CIO FROM IDG | Red Hat | sysdig

How to stay PCI Compliant in a container environment

Hardly a week goes by without a high-profile data breach. No wonder that the worst of the worst of these, including credit card information, can keep CISOs and security staff up at night.

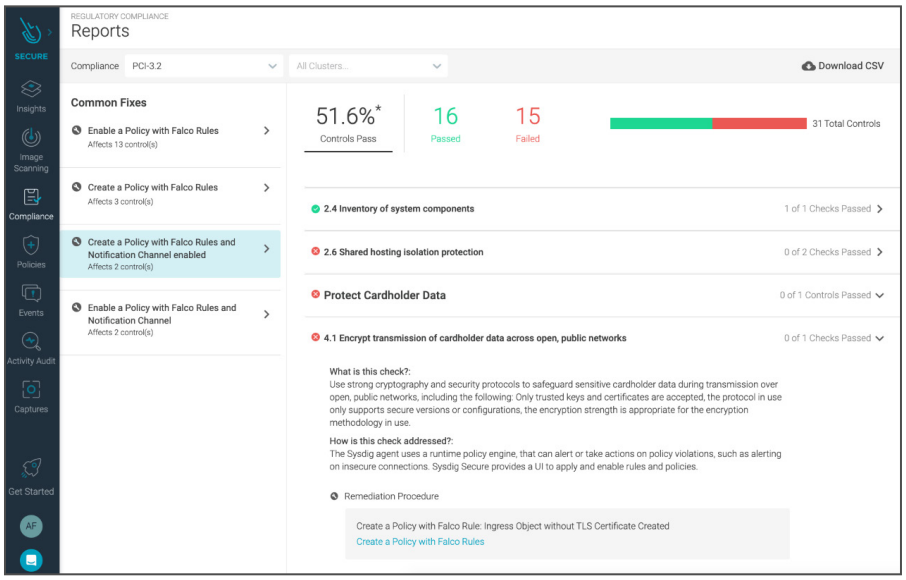
It's with good reason, then, that there are stringent regulations in place to ensure that organisations are treating their payment data with the gravity that it deserves. Chief among these is PCI DSS, the Payment Card Industry Data Security Standard and commonly referred to as PCI compliance, which establishes requirements for security policies, technologies and ongoing processes to merchant and financial institution payment systems from breaches and theft of cardholder data.

Although the PCI Security Standards Council that defines the PCI has no enforcement power, the standard has been adopted and is enforced by the five credit card brands that founded the organisation and share equally in ownership, governance, and execution of the Council's work: American Express, Discover, JCB International, MasterCard and Visa Inc.

Complicated compliance regime

Credit cards are distributed by "issuing banks" under the JCB, MasterCard, and Visa brand logos, or directly by American Express and Discover. When merchants accept a card as payment it is authorized and accepted by the merchant's "acquiring bank." Those acquiring banks are subject to financial penalties if they or their merchant and service provider customers are found to have been in non-compliance with PCI, and those banks often impose fines on merchants deemed to have been responsible.

That makes for a complicated compliance regime, particularly as the PCI DSS is updated on a two-year schedule. Compliance requires scoping of "all system components that are located within or connected to the cardholder data environment" and annual assessment by a Qualified Security Assessor who verifies the technical information given by merchants or service providers, and validates the scope of the assessment culminating in a Report on Compliance.



"Compliance with PCI DSS represents a baseline of security, and is certainly not a guarantee against being hacked," writes CSO. According to the annual payment security report issued by Verizon Business, less than 28% of global organisations maintained full compliance with PCI DSS.

So, it's no surprise that many merchants, service providers, and even banks, view PCI DSS compliance as a burden, particularly as a successful assessment really only applies to the moment in time of that assessment, and any subsequent systems modifications can move a company outside of compliance.

As applications migrate to the cloud, there are three key attributes of containerized environments that make PCI container compliance challenging:

- **Container sprawl** – Containers spin up and down and IP addresses are constantly changing, making any form of PCI audit extremely difficult.
- **Container lifespan** – Sysdig's container usage research found that 52% of containers live for five minutes or less, while six percent of containers live longer than a week. Organisations must establish a way to record detailed container activity as proof of compliance after the container has disappeared.
- **Open-source packaging** – When using open source, companies must be as diligent about updating their open source dependencies as they would be about updating their own code. Preventing known vulnerabilities and flagging newly identified vulnerabilities not only reduces risk, but it is also a step in passing PCI audits.

Taking advantage of modern software development

Organisations are risk-averse in making changes to payment systems, such as adopting modern software development processes and containers, which are not specifically cited in the PCI DSS specification. Traditional security tooling built for legacy architectures does not provide visibility into dynamic container environments. But businesses that design in appropriate security should not have to pass up the opportunity to use modern development tools and methodologies that provide greater agility.

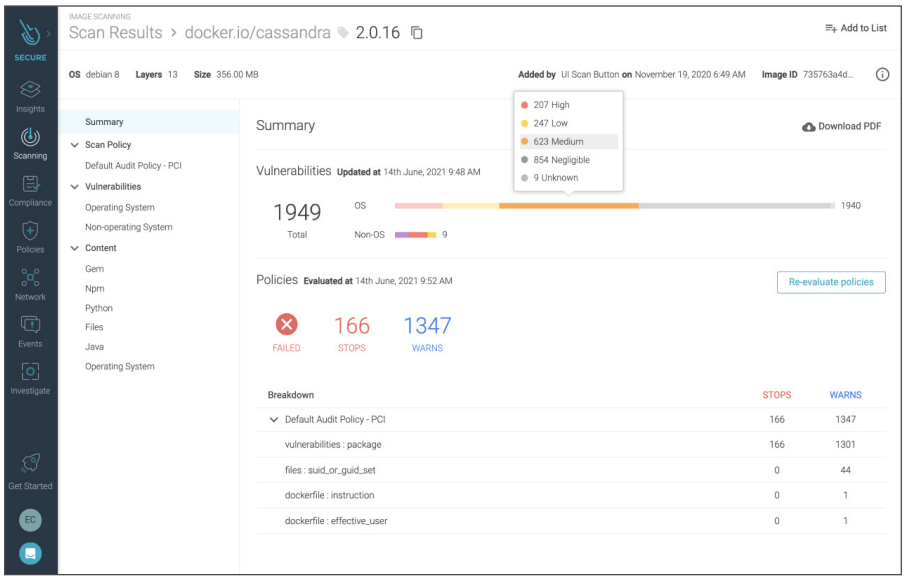
Software today is generally assembled, not built from scratch; many organisations are adopting open-source code as the fastest way to drive innovation, speed, and lower cost. Increasingly, they are utilising container and Kubernetes-based platforms to implement their IT systems.

Meeting PCI-DSS requirements can be complex in fast-changing container environments where containers change continually. It can be difficult to detect when assets in a dynamic Kubernetes environment fall out of PCI compliance. Validating compliance requires mapping the requirements of the standard and associated controls to specific policies and checks during the build phase of the software development life cycle and runtime checks to ensure continual compliance, manage security risk and pass security audits.

Container orchestration with Red Hat® OpenShift®

Organisations subject to PCI DSS can remain compliant and vigilant with a unified security and compliance DevOps platform for containers, Kubernetes and cloud. That can position companies to have full visibility of their estate and to handle customers' most important data confidently.

Red Hat OpenShift Container Platform is a container orchestration solution that enables organisations to run both cloud-native and traditional applications, in containers, at scale. Certified Kubernetes is at the core of OpenShift, which brings added-value features to complement Kubernetes, including built-in security controls.



Red Hat engaged Coalfire Systems, Inc., a respected payment card industry Qualified Security Assessor company, for an independent assessment that OpenShift could be configured and deployed in a way that would satisfy the PCI DSS.

Run more confidently on the cloud with Sysdig

The Sysdig Secure DevOps Platform extends Red Hat OpenShift capabilities across the container lifecycle and tracks progress using compliance dashboards. Starting with the infrastructure layer, Sysdig performs specific host and platform compliance checks, like Kubernetes benchmarks and Docker CIS benchmarks, and also provides remediation guidance for policy violations occurring in OpenShift master or worker nodes.

Using the Sysdig platform and Red Hat OpenShift, organisations can readily validate their PCI DSS compliance and reduce risk. Internal and external compliance and audit teams can analyze their security posture, quickly visualize patterns and trends, and gain valuable insights into their compliance posture.

Sysdig provides extensive image scanning, including third-party libraries, configuration validation and vulnerability management – as well as runtime security to detect and block attacks, implement zero-day threat protection, incident response, container forensics, and audit with deep visibility into container activity.

Red Hat OpenShift

Sysdig Secure DevOps Platform

With stringent security controls in place, Red Hat and Sysdig help companies to take the next steps in their environment to be PCI DSS compliant, including:

- Red Hat Enterprise Linux security features built into Red Hat OpenShift nodes such as Linux namespaces, SELinux, Cgroups, and secure computing mode (seccomp).
- Strong identity management and role-based access control (RBAC) to control access levels to clusters and projects within a cluster.
- Multi-tenancy security to enable different teams to use a cluster while preventing unauthorized access to each other's environments.
- Accelerate detecting and remediating container & cloud vulnerabilities.
- Streamline troubleshooting and forensics with a combination of detailed syscall data and rich Kubernetes context.
- Reduce your operational resource needs to validate compliance by as much as 50% or more using SaaS.
- Enable DevOps teams to own application security and ship PCI compliant applications faster.