

Using VMware VDI and vmSight for Stronger and Sustainable HIPAA and PCI Compliance

IT Audit and Compliance in a Virtual Desktop Environment



Contents

Challenges of HIPAA and PCI Compliance	1
Introduction to VMware VDI	2
Compliant Advantages of VMware VDI	2
Best Practices for Stronger and Sustainable HIPAA and PCI Compliance	4
Compliance Costs and Virtualization Savings	4
Introduction to vmSight Virtual Network Intelligence	5
Regulations Addressed by vmSight Monitoring and Reporting	7
vmSight Compliance Areas	8
Audit of Secure Communications.....	8
Audit of Access Authorization	8
Audit of Sensitive System Access.....	9
Validation of Compliance Procedures	9
Validation of Compliance Configuration	10
Malicious Code Prevention.....	10
Conclusion	11

Challenges of HIPAA and PCI Compliance

Organizations responsible for handling and storing customer information have increasing obligations to protect personal data, including health records and financial information. In the United States and abroad, regulatory statutes such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI) have been established to define responsibilities and practices, and increasingly are backed by financial penalties for public or private organizations that fail to comply, or where personal data is actually breached. Starting in 2008, for example, many organizations may face monthly fines for failure to verify PCI compliance.

When evaluating compliance, an auditor will seek the following:

- A firm accounting of sensitive systems and environments where protected information resides in the information technology environment
- A complete list of users authorized to access sensitive data, including user information from central user directories and user account information from local systems
- Change account logs and management review records for the list of authorized users indicating the conscious review, authorization, and de-authorization of privileges

Obtain information on the PCI standard from the PCI Security Standards Council at: <https://www.pcisecuritystandards.org/>

Find information on penalties related to HIPAA violations at: <http://www.ama-assn.org/ama/pub/category/11805.html>

- Complete access audit logs for sensitive systems during a given time period, as well as related audit logs providing information on user logins on specific machines used to access the sensitive systems
- Violations and subsequent actions undertaken by the organization and management for integrated safeguards throughout the environment
- Review documentation that indicates the methodology in which policies are approved, modified, and enforced throughout the organization
- Complete logs of any security assessments or security configuration updates for all sensitive systems and for all machines used to access sensitive systems during a given time period

The auditor would then review all this data, manually trying to cross-reference the information to determine if the sensitive systems are properly controlled. The effort would be necessary for up to twelve months of logs and multiplied by the number of systems and users in the environment. This process is time consuming and therefore often costly. PCI has over 226 separate requirements, and HIPAA has over 54.

As the audit effort is an examination of past performance and adherence, the organization only understands historic control weaknesses. Even with such an audit process in place, without continuous monitoring there are many opportunities for data breaches that may even go undetected. Routine reporting and automatic reviews by management ensures that unauthorized events are detected early and remedied rapidly.

Numerous reports show that most organizations fail HIPAA or PCI audits because they are:

- 1) Unable to verify that they have properly identified and monitored users that are accessing sensitive systems
- 2) Unable to show that they have appropriate review processes in place for user access authorizations
- 3) Unable to prove that they regularly test systems and monitor activity to ensure ongoing access control and secure configurations fines for failure to verify PCI compliance.

For more information on virtual desktop infrastructure:
http://www.vmware.com/products/desktop_virtualization.html

For more information on virtual network compliance monitoring:
<http://www.vmsight.com>

This paper discusses how organizations can augment existing internal practices and systems, and achieve stronger and sustainable HIPAA and PCI compliance using virtual desktops and by leveraging VMware Virtual Desktop Infrastructure (VDI) and vmSight's virtual network compliance monitoring solution.

Introduction to VMware VDI

VMware Virtual Desktop Infrastructure (VDI) transforms the way customers deploy, manage, and access standard desktop operating systems such as Windows XP and Vista. This solution leverages the power and robustness of the proven virtualization platform, VMware Virtual Infrastructure, to create an end-to-end solution for a flexible, reliable, and available desktop environment. Organizations can rapidly deploy and provision desktops and manage the environment efficiently.

Deploying desktop instances in centralized or regional secure data centers enables organizations to utilize data center capabilities such as high availability and disaster recovery and ensure that data and enterprise information is secure, inside the data center and off local devices susceptible to theft or loss. Each desktop instance is isolated inside its own virtual machine, so there are none of the application compatibility issues often found in traditional server based computing solutions. This desktop isolation also provides a personal desktop computing experience and increases user acceptance. VMware VDI integrates into existing infrastructure or combines with third-party application virtualization or application delivery solutions for a dynamic desktop environment.

Compliant Advantages of VMware VDI

The use of personal computers, including company issued laptops, office desktops, and at home workstations, as a means to access sensitive systems makes the goal of protecting sensitive data, and complying with the associated regulations, extremely difficult. The more remote and unmanaged the personal machines are, the greater the challenges. In addition to the difficulties listed below, accessing sensitive data remotely on insecure and unmonitored systems violates many government and industry regulations (PCI DSS 12.3.10).

Personal desktop computers present the following issues from a compliance and data protection perspective:

- Private data accessed via the computer may be stored locally, and that local data or even the computer itself may be stolen or compromised, thereby compromising the private personal data.
- Storage peripherals may be installed on the device, permanently or temporarily, and private data may be transferred to these devices purposely or accidentally, also presenting the risk of data breach. Depending on the location and ownership of the personal desktop, it may be difficult or impossible to ensure the regular assessment of the desktop configuration and of the users accessing the desktop.
- Depending on the location and ownership of the personal desktop, and the configuration of the network used to connect the personal desktop to sensitive systems, it may be difficult or impossible to provide regular or continuous monitoring of access to sensitive systems.
- Depending on the configuration of the personal desktops and network authentication mechanisms, it may be difficult or impossible to identify machines with more than varying IP addresses or to associate users with machines at specific points in time.
- Transference of data to personal computers inhibits the ability of data protection safeguards that are deployed based on data classification.
- Personal systems are general use systems that are utilized beyond basic work functions, and therefore introduce foreign code that is not subject to testing and user permissions generally exceed necessary privilege levels.
- Personal systems that are mobile or located outside the physical safeguards of the organization are subject to theft, sale, and corruption.

VMware provides a TCO Calculator on its website:
<http://www.vmware.com/products/vi/calculator.html>.

The tool compares your current environment to a virtualized (VMware) environment, including Desktop Control and Manageability Cost Savings.

Many organizations are now considering virtual desktops as an alternative to physical desktops. This is often considered for the financial savings related to reduced hardware costs, reduced software licenses (including anti-virus, host-firewall solutions, etc), reduced energy costs and reduced IT administration (including patching, backups, role access, etc) costs. In fact there exist tools online to facilitate the determination of such practical savings that an organization may achieve – one such Total Cost Calculator is provided by VMware.

Virtual desktops, however, also can provide a number of significant advantages in protecting private data and achieving broader HIPAA and PCI compliance more easily, namely:

- Private data that is intentionally or inadvertently “stored” on a virtual desktop is protected inside the data center.
- Data is maintained within a sandbox that is constantly monitored and secured.

- The configuration of virtual desktops can be regularly and fully monitored.
- User and application activity from virtual desktops can be continuously monitored within the virtual network without the complexities and costs of additional network equipment.

Best Practices for Stronger and Sustainable HIPAA and PCI Compliance

If an organization is seeking to comply with HIPAA or PCI, and to protect sensitive personal data and reduce the risk and costs of data breach, the following are emerging best practices that leading organizations are now implementing in addition to current best practices such as regular scanning and audit log collection:

- 1) Implement virtual desktops using an efficient and highly manageable virtual desktop infrastructure such as VMware Virtual Desktop Infrastructure (VDI) and only allow access to sensitive systems through virtual desktops.
- 2) Ensure that all virtual desktops are based on a secure configuration, and implement regular assessment and patching of virtual desktops to ensure that configurations remain secure.
- 3) Integrate a continuous monitoring system such as vmSight with your virtual desktop environment to provide visibility and auditing of all user access to sensitive systems and to validate that compliance policies and configurations are met.
- 4) Establish an ongoing review and approval process for reports produced by the monitoring system, to make sure that compliance is maintained and potential issues or violations do not go unnoticed.

Compliance Costs and Virtualization Savings

In order to maintain compliance, organizations face a number of on-going costs, such as:

- Fees for annual third-part audits
- Employee costs to prepare for audits and collect data for auditors
- Costs to automate the reporting and data collection for compliance audits
- Employee and systems costs to remediate compliance issues
- Fees for third-party re-audits after failed audits

In addition to the annual costs, organizations also face risks due to failure to comply or data breach that may result in additional costs, such as:

- Monthly fines resulting from failed or incomplete audits
- Discovery, notification and replacement costs for stolen cards or patient records

- Damages and legal fees from lawsuits when data breach occurs
- Business impact of reduced customer confidence following data breach

Through virtualization's improved manageability and with an integrated monitoring system, organizations can drastically reduce the IT costs associated with annual compliance audits, and can reduce the risk of data breaches and therefore affect the bottom line impact that might be associated with data breaches. Annual IT efforts to support compliance audits may be reduced by 50 percent or more, and the risk of data breach may be reduced by 25 percent or more. A large contributor to the reduced costs associated with data breach is the increased assurance of early

detection that continuous monitoring provides. Environments that have integrated monitoring increase the likelihood of early detection, and therefore prevention of larger data breaches, by 75% or more. It is possible to model compliance costs and risks, and then to calculate the savings due to virtualization and integrated compliance monitoring. One such tool for calculating the cost savings is available from vmSight.

vmSight provides a Cost Savings Calculator on its website:

http://www.vmsight.com/documents/compliance_savings.xls

This tool compares your current compliance costs and risks to a virtualized environment with integrated compliance monitoring.

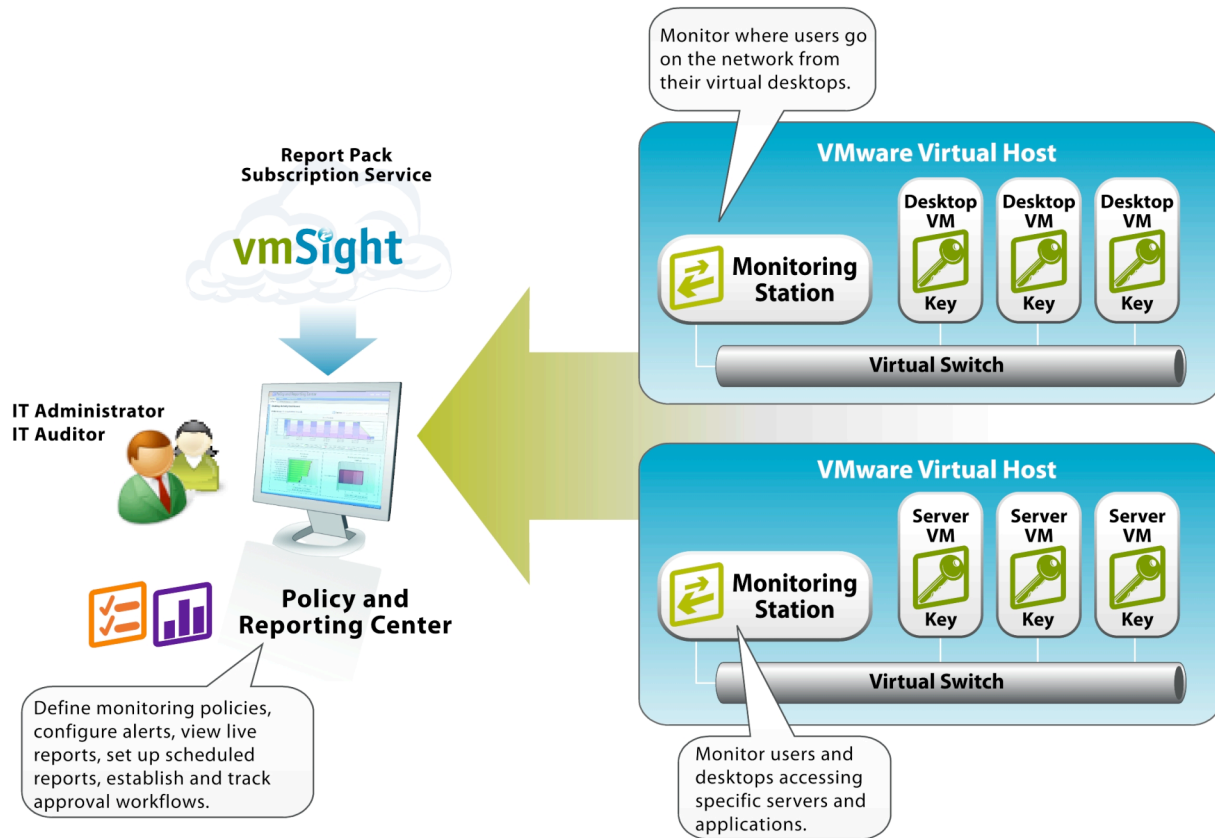
Introduction to vmSight Virtual Network Intelligence

The vmSight virtual network intelligence product suite enables real-time monitoring of compliance policies anywhere inside the virtual network, and provides extensive reporting capabilities along with analytics and alerts on all activities monitored in the virtual network. You can easily monitor activity by user or group (including integration with user directories such as Microsoft Active Directory). You can see activity between virtual machines or between virtual and physical machines. Auditors receive extensive information to validate regulatory compliance, at a fraction of the time and cost of alternative methods for audit data collection.

The vmSight product suite includes VdeskTools monitoring components for virtual desktops, and VserverTools monitoring components for virtual servers. The vmSight suite relies on vmSight's patented Connector ID technology that provides "caller ID" type of capabilities for network connections.

The vmSight product and monitoring components deploy easily and quickly within the virtual environment with little or no effect on system performance. Monitoring policies are easily defined and managed, and reports can be generated on-demand or run on a scheduled basis. Administrators can also setup approval workflows for compliance reports, so that regular reviews can be automated and results captured.

The vmSight product components are:



- **Connector ID Keys** install on the virtual desktops or virtual servers, and enable continuous tracking of users, applications and machines. Connector ID Keys are available for multiple versions of Windows and Linux.
- **Monitoring Stations** connect passively to virtual switches for monitoring of all activity including real-time monitoring of compliance policies as well as service levels. Monitoring Stations are currently available for VMware ESX and VMware Server.
- The **Policy and Reporting Center**, installed on any VMware host, provides a browser-based management and reporting system for the central management of all vmSight components, for all compliance and other policies, and for all report generation. The ability to define and track approval workflows related to compliance is included.

The vmSight Virtual Network Intelligence product suite is available in a free Basic edition, and in the Professional and Enterprise editions. The suite is available for VMware® ESX and VMware Server, and is compatible with VMware Virtual Desktop Infrastructure (VDI) and VMware ACE. The vmSight Enterprise edition comes with the vmSight Report Pack subscription, and the Report Pack contains numerous report templates for HIPAA and PCI compliance, covered in more detail in the following sections.

Regulations Addressed by vmSight Monitoring and Reporting

The following table highlights the key sections of the HIPAA and PCI DSS regulations addressed by vmSight compliance reports. Further details are discussed in the following section of this document.

Applicable Regulatory Table

Mandate	Section	Description
HIPAA	164.306(e)	Maintenance
HIPAA	164.308(a)(4)	Information Access Management
HIPAA	164.308(a)(8)	Evaluation
HIPAA	164.308(a)(5)(ii)(B)	Protection from Malicious Software
HIPAA	164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis
HIPAA	164.310(b)	Workstation Use
HIPAA	164.312(a)(2)(i)	Unique User Identification
HIPAA	164.312(b)	Audit Controls
HIPAA	164.312(c)(1)	Integrity
HIPAA	164.312(e)(2)(i)	Integrity Controls
HIPAA	164.312(e)(2)(ii)	Encryption
HIPAA	164.312(d)	Person or Entity Authentication
PCI DSS V1.1	Section 1.1.6, 1.1.7	Least Functionality Configurations
PCI DSS V1.1	Section 2.2.1, 2.2.2, 2.2.4	Secure Configurations
PCI DSS V1.1	Section 2.3	Encrypt all non-console administrative access
PCI DSS V1.1	Section 7.1, 7.2	Limit, and Monitor Access
PCI DSS V1.1	Section 8.1	Unique User Identities
PCI DSS V1.1	Section 10.1	Link access to systems by unique user
PCI DSS V1.1	Section 10.2.1, 10.2.3	Audit and Record User Access Attempts
PCI DSS V1.1	Section 10.3.1, 10.3.5	Record user identification and events
PCI DSS V1.1	Section 11.1, 11.2, 11.3.1	Regularly Test Systems
PCI DSS V1.1	Section 11.4	Deploy automated and alerting systems

vmSight Compliance Areas

The following are the compliance areas covered by vmSight monitoring and the reports that come with either vmSight Live Reports or the vmSight Report Pack subscription. All report templates can be customized (using the open source BIRT report designer) and further custom reports can also be developed. It is a simple process to add report templates to the vmSight Policy and Reporting Center, and to setup regular schedules for running reports. Reports can be delivered via email, and you can also setup review and approval workflow for each report.

Audit of Secure Communications

Ensure that communications to and from sensitive systems where virtual machines are involved are properly secured, by monitoring and reporting on the use of secure channels, identifying active channels, and maintaining an up-to-date inventory of authorized connection protocols and workstations. The report facilitates the management and access to sensitive data, such as protected credit card and PCI, by maintaining a real time approval and utilization record of communications.

Regulatory support:

- Supportive of requirements to ensure communications are done through encrypted channels to safeguard information interfacing with critical assets.
HIPAA 164.312(e)(2)(i), 164.312(e)(2)(ii);
PCI DSS v1.1 Section: 2.3
- Supportive of validating mandates that require network restrictions, documentation, and justification for the use of secure and insecure protocols.
PCI DSS v1.1 Section: 1.1.6, 1.1.7
- Supportive of workstation requirements where policy and procedures dictate how systems may be accessed (securely, remotely) and usage.
HIPAA 164.310(b)

Audit of Access Authorization

Monitor and validate access to all critical systems—either virtual servers or by those using virtual desktops—through the implementation of management policies on user access activities. Document and support access privileges and report activities with management review and approvals. Provide inventory and validation of policy compliance and real-time exceptions.

Regulatory support:

- Supportive of monitoring and validating that systems with multiple users restrict access based on a user's need to know, and all exceptions are reported.
HIPAA 164.308(a)(4);
PCI DSS v1.1 Section 7.1, 7.2
- Supportive of validating that all Desktops are inventoried, managed, and all identities of systems are identified. Identification process ensures no false systems gain access to sensitive data.
HIPAA 164.312(d)

- Supportive of requirements that mandate unique user identification be established within the environment.
HIPAA 164.312(a)(2)(i), 164.312(c)(1)

Audit of Sensitive System Access

Provide summary and detail audit of all individual users accessing sensitive data on virtual servers or via virtual desktops to detail the number of times they attempted those connections, along with the desktops and applications used during those access attempts, and identify those users whose access was not authorized by pre-defined compliance policies. Satisfy monitoring requirements through policy violation reports.

Regulatory support:

- Supportive of the requirements to implement technical policies and validate authorized user identity activities.
**HIPAA 164.312(a)(2)(i);
PCI DSS v1.1 Section 8.1**
- Supportive of monitoring audit controls required to record and examine activity in information systems that contain or use protected information.
**HIPAA 164.312(b);
PCI DSS v1.1 Sections 10.1, 10.2.1, 10.2.3, 10.3.1, 10.3.5**

Validation of Compliance Procedures

Validate that regular and automated compliance checks, patch updates and the like are occurring on a regular basis for all virtual machines that house sensitive data and for all virtual desktops that are used to access any sensitive servers, and identify any virtual machines that are out of date on compliance procedures.

Regulatory support:

- Supportive of the requirements to validate that software has the latest patches and that all systems comply with the organization secure configuration policy and procedures
PCI DSS v1.1 Section 6.1
- Supportive of conducting periodic security evaluation requirements. Evaluations may validate and identify compliant and non-compliant postures for the systems. This component is supported for technical host and technical network validations.
**HIPAA 164.308(a)(8), 164.306(e);
PCI DSS v1.1 Sections 11.1, 11.2, 11.3.1**

Validation of Compliance Configuration

Validate that virtual machines adhere to company architecture policies by detecting use of non-compliant applications. Demonstrate only authorized practices are followed when administrating and operating the systems. Provide inventory of systems that violate policies.

Regulatory support:

- Supportive of implementing single function servers
PCI DSS v1.1 Section 2.2.1
- Supportive of requirements to disable all insecure and unnecessary services not required for the core function of the system
PCI DSS v1.1 Section 2.2.2
- Supportive of the removal of unnecessary functionality from the systems (i.e. Least Function)
PCI DSS v1.1 Section 2.2.4

Malicious Code Prevention

Monitor and record application activity on virtual machines, either incoming or outgoing on sensitive servers and on desktops used to access sensitive servers, that is coming from an unusual or unknown application or from an application that is known to be malicious, and therefore possibly represents that the host machine has been compromised by external malicious code.

Regulatory support:

- Supportive of the need to detect and manage malicious queries against the environment
HIPAA 164.308(a)(5)(ii)(B)
PCI DSS v1.1 Section 11.4

Conclusion

For many organizations, HIPAA and PCI compliance is no longer optional. Penalties are increasingly stiff, and the ultimate cost of non-compliance – the breach of personal data – can damage organizations in multiple ways. Compliance, and validation of compliance, is not easily achieved. It is especially difficult when computing environments are widely distributed and not all computers are centrally managed.

Virtualization technologies, including virtual desktops, offer an improved means to centralize computing, management and monitoring while still providing users local access and full functionality. For organizations seeking stronger HIPAA and PCI compliance, relying on virtual desktops for access to sensitive systems provides both cost savings and increased manageability and security. With an integrated compliance monitoring and reporting system such as the vmSight virtual network intelligence suite, virtual desktops can be used to increase compliance and reduce data breaches while also reducing IT costs.

About VMware, Inc.

VMware (NYSE:VMW) is the global leader in virtual infrastructure software for industry-standard systems. Organizations of all sizes use VMware solutions to simplify their IT, fully leverage their existing computing investments and respond faster to changing business demands. VMware is based in Palo Alto, California and majority-owned by EMC Corporation (NYSE:EMC). For more information, visit www.vmware.com.

About vmSight

vmSight is the first and leading provider of virtual network intelligence, which provides extensive analytics and alerts on all activities within virtual networks. The vmSight product suite relies on the patented Connector ID technology, providing “caller ID” capabilities for network connections. vmSight’s product suite integrates directly into the virtual network fabric and lets users ensure quality of service, strengthen regulatory compliance, and improve billing methods. Offered in Basic, Professional and Enterprise editions with support for VMware® ESX or VMware Server, the vmSight product suite is compatible with VMware Virtual Desktop Infrastructure (VDI) and VMware ACE. vmSight is a VMware Technology Alliance Partner. For more information, visit www.vmsight.com.

vmSight
3600 Mansell Road | Suite 200 | Alpharetta, GA 30022
678.397.0450 main | 678.397.0339 fax | info@vmsight.com
www.vmsight.com

Revision: 20080124 Item: WP-048-ISV-01-01



VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com
© 2007 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,961,941, 6,961,806, 6,944,699, 7,069,413; 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149, 843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, and 7,281,102; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

