How Oracle Linux Promotes PCI DSS Compliance

Optimizing Systems in a Cardholder Data Environment

ORACLE WHITE PAPER | OCTOBER 2015

Introduction

For any business that processes, transmits, or stores payment card information, fraud is a dominant concern. According to The Nilson Report (Issue 1068, July 2015), the worldwide payment card industry experienced $16.31 billion in fraud-related losses last year. Indeed, reports of payment card fraud or data compromise against major retail or banking organizations are recurring stories in the news.

In 2004 leading vendors in the card services industry collaborated in an effort to define a unified set of cardholder data protection standards. They formed the PCI Security Standards Council to create and maintain the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS outlines a set of requirements for evaluating the handling and storage of cardholder information and authentication data. These requirements constitute the basis of internal security reviews, periodic evaluations, and formal compliance assessments. The current PCI DSS standard (revision 3.1) defines 12 requirement categories that apply to operational practices, staff responsibilities, and technology components in the cardholder data environment (CDE). It addresses system and data protection mechanisms that must be in place across equipment, services, and applications.

This paper describes best practices for Oracle Linux implementations and Oracle Linux operating system (OS) features that help to meet requirements listed in the PCI DSS Requirements and Security Assessment Procedures document. It discusses deployment strategies that can narrow the scope of a PCI DSS assessment and improve overall system and data security. It examines each of the 12 requirement categories, highlighting Oracle Linux features, implementation practices, and relevant Oracle technologies that can help to achieve PCI DSS compliance.

Implementing Oracle Linux securely is only one design aspect in achieving an overall PCI DSS-compliant infrastructure. The goal of this paper is to help businesses safeguard cardholder data in an Oracle Linux deployment. Additional security mechanisms are required for other infrastructure components—along with effective configuration architectures and sound operational practices—to realize a fully compliant PCI DSS environment.

Best Practices for a Secure Oracle Linux Deployment

Adhering to common security practices for Oracle Linux implementations helps to safeguard data in a cardholder data environment (CDE) and protects applications and systems from compromise. Such practices are applicable not only to achieving PCI DSS compliance but also to meeting corporate, privacy, and other regulatory mandates (such as HIPPA, Sarbanes-Oxley, etc.). Best practices with respect to security in any Oracle Linux implementation include:

» Segmenting and isolating applications that transmit or process sensitive data. A well-designed architecture segments workloads on different physical or virtual machines. As an example, separating database, application, and web services using different Oracle Linux servers prevents a compromised service from impacting other services. Placing services that aren't related to the CDE (such as corporate e-mail or file services) on other machines and networks improves architectural security and narrows the scope of a compliance assessment.

Oracle Linux supports Linux Containers (LXC), a lightweight virtualization feature that allows Linux processes to have a private operating system view—with a container-specific process ID space, file system structure, and virtual networks—while sharing the same kernel. For applications that require a fully virtualized environment and full kernel isolation, Oracle VM is a true hypervisor-based virtualization software that hosts isolated virtual machines running Oracle Linux, Oracle Solaris, or Microsoft Windows operating systems. Using Oracle VM, applications can be sandboxed on Oracle Linux with isolated virtual networks.

» Minimizing installed software. When installing the Oracle Linux operating system, best practice is to install only the minimal set of software packages, thus limiting potential avenues of compromise. When installing an Oracle Linux 7 server, the default software configuration is limited to a "minimal install" that installs only the base set of software packages.

» Restricting network access and minimizing network services. Careful design of networks and limiting network services to only those that are absolutely required decreases the number of exposure points and narrows the scope of a PCI DSS assessment. By configuring firewall services built into Oracle Linux, an Oracle Linux host can block unauthorized traffic, which can thwart unsanctioned access and reduce possible attack vectors.

» Securing access to applications and systems. In addition to restricting network access and services, system administrators should assign unique accounts and passwords to each user. Oracle Linux systems should be configured so that administrators log in with a regular user account before using `su` or `sudo` to perform privileged root operations.

» Configuring system logs and auditing to identify suspicious activity and detect signs of compromise. Oracle Linux supports log collection and reporting, as well as detailed system auditing capabilities.

» Keeping software up-to-date. Applying patches and updates promptly is critical to maintaining application and system security. Ksplice, an innovative technology included with an Oracle Linux Premier Support subscription, applies critical kernel updates and security errata without the need for a reboot. Rather than delaying the installation of crucial updates until a planned outage, Ksplice allows kernel security patches to be applied immediately, without downtime, reducing the exposure window for Oracle Linux systems.

» Managing systems and system lifecycles. Oracle Linux Premier Support and Basic Support subscriptions include access to Oracle Enterprise Manager 12*c*, an intuitive interface to control the full Oracle-based infrastructure stack, including Oracle Linux provisioning, patching, monitoring, administration, and configuration management. Oracle Enterprise Manager 12*c* can also be used in conjunction with Oracle VM software to manage virtual servers and Oracle Linux guests.

» Staying informed about security vulnerabilities, available errata, and pertinent security-related announcements. Oracle provides email notification about errata and maintains web sites for identified errata and Common Vulnerabilities and Exposures (CVEs). With a support subscription, organizations can access the comprehensive resources of the Unbreakable Linux Network (ULN) to obtain software patches, updates, and fixes for Oracle Linux and Oracle VM. For test and development systems that don't require support, the same security errata and bug fixes are freely available on the Oracle Linux Public Yum server (public-yum.oracle.com).

Oracle applies these general practices even within its own data centers. Oracle Cloud Services, for example, is a revenue-generating Oracle business that hosts mission-critical applications as customer-facing cloud services. This organization implements Oracle software applications (including Oracle Database, Oracle Fusion Middleware, and applications such as Oracle's PeopleSoft, JD Edwards EnterpriseOne, and Siebel Customer Relationship Management) using Oracle Linux servers and Oracle VM to provide segmentation and isolation of application workloads. Oracle Cloud Services administrators use Oracle Enterprise Manager 12*c* to monitor and provision virtual servers and apply kernel security errata for identified vulnerabilities using Ksplice technology.

The security page for Oracle Linux and the references section at the end of this paper list a number of useful resources to help IT organizations and administrators harden Oracle Linux implementations. In addition, Oracle offers a number of consulting services designed to help customers deploy hardened and secure application environments. Oracle Security Design and Hardening Support, for example, is a comprehensive database analysis and configuration offering that implements Oracle Database security product sets, processes and procedures, applying best practices to meet demanding security requirements.

Mapping PCI DSS Requirements to Oracle Linux Technologies

The 12 PCI DSS requirement categories that are evaluated during a PCI DSS review or formal compliance assessment reflect the best practices and security principles outlined above. The following pages examine each of the 12 categories, describing the required elements in each category and details of how Oracle Linux features and technologies help to meet PCI DSS compliance. The table below summarizes requirements and how Oracle Linux (and related Oracle technologies in a deployment) can help to achieve compliance.

AN OVERVIEW: MEETING PCI DSS COMPLIANCE USING ORACLE LINUX

Category	High-Level PCI DSS Requirements	How Oracle Linux Promotes Compliance
Build and Maintain a Secure Network	1: Install and maintain a firewall configuration to protect cardholder data 2: Do not use vendor-supplied defaults for system passwords and other security parameters	» *Oracle Linux provides built-in host-based firewall capabilities through the kernel Netfilter subsystem.* » *TCP wrappers filter traffic & block unauthorized service requests.* » *The Oracle Secure Configuration Program emphasizes "secure by default" installations of all Oracle software, including Oracle Linux.* » *The Oracle Linux installation wizard includes a "minimal server" software configuration to follow best practice of minimization.* » *Default accounts in the OS (except for root) are locked with a password that cannot be hashed (e.g., "*"). During installation a root password should be specified. Administrators should assign a unique account & password for each user.* » *Configuration standards and best practices are listed on the Oracle Linux Security page at linux.oracle.com/security/.*
Protect Cardholder Data	3: Protect stored cardholder data 4: Encrypt transmission of cardholder data across open, public networks	» *Oracle Linux supports LUKS encryption of block devices.* » *SELinux mediates access based on security policy.* » *OpenSSL manages digital certificate and encryption key security.* » *Oracle Linux includes strong encryption capabilities and network protocols to protect data at rest as well as data in motion.* » *Oracle Linux can take advantage of hardware cryptographic acceleration technologies such as AES-NI on certain x86/x64 processors to accelerate encryption & decryption.*
Maintain a Vulnerability Management Program	5: Use and regularly update anti-virus software 6: Develop and maintain secure systems and applications	» *An Oracle Linux Premier Support subscription provides Ksplice.for zero downtime kernel patching.* » *Support customers can access Oracle Linux patches & updates on ULN. For servers without support (e.g., Test or Dev systems), the same patches are freely available on Oracle's public yum site.* » *Oracle Linux features a built-in file integrity-checking tool (AIDE).* » *Oracle Linux provides OpenSCAP libraries and tools, including the* `oscap` *scanner and CVE information in OVAL.* » *Oracle publishes errata and CVE mailing lists.* » *Oracle Enterprise Manager 12c and Spacewalk can automate systems management tasks.*
Implement Strong Access Control Measures	7: Restrict access to cardholder data by business need-to-know 8: Assign a unique ID to each person with computer access 9: Restrict physical access to cardholder data	» *SELinux provides Mandatory Access Control (MAC) and can be extended to cover new application domains. SELinux also facilitates Role-Based Access Control (RBAC).* » *Oracle Linux supports centralized identification & authentication using IPA, Kerberos, LDAP, NIS, Winbind, etc.* » *Oracle Linux uses an industry-standard SHA-512-based hash to secure passwords.* » *Pluggable Authentication Module (PAM) technology can enforce specific authentication and password policies.*

Category	High-Level PCI DSS Requirements	How Oracle Linux Promotes Compliance
Regularly Monitor and Test Networks	10: Track and monitor all access to network resources and cardholder data 11: Regularly test security systems and processes	» *Logging daemons capture system events. Logwatch can be customized and run to report suspicious log entries.* » *Auditing collects data at the system, kernel, and file system level, including events that require the use of privilege.* » *The OpenSCAP vulnerability checker oscap reports weaknesses or signs of compromise.* » *Oracle Linux DTrace can be used to perform kernel tracing, gathering information to help detect intrusion or possible compromise.*
Maintain an Information Security Policy	12: Maintain a policy that addresses information security	» *Oracle Enterprise Manager 12c and Spacewalk standardize Oracle Linux server deployments, applying security policy more consistently.* » *Deployment best practices are documented in the Oracle Linux Security Technical Implementation Guides (STIGs) and Oracle Linux Security Guides.*

1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

The PCI DSS requirements in this category focus on designing and configuring networks in the cardholder data environment (CDE) to restrict and control network traffic. The primary goal of these requirements is to safeguard CDE systems from unauthorized access from untrusted networks. Compliant network architectures must contain firewalls on all connections between public networks and the DMZ, as well as between the DMZ and internal networks (Figure 1). Firewalls can be physical devices or software-based. Documentation must list and justify all network services, protocols, and ports to achieve compliance with requirements in this section. Network services that are considered insecure (such as FTP, Telnet, POP3, IMAP, and SNMP v1 and v2) must be disabled or removed. If these services are absolutely required, they must be implemented with additional industry-proven, well-documented, and tested security features.

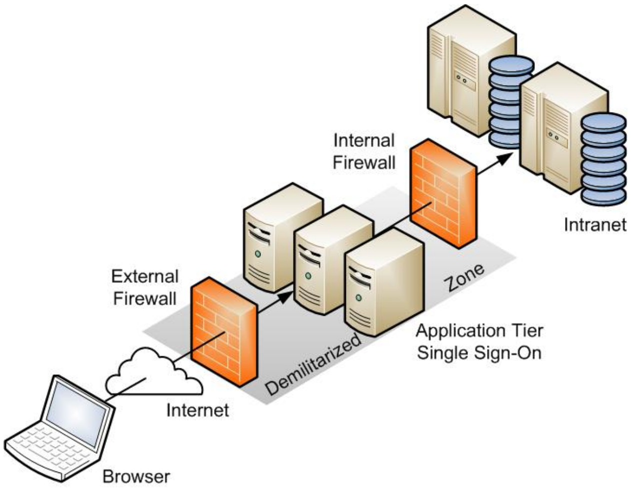

Figure 1. Proper network design (including firewalls) impedes unauthorized access attempts.

To help meet requirements in this category, Oracle Linux includes host-based firewall capabilities using Netfilter, a kernel subsystem that applies configured filtering rules to block unauthorized network traffic. Netfilter performs packet filtering, network address translation (NAT), and IP masquerading, which can meet requirements to obscure internal IP addresses. Netfilter rules are configured using `firewalld` in Oracle Linux 7 or with `iptables` in Oracle Linux 6 or Oracle Linux 7. The `firewalld` service, which is enabled by default in Oracle Linux 7, is an improved interface for managing `iptables` rules, allowing them to be modified without the loss of existing connections.

Oracle Linux also supports TCP wrappers to filter incoming network traffic. When a remote connection request for a wrapped network service occurs, access is denied or allowed based on the configured rules. In this way identified hosts or networks can access the required network services while preventing unauthorized access. TCP wrappers can also be used to block and signal intrusion attempts from known malicious sources.

Additional network access authentication and control mechanisms are included in many built-in applications and protocols. For example, the Apache HTTP Server (`httpd`) that is included in Oracle Linux contains modules that can be configured to control access to web site resources or to perform authentication and authorization of web server requests. Postfix is configured as the default Mail Transfer Agent (MTA) on Oracle Linux and supports industry-standard authentication based on SASL, the Simple Authentication and Security Layer, allowing SMTP clients to establish an authentication protocol with an SMTP server.

A PCI DSS environment must also document enabled network services, protocols, and ports. The Oracle Linux `netstat`, `lsof`, and `nmap` commands list open TCP ports and services. (Before installing or using `nmap`, check local legislation regarding port scanning software as possession or use may be unlawful in some jurisdictions.)

2: Do Not Use Vendor-Supplied Defaults for Passwords & Parameters

Requirements in this category focus on the use of best practices and industry-accepted standards for system hardening, configuring security parameters, and eliminating any vendor-supplied defaults for passwords and user accounts.

Recognizing the role of software security assurance in protecting customer deployments, Oracle maintains an intense focus on secure product development, vulnerability handling, and security testing. Part of this focus includes secure software development practices and a secure configuration program that stresses that all Oracle products install out-of-the-box into a secure state. Because of this emphasis, Oracle Linux is designed to be "secure by default." The installation process allows initial user accounts and passwords to be set up by an administrator at installation time. Default accounts in the OS (except for root) are locked with a password that cannot be hashed, such as "*". When an initial user account is defined during installation, the installer rejects null passwords and issues a warning if weak passwords are entered. A root password should also be configured at installation time.

By default network services that are high-risk (such as FTP and Telnet) are disabled. Secure Shell (SSH) is enabled only for administrative non-console connections. Directly logging in as root via the `ssh` command should be disabled so that privileged root operations are always attributed directly to an individual user. Auditing can then capture a specific user identity for actions performed using `su` or `sudo`.

Additional PCI DSS required elements in this category stipulate that a CDE implementation should follow configuration standards, including the best practices of segmentation, isolation, minimization, and management introduced earlier. Linux Containers (LXC) support lightweight virtualization in the form of container-specific process ID spaces. Segmentation and isolation requirements are also frequently met by deploying a single service (such as an individual web, application, or database service) on an Oracle Linux server configured as an Oracle VM guest.

Standardizing configurations using Oracle VM templates, Kickstart, or scripts is also recommended since this standardization reduces the likelihood of errors, reducing risk and narrowing assessment scope. A centralized management tool (such as Oracle Enterprise Manager 12*c*) helps to standardize deployment configurations and enables effective monitoring, patching, and management of Oracle VM servers and Oracle Linux instances in the CDE. Using a pretested Kickstart profile also promotes easily repeatable, standardized configurations.

When installing Oracle Linux, administrators should deploy the “minimal install” software configuration and only add additional RPM software packages based on a valid and documented business need. When installing systems and application software, only accept RPM packages that have been digitally signed (the repository configuration file should contain `gpgcheck=1` to import the supplier’s GPG key). All Oracle Linux RPMs are cryptographically signed with an Oracle-specific GPG key to verify the integrity and authenticity of installed packages.

The PCI DSS requirements in this section also mandate that administrators follow industry-accepted standards for system hardening (such as standards from CIS, ISO, SANS, or NIST. Relevant industry standards for Oracle Linux are listed in the Oracle Linux security page, including the CIS Security Configuration Benchmark for Oracle Linux 7 and the Oracle Linux 6 STIG Version 1.

3: Protect Stored Cardholder Data

The third requirement category focuses on maintaining the security of cardholder data at rest. Cardholder data consists of primary account numbers (PANs), authentication data such as card validation codes (CVCs) and PINs, and transaction data, including customer and merchant identities. This section outlines PCI DSS requirements for data retention and disposal, data storage and encryption, encryption key protection and management, and documentation of related policies and operational procedures. In addition to strong and effective data security processes and policies, techniques such as encryption, truncation, masking, and hashing are fundamental approaches for protecting cardholder data at rest.

Key features in Oracle Linux to address these requirements include support for encryption and hashing using strong cryptography. Oracle Linux supports block device encryption using `dm-crypt` and the Linux Unified Key Setup-on-disk-format (LUKS). An administrator uses the `cryptsetup` command to set up device encryption and authentication at installation, and can specify encryption for both file systems and swap. Once encryption is set up, data cannot be accessed when the system is off, preventing compromise in the event of physical device loss or theft. When the system boots and an administrator enters the appropriate passphrase, the device is decrypted and data is accessible.

Oracle Linux includes support for OpenSSL, a cryptography toolkit and library that implements cryptographic algorithms, including ciphers (AES, RC5, etc.), cryptographic hash functions (including MD5, MD4, SHA-1, SHA-2, etc.), and public key cryptography (RSA, DSA, Diffie-Hellman, etc.). Administrators can use the `openssl` command line tool to access cryptography functions implemented in the library.

OpenSSL can be used to manage the security of encryption keys to safeguard them from unauthorized access—one of the PCI DSS requirements in this section. OpenSSL includes capabilities for the creation and management of private keys, public keys and parameters; public key cryptographic operations; the creation of X.509 certificates; the calculation of signed message digests; and file encryption/decryption operations using ciphers. Oracle Linux includes OpenSSL library modules validated as compliant with Federal Information Processing Standard (FIPS) Publication 140-2, a standard for cryptographic modules.

Java applications typically use a keystore supplied with the JDK to store cryptographic keys, X.509 certificate chain information, and trusted certificates. On Oracle Linux the default JDK keystore is `/etc/pki/java/cacerts`, and the `keytool` command manages self-signed certificates for the JDK keystore.

To protect applications and data, Oracle Linux also includes Security Enhanced Linux (SELinux), which provides mandatory access controls (MAC) to limit access to files, processes, devices, users, and applications based on security policy. Developed initially by the U.S. National Security Agency, SELinux is configured as Oracle Linux boots, and by default the operating system runs SELinux in “enforcing” mode. In this mode the operating system implements Mandatory Access Controls (MAC) in addition to traditional Discretionary Access Controls that grant access based solely on a user’s identity. SELinux mediates access according to MAC policies that enforce access decisions in the kernel and features three predefined policies, which can be further customized as necessary:

- Targeted (default). Specific processes (`httpd`, `named`, `sshd`, and privileged processes) run in an SELinux confined domain that denies access to any domain-external resources.
- Strict. This policy is similar to “targeted” but restricts access more pervasively and aggressively.
- Multilevel Security (MLS). This policy implements the Bell-LaPadula model for multi-level system security, which mediates access using security labels (Secret, Top Secret, etc.)

For more information see the SELinux documentation in the Oracle Linux Security Guide.

4: Encrypt Transmission of Cardholder Data Across Public Networks

Requirements in this category focus on the security of cardholder data while in transit and mandate the use of trusted keys and certificates, secure protocols, and strong encryption algorithms The requirements mandate effective network configurations (including Internet, mobile, and wireless network configurations) along with the use of industry-tested and accepted standards for encryption and authentication protocols to safeguard cardholder data transmitted over public networks.

As with data at rest, Oracle Linux supports strong encryption to protect data in motion. Recent generations of x86/x64 system processors include support for hardware-based cryptography that can accelerate encryption and decryption operations. Both Intel and AMD offer processor families that incorporate Advanced Encryption Standard (AES) extensions to the core instruction set architecture. Functionality in Oracle Linux (such as `openssl`) can take advantage of hardware acceleration technologies such AES-NI to speed up common cryptographic operations on x86/x64 architectures.

Public-key cryptography can be used to encrypt data traffic on public networks and validate connection identities. Digital certificates establish trust between connection endpoints and safely distribute public keys. Highlighted in the previous section, the OpenSSL implementation in Oracle Linux supports key management and industry-standard cryptographic algorithms. OpenSSL supports TLS1.0, TLS1.1 and TLS1.2 including ciphers that provide perfect forward secrecy. For relatively insecure legacy applications it can also support SSLv2 and SSLv3. These encryption capabilities and protocols help to implement Virtual Private Networks (VPNs), Secure Shell connections, and password protection.

Administrators commonly use the Secure Shell (`ssh`) for protected, encrypted communications with other systems. Oracle Linux supports OpenSSH using either SSH protocol version 1 (SSH1) or version 2 (SSH2). Since SSH is an entry point into a server, the service should be disabled if it is not needed. If enabled, SSH enables secure access to remote systems using built-in encryption, protecting traffic over the wire (see the blog article Oracle Linux Tips and Tricks: Using SSH); configuring parameters in the configuration file `sshd_conf` can help to restrict connections, creating an `ssh` tunnel, limiting `ssh` access (such as to a specific group or certain users), or timing out an `ssh` client automatically after a period of inactivity.

OpenSSH supports several authentication mechanisms, including public key authentication. The OpenSSH `ssh-keygen` utility can be used to generate a public and private key pair specific to each user. The user’s private key is then used instead of a password to authenticate remote access (password authentication can be disabled). As an extra security measure, the key generation utility can accept a passphrase to encrypt the private key, and then the passphrase must also be entered each time the key is used.

5: Protect Against Malware and Update Anti-Virus Software

Requirements in this category are applicable to operating systems commonly affected by malware such as worms, viruses, spyware, and Trojan horses. Organizations must ensure that anti-virus mechanisms are in place, kept current, and performing periodic scans to avert vulnerabilities. Auditing (see requirement #10) must monitor virus and malware activity.

While Linux servers are not as commonly subject to malware attacks as some other operating systems, many organizations install and regularly update an anti-virus solution to protect against malware. A number of third party anti-malware solutions are available for Linux operating systems.

In addition to installing a third-party anti-malware software solution, updating it regularly, and performing periodic scans, other intrusion detection mechanisms help to detect if a system has been compromised. The Oracle Linux 7 release includes RPM packages for AIDE (Advanced Intrusion Detection Environment), an open source file integrity-checking tool. (See Requirement #11: Regularly Test Security Systems and Processes, page 12).

6: Develop and Maintain Secure Systems & Applications

Requirements in this category focus on implementing secure operational processes to configure, patch, and maintain systems and applications at a hardened level. Keeping informed about vulnerabilities, assigning a risk ranking, and installing vendor-supplied security patches are key requirements in protecting systems and applications. When a software error that potentially enables unauthorized access to systems, networks, or data is identified, it is assigned a Common Vulnerabilities and Exposures (CVE) identifier. The MITRE Corporation maintains a list of CVEs that describe publicly known cyber security issues—this list is an RSS data feed for the U.S. National Vulnerability Database (NVD), which adds metrics such as severity scores and impact ratings. For CVEs that are deemed critical, PCI DSS requirements stipulate the installation of security patches within one month of their release.

Oracle simplifies the processes of staying informed about security issues and keeping Oracle Linux systems up-to-date. The Oracle Linux security page includes a link to all errata releases, listed by type, severity, advisory, summary and release date, as well as a link to security errata by CVE identifiers. The page also allows administrators to subscribe to Oracle Linux and Oracle VM errata mailing lists to receive notifications automatically about identified software issues. If administrators want to generate a list of errata or CVE information for a currently running Oracle Linux server, the `yum-plugin-security` package outputs known operating system errata. To keep other Oracle software products up-to-date (such as Oracle Database, Oracle Fusion Middleware, and other Oracle applications), Oracle customers can sign up to be notified of Critical Patch Update Advisories and Security Alerts to help meet vulnerability management requirements. Oracle issues Security Alerts for any vulnerability fixes deemed too critical to wait for distribution in the next quarterly Critical Patch Update.

Automating processes related to security configuration best practices and vulnerability management is an effective technique for protecting systems and applications in a CDE. The National Vulnerability Database (NVD) provides a repository for U.S. government Security Content Automation Protocol (SCAP) standards that can be used to find system vulnerabilities and evaluate compliance. Oracle Linux provides OpenSCAP libraries and tools based on the open source OpenSCAP project, which received SCAP 1.2 certification from NIST on 04/29/2014. The OpenSCAP packages include the `oscap` command-line configuration and vulnerability scanner (see also Requirement #11: Regularly Test Security Systems and Processes, page 12). The OpenSCAP toolkit is also distributed with Oracle VM Server for x86 and Oracle Solaris 11.2, so it can be used to analyze compliance of Oracle Linux and Oracle Solaris servers running as Oracle VM guests.

Efficient PCI DSS security practices require installing security updates and software patches as soon as possible after they're published. Oracle Linux offers a distinct advantage in keeping servers in the CDE patched and up-to-date. In many mission-critical environments, applying errata to the operating system kernel means waiting until a scheduled maintenance window so that servers can be taken offline and rebooted. Security updates are often postponed until a planned outage is practical and convenient—thus servers and applications remain online and accessible even though they're unprotected from identified kernel vulnerabilities. To eliminate this exposure and the risk of compromise, Oracle Linux Premier Support includes access to Ksplice, an innovative technology that allows administrators to apply kernel security updates, patches, and critical bug fixes without a reboot.

Ksplice improves security, reliability, and availability of Oracle Linux by enabling zero downtime kernel updates, helping to keep systems up-to-date without service disruption. By configuring Ksplice to use the Oracle Unbreakable Linux Network (ULN), administrators can automatically retrieve and apply Ksplice modules to virtual and physical Oracle Linux servers. Ksplice minimizes the risk of security exposure and data compromise since it can apply kernel patches without needing to wait until a planned outage.

With Oracle Linux Basic and Premier Support subscriptions, Oracle includes no-charge access to Oracle Clusterware (which provides HA) and Oracle Enterprise Manager 12*c* (which empowers comprehensive lifecycle management), as well as support for Spacewalk (an open source project for Linux systems management). In large data centers, centralizing and automating management is critical to consistent and secure operations. Using a centralized management tool such as Oracle Enterprise Manager 12*c* or Spacewalk can help to keep systems up-to-date and prevent errors that can occur from manual maintenance processes.

Oracle Enterprise Manager 12*c* provides a "single pane of glass" interface to control provisioning, patching, monitoring, administration, and configuration management—not only for Oracle Linux but for an entire Oracle-based applications infrastructure. Oracle Enterprise Manager 12*c* provides a holistic view of the end-to-end Oracle stack, across the full range of Oracle hardware, virtualization, operating system, middleware, database, and application solutions. Oracle Enterprise Manager 12*c* software includes complete Role Based Access Control as well as LDAP and Directory Services integration for end-to-end secure management of cardholder data environments.

As an alternative, Spacewalk is a systems management tool that can automate management tasks for Linux-only servers. It can be used to perform system maintenance and configuration tasks on Oracle Linux servers deployed either as physical machines or virtual guests.

7: Restrict Access to Cardholder Data by Business Need-to-Know

Requirements in this category focus on restricting access to cardholder data on a need-to-know basis, and are largely applicable to operational processes, staffing responsibilities, and business logic. The requirements follow the security principle of least privilege, which dictates that users should be given the least amount of privilege necessary to perform their jobs.

Many requirements in this category are not directly pertinent to an Oracle Linux implementation since they are process-related. However, Oracle Linux does incorporate the principle of least privilege in several respects. Mandatory Access Control features in SELinux, for example, restrict access to system resources based on security policy. SELinux also facilitates Role-Based Access Control (RBAC); privileges to perform certain operations are assigned to roles, and users are able to assume these roles based on specific job functions. For example, creating accounts is typically a task assigned to the role of System Administrator, while assigning passwords to accounts is the responsibility of users given the role of Security Officer.

8: Identify & Authenticate Access

The requirements in this category focus on user account management and authentication, and mandate sound operational practices to meet compliance. Administrators must assign each user a unique account and one-time use password before allowing access. Terminated or inactive accounts should be immediately disabled and removed. All system and user accounts should be protected by strong passwords, and password policies for complexity, aging, lockout must be implemented.

Meeting identification and authentication requirements in this category is largely dependent on effective administrative practice and proper configuration settings. From a best practice perspective, a centralized user authentication method (such as the Lightweight Directory Access Protocol, LDAP) can simplify authentication administration and management tasks, lowering the risk of unused accounts and accounts with null passwords that could be possible attack vectors.

Oracle Linux supports both local and remote storage of identification and authentication data. Locally accounts and passwords are stored separately in the `/etc/passwd` and `/etc/shadow` files. When user passwords are created, all passwords are encrypted using a strong hashing algorithm (SHA-512). For centralized, remote storage of authentication data, Oracle Linux offers a number of options: OpenLDAP (an LDAP implementation), Identity Policy Audit (IPA), Network Information Services (NIS), or Winbind. The Kerberos authentication protocol can be used in conjunction with LDAP, IPA, and NIS to provide secure remote connections.

Oracle Linux provides authentication configuration tools (both a configuration GUI and a command line interface, `authconfig`) to specify the authentication mechanism and related parameters. These administrative interfaces adjust settings in Pluggable Authentication Module (PAM) configuration files located in the `/etc/pam.d` directory. PAM support in in Oracle Linux makes it easier to enforce strong user authentication and password policies, including rules that enforce password complexity, length, age, and expiration. Using multifactor identification techniques (such as card keys, biometric identification, and so on) in addition to strong password rules can add an additional level of identification control, and is mandated for remote network access in a PCI DSS environment.

Oracle provides a spectrum of products that can augment Oracle Linux deployments to enhance security in cardholder data environments. For businesses that need to balance the objectives of access, security, and regulatory compliance, Oracle offers a suite of access and identity management products, including Oracle Access Management, Oracle Identity Governance, and Oracle Directory Services. The Oracle family of identity management products can help organizations secure sensitive applications and data by managing user access to achieve compliance with regulatory mandates.

9: Restrict Physical Access to Cardholder Data

Requirements in this category focus on physical security and restricting physical access to the facilities, networks, and equipment that store and process cardholder data. The requirements also mandate controls for physically securing all media, including backups as well as data on paper or other storage media.

While these requirements have no direct impact on how Oracle Linux is implemented, keeping systems in a locked data center and limiting access to authorized and trained personnel is an important security precaution. Administrators can use a secure console to access Oracle Linux instances on headless physical servers in a protected data center.

To secure media (including removable media), Oracle Linux supports full-disk encryption using `dm-crypt` and LUKS. These technologies encrypt device partitions using a passphrase that must be entered at boot. In addition, Oracle Linux includes eCryptfs utilities that can be used to encrypt individual file systems.

Password protection mechanisms are also typically built into the BIOS of many x64 systems. On Oracle Linux systems, the GRUB boot loader can be configured to require a valid password before a system can be booted. BIOS and GRUB precautions prevent an unauthorized user with physical access from modifying a system's BIOS, altering the boot device, and booting from an alternate medium. The Oracle Linux Security Guide gives instructions on how to configure a GRUB boot loader password.

10: Track and Monitor Access to Network Resources and Cardholder Data

Requirements in this category focus on ability to log, audit, and track access to resources and data in the CDE. The requirements mandate a means of identifying individual users that perform privileged operations or access cardholder data, audit data, system components, or other security-relevant information. PCI DSS requirements stipulate the secure handling of audit trails and system logs. In addition, formal review processes (performed via automated tools or manually) are required to identify suspicious activity, unauthorized access attempts, and other evidence of attempts to breach security.

Oracle Linux includes capabilities to capture both system logs as well as detailed audit trails. System logs record security-relevant events from the kernel, system services, and running applications. In a compliant PCI DSS environment, privileged actions must always be associatedwith an individual user and logged; Oracle Linux should be configured so that a specific user must authenticate as root before performing such actions.

Oracle Linux uses the logging daemons `rsyslogd` (in Oracle Linux 6 and Oracle Linux 7) and `journald` (a new daemon in Oracle Linux 7) to track system events. (`Journald` records system messages in non-persistent journal files in memory, but can be configured to forward messages to `rsyslogd`, which by default archives only `syslog` messages). It is best practice to configure multiple centralized `syslog` servers and run `logwatch(8)`, a customizable tool for analyzing system log files, to report log entries that reflect suspicious activity. Log files should be captured on isolated, non-root file systems to prevent "file system full" errors from impacting log collection.

Auditing is more pervasive and verbose, capturing specific events such as system logins, account modifications, and the actions of `su` or `sudo` (by default). Auditing can also be configured to capture detailed system call activity or modifications to certain files. The configuration file (`/etc/audit/auditd.conf`) defines the data retention rules, the audit volume's maximum capacity (andwhat action to take if that capacity is exceeded), and local or remote audit trail locations. Audit trails are typically stored using a sequence of volumes in rotation so that audit operations can continue uninterrupted even if a volume becomes full. The kernel audit system daemon (`auditd`) records configured events, including the event type, a timestamp, the associated user ID, and success or failure of the system call. PCI DSS requirements also mandate the use of NTP to synchronize system timestamps and can be set up during the installation of Oracle Linux servers. Procedures must also be in place in a compliant CDE to protect the integrity of log files and audit trails and to conduct regular reviews of collected data to uncover suspicious activities or signs of compromise.

In addition, DTrace in Oracle Linux is a tool that a security analyst could use to investigate suspicious activity or look for signs of compromise. Probes can be developed to detect changes at the operating system level and compile reports that can be further examined. While DTrace can be used to detect intrusion, a more formal intrusion detection product is traditionally deployed in a PCI DSS environment. DTrace in Oracle Linux can be used to complement such a solution.

11: Regularly Test Security Systems and Processes

Requirements in this category focus on operational processes for vulnerability scans and penetration testing. Qualified personnel must run internal and external network vulnerability scans each quarter and after any changes are made to the CDE infrastructure. The requirements also mandate resolving any identified high-risk problems and conducting rescans. External and internal penetration testing (that simulates ways that an attacker might exploit potential vulnerabilities) is also part of the PCI DSS security testing requirements. A proactive approach to intrusion detection and file integrity checking is also mandated to detect and thwart intrusion attempts.

To aid in the process of conducting vulnerability scans, Oracle Linux provides the `oscap` scanner, an automated and standardized way of identifying system vulnerabilities. The `oscap` scanner checks system configuration settings and evaluates systems for signs of compromise against a set of Security Content Automation Protocol (SCAP) security policies and standards. Over time, the National Vulnerability Database (NVD) is migrating security configuration checklists from the National Checklist Program (NCP) repository to conform to SCAP. For Oracle Linux 5 and Oracle Linux 6, checklists are currently available in the NVD repository as Oracle Linux Security Technical Implementation Guides (STIGs). (At this time the STIG for the Oracle Linux 7 release is still under development.)

Oracle Linux Premier and Basic support contracts include support for Oracle Enterprise Manager 12*c* and Spacewalk system management. Oracle Enterprise Manager 12*c* Cloud Control provides lifecycle management that includes an extensive compliance management framework. Using the management console, administrators can configure compliance standards and evaluate target systems against best practices for configuration, security, and data storage. For Linux administrators that use Spacewalk for systems management, it includes the ability to perform compliance checks. Spacewalk can automate OpenSCAP compliance audits against industry-standard security checklists and generate reports about possible vulnerabilities.

There are several available open source and commercial file integrity checking tools, including AIDE (Advanced Intrusion Detection Environment) and Tripwire. The Oracle Linux 7 release includes the RPM package for AIDE. When installed and first configured, AIDE performs an initial file system scan and records cryptographic hashes of each file in a database. During subsequent checks, which can be automated to run regularly using `cron`, the tool compares the stored checksums to files within the file system, detecting and recording any changes from the baseline. (For more information, see the open source project web site for AIDE or the `aide(1)` man page.)

12: Maintain an Information Security Policy

Requirements in this category focus on maintaining and disseminating information security policy to personnel (including employees, contractors, vendors, or service providers) that access CDE data and systems. The requirements mandate usage policies and processes for conducting risk assessments to identify and formally document threats and vulnerabilities for CDE assets. Policies and procedures must clearly delineate responsibilities and roles with respect to security, including the formal assignment of a Chief Security Officer. In addition, the organization must have an annually verified incident response plan to respond to a system security breach or incidents in which cardholder data is compromised.

While many of the requirements in this section are process-related and not directly applicable to an Oracle Linux implementation, configuration and best practices standards (such as the Oracle Linux Security Technical Implementation Guides (STIGs) can be used as a baseline for documentation purposes. Role-Based Access Controls in SELinux also form a foundation to define different security-related roles and assign responsibilities with respect to privileged system operations, maintenance, and security management procedures. In a typical PCI DSS environment that includes many Oracle Linux servers (perhaps many virtual servers deployed using Oracle VM), using a centralized management tool such as Oracle Enterprise Manager 12*c* or Spacewalk can implement security policies more consistently and pervasively than manual administration methods across many servers.

Conclusion

Oracle maintains a strong business focus on products and deployment strategies that optimize security and protect data. Oracle Linux is a secure enterprise-class operating system that can help to safeguard systems, networks, and data integrity for production environments that must comply with PCI DSS requirements. Because of its basis in open source technologies, Oracle Linux benefits from security improvements that have originated from the open source Linux development community, including innovations such as access control lists (ACLs), cryptographic libraries, and trusted utilities.

Implementation best practices (especially those discussed here and covered more thoroughly in the Oracle Linux Security Guide for Release 6 or Oracle Linux Security Guide for Release 7) apply broadly to environments that seek stringent application, system, and data protections. Techniques such as segmentation, isolation, and minimization are typical deployment strategies for many business-critical application environments. Strong encryption capabilities help to protect both data at rest and data in motion. Using Ksplice technology to apply kernel security errata rapidly when software vulnerabilities are identified and addressed reduces the time that Oracle Linux servers are exposed to unmitigated risks. And the availability of built-in security tools—such as the OpenSCAP vulnerability scanner and the AIDE file integrity checker—can help to identify weaknesses, thwart avenues of attack, and foster compliance with many of the PCI DSS requirements.

References

Resource	**URL**
PCI Security Standards Council (PCI SSC)	pcisecuritystandards.org
PCI Data Security Standard Requirements and Security Assessment Procedures	pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss
PCI DSS Quick Reference Guide v2.0	pcisecuritystandards.org/documents/PCI_SSC_Quick_Reference_Guide.pdf
Oracle Software Security Assurance	oracle.com/us/support/assurance/overview/index.html
CIS Security Configuration Benchmark for Oracle Linux 7	benchmarks.cisecurity.org/tools2/linux/CIS_Oracle_Linux_7_Benchmark_v1.0.0.pdf
Oracle Linux Security	linux.oracle.com/security/
Oracle Critical Patch Update Advisories and Security Alerts	oracle.com/technetwork/topics/security/alerts-086861.html
Oracle Linux Errata	linux.oracle.com/errata
Oracle Linux Home Page	oracle.com/us/technologies/linux
Oracle Linux 7 Documentation	docs.oracle.com/cd/E52668_01/index.html
Oracle Linux Security Guide for Release 7	docs.oracle.com/cd/E52668_01/E54670/html/ol7-nmon-sec.html
Oracle VM Security Guide for Release 3.3	docs.oracle.com/cd/E50245_01/E50254/html/index.html
Oracle Enterprise Manager Documentation	docs.oracle.com/en/enterprise-manager/
Oracle Enterprise Manager Ops Center Administration Guide	docs.oracle.com/cd/E40871_01/doc.122/e38534/toc.htm
Oracle Technology Network article: *Tips for Hardening an Oracle Linux Server*	oracle.com/technetwork/articles/servers-storage-admin/tips-harden-oracle-linux-1695888.html
Oracle Technology Network article: *Tips for Securing an Oracle Linux Environment*	oracle.com/technetwork/articles/servers-storage-admin/secure-linux-env-1841089.html

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

B blogs.oracle.com/oracle

f facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

How Oracle Linux Promotes PCI DSS Compliance
October 2015