Solaris 11, the initial configuration, maintenance and compliance reporting activities associated with operating systems have been greatly simplified. The following key features directly align with the PCI DSS requirements and can help administrators meet the evolving compliance and security needs of their environments:

- PCI DSS segmentation options within Oracle Solaris 11 including multiple methods of virtualization
- System Software Management to assist in meeting patch and change management principles outlined in section six of the PCI DSS
- System Configuration with the Service Management Facility (SMF) to ensure only necessary functionality is enabled for fully compliant configurations
- Compliance Reporting tools to assist with all audit and assessment efforts
- Continuing external evaluation to ensure the Oracle Solaris 11 platform and independent third-party products meet stringent security requirements

This guidance paper can be of great benefit to QSAs who are reviewing environments that contain instances of Oracle Solaris 11. QSAs should refer to the subsequent section titled “Mapping PCI DSS Requirements to Oracle Solaris 11” for detailed information on Oracle Solaris 11 PCI DSS requirement mappings.
Mapping PCI DSS Requirements to Oracle Solaris 11

The following section provides details on the specific PCI DSS requirements that must be met by Oracle Solaris 11 for deployment in a PCI DSS compliant environment as well as additional requirements that would benefit from the Oracle Solaris 11 features detailed within this guidance document. Organizations that must adhere to the PCI DSS should always consult with their own PCI Qualified Security Assessor (QSA) to validate the scope and applicability of the requirements to their cardholder data environment. The format of each of the following PCI DSS control areas is as follows:

**PCI DSS Section Number:** A brief description of the PCI DSS control area and its applicability to Oracle Solaris 11.

**Applicable Requirements:** These are the PCI DSS requirements within a PCI DSS section that are applicable to Oracle Solaris 11.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>In-Scope Justification</th>
<th>Oracle Solaris 11 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>The actual PCI-DSS requirement narrative(s).</td>
<td>How or why the listed PCI DSS requirement applies to Oracle Solaris 11 instances.</td>
<td>Specific Oracle Solaris 11 information and features that support a compliant configuration.</td>
</tr>
</tbody>
</table>

**Supported Requirements and Oracle Solaris 11 Features:** This area will detail how the features offered in Oracle Solaris 11 can be utilized to support compliance across other PCI DSS requirements that are not directly applicable to Oracle Solaris 11 implementations.
**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

**Applicable Requirements:** Section one primarily focuses on the security of network components and the architecture of the cardholder data environment. As such, there are no PCI DSS requirements that are directly applicable to Oracle Solaris 11 implementations; however, there are features available in Oracle Solaris 11 that can be used to help support compliant processes across many PCI DSS requirements.

**Supported Requirements and Oracle Solaris 11 Features:** There are multiple control requirements in this section that require proper network segmentation and traffic control. Oracle Solaris 11 offers multiple features and technologies that can be utilized when designing and implementing a cardholder data environment.

**IP Filter as a host-based firewall:** IP Filter can be utilized within Oracle Solaris 11 to provide a host-based firewall solution. This can be used to restrict traffic to and from Oracle Solaris 11 environments in accordance with the PCI DSS section one requirements. When used in this manner, the IP Filter host-based firewall will be applicable to the majority of PCI DSS requirements in this section. When Oracle Solaris 11 is utilized as a workstation or laptop, the IP Filter firewall can be used to satisfy the following requirement:

- **Requirement 1.4:** Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.

**Oracle Solaris Zones and Virtual NICs/VLANs:** Oracle Solaris Zones and virtual network components can be implemented to provide PCI DSS segmentation without the use of dedicated hardware-based firewalls. These features offer flexibility when designing, implementing and maintaining a cardholder data environment. The use of Oracle Solaris Zones with virtual network components (such as VLANs and NICs) must be done with proper PCI DSS segmentation in mind. As such, traffic into and out of in-scope Oracle Solaris Zones must be adequately controlled and must comply with all PCI DSS requirements outlined in PCI DSS section one.

**Secure by Default Configuration:** Oracle Solaris 11 comes pre-packaged as a “Secure by Default” implementation. The PCI DSS prohibits the use of risky or insecure protocols within a CDE. These services are disabled by default in Oracle Solaris 11, which supports the following PCI DSS requirement:

- **Requirement 1.1.5:** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
PCI DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Applicable Requirements: This section details the requirements for configuration standards and security parameters. Oracle Solaris 11 excels in this section due to its “Secure by Default” principle. In addition, the extensive implementation documentation and hardening guidelines maintained and offered by Oracle make developing configuration standards easier for Oracle Solaris 11 users.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>In-Scope Justification</th>
<th>Oracle Solaris 11 Features</th>
</tr>
</thead>
</table>
| Requirement 2.1: Always change vendor-supplied defaults   | Oracle must provide implementation guidance to customers on how to securely configure and implement Oracle Solaris 11 instances. Oracle maintains high-quality configuration standards that can be used as a baseline for customer configurations. For additional information and documentation, please visit: http://www.oracle.com/technetwork/server-storage/solaris11/documentation/index.html
| before installing a system on the network, including but | Additionally, the CIS community has created a benchmark with the recommended security settings for the Oracle Solaris 11 operating system. This document can be obtained from the CIS Security website at: http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris11.100                                                                                                           | “Secure by Default”: Oracle Solaris 11 comes with many security features enabled by default, which makes maintaining a secure configuration in a CDE environment easier. They include the following key points:
| not limited to passwords, Simple Network Management     |                                                                                                                                                                                                                                                                                                                                                         | • Risky protocols are disabled by default (FTP, Telnet)
| Protocol (SNMP) community strings, and elimination of   |                                                                                                                                                                                                                                                                                                                                                         | • SSH only for administrative non-console connections
| unnecessary accounts.                                     |                                                                                                                                                                                                                                                                                                                                                         | • Direct login as root via SSH is disabled by default
|                                                           |                                                                                                                                                                                                                                                                                                                                                         | • Oracle Solaris 11 does not come with any pre-installed passwords. Initial passwords are set by the administrator during the installation process.                                                                                                                                                         |
|                                                           |                                                                                                                                                                                                                                                                                                                                                         | **Oracle Solaris Zones**: If PCI DSS applications are configured to run within Oracle Solaris Zones, then they will not have access to device drivers as Zones do not inherently have this access enabled.                                                                                                                  |
**Requirement 2.2:** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to:
- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS) Institute
- National Institute of Standards and Technology (NIST) standards.

Oracle must provide implementation guidance to customers on how to securely configure and implement Oracle Solaris 11 instances. Oracle maintains high-quality configuration standards that can be used as a baseline for customer configurations. For additional information and documentation, please visit:


Additionally, the CIS community has created a benchmark with the recommended security settings for the Oracle Solaris 11 operating system. This document can be obtained from the CIS Security website at:

http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris11.100

---

**Requirement 2.2.1:** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server (for example, web servers, database servers, and DNS should be implemented on separate servers).

Oracle maintains high-quality configuration standards that can be used as a baseline for customer configurations. For additional information and documentation, please visit:


Additionally, the CIS community has created a benchmark with the recommended security settings for the Oracle Solaris 11 operating system. This document can be obtained from the CIS Security website at:

http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris11.100

---

**“Secure by Default” Oracle Solaris Zones**

Oracle Solaris Zones: Oracle Solaris Zones, Oracle Virtualization Manager and Workload Isolation are some of the Oracle Solaris 11 features that can be utilized for virtual segregation. Resources and network bandwidth can be throttled and controlled across all Oracle Solaris Zones as needed.
Oracle Solaris 11 and PCI DSS Compliance

<table>
<thead>
<tr>
<th>Requirement 2.2.2: Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.</th>
<th>Oracle Solaris 11 administrators will need to ensure that unnecessary services and protocols are disabled. The principle of “Secure by Default” will assist with this exercise by ensuring that many risky protocols and services are disabled by default. This will need to be executed in conjunction with the organization’s configuration standards. Oracle maintains high-quality configuration standards that can be used as a baseline for customer configurations. For additional information and documentation, please visit: <a href="http://www.oracle.com/technetwork/server-storage/solaris11/documentation/index.html">http://www.oracle.com/technetwork/server-storage/solaris11/documentation/index.html</a></th>
<th>“Secure by Default” Oracle Solaris Zones IPS: Oracle IPS makes removing software easier. This helps Oracle Solaris 11 users meet requirement 2.2.4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.</td>
<td>Setting for the Oracle Solaris 11 operating system. This document can be obtained from the CIS Security website at: <a href="http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris11.100">http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.solaris11.100</a> Note: Although virtualization and cloud computing can introduce additional risks if not managed properly, it does not inherently preclude compliance with the PCI DSS. Refer to the PCI Security Standards Council (PCI SSC) document regarding mixed-mode virtualization and PCI DSS compliance for additional information: Information Supplement: PCI DSS Virtualization Guidelines -June 2011</td>
<td></td>
</tr>
<tr>
<td>Requirement 2.2.3: Configure system security parameters to prevent misuse.</td>
<td>Additionally, the CIS community has created a benchmark with the recommended security settings for the Oracle Solaris 11 operating system.</td>
<td></td>
</tr>
<tr>
<td>Requirement 2.2.4: Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Page 16
Oracle Solaris 11 and PCI DSS Compliance

| Requirement 2.3: Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. | All in-scope system components must provide a method for secure non-console administration. Oracle Solaris 11 offers several secure methods for connectivity. | "Secure by Default": Risky communication such as Telnet and FTP protocols are disabled by default in Oracle Solaris 11. Oracle Solaris 11 offers secure protocols such as SSH and SSL/TLS. |

Supported Requirements and Oracle Solaris 11 Features: The majority of requirements in PCI DSS section two are directly applicable to Oracle Solaris 11 instances; however, Oracle’s "Secure by Default" principle will assist system administrators with meeting and maintaining compliance with all PCI DSS configuration requirements. In addition, the strong security controls built into Oracle Solaris Zones and Oracle’s Virtualization Manager make it easier to implement virtualized environments in a PCI DSS compliant manner.
**Requirement 3: Protect stored cardholder data**

**Applicable Requirements:** Section three focuses on the security of the cardholder data at rest. As such, there are no PCI DSS requirements that are directly applicable to Oracle Solaris 11 instances; however, the features available in Oracle Solaris 11 can be used to help support compliant processes across many of these data protection PCI DSS requirements.

**Supported Requirements and Oracle Solaris 11 Features:** There are several features native to Oracle Solaris 11 implementations that can be utilized by Oracle customers to protect data at rest. It’s important to note that these features can be utilized to protect all sensitive data types and not just cardholder data as specified in the PCI DSS.

**Oracle Solaris ZFS and the Oracle Solaris Cryptographic Framework:** These features allow Oracle Solaris 11 users to protect sensitive data of all types including log files, database repositories, configuration files, etc. Oracle ZFS allows users to select from a number of supported encryption algorithms and associated key lengths.

**Key Management Integration Capabilities:** Oracle Solaris 11 allows Hardware Security Module (HSM) functionality (such as the Sun SCA6000) to be directly integrated into Oracle Solaris 11 to allow additional key management capabilities.

**Oracle Key Management & ZFS:** By using a combination of ZFS encryption and the Oracle Key Manager appliance, the NIST 800-57 guidelines for encryption key lifetimes can be met to help Oracle customers comply with the following PCI DSS requirements associated with key management:

- **Requirement 3.6:** Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:
  - **Requirement 3.6.1:** Generation of strong cryptographic keys
  - **Requirement 3.6.2:** Secure cryptographic key distribution
  - **Requirement 3.6.3:** Secure cryptographic key storage
  - **Requirement 3.6.4:** Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).
• **Requirement 3.6.5:** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised.
  
  Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.

• **Requirement 3.6.6:** If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).
  
  Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.

• **Requirement 3.6.7:** Prevention of unauthorized substitution of cryptographic keys.

• **Requirement 3.6.8:** Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

---

**Requirement 4: Encrypt transmission of cardholder data across open, public networks**

**Applicable Requirements:** Section four focuses on the security of cardholder data while in transit. As such, there are no PCI DSS requirements that are directly applicable to Oracle Solaris 11 instances; however, the features available in Oracle Solaris 11 can be used to help support compliant processes across many of these data transmission PCI DSS requirements.

**Supported Requirements and Oracle Solaris 11 Features:** Oracle Solaris 11 is able to support multiple public-transport encryption protocols and the native Oracle Solaris Cryptographic Framework will support crypto-acceleration when running on T-Series SPARC hardware.

**Supported Communication Protocols:**

- SSLv3/TLS
- SSH
Requirement 5: Use and regularly update antivirus software or programs

Applicable Requirements: The PCI SSC has regulated that PCI DSS section five is only applicable to operating systems that are commonly affected by malicious software. The Oracle Solaris 11 operating system is not commonly affected by malicious software within server architecture. For workstation implementations it is the customer’s responsibility to implement PCI DSS compliant antivirus (A/V) and anti-malware solutions.

Supported Requirements and Oracle Solaris 11 Features: There are third-party antivirus and anti-malware solutions that are available to Oracle Solaris 11 users that want to use traditional solutions to address this requirement. As mentioned above, if Oracle Solaris 11 is utilized as a workstation solution, then selecting and implementing an antivirus solution will be necessary for PCI DSS compliance. Outside of traditional A/V solutions, Oracle Solaris 11 also offers the following security controls that are closely aligned with these requirements:

• Oracle ZFS supports direct integration with antivirus and anti-malware solutions configured within the underlying network infrastructure. This means that A/V controls can be applied to ZFS data without an Oracle Solaris 11 client installation.
• As part of the Image Packaging System (IPS), package verification can be used to check and verify the integrity of all Oracle Solaris 11 operating executables and will report on any detected damaged or altered OS files. Installation packages and updates from Oracle are always digitally signed.
• Oracle Solaris Zones can be configured as read-only for security purposes. Applications running within these Zones would not be able to adversely affect any OS executable or configuration files.
PCI DSS Requirement 6: Develop and maintain secure systems and applications

Applicable Requirements: The intent of PCI DSS section six is to implement secure development processes and ensure systems are patched and maintained at a hardened level. While the development-focused requirements are not applicable to Oracle Solaris 11 instances directly, the patching and change management requirements are fully supported by Oracle Solaris 11.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>In-Scope Justification</th>
<th>Oracle Solaris 11 Features</th>
</tr>
</thead>
</table>
| 6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. | The Oracle Solaris 11 system will need to be fully supported by Oracle to meet this requirement. Oracle has mature and dedicated processes in place for updating and patching their products. | Image Packaging System (IPS): The patching process has changed from previous versions of Oracle Solaris. Full package updates are now utilized and when implemented, they affect the security of all Oracle Solaris Zones implemented on a server. Previously, customers may have had difficulty determining which components had changed on Oracle Solaris patches and may not have been able to tell if their environments were fully up to date. That has been greatly simplified in the new process with the IPS. Now, at a glance, customers will know whether or not they have the latest updates.  
Oracle Solaris Support Repository Updates (SRUs): Oracle patches and fixes (SRUs) are provided by Oracle on roughly a monthly basis. Quarterly, these updates are combined into Critical Patch Updates (CPUs).  
Oracle Software Security Assurance: This program ensures that all Oracle products are patched and updated as needed. For more information on this process, please visit:  
**Supported Requirements and Oracle Solaris 11 Features:** There are numerous Oracle Solaris 11 features that can be utilized to help support vulnerability awareness programs, change management processes and secure development methodologies:

**Oracle Security:** Oracle offers a number of security notifications to help users meet their vulnerability management requirements. Users can review the Oracle Critical Patch Update Advisory and the Oracle Software Security Awareness Blog to ensure they have the most recent information available on Oracle systems and products. To learn more about these notifications please visit: [http://www.oracle.com/technetwork/topics/security/whatsnew/index.html](http://www.oracle.com/technetwork/topics/security/whatsnew/index.html) This will help users satisfy the following requirement:

- **Requirement 6.2:** Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

**Oracle Solaris Zones:** Oracle Solaris Zones can be utilized as a segmentation method to isolate the development and test platforms from the production environment. This could be used to help satisfy the following PCI DSS requirements:

- **Requirement 6.4.1:** Separate development/test and production environments.
- **Requirement 6.4.2:** Separation of duties between development/test and production environments.

**Boot Environments:** The Boot Environment capability of Oracle Solaris 11 aligns with a strong change management process. Oracle encourages system administrators to take a snapshot of the current boot environment before making any administrative changes to the system. Utilizing the underlying ZFS snapshotting technology, system administrators would then have a fallback bootable environment if there are any problems. Administrators can create boot environments as needed for the root file system; however, backup boot environments are created by default during an Oracle software system update. Documenting this capability within an organization’s change management procedures makes it easy for users to meet the back-out procedures requirement. For additional information on managing boot environments please visit the following link:


- **Requirement 6.4.5.4:** Back-out procedures.

**Oracle Solaris 11 Functionality to Support Secure Development Guidelines:** Oracle Solaris 11 has native functionality than can be utilized by developers to help develop secure applications:

- **Requirement 6.5.2:** Buffer overflow (Validate buffer boundaries and truncate input strings.)
Oracle Solaris 11 and PCI DSS Compliance

- After the Oracle Solaris 11 update 1 release, developers can enable Address Space Layout Randomization (ASLR)
- The stack is not executable for native Oracle Solaris 11 64-bit applications
- The stack is tagged as “not executable” for native Oracle Solaris 11 32-bit applications.

**Requirement 6.5.3: Insecure cryptographic storage (Prevent cryptographic flaws)**
- Oracle Solaris 11 offers key management and key functions at the OS level that can be utilized to help meet this requirement. This includes the Oracle Solaris Cryptographic Framework.

**Requirement 7: Restrict access to cardholder data by business need-to-know**

**Applicable Requirements:** The responsibility for restricting access to cardholder data clearly lies with Oracle Solaris 11 customers and as such, most of the requirements in this section are not directly applicable; however, functionality within Oracle Solaris 11 can be utilized to support an organization’s access control paradigm.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>In-Scope Justification</th>
<th>Oracle Solaris 11 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 7.2: Establish an access control system for systems components with multiple users that restricts access based on a user’s need-to-know, and is set to “deny all” unless specifically allowed.</td>
<td>Requirement 7.2.3 states that all in-scope access control systems have a default “deny-all” setting. Oracle Solaris 11 meets this requirement.</td>
<td>“Secure by Default”</td>
</tr>
</tbody>
</table>

**Supported Requirements and Oracle Solaris 11 Features:** Within Oracle Solaris 11, Role-Based Access Control (RBAC) is always utilized. When implementing an access control paradigm, Oracle customers can utilize the User Privilege Rights Management system to empower or restrict users appropriately.

- **Requirement 7.1.2:** Confirm that privileges are assigned to individuals based on job classification and function (also called “role-based access control” or RBAC).
Requirement 8: Assign a unique ID to each person with computer access

Applicable Requirements: As in the previous PCI DSS section, the responsibility for implementing a compliant access control paradigm falls upon Oracle Solaris 11 administrators. The majority of the requirements outlined here deal with user account management and password controls. It’s important to note that while the majority of these controls are not directly applicable to Oracle Solaris 11 instances, Oracle Solaris 11 can be configured to meet each of the control objectives detailed here.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>In-Scope Justification</th>
<th>Oracle Solaris 11 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement 8.4: Render all passwords unreadable during transmission and storage on all system components using strong cryptography.</td>
<td>All in-scope system components must protect user and account passwords compliantly.</td>
<td>“Secure by Default”: Oracle Solaris 11 user passwords are protected via SHA-256 hashing (with salt) by default.</td>
</tr>
</tbody>
</table>

Supported Requirements and Oracle Solaris 11 Features: Oracle Solaris 11 can be configured in a manner that meets or exceeds all PCI DSS section 8 requirements. Key areas to highlight are as follows:

“Secure by Default”: In Oracle Solaris 11, default remote access to the root account is disabled. “Root as a role” is configured by default and users will need to login with their own unique IDs to facilitate this type of access. This helps facilitate compliance with the following requirements:

- **Requirement 8.1:** Assign all users a unique ID before allowing them to access system components or cardholder data.
- **Requirement 8.5.8:** Do not use group, shared, or generic accounts and passwords, or other authentication methods.

Remote Access: Pluggable Authentication Modules (commonly referred to as PAM modules) can be utilized to integrate two-factor remote access solutions directly into Oracle Solaris 11; however, PAM modules for multi-factor authentication are not installed by default.

- **Requirement 8.3:** Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.
Oracle Solaris 11 and PCI DSS Compliance

Oracle Solaris 11 Configuration: Oracle Solaris 11 can be configured to meet or exceed each of the following user access control requirements:

- **Requirement 8.5.3**: Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.
- **Requirement 8.5.5**: Remove/disable inactive user accounts at least every 90 days.
- **Requirement 8.5.9**: Change user passwords at least every 90 days.
- **Requirement 8.5.10**: Require a minimum password length of at least seven characters.
- **Requirement 8.5.11**: Use passwords containing both numeric and alphabetic characters.
- **Requirement 8.5.12**: Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **Requirement 8.5.14**: Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
- **Requirement 8.5.15**: If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

Requirement 9: Restrict physical access to cardholder data

Applicable Requirements: There are no applicable PCI DSS requirements to Oracle Solaris 11 implementations within this section as they focus on physical security. Oracle customers will need to implement strong physical security controls to protect Oracle Solaris 11 servers when they are utilized within PCI DSS environments.

Supported Requirements and Oracle Solaris 11 Features: There are no relevant Oracle Solaris 11 features for this PCI DSS section.
Requirement 10: Track and monitor all access to network resources and cardholder data

Applicable Requirements: This PCI DSS section requires that all in-scope system components have the ability to log, audit and track access to in-scope resources and cardholder data. As detailed below, Oracle Solaris 11 implementations can meet all applicable requirements in this section. “Solaris Audit” is enabled by default on installations of Oracle Solaris 11 to meet accountability requirements; for more information on the Oracle Solaris Audit configuration capabilities, please visit the following link: http://docs.oracle.com/cd/E23824_01/html/821-1456/auditref-34.html#scrolltoc

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>In-Scope Justification</th>
<th>Oracle Solaris 11 Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirement 10.1:</strong> Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</td>
<td>This requirement is fully applicable to Oracle Solaris 11 instances and needs to be documented within Oracle implementation guidance.</td>
<td>Oracle Solaris 11 implementations can be configured to meet this requirement.</td>
</tr>
<tr>
<td><strong>Requirement 10.2:</strong> Through interviews, examination of audit logs, and examination of audit log settings, perform the following:</td>
<td>All of the user activity detailed within the section 10 requirements needs to be captured by audit log systems within Oracle Solaris 11, with the exception of requirement 10.2.1: Verify all individual access to cardholder data is logged. Ensuring that all access to cardholder data is logged will be the responsibility of the Oracle customer; however, Oracle Solaris 11 can help facilitate this process.</td>
<td>Oracle Solaris 11 implementations can be configured to meet this requirement. Oracle recommends that Oracle Solaris 11 implementations in a PCI DSS environment enable the CUSA audit class. Enabling this class will help Oracle Solaris administrators meet these logging requirements.</td>
</tr>
<tr>
<td>- 10.2.2 Verify actions taken by any individual with root or administrative privileges are logged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- 10.2.3 Verify access to all audit trails is logged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- 10.2.4 Verify invalid logical access attempts are logged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- 10.2.5 Verify use of identification and authentication mechanisms is</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Requirement 10.3: Record at least the following audit trail entries for all system components for each event:

- 10.3.1 User identification
- 10.3.2 Type of event
- 10.3.3 Date and time
- 10.3.4 Success or failure indication
- 10.3.5 Origination of event
- 10.3.6 Identity or name of affected data, system component, or resource

Audit logs generated by Oracle Solaris 11 instances will need to contain all of the information detailed in the requirements to the left.

Oracle Solaris 11 audit logs contain all of this required information by default. No additional configuration from the default installation is necessary for meeting this requirement.

### Requirement 10.4: Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

Oracle Solaris 11 will need to meet all of the PCI DSS requirements for time synchronization.

Oracle Solaris 11 implementations can be configured to meet this requirement. It can be configured to utilize NTP or integrate with an organization’s time synchronization solution.

### Requirement 10.5.1: Limit viewing of audit trails to those with a job-related need.

Oracle Solaris 11 will need to provide the means for restricting access to audit logs and audit trails.

Oracle Solaris 11 implementations can be configured to meet this requirement. "Secure by Default": Only users that have been granted a role with the “Audit Review Rights Profile” will have the ability to access log files and audit trails.
Supported Requirements and Oracle Solaris 11 Features: Oracle offers several security features that can help customers meet the log centralization, storage and review requirements:

Oracle Solaris Audit and Audit Vault: In Oracle Solaris 11 update 1, instances can be configured to send audit trails to a centralized repository with integrity, privacy and authentication. The Oracle Audit Vault product is not part of Oracle Solaris 11 installations; however, it can be utilized as a log correlation and review utility. Using the Oracle Solaris 11 audit configuration along with the Oracle Audit Vault product can help administrators meet the following PCI DSS requirements:

- **Requirement 10.5:** Secure audit trails so they cannot be altered.
- **Requirement 10.5.2:** Protect audit trail files from unauthorized modifications.
- **Requirement 10.5.3:** Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

BART: The Basic Audit and Report Tool (BART) is a default installation within Oracle Solaris 11. It may be utilized to help meet file-integrity monitoring requirements:

- **Requirement 10.5.5:** Verify the use of file-integrity monitoring or change-detection software for logs by examining system settings and monitored files and results from monitoring activities.
**Requirement 11: Regularly test security systems and processes**

**Applicable Requirements:** This section primarily covers the scanning and testing processes expected to cover PCI DSS environments. As such, there are no directly applicable requirements with regard to Oracle Solaris 11 implementations.

**Supported Requirements and Oracle Solaris 11 Features:** There are no directly applicable requirements outlined in this section; however, there are Oracle Solaris 11 features that can be utilized by Oracle customers to help support these processes.

**Oracle Security:** Oracle offers a number of security notification services to help users meet vulnerability management requirements. Users can review the Oracle Critical Patch Update Advisory and the Oracle Software Security Awareness blog to ensure they have the most recent information available on Oracle systems. To learn more about these notifications, please visit: [http://www.oracle.com/technetwork/topics/security/whatsnew/index.html](http://www.oracle.com/technetwork/topics/security/whatsnew/index.html)

This will indirectly help satisfy the following requirements:

- **Requirement 11.2:** Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

- **Requirement 11.3:** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:
  - 11.3.1 Network-layer penetration tests
  - 11.3.2 Application-layer penetration tests

**BART:** The Basic Audit and Report Tool (BART) is a default installation within Oracle Solaris 11. It may be utilized to help meet file-integrity monitoring requirements. In addition, the package-verify command (part of IPS) uses checksum values to ensure the integrity of OS files and executables after IPS updates.

- **Requirement 11.5:** Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
Requirement 12: Maintain a policy that addresses information security for all personnel

Applicable Requirements: This PCI DSS section details the responsibilities for maintaining an information security policy, assigning information security management responsibilities, implementing security awareness programs for employees, and managing an Incident Response Plan (IRP). This section is not applicable to Oracle Solaris 11 instances.

Supported Requirements and Oracle Solaris 11 Features: This section is not applicable to Oracle Solaris 11 instances; however, it should be noted that Oracle maintains high-quality configuration standards that can be used as a baseline for customer configuration documentation.

For additional information and documentation, please visit:

References & Resources

3. (2010). *Oracle Key Manager Overview* 

Additional Oracle Solaris 11 information can be found at:


Oracle Software Security Assurance:


The following referenced PCI SSC documents can be viewed and downloaded from the PCI SSC website at: https://www.pcisecuritystandards.org/

- Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures Version 2.0
- Information Supplement: PCI DSS Virtualization Guidelines, June 2011
About Oracle

Oracle Corporation is a $37.1 billion public company headquartered in Redwood Shores, California, and is the world’s largest enterprise software company with more than 115,000 employees worldwide. Oracle is a leading provider of computer hardware products and services. Oracle develops, manufactures, markets, distributes and services database and middleware software; applications software; and hardware systems, consisting primarily of computer server and storage products. Oracle products are built on industry standards and are engineered to work together or independently within existing customer IT, including private and public cloud computing environments. Oracle has a presence in 145 countries and occupies 24.9 million square feet of space, including 2.1 million at the Corporate Headquarters.

About Coalfire

Coalfire is a leading independent information technology Governance, Risk and Compliance (IT GRC) firm that provides IT audit, risk assessment and compliance management solutions. Coalfire has offices in Dallas, Denver, Los Angeles, New York, San Francisco, Seattle and Washington, D.C. and completes thousands of projects annually in the retail, financial services, healthcare, government, and utilities industry sectors. Coalfire offers a new generation of cloud-based IT GRC tools under the Navis brand that are used to efficiently manage IT controls and keep pace with rapidly changing regulations and best practices. Coalfire’s solutions are adapted to requirements under the PCI DSS, GLBA, FFIEC, HIPAA/HITECH, NERC CIP, Sarbanes-Oxley FISMA/FedRAMP, and emerging data privacy legislation. Coalfire is a Qualified Security Assessor (QSA) and Payment Application QSA (PA-QSA) firm, and is also a HITRUST CSF Assessor firm. For more information, visit: www.coalfire.com

Acknowledgments

The author would like to acknowledge the following individuals from Oracle for their contributions to this paper: Darren Moffat, Alexander Barclay, Joel Weise, Gary Winiger and Glynn Foster. In addition, the author recognizes Dirk Anderson of Coalfire for his significant contributions to this paper.
About the Author

Matt Getzelman (matt.getzelman@Coalfire.com) is the PCI Practice Director for Coalfire, a QSA Company headquartered in Louisville, Colorado. Matt has over nine years of experience working with financial systems security. His experience covers a broad spectrum of security disciplines from application and systems development to securing multiple distributed platforms, mainframe and acquiring financial environments. This includes experience across multiple audit and security standards including PCI DSS, TR-39, ISO, SOX, SAS 70 and GLBA.