CATBIRD®

VIGITRUST
Compliance as a Service

PCI COMPLIANCE & VIRTUAL ASSET MANAGEMENT

Best Practices for Overcoming the Challenges of PCI Scoping in Virtual Environments

Payment Card Industry Data Security Standard (PCI DSS) v3.0 was announced at the PCI Community Meetings in Las Vegas (September 2013), Nice (October 2013), and Kuala Lumpur (November 2013). It was officially published in November 2013[i].

In the highlights published by the PCI Security Standards Council (SSC) in August 2013, the PCI SSC focused on "more robust requirements for penetration testing and validating segmentation". This is clearly aimed at ensuring that PCI scoping has been done correctly and that no assets which may either be used to store, transmit or process credit cardholder data (CHD) have been left out of the applicable Cardholder Data Environment (CDE).

One other notable change is the focus on continuous compliance to "make PCI DSS business as usual" and integrate it in your organization's security strategy rather than as a standalone compliance silo.

Table of Contents

FEBRUARY 2014

Introduction

If your organization has gone the virtualization route, then the PCI DSS v3.0 changes mentioned above will have an impact on how you validate. QSAs will indeed have to spend more time checking that PCI scoping includes all virtual assets that may touch CDE.

So what constitutes best practices in terms of PCI and CDE scoping in Virtual environments? How can entities make sure that they have an update and fully comprehensive virtual-asset inventory? Moving forward, how does Virtual asset management fit into continuous compliance?

This paper addresses PCI scope management, preparing for a PCI assessment, and overcoming the challenges, including continuous compliance considerations and operational impact.

PCI Scope Management

PCI is designed to protect CHD and represents an iterative and mature model which incorporates best practices to securing IT infrastructure. The nature of the structure and enforcement makes PCI a difficult and occasionally onerous process. While most professionals would agree that the spirit and structure of PCI is consistent with solid operational security, the cost and risk around official assessments make scope management a challenge for many organizations.

An important aspect in scope management is the distinction between the CDE and PCI assessment scope. CDE generally includes the actual servers and infrastructure where the cardholder data is present. These would include the web, application, and database servers that send and receive the data. It also includes storage, switches, and other devices across which the data traverses. PCI requires isolation of the CDE from the rest of the network environment.

Many organizations have been dismayed when assessors have requested and required information that includes infrastructure beyond the CDE. PCI scope will tend to include not only the CDE but also adjacent assets to check that no other system linked to the CDE may actually contain or transmit CHD. Authentication servers, such as Active Directory, which can connect to the CDE will therefore also likely be in scope. Administration servers, boot hosts, proxy servers, and other core infrastructure elements may also be called into scope. If an assessor determines that an organization's controls are tied to non-CDE infrastructure, it will tend to be included.

It's rare for an IT organization to fail to grasp the tremendous leverage and efficiency which virtualization can deliver. PCI production workloads have tended to lag the broader adoption. Scope management is certainly a factor in this slower pace of adoption. If being able to discriminate between CDE and non-CDE assets is challenging, and predicting what will be in scope can be almost impossible to predict, virtualization, pardon the pun, tends to cloud the issue further.

Assessment preparation and the use of the proper security and compliance tools can make this challenge far more tractable.

Preparing for the Assessment

To prepare for an audit, organizations need to provide both an inventory and a network diagram. In addition assessors are very receptive to diagrams detailing how CHD flows between different business units, often referred to as Ecosystem Diagrams™[ii]. These documents form the core of the initial information, set the stage for the discussion of scope, and provide an initial view to the auditor about the maturity and rigor of the environment. It is at this stage that your organization has the opportunity to demonstrate to assessors that you are in control of CDE and CHD – even if your own view differs from that of the assessor, it means you take PCI DSS seriously. Some organizations estimate that audit preparation and compliance activities reduce their productivity by more than 30%. A significant challenge for these organizations is the manual exercise required to gather and document the inventory and network flow, and substantiate its accuracy.

In order to avoid unexpected findings, organizations work to ensure their ability to demonstrate that proper firewalls are deployed and that firewall rules are in place as well as that changes in the environment are adequately reflected in the on-going management of the firewall access control lists (ACL). In addition to appropriate firewalling, in-scope assets need to be able to have appropriate scanning, anti-virus, and logging. The network must be subject to intrusion detection and penetration testing.

The virtual environment makes this task significantly more challenging. The vast majority of software development around the virtual environment has been developed with the goals of efficiency and harnessing the value proposition of virtualization through increasing the speed of deployment, improving asset utilization, and abstracting the production applications from the underlying physical hardware. The prospect of deploying virtual infrastructure with existing security and compliance tools that have limited visibility and control, has forced many organizations to defer on the efficiency of virtualization due to the near impossibility of preparing and managing security audits in addition to the perceived risk.

Overcoming the Challenge

Beyond the hype, cloud and virtualization technologies are software tools. It stands to reason that software infrastructure needs to take advantage of software solutions. Trying to use an approach grounded in the physical isolation of servers and networks that pre-date virtualization demonstrably fails to track and secure virtual assets. There are alternatives.

There are, in fact, an increasing number of options for organizations which offer software tools that address the challenges of scope management and reporting while permitting organizations to leverage virtualization and deliver better service with increased efficiency and reliability.

It's important to choose a tool that is compliance-centric. In the new, software-defined data center, it's not necessary to have separate tools to administer operations, compliance, and security. By choosing a tool that addresses compliance as well as operations and security, organizations can reduce the administrative burden and risk, allowing an increased focus on business value and agility. Put differently, the software defined data center is different and traditional software silos should not be assumed.

The appropriate software should be able to demonstrate the ability to capture inventory information and track assets through their lifecycle. Additionally, it needs to tie the virtual asset to network traffic. If the software selected can also administer and demonstrate the application of firewall rules, IDS, and scans, significant leverage is provided. In the best case, compliance enforcement should be a feature. This may be expressed by the isolation of an asset which falls outside of compliance, up to and including network isolation or powering the virtual machine off.

This approach can take the periodic exercise of compliance and transform it into continuous compliance enforcement while increasing the efficiency and transparency of previously "cloudy" virtual assets.

PCI Continuous Compliance Considerations for Virtualized Environments

If you have ever heard that PCI compliance is a journey not a destination, you will understand immediately that PCI requires a lot of ongoing work. PCI is a mix of recurring daily, weekly, monthly, and yearly tasks categorized in policies and procedures, technical solutions, and user education (technical training as well as generic awareness).

The Verizon Data Breach Investigation Report[iii] indicates that some of the biggest breaches in the last year were linked to poor compliance management, whereby a compliant environment at the time of an official assessment changed and evolved quickly for business requirements, but security and compliance did not keep up well enough to protect the environment. The result: attack surfaces increased, scope widened, and entities fell out of compliance very easily.

The above structure obviously applies to the virtualized environment. As additional virtualized machines are being provisioned within the CDE, the overall attack surface increases. It is vital for organizations to keep abreast of new security issues affecting the virtual environment, be they weaknesses in the virtual infrastructure, hypervisor vulnerabilities, cross-virtualization leakage, or others. However, in order to be able to monitor for suspicious activity, organizations need to fully control their virtual environment which clearly requires asset inventory, behaviour monitoring and regular security checks.

QSAs will want to see documents in place demonstrating that continuous compliance controls are active and fully applied to the whole CDE, including its virtual part as well as any other network connected to it.

Operational Impact on PCI Effort

In February 2013, PCI SSC published Cloud Computing Guidelines[iv] which built on the recommendations of the PCI DSS Virtualization Guidelines. Moreover, PCI SSC must be praised for creating Special Interest Groups for Virtualization and Cloud[v].

These documents are a good starting point to help understand some of the more complex operational aspects of PCI compliance in a virtualized private environment or in another type of cloud infrastructure. They are, however, somewhat geared towards greenfield sites where virtualization has not been rolled out fully. Generally speaking, it is hard to retrofit the advice within the documents into existing virtualized infrastructures unless one is ready to make structural changes to the virtual part of the CDE.

This is where tools that allow your organization to map out virtual assets, their settings, and how they are controlled from a security and continuous compliance perspective adds a lot of value. Imagine being able to discover your virtual assets within your CDE in just a few clicks. The opportunity to reduce the operational impact of PCI compliance is huge and should definitely be embraced.

It is therefore advisable for organizations to:

- Educate themselves on PCI requirements for continuous compliance
- Understand the dangers associated with evolving virtualization technology
- Choose virtualization vendors who can provide continuous security and usage monitoring of inventoried virtual assets

The Way Forward
Do’s & Don’ts of Virtualization Security

Virtualization technology has evolved a lot in the last two years and so have threats to virtual environments. Here are a few quick do’s and don’ts to help your PCI team address PCI virtualization challenges.

Do

- Map out your ecosystem including all virtual assets to demonstrate to QSAs that you know where CHD is and that you are able to ring-fence your CDE
- Automate as much of the virtual asset discovery and management process as possible using available technology
- Keep abreast of threats to virtual environments and educate your staff on what’s happening within the industry
- If you use Cloud providers, read the contract and ensure that you can perform your own assessment on the structure they tell you will ”securely” host CHD – ensure your data is isolated from other clients’ data
- Circle with security experts and QSAs if you have any doubt about whether cloud or any other virtual assets increase your PCI scope and attack surface

Don’t

- Assume that your virtual assets are not used to store, transmit, or process CHD – they just might and, if so, they are within the CDE
- Assume that QSAs won’t request an inventory of all in-scope virtual assets – they will because they have to!
- Assume that CHD within a protected virtual CDE is secure from internal fraud or insider threat to cross-virtualization leakage – be aware that threats apply
- Look after the security of virtual assets once a year as you complete SAQs or await your official onsite assessment – remember, continuous compliance is key!
- Become complaisant with virtual security!

Final Remarks

Scoping for PCI is one of the fundamental layers of a successful compliance strategy. It needs to include all areas of the CDE and cover any in-scope component whether physical or logical, including any virtual assets or cloud-based assets.

Managing this environment can indeed be costly and add an operational burden to organizations if they don’t use available technologies to inventory, secure, and manage such assets within their CDE.

The good news is that entities can easily benefit from available and proven best practice methodologies on how to map out CDE through Ecosystem Diagrams as well as innovative technical solutions addressing security threats and compliance management for virtual assets.

This white paper has been produced by Catbird and VigiTrust who together offer a compelling value add suite of services and solutions allowing entities to address compliance challenges for PCI environments.

[i] *As with every PCI DSS lifecycle, there will be a period during which entities can choose to finalize their compliance with the old version but from January 2015, v3.0 is the one to comply with.*

[ii] *Ecostystem Diagrams is a VigiTrust Trademark audit process & tool*

[iii] *http://www.verizonenterprise.com/DBIR/2013/*

[iv] *https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf*

[v] *https://www.pcisecuritystandards.org/get_involved/special_interest_groups.php*

About the Authors

Randal Asay, Chief Technology Officer, Catbird

Randal Asay is the CTO of Catbird. Bringing over 15 years of experience in network security, architecture, implementation, and security best practices in commercial and government environments, he joined Catbird in 2013. Prior to Catbird, he served as Director of Engineering at Walmart Stores Inc., developing industry-leading code analysis practices to support security and compliance initiatives as well as addressing enhancements to perimeter and network security and overall policy enforcement. He lead the E-commerce Infrastructure teams through extensive growth, delivering capacity management and technology refresh methods impacting network design, storage capacity and database tuning. Prior to Walmart, he applied his security expertise to the Information Assurance division of the United States Air Force. Randal holds Masters degrees in Information Technology Management and Business Administration from Webster University as well as a Bachelor of Science degree from Weber State University.

Mathieu Gorge, CEO & Founder, VigiTrust

Mathieu Gorge is the CEO and founder of VigiTrust. He has been in the security industry for the past 10 years. In 2003, Mathieu identified a gap in the market to provide pro-active consultancy services around key legal aspects of corporate security such as compliance with international data protection legislation as well as industry security frameworks. He started VigiTrust which focuses on enabling organizations to achieve and maintain compliance with PCI DSS, PA-DSS, Cloud Security, HIPAA and ISO 27001. He is a regular speaker at international security conferences (RSA, ENISA, ISACA) and a well-respected figure in the security industry in EMEA and North America. Mathieu is also the creator of the 5 Pillars of Security Frameworks™ which is a simple, cost-effective, efficient security & compliance framework for SMEs.

Whitepaper Sponsors

Catbird

Catbird brings the power, agility and automation of the cloud to security policy and compliance, with a solution that automates, instruments and enforces policy while providing proof of continuous compliance. Customers rely on Catbird for managing cloud and virtualized infrastructure subject to compliance requirements including HIPAA, PCI-DSS, FISMA, DIACAP, and SOX.

VigiTrust

VigiTrust helps its international blue chip clients achieve and maintain compliance with legal and industry data security & governance mandates. Thanks to its cloud based eLearning programs, security compliance portals and GRC services, clients in the financial services, healthcare, higher education, retail & government pro-actively ensure they protect credit card data, personal data/PII as well as PHI. VigiTrust's cloud solutions and services are based on the 5 Pillars of Security Framework™.