VISTA INFOSEC®

TRUSTED ADVISORS, ASSURED COMPLIANCE™

PCI DSS & Virtualization

Top Risks and Mitigation Strategies you should be knowing

W: www.vistainfosec.com | E:info@vistainfosec.com

US Tel: +1-415-513-5261 | SG Tel: +65-3129-0397 |
IN Tel: +91 73045 57744

An ISO27001 Certified Company, CERT-IN Empanelled, PCI QSA, PCI QPA

USA. SINGAPORE. INDIA. UK. MIDDLE EAST. CANADA.

Introduction

Virtualization is a technology that has greatly benefited businesses around the globe. The technology has a significant impact on the modern IT landscape and today plays a key role in the development and delivery of cloud computing solutions. However, the adoption of this advanced technology has major security implications on businesses today. The adoption of Virtualization has opened doors to a broad range of challenges for businesses in the industry. Especially, for organizations that are PCI regulated and required to comply with PCI DSS Standards, the challenges in this area only seem to grow.

For most businesses, security is clearly the top priority. More so, for PCI-regulated businesses, their security teams are expected to tackle sophisticated cyber-attacks and deal with the rapidly evolving IT infrastructure. So, clearly, with the increasing adoption of virtualization the fundamental implications of security and sustaining compliance with PCI DSS is a major concern. Covering top risks of virtualization and mitigation strategies, the article explains various PCI Compliance challenges and ways to tackle them.

PCI DSS & Virtualization

Virtualization is the most trending and highly discussed topic in the area of digital payments. The technology offers many benefits in terms of reliability, cost-efficiency, management, and scalability. However, these benefits come along with their share of challenges. Virtualized environments pose a huge security challenge for businesses. Addressing this issue the Payment Card Industry Security Standards Council released PCI Data Security Standard Guidelines for Virtualization of System Components. With this, adapting virtualization for the Cardholder Data Environment (CDE) without appropriate evaluation and implementation of relevant measures may result in non-compliance.

The PCI DSS Virtualization guidelines are designed to help merchants understand and mitigate the security risks in a virtual environment. With an increasing number of businesses adopting virtualization, it is essential that such system components comply with PCI DSS. The PCI DSS Virtualization Guideline focuses on the different classes of virtualization, and also suggests how virtual environment should be deployed to comply with PCI DSS. A cardholder data environment that relies on virtualization can be effectively secured by implementing operational and process-level security controls. That said, businesses must implement necessary information security controls during the planning, deployment, and maintenance phase to ensure compliance.

The PCI DSS Virtualization Guidelines focuses on four principles for virtualization to meet PCI Standards:

- **If virtualization technologies are used in a cardholder data envi ronment, PCI DSS requirements must be applied.**
- **Virtualization technologies introduce new risks that may not be relevant to other technologies.**
- **Businesses must perform thorough due diligence to identify and document their virtualized implementations, including all interactions with payment transaction processes.**
- **Depending upon how virtualization is used and implemented, specific controls and procedures will vary for each environment.**

Organizations should consult experts before adopting the technology for their digital payment environment. Understanding the implications and risk involved is critical for achieving compliance. That said, given below are some of the security and compliance challenges of implementing Virtualization.

Security and Compliance Challenges of Virtualized Environment

Virtualization offers a range of benefits to businesses, enabling a great level of flexibility, efficiency, and scalability in their IT infrastructure. However, for organizations that are required to manage and secure sensitive data, virtualized environments pose a host of challenges as mentioned below.

1. Vulnerabilities in the Physical Environment Apply in a Virtual Environment

Physical threats and vulnerabilities also apply to virtual implementations. Similar to the attacks and vulnerabilities that exist in physical infrastructure, virtual systems and networks are also subject to the same vulnerabilities. So, for instance, applications that have configuration flaws or vulnerabilities will also have those in the virtual implementation when installed. Another good example of this would be a poorly configured virtual firewall that can expose systems to a range of internet-based attacks which is similar to the possible threats resulting due to the misconfiguration on a physical firewall. So, the even most securely configured virtual systems and networks will still need implementation of physical security controls for the protection of hardware. For these reasons, hardware systems cannot be completely off guard when it comes to securing systems and infrastructure.

2. Hypervisor creates a new attack surface

The hypervisor also known as Virtual Machine Monitor provides a single point of access into the virtual environment. So, misconfiguration of the hypervisor can result in security failure of all virtual machines hosted on it. So, no matter how secure the individual virtual machines or components may be configured, a compromised hypervisor can expose systems to risk and also unauthorized access to the sensitive virtual system. Further, the hypervisor may also create a new attack surface and open doors to direct attacks.

Any vulnerabilities in hypervisor isolation technology, access controls, security hardening, and patching can result in attackers exploiting and gaining access to VMs. So, unless appropriately configured and access is restricted to least privilege, even a secure hypervisor can potentially be exploited.

3. Increased Complexity of Virtualized Systems and Networks

Virtualization can encompass both systems and networks which may involve the transmission of data through the hypervisor, or even over virtual network connections or through virtual network security like virtual firewalls. While such configurations provide operational benefits, but it also increases the complexity of system/network functioning. That said, it will accordingly require additional security controls and complex policy management to ensure appropriate implementation of security at each level. Increased complexity and added potential vulnerabilities in virtual operating systems and applications, may result in misconfiguration or creating new threat surface unforeseen by the system designers. Such vulnerabilities could result in significant compromise across the entire virtual and physical environment as well.

4. More Than One Function per Physical System

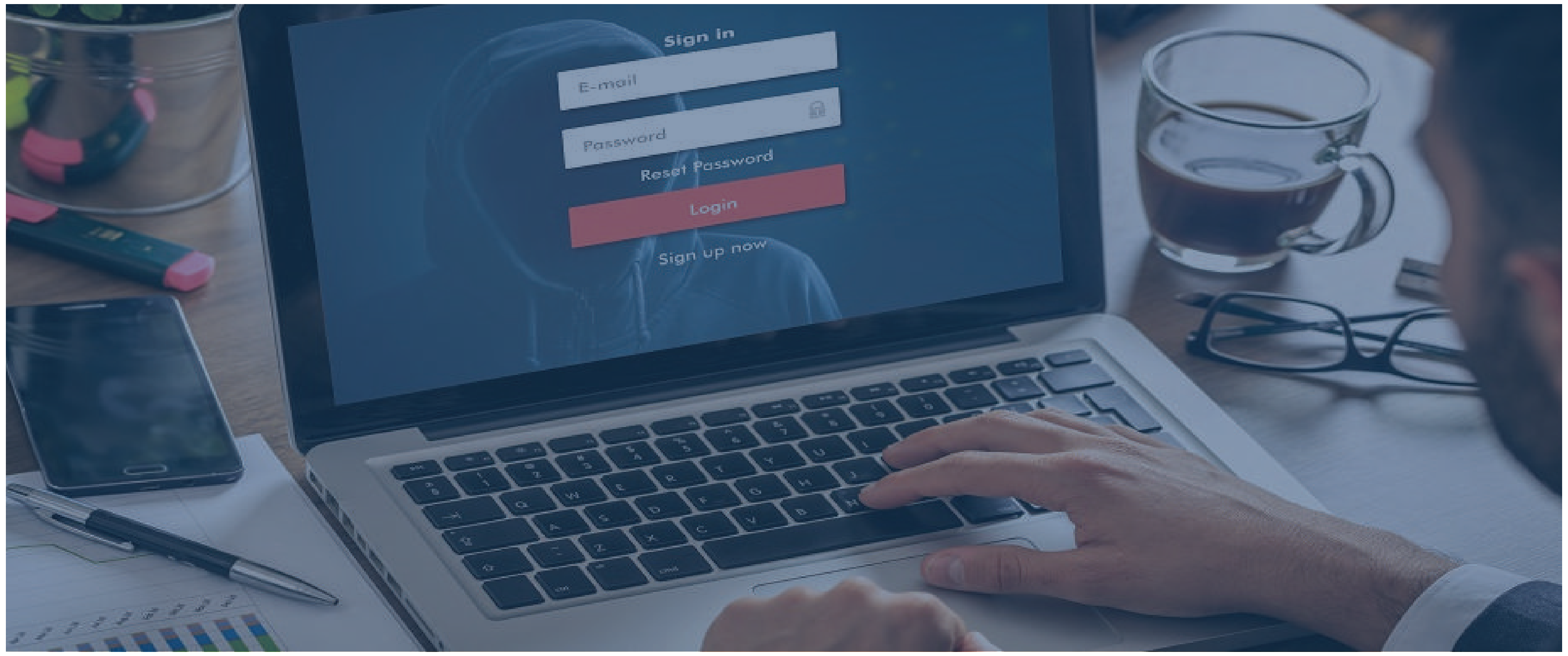
In the virtual environment compromise in even one virtual system function could result in compromise of other functions on the same physical system. Compromised Virtual Machines may use virtualization-layer communication mechanisms to launch attacks on other Virtual Machines on the same host or even the hypervisor. So, these multiple functions hosted on one system increase the possible scope of compromise should an attacker gain physical access to the host system. While the Virtualization technology may mitigate the risk by segregation of different functions, yet one must consider the risk associated with locating multiple functions or components on a single physical system.

5. Mixing VMs of Different Trust Levels

There is always a huge risk of hosting multiple Virtual Machines with different levels of security on the same host. This needs careful evaluation because a Virtual Machine with a lower level of security controls can also impact the security of Virtual Machines with higher security controls. The lower level security control can be easily compromised resulting in opening doors to the higher-risk and exposure to even sensitive Virtual Machines on the same system. So technically hosting Virtual Machines of different security levels on the same hypervisor or host reduces the overall security for all components. With increased risks and configuration challenges, the security and risk level associated with each Virtual Machine function should be considered when designing the virtualized system. Further systems that store cardholder data require a higher security level than the ones having non-sensitive data stored.

6. Lack of Separation of Duties-

In a virtualized environment having access to the hypervisor would mean gaining access to a broad range of systems, networks, and key infrastructure components. This may include access to switches, firewalls, payment applications, log-aggregation servers, databases, etc. Such increased access to multiple virtual devices and functions from a single logical location or a user can result in a security collapse. This is why defining



separate roles/duties is crucial in a virtual environment. But defining roles and maintaining separate authority for access can be very challenging. For instance, having a separate role defined for network administrator and server administrator and having different access policies across the distributed virtualized environment can be very difficult. Here the risk of failing to appropriately define roles and access policies can result in a significant security compromise.

7. Dormant Virtual Machines

Virtualized platforms often house dormant Virtual Machines that may no longer be in use. These dormant machines could however still have several sensitive data such as authentication credentials, encryption keys, or critical configuration information stored in them. Since the machines are not in use they may often be overlooked and inadvertently left out of scope during the security procedures. Sensitive data captured in its dormant state results in unintentional storage and only gets discovered in an event of a data breach. Further, Inactive machines get neglected and likely not be updated with the latest security patches, resulting in the system being exposed to known vulnerabilities and organizations unaware of the same. Such machines are also most likely to have not been included in the updated access policies and may also be excluded from security and monitoring procedures. Looking at this, it is clear that inactive Virtual Machines create a viable security threat. For these reasons it should be identified and tracked so appropriate security controls can be applied.

8. Virtual Machine Images and Snapshots

Virtual Machine images and snapshots quickly deploy or restore virtual systems across multiple hosts within a short period. However, these VM images and snapshots may capture sensitive data present on the system at the time the image was taken, including contents of active memory. This could result in the inadvertent capture, storage, or even deployment of sensitive information throughout the environment. Moreover, if such images are not appropriately secured can result in modification, unauthorized access, and insertion of vulnerabilities or malicious code into the image. This could then further lead to deployment of vulnerabilities throughout the environment leading to rapid compromise of multiple hosts.

9. Immaturity of Monitoring Solutions

While virtualization offers benefits in terms of operational efficiency and management yet it falls short of technology and solutions for monitoring and logging virtual environment. The tools to monitor the virtual networks, virtual firewalls, virtual compliance systems, etc. are not as mature as their physical counterparts. They do not provide the same level of insight or monitoring within intra-host communications or traffic flowing between Virtual Machines on a virtual network. Specialized tools for monitoring and logging virtual environments are required to capture the level of detail from multiple systems and network components, including hypervisors, management interfaces, virtual machines, host systems, and virtual appliances.

10. Information Leakage between Virtual Network Segments

The potential risks of information leakage between logical network segments should be understood when considering network virtualization. Information leakage at the data plane results in sensitive data existing outside of known locations, circumventing the data protection controls that would otherwise apply. Information leakage at the control plane or management plane can be exploited to enable information leakage at the data plane or to influence network routes and forwarding behavior to bypass network-based security controls. Ideally, virtualization capabilities at all three planes of operation in the network infrastructure should provide controls and features to secure the virtualized infrastructure at a level equivalent to individual physical devices.

11. Information Leakage between Virtual Components

Information leakage between virtual networks can occur when there are multiple access granted for components on the same host. One compromised component can result in an attacker gaining access to other components in the same host. This can result in gaining access to sensitive information from multiple components and potentially leading to further compromise. Even a misconfigured hypervisor can lead to information leakage between hosted virtual components and networks. It is therefore essential that all physical resources such as memory, CPU, network, are isolated to prevent information leakage between Virtual Machines and other components or networks on the same host.

With this, the PCI Council has provided recommendations and standards for best practices to implement for the virtual environment to ensure PCI DSS Compliance and for risk mitigation. Given below are some of the recommendations outlined in the official guide.

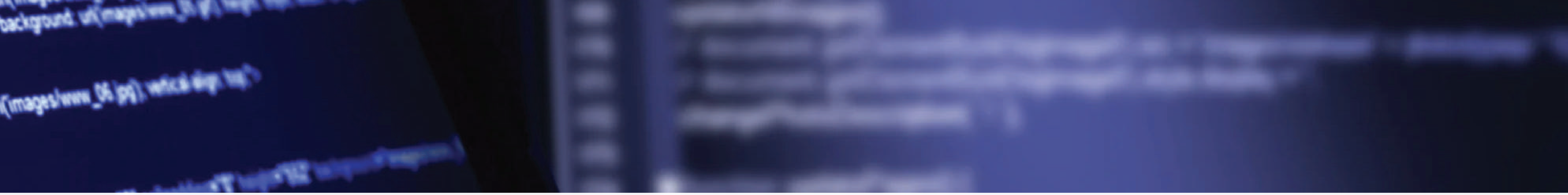
General Recommendations for Risk Mitigation

1. Evaluate risks associated with virtual technologies-

Entities should first evaluate the risks concerning the implementation of virtual technology in their environment. The technology should be only deployed after considering all the pros and cons of virtual solutions and after defining a set of effective systems, applications, data, and environmental controls for the same. The risk evaluation and management should be accurately documented as part of this risk assessment process to ensure that all risk areas are identified and appropriately mitigated. Risk Assessment should be an ongoing annual process for Virtualized environments and system components.

2. Understand the Impact of Virtualization to scope of the CDE

Virtualization makes systems and network configurations complicated. Consolidating the environment into one or more physical hardware platforms makes it difficult to determine the boundaries or scope of the Cardholder Data Environment. For these reasons, the scope of PCI DSS across virtual components must be thoroughly evaluated, verified, and documented. The environment should be evaluated using the guidance provided in the Scope of Assessment for Compliance with PCI DSS Requirements. Designing virtualized components need careful attention and consideration, taking into account even components out of scope to meet the PCI DSS security requirements. This will provide a secure baseline for the entire virtual environment and also reduce the overall complexity and risk associated with managing multiple security profiles. It also lowers the additional effort required to maintain and validate compliance of the in-scope components. So, it is technically recommended that any part or components on a single hypervisor should be considered in-scope to ensure tight security measures for the environment.



3. Restrict Physical Access

Hosting multiple components on one physical system could greatly increase the possibility of unauthorized access to that host system. Therefore physical access controls are essential in virtualized environments to strengthen the security measures and mitigate the associated risks. Entities must consider the potential risk and impact of an unauthorized or malicious individual gaining simultaneous access to all virtual machines, networks, security devices, applications, and hypervisors on a single host. It is also important to ensure all the unused physical interfaces are disabled, and physical or console-level access is restricted and monitored.

4. Implement Defence in Depth

Implementing defense-in-depth for a virtualized environment is crucial. Appropriate security controls should be identified and implemented in a virtualized environment that provides the same level and depth of security as in a physical environment. Entities must consider implementing security controls to each technical layer, including physical device, hypervisor, host platform, guest operating systems, VMs, perimeter network, intra-host network, application, and data layers. Further, physical controls, documented policies and procedures, and training of personnel should also be a part of a defense-in-depth approach to secure the virtual environment. Adopting a defense-in-depth approach that encompasses preventive, detective, and responsive controls is the best practice for securing data and other virtual systems and networks of an organization.

5. Isolate Security Functions

The security features for the virtual machine should be implemented the same way as for the physical environment. In fact, it is recommended that the security requirement to be enforced for the virtualized system should be stringent, especially in a way that it complicates the efforts required by an attacker to compromise multiple Cardholder Data Environment system components. There should be multiple layers of security with the level of isolation between security functions in a way that they can be considered as being installed on separate machines. For instance security controls, processes controlling network segmentation, and the log aggregation function that would detect tampering of network segmentation controls should not be combined and should implement each security function in isolation. This strengthens the defense against unknown threats and makes hacking complicated for the attacker.

6. Enforce Least Privilege and Separation of Duties

Entities should enforce limited access controls for administrative access to the hypervisor. This should be implemented depending on the level of risk exposure evaluated in the environment. Entities should consider implementing two-factor authentication or establish dual or split-control of administrative passwords between multiple administrators. Further, access controls for both local and remote access to the hypervisor and management system should be periodically assessed. For every virtual component appropriate role-based access controls (RBAC) and separation of duties must be established to prevent unauthorized access to resources. Administrative privileges should also be appropriately segregated or it may result in undetected tampering and data loss. As a best practice, administrative access should be restricted based on specific virtual machine functions, virtual networks, hypervisor, hardware, application, and data storage.

7. Evaluate Hypervisor Technologies

Testing the security of the hypervisor before deployment is highly recommended. There should also be appropriate patch management and other security controls in place to respond to threats and exploits. Entities must identify and implement technologies that facilitate strong security practices as not all hypervisors or virtual machine management have the functionality to support appropriate security controls.

8. Harden the Hypervisor

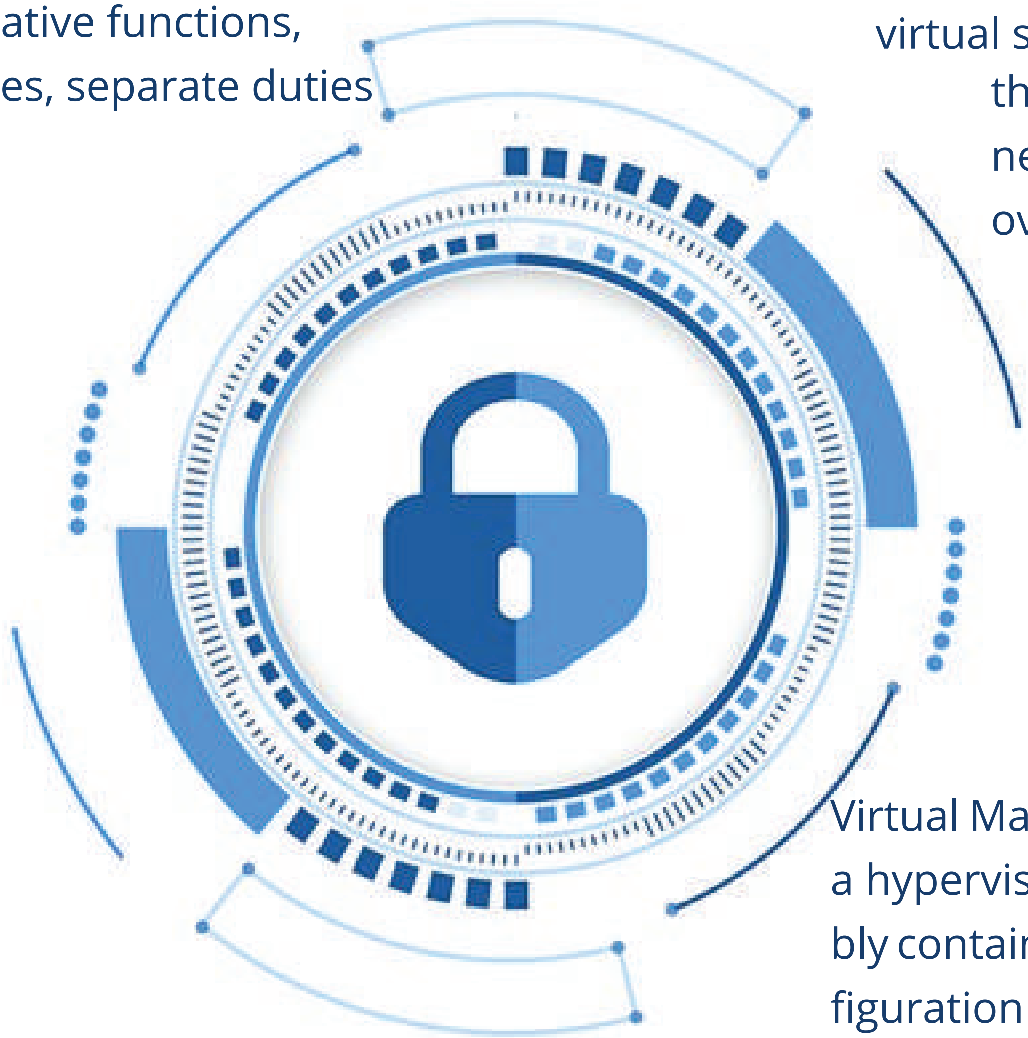
Hypervisor platforms should be deployed in a secure manner adopting the industry-d best practices and security guidelines. Careful management of virtual system configurations, patching, and change-control processes are essential to ensure that all hypervisor changes are monitored, authorized, fully tested, and carefully controlled. Due to the potential severity of a hypervisor compromise, patches, and other mitigating

controls should be deployed as soon as possible whenever new security vulnerabilities are discovered and include immediate testing for the vulnerability to confirm the risk has been addressed. Because the hypervisor represents a single point of failure, an unauthorized or malicious modification could threaten the integrity of all hosted systems in the environment. Other additional controls recommended for the hypervisor and significant management tools include implementing restricted administrative functions, multi-factor authentication for all administrative functions, separate administrative functions, monitor audit logs to identify suspicious activities, separate duties for administrative functions, and verify security control solution support virtualization to minimize the risk of compromise to the hypervisor.

9. Harden Virtual Machines & Other Components

Every virtual machine must be installed and configured securely in accordance with the industry best practices and security guidelines. The recommendations provided for hardening the hypervisor are also applicable to all virtual machines and components. Further, every security control implementations should be evaluated individually to confirm.

- Removal of unnecessary interfaces, ports, devices, and services,
- Ensure secure configuration of all virtual network interfaces and storage areas.
- Limit the usage on virtual machines, and ensure hardening of operating systems and applications in a virtual machine.
- Send logs to separate, secured storage as close to real-time
- Validate the integrity of the cryptographic key-management operations;
- Harden individual virtual hardware and containers;
- Other security controls as applicable.



10. Define Appropriate Use of Management Tools

Management tools allow administrators to perform system back-up, restore, remote connectivity, migration, and configuration changes to virtual systems. Since Management tools directly impact the security and functioning of the in-scope components they should also be considered in scope. Moreover, entities should enforce limited access to management tools based on the job requirement. Segregation of roles and responsibilities is highly recommended for management tool functions, and the use of management tools should be regularly monitored and logged for enhanced security.

11. Recognize the Dynamic Nature of Virtual Machines

Virtual Machines are data that can reside in an active state on a hypervisor or in a dormant state. Dormant VMs may possibly contain sensitive information and other virtual device configuration details. So implementing measures for access to dormant VMs should therefore be restricted, monitored, and carefully controlled. Inactive VMs should be secured equally with the same level of sensitivity and have the same safeguards as any other cardholder data store. Further, entities should evaluate migration paths of inactive VMs, take backups of VMs (active VMs, and inactive VMs) and securely delete the data when no longer needed. Implementing an effective change-management, monitoring, and alerting processes is essential

to ensure only authorized VM's are added to and removed from the environment, and all related activities are recorded and monitored.

12. Evaluate Virtualized Network Security Features

Effective security measures at the data plane, control plane, and management plane should be implemented for any deployment of virtualized network infrastructure. This minimizes the possibility of direct and indirect vulnerability impact on all three operational planes and compromise of the virtual network devices. It is important to ensure that the underlying physical components are adequately isolated and secured leaving no scope or path between virtual network devices for vulnerabilities to percolate. Entities must maintain security isolation between virtualized network devices in a way that virtual systems are treated as separate hardware. Every virtualized device should have independent access-controlled configurations. Further, the audit trails for virtual infrastructures should be detailed in a way that facilitates the identification of access and activities performed on every virtual component. Not just that, the access controls implemented should be the least privilege for each device and across the entire platform.

13. Clearly define all Hosted Virtual Services

In cases where entities use shared hosting where the service providers virtualize their offerings, provisioning separate workloads to customers rather than provisioning separate physical systems, the entities should ensure there is an enforcement of administrative, process, and technical segmentation to isolate every hosted entity's environment. This isolation should include the implementation of all PCI DSS controls, including but not limited to segmented authentication, network and access controls, encryption, and logging. It is also critical to ensure that all responsibilities for maintaining controls that could affect the security or integrity of sensitive data or that could impact the entity's PCI DSS compliance should be well-defined and documented in a formal agreement.

14. Understand the technology

Virtualized environments are very different from the traditional physical environment. So entities must understand the virtualization technology to effectively evaluate and secure their environment. Entities must also be aware of the industry best practice and guidelines for securing virtualized environments. Entities must take guidance from insightful resources and publication like The Center for Internet Security (CIS), International Organization for Standardization (ISO), ISACA (formerly the Information Systems Audit and Control Association), National Institute of Standards Technology (NIST), SysAdmin Audit Network Security (SANS) Institute to name a few for effective implementation of security controls and standards.

Conclusion

Entities need to understand that there is no specific solution for securing data in a virtualized environment. However, as outlined in the PCI DSS standard guidelines, it is a mandate to implement all the 12 requirements including the use of firewalls, encryption, prohibition of direct public access to the Internet, system hardening, deploying antivirus, and two-factor authentication for remote access, logging, and intrusion-prevention systems in the virtual and cloud environments. Neglecting these requirements will result in heavy penalties such as fines, increased transaction fees, or even losing the right to access a payment card network's resources. The process may seem quite complicated for entities to implement PCI compliance in a virtual environment. So, it is highly recommended that entities obtain professional guidance to make it a hassle-free process. An experienced professional can perform a PCI gap assessment that addresses specific requirements for application, network, physical, and database compliance and accordingly guide entities in implementing security measures and achieve PCI compliance for virtual and cloud environment.

About Us

VISTA InfoSec is a Global Cyber Security Consulting firm offering exceptional Cyber Security Consulting & Audit Service, Regulatory & Compliance Consulting Services and Infrastructure Advisory Solutions. With strong industrial presence since 2004, we have been serving clients from across the world with our robust, end-to-end security services and solutions. We are a 100% vendor neutral company with strict no outsourcing policy and built on our core values of strict code of ethics, transparency and professionalism.

OUR SERVICES OFFERINGS

Compliance & Governance

- SOC 1 Consulting & Audit
- SOC 2 Consulting & Audit
- PCI DSS Advisory and Certification
- PCI PIN Advisory and Certification
- PA SSF Advisory and Certification
- ISO 27001 Advisory and Certification
- ISO 20000 Advisory and Certification
- Business Continuity Management (ISO22301)
- Cloud Risk CCM / CStar / ISO27017
- Information Security Audit
- Software License Audit
- ATM Security Assessment

Technical Assessment

- Vulnerability Assessment
- Penetration Testing
- Web App Security Assessment
- Mobile Security Assessment
- Thick Client Application Security Assessment
- Virtualization Risk Assessment
- Secure Configuration Assessment
- Source Code Review

Regulatory And Compliance

- GDPR Consulting and Audit
- HIPAA Consulting and Audit
- CCPA Consulting and Audit
- NESA Consulting and Audit
- MAS-TRM Consulting and Audit
- NCA ECC Compliance
- SAMA Compliance

Managed Service

- Adaptive Security Managment Program
- DPO Consultancy Services
- CISO Advisory
- Managed Compliance Services
- Managed Security Services

IT Audit & Advisory

- Infrastructure Audit
- Infrastructure Design & Advisory
- Datacenter Design & Consultancy Services

Training & Skill Development

- Training & Skill Development

OUR OFFICES

USA

📍

VISTA INFOSEC LLC
24007 VENTURA BLVD
SUITE 285
CALABASAS CA 91302

☎

+1-415-513-5261

✉

USSALES@VISTAINFOSEC.COM

SINGAPORE

📍

VISTA INFOS EC PTE. LTD
20 COLLYER QUAY
#09-01
20 COLLYER QUAY
SINGAPORE (049319)

☎

+65-3129-0397

✉

SGSALES@VISTAINFOSEC.COM

INDIA

📍

VISTA INFOSEC PVT. LTD
001, NORTH WING,
2ND FLOOR,
NEOSHINE HOUSE,
LINK ROAD, ANDHERI (W)
MUMBAI - 400053

☎

+91 99872 44769
+91-22-26300683

✉

SALES@VISTAINFOSEC.COM

UK

📍

6 AMBER COURT
GOLDSMITH CLOSE
HARROW, GREATER LONDON
UNITED KINGDOM
HA20EZ

☎

+447405816761

✉

UKSALES@VISTAINFOSEC.COM

Webinar : PCI DSS & Virtualization
Top Risks and Mitigation

CONTACT US

VISTA INFOSEC®
TRUSTED ADVISORS, ASSURED COMPLIANCE™

☎ US Tel: +1-415-513-5261 | SG Tel: +65-3129-0397 | IN Tel: +91 73045 57744

W: www.vistainfosec.com | E: info@vistainfosec.com

You can reach us on