PCI GUIDELINES FOR CLOUD COMPUTING AND CONTAINERS

Those who operate in the enterprise tech space have a responsibility to ensure that new advances in technology comply with overarching standards and regulations like ISO, GDPR, HIPAA, and, of course, PCI. Indeed, any company that collects, holds or processes personal credit card information must adhere to PCI Payment Card Industry Data Security Standards, or PCI DSS. The PCI DSS helps thwart security breaches and identity theft across e-commerce platforms.

However, as it pertains to the use of containers with applications involving credit card data, little guidance had been provided until earlier this year when the PCI Security Standard Council created an updated version of their Cloud Computing Guidelines. The first update in five years, it's an important one given the depth and breadth of utility that containers offer enterprise businesses and its fast-paced adoption.

Indeed, containers provide businesses with an easier, more standardized solution to digital service deployment, enabling them to leverage multiple cloud service platforms while streamlining their deployment process. These operational efficiencies become even more pronounced as enterprises scale their cloud operations.

Keep reading to learn why compliance is important to cloud computing, and how the update to these Cloud Computing Guidelines could impact your enterprise organization.

A Brief Look at the History of Containers and Cloud Computing

Containerization seems to have emerged rapidly over the last three or four years, but it's a concept that had been in the works well before that. It was sometime around the turn of the Millennium that Linux developers started playing with the idea of creating a contained virtual server that could run in an isolated environment with both security and independence.

This project by Jacques Gélinas was called the VServer Project.

As a first-time effort, the project was groundbreaking but had some drawbacks. Ultimately, VServer technology lacked some important features of containerization with too much administrative overhead resulting from the requirement that VServer needed a patched kernel to run.

In 2007, Paul Menage of Google made containerization possible on an existing Linux kernel with minimal overhead. It was this development that served as a catalyst for container innovation that we see today.

For developers and cloud operations personnel alike, today's container platforms solve an important issue: how to ensure software runs the same in different environments.

There are a number of scenarios where software in development may need to run in different environments. For instance:

- Throughout the software development lifecycle, microservices might transfer from a dev's laptop to a test environment, or from Staging to Production.
- A developer may be testing on Debian whereas production runs on Red Hat
- A piece of deployed software may transition from a data center to a virtual server.

You get the idea. There are a number of environments in which software can be developed and used. And depending on the environment glitches and other unanticipated problems can occur.

Containers offer an all-in-one runtime solution where everything needed to run the application properly is bundled into one unit that can pass through different environments.

Types of Containerization

Containerization is a process by which an entire run-time environment can be isolated into a single package that doesn't require its own OS kernel. They are lighter weight, startup more quickly than VMs, and use resources more effectively.

Capitalizing on existing technology, several container platforms exist for users today. These include:

- Docker
- Google Kubernetes
- Amazon AWS
- Cloud Foundry; and
- CoreOS'rkt

Using containers offers a number of benefits that were discussed at length here, and will be listed below. The benefits of developing in a container environment include the following:

- Faster startup
- Light weight, greater density

- Multi-cloud supported
- Offers testing and continuous deployment
- Version control
- Isolation and security
- Portability
- Easy to reproduce

While the implementation of containers in a DevOps environment is often straightforward, remaining compliant is not always as clear-cut.

Why Compliance is Important in Every Environment

When it comes to cloud computing, CIOs face numerous compliance concerns. Generally, these include:

Being Aware of Challenges to IT Workload

It isn't enough for enterprise business leaders to look for typical compliance challenges when selecting a cloud vendor. Once the baseline compliance needs are met, IT departments must look at unique compliance needs and determine how the vendor will be able to add value while remaining compliant. Mapping these requirements to vendor controls can cause challenges in the IT workload.

Making Security Priority One

As an early adopter of new technology, the enterprise must make cloud security a top priority in order to remain compliant. While the cloud itself is not insecure, the way the enterprise uses it often leads to security and compliance violations. In fact, an overwhelming majority of business leaders cite security as their #1 concern with the public cloud. On the plus side, moving to the cloud may help enterprise businesses formalize the process of risk assessment audits for their organization. This trend can help enterprises become more compliant.

Tracking Changes in Standards

In addition to formalizing a risk audit process, organizations must be ready to track changes in standards as they occur such as the PCI updates which will be discussed below.

The Evolution of the PCI Standards

Every entity that accepts credit or debit cards, regardless of their size, must comply with the 250 regulations outlined by the PCI DSS. It's important for companies to understand the significance of abiding by the PCI DSS rules and the consequences of non-compliance.

Initially, the rules were only applied to the credit card companies (i.e.. Visa, MasterCard, Discover, etc.). However, this quickly led to disparities in understanding how the standards should be adhered to. As a result, in 2004, the major credit companies came together to create a unified security standard or the first version of PCI DSS. Shortly after, the PCI Security Standards Council was born, an autonomous body responsible for continuing to build and manage the standards and educate entities (merchants) as well as banks as to their application.

Consequences of PCI Non-Compliance

In general, penalties have ranged from verbal warnings to large fines -- in some cases up to $500,000. Such fines usually go hand-in-hand with increased transaction fees. And in the case of repeat offenders, PCI might revoke their privilege to accept payment cards altogether. As you might imagine, for many businesses, this would be a death sentence.

Compliance for Containers

As mentioned above, PCI has been slow to address how to use containers with applications involving credit card data. As a result, many organizations relied on container management companies who were PCI-compliant. However, as you are well aware, the onus rests on you as the business leader to ensure compliance.

This meant that organizations were left to internally audit their own container systems for compliance without the standardization of a compliance organization behind them.

But just because containers are new doesn't mean they are entirely different than the enterprise systems that have powered development for many years. It stood to reason that the self-contained run-time environment can be audited just like any other cloud development environment that did have established guidelines. Existing compliance standards around security, confidentiality, availability, and integrity were used as a baseline for container compliance guidance.

To clear up any confusion, PCI finally updated their guidelines to include compliance for containers.

PCI Guidelines 3.0 Update

While the updated guidelines cover several issues that have arisen since the 2013 update, section E7 deals specifically with container compliance. Here are the PCI container guidelines your organization needs to be aware of and integrated into your overall risk management approach.

- Proper access points to orchestration framework and containers with special care being taken to protect sensitive information
- Process isolation with best practices listed
- Significant access restrictions to containers and container files
- Implementing a container-specific system-call firewall
- Separation between network and administrative containers with different workloads that meet certain protocols
- Kernel separation where possible
- A defined audit system where access logs can be generated, and other components can be reviewed
- Ensure strong CI/CD protocols with review of pipeline and change controls
- Secure management of repository storage for containers
- Containers that use open-source images should be patched and undergo vulnerability testing according to guidelines
- Whenever supported, read-only containers should be used

The above list provides a condensed look at the most important guidelines. However, we recommend that you download the full text click here. The document outlines various scenarios and

examples of appropriate responses to ensure compliance.

Final Thoughts

Cloud and container security is challenging, if only because of the supercharged velocity of change. Qualified security talent is scarce, and so automation is all the more important to keep enterprise IT propelling the business forward is a secure and compliant manner. For enterprises adopting new technology, the importance of ensuring compliance cannot be overlooked. For most organizations, that means making sure security measures are met, being aware of potential challenges, and of course, staying on top of industry trends in compliance.

Recently, PCI made this last part a little easier by updating their cloud computing standards to take some of the guesswork out for organizations using compliance guidelines that pre-date containers themselves. This should be a gamechanger for organizations who want to pursue a DevOps approach.