WHITE PAPER

PCI and Virtualization

Key Requirements for Securing Cardholder Data in Dynamic, Virtualized Environments

Executive Summary

Virtualization has brought enormous benefits to hundreds of thousands of businesses across the globe. However, the move to these systems has also posed significant implications for security teams—especially for those in organizations that must comply with the Payment Card Industry Data Security Standard (PCI DSS). Based on the expert insights of qualified security assessors (QSAs), this paper examines the security and compliance challenges that arise in virtualized environments. Then the paper outlines some key approaches for effectively addressing requirement 3 of the PCI DSS when cardholder data resides on virtual systems.

Introduction: The Profound and Broad Impact of the PCI DSS

First unveiled in 2004, the Payment Card Industry Data Security Standard (PCI DSS) has had a significant and broad impact on businesses across EMEA. In a recent SC Magazine survey that included companies from virtually all major industries, 63% indicated that PCI DSS has had an impact on their organization's risk management or compliance approaches.

There's no doubt that because it established common security best practices, along with a combination of audit deadlines, penalties for non-compliance, and independent auditors, the PCI Security Standards Council provided ample incentive for regulated organizations to comply with this mandate. It also seems clear that by offering comprehensive guidance on security practices, PCI DSS represents a baseline set of standards that is useful for non-PCI-regulated organizations as well.

The Pervasive Use of Virtualization—and its Ramifications

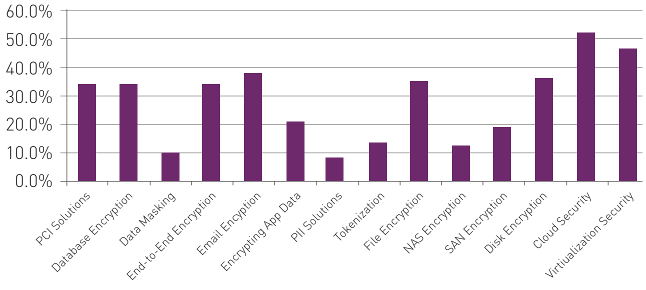
For any organization, security is clearly never done. To the contrary, the stakes and challenges only seem to grow, with security teams forced to contend with more sophisticated and well-funded criminals on one hand, and with a rapidly evolving IT infrastructure on the other hand. In this latter arena, virtualization represents one computing trend that's eclipsing all others, both in terms of rate and scale of adoption, and in terms of the fundamental implications it poses to sustaining compliance with PCI DSS and security policies.

Virtualization technologies, whether from VMware, Microsoft, Citrix, Oracle, Red Hat, or a host of other vendors, have had an incredibly rapid and pervasive impact on the modern IT landscape. Further, it is clear that these technologies will be playing a foundational role in the development and delivery of another paradigm shift in IT: cloud computing.

Today, virtualization and its security implications represent a key challenge for a broad range of companies in EMEA. The SC Magazine survey found that 35% of all organizations, across all industries, store sensitive data in virtual machines today. That number is sure to be higher in organizations that manage and store PCI regulated data, and it is a number virtually guaranteed to grow in the coming months as virtualization technologies and cloud services continue to be more broadly adopted.

The SC Magazine survey reveals that securing data in virtualized environments is top of mind for IT security executives. Virtualization security was a specific area of interest for 45.9% of respondents. Only cloud security, with 52.4%, rated higher.

What is your specific data security interest?



For organizations across EMEA, security in virtualized environments is one of the top areas of interest. Source: SC Magazine and SafeNet Survey

The Security and Compliance Challenges Posed by Virtualization

Virtualization has provided businesses with a range of benefits, enabling IT organizations to get more flexibility, efficiency, and scalability from their infrastructure investments. For the organizations tasked with managing sensitive data, however, these virtualized environments present a host of challenges:

- **Multi-tenancy.** Often, virtualized computing resources are pooled together for multiple clients or departments. Consequently, traditional boundaries and controls start to blur, potentially enabling unauthorized groups and users to access sensitive assets.
- **Administrative access.** In virtualized environments, administrators have great visibility and control over all their virtualized resources, and the assets residing on those resources. The flipside is that it can be difficult for security teams to enforce the separation of duties and granular access controls needed to mitigate the threat of administrators abusing their super-user privileges.
- **Data mobility.** In virtualized environments, resources are constantly in flux, with data and processing regularly migrating across systems. Consequently, these dynamic environments can make it difficult to guard against unauthorized copying of virtual instances.
- **Limited visibility.** With data and processing migrating so rapidly, it can be challenging to understand, let alone track and report on, exactly where sensitive assets reside at any given time. In organizations that handle PCI DSS-regulated data, security teams need to gain the fundamental visibility required to understand where, when, and how sensitive assets in virtual environments are being used.
- **Data destruction.** In virtualized environments, when it comes time to remove a given asset, it grows increasingly difficult to authoritatively ensure that all copies of a virtual instance, and the sensitive assets on that instance, are permanently removed.

New PCI DSS Virtualization Guidelines

In June 2011, the PCI DSS Virtualization Guidelines were published, which provide a number of recommendations and considerations administrators should take into account when managing cardholder data in virtualized environments. These guidelines include considerations as they pertain to each of the 12 rules in the PCI DSS.

The following sections will focus on a specific rule within the PCI DSS standard, requirement 3, which is focused on protecting stored cardholder data. Given the highly dynamic nature of virtualized environments, and the risks they present to stored cardholder data, addressing this requirement will present some pressing challenges, as well as significant potential benefits, for many organizations.

> "In the early days of PCI DSS, it was very common for companies to use a compensating control to reach compliance with requirement 3.4," explained Alexandre Pinto, Senior Technical Manager and QSA with Cipher Security. "This was because the challenges and outcomes of database encryption were very poorly understood. Now, however, the technology and implementation techniques have evolved dramatically, and companies are shifting their compliance strategy to include encryption from the start of the programme."

Addressing Requirement 3 of the PCI DSS in Virtualized Environments

Since the PCI DSS rules were first published, requirement 3 has been a particularly onerous one for many organizations to comply with. A lot of this has had to do with the fact that, before they could effectively deploy encryption or the other safeguards required to make stored cardholder data unreadable to unauthorized users, security teams encountered a number of issues that needed to be addressed:

- First and foremost, this entailed identifying which systems stored PCI regulated data, which isn't a trivial endeavor for many organizations.
- Second, once that was done, many organizations realized they needed to reduce the number of systems housing PCI DSS-regulated data, so they could reduce the upfront and ongoing cost and effort of encryption.
- Finally, once these barriers were overcome, the deployment of encryption was simply too complex for many organizations. This has been and continues to be true because encryption is integrally attached to the data and is persistent across the complex lifecycle of that data. Further, the associated key management requirements were also too labor intensive for many organizations to adhere to.

Consequently, the PCI Security Standards Council, with its second release of the PCI DSS, version 1.1, added the provision that enabled organizations to apply compensating controls. By employing such measures as physical isolation, tighter management controls, and IPS level functionality, organizations were able to avoid having to employ encryption. However, those organizations that employed these types of compensating controls, and who are now looking to migrate PCI regulated data into virtualized environments, now confront a significant obstacle: Quite simply, the notion of physical isolation goes away in a virtualized environment. Consequently, when organizations undergo their mandatory annual reviews, control requirements may not be met, and encryption may be unavoidable in order to address this specific requirement.

"Compensating controls can always be applied if something is not technically or cost feasible within a given organization," said Tim Holman, QSA, Blackfoot. "However, the compensating controls that are acceptable in virtualized environments may have to vary substantially from those employed in the past."

To meet PCI DSS requirements and effectively secure sensitive data in virtualized environments, many organizations are looking to move away from their reliance on compensating controls and beginning to leverage proactive, robust security controls enabled by encryption.

> "Compensating controls can always be applied if something is not technically or cost feasible within a given organization," said Tim Holman, QSA, Blackfoot. "However, the compensating controls that are acceptable in virtualized environments may have to vary substantially from those employed in the past."

"In the early days of PCI DSS, it was very common for companies to use a compensating control to reach compliance with requirement 3.4," explained Alexandre Pinto, Senior Technical Manager and QSA with Cipher Security. "This was because the challenges and outcomes of database encryption were very poorly understood. Now, however, the technology and implementation techniques have evolved dramatically, and companies are shifting their compliance strategy to include encryption from the start of the programme."

Following are some key requirements for addressing requirement 3.4 in virtualized environments.

The Need for Multi-level Encryption

To realize optimal levels of security, organizations need to begin to leverage multi-level enryption in virtual environments. This is a highly effective way to address PCI DSS section 3.4. This includes employing encryption in the following areas:

- **Instance encryption.** By encrypting virtualized instances, organizations can guard against a host of vulnerabilities. For example, this significantly reduces the number of ways users can get sensitive data off physical images. It also enables organizations to enforce the separation of duties required.
- **Data level encryption.** Through database and application encryption solutions, organizations can more granularly apply security policies to specific subsets of data, for example at the column level in a database. This represents a way to have data secured as it progresses through workflows, and represents an ideal complement to instance encryption.

> In many organizations, keys have been stored insecurely, for example in software on general purpose servers, and rules around key rotation haven't been consistently complied with. These challenges will only get exacerbated in dynamic virtualized environments.

Key Management Requirements

Traditionally, key management has represented a significant challenge for organizations that deploy encryption. PCI requirements around key storage, rotation, deletion, and other areas can pose a significant amount of administrative overhead and cost. In many organizations, keys have been stored insecurely, for example in software on general purpose servers, and rules around key rotation haven't been consistently complied with. These challenges will only get exacerbated in dynamic virtualized environments.

To meet their efficiency and security demands, organizations need to leverage hardware security modules (HSMs) that store cryptographic keys in secure, purpose-built devices, and that encrypt the keys themselves. By storing keys in HSMs, organizations can ensure the highest level of security is realized. Further, advanced HSMs and encryption appliances offer capabilities that streamline such activities as key rotation and deletion. From a PCI DSS perspective, this means that most of the items and testing procedures described in requirements 3.5 and 3.6 can be addressed with relative ease.

Finally, organizations should look to work with platforms that support such standards as NIST 800-57 and OASIS KMIP. These standards offer flexibility and broad interoperability, enabling organizations to begin to centralize the management of cryptographic keys across disparate encryption platforms, which yields benefits in both security and administrative efficiency.

Deployment Flexibility

To efficiently manage encryption in virtualized environments, organizations need capabilities that ensure optimal deployment flexibility, so they can employ encryption in the manner that's best suited to their technological, security, and business imperatives. For example, look for solutions that can be deployed on virtualized platforms in the enterprise data center and that support the encryption of data in the cloud provider's virtualized infrastructure, while enabling organizations to retain control over cryptographic keys and policies. In addition, look for solutions that offer the dynamic provisioning required to ensure encryption mechanisms are automatically adapted to the changes that occur constantly in virtualized platforms.

Conclusion

For organizations that manage data regulated by PCI DSS, virtualization can present a host of questions and challenges with respect to security. Encryption offers a strong means for safeguarding sensitive data in virtualized environments, and so can be a key enabler for organizations looking to leverage the business benefits of virtualization, while ensuring continuous PCI DSS compliance.

About the SC Magazine and SafeNet Survey

This white paper draws from the experiences of veteran PCI QSAs, as well as from the findings of a recent SC Magazine survey, which was taken in conjunction with SafeNet. The survey gathered the responses of 170 IT security managers in EMEA. Respondents represented a broad range of industries, including retail, utilities, software, banking, telecommunications, government, and more. The survey was conducted in June, 2011.

About Gemalto's SafeNet Identity and Data Protection Solutions

Through its acquisition of SafeNet, Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto's newly expanded portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com
Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

gemalto
security to be free