



**EMC Virtual Infrastructure
for Physical Security**

Enabled by EMC CLARiiON,
VMware ESX/ESXi, and Genetec Omnicast

Reference Architecture

EMC Information Infrastructure Solutions



Copyright © 2010 EMC Corporation. All rights reserved.

Published November, 2010

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Benchmark results are highly dependent upon workload, specific application requirements, and system design and implementation. Relative system performance will vary as a result of these and other factors. Therefore, this workload should not be used as a substitute for a specific customer application benchmark when critical capacity planning and/or product evaluation decisions are contemplated.

All performance data contained in this report was obtained in a rigorously controlled environment. Results obtained in other operating environments may vary significantly.

EMC Corporation does not warrant or represent that a user can or will achieve similar performance expressed in transactions per minute.

No warranty of system performance or price/performance is expressed or implied in this document. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Part number: H8087

Contents

Table of Contents

Reference architecture overview..... 4
Key components 7
Physical architecture 9
Minimum virtualized configuration 11
Validated environment profile..... 12
Software resources 16
Conclusion..... 17

Reference architecture overview

Document purpose This document provides an overview of the EMC Virtual Infrastructure for Physical Security solution enabled by EMC® CLARiiON®, EMC Celerra®, VMware vSphere 4, ESX/ESXi 4.x, and Genetec Omnicast.

This document also includes configuration guidelines and resource specifications for the solution components and storage arrays. For detailed information regarding installation and implementation, please consult the Proven Solution Guide for EMC Virtual Infrastructure for Physical Security Enabled by EMC CLARiiON, VMware ESX/ESXi, and Genetec Omnicast.

Solution purpose The purpose of this solution is to present a reference architecture that provides a platform for integrating legacy and state-of-the-art physical security and surveillance infrastructures, while using virtualization technology to:

- Increase resource utilization
- Decrease the number of servers and their associated costs
- Maximize server manageability

Using the EMC and Genetec integrated solution, a security team can view realtime video while also receiving policy-based and anomaly-based alerts generated from sophisticated software analysis of the data from remote locations and historical archives.

The business challenge Private businesses and public entities have responded to rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. These organizations face two key challenges:

- Managing and protecting their ever-growing volume of physical security information
- Maximizing the performance and utilization of their network and storage infrastructure

The ability to access the right data at the right time from anywhere is crucial to supporting physical security and surveillance needs. But comprehensive solutions may be hindered by:

- Proprietary software and closed hardware platforms
- Lack of archive management capabilities
- Data retrieval wait times or lost data
- Content authenticity

These limitations are amplified by the high expansion costs of legacy video surveillance systems based on CCTV, digital video recorders (DVRs) or networked video recorder (NVR) technologies; and non-integrated IT and physical security systems.

The technology solution

The EMC Virtual Infrastructure for Physical Security Enabled by EMC CLARiiON, VMware ESX/ESXi, and Genetec Omnicast solution provides the ability to control video surveillance and analyze security incidents in real time from anywhere, while monitoring and collecting evidence faster through realtime data and active archiving capabilities.

This solution integrates EMC and Genetec technology in a virtualized architecture to help meet the challenges of video surveillance information convergence and management.

Genetec Omnicast is an open video management platform; it can control and record cameras from most manufacturers on the market. With its scalable and flexible design it meets the expectations of the most demanding customers with many advanced features:

- High availability with built-in failover
- Alarm management with an escalation process
- Support for cameras and software-based video analytic
- Video Wall Integrations
- Advanced floor plans and GIS maps
- Multi-site deployments with the Federation feature
- Offsite cording and monitoring
- Indexing of video with metadata (point-of-sale, access control, and so on)
- Integration of CCTV equipment (matrix, CCTV keyboards)

The Genetec Archive application is compatible with RSA, The Security Division of EMC, and the SecurID Windows Authentication agent, providing multiple layers of secure access to the physical security infrastructure and authenticated tamper-proof video data for increased conviction rates.

The core storage architecture is based on enterprise-class EMC CLARiiON storage systems to cost-effectively scale the solution as security requirements grow, with industry-leading reliability, availability, scalability, and storage-based functionality.

To reduce the footprint of an Omnicast installation, the servers and recorder can be run on virtual machines using VMware vSphere 4, including the Omnicast Gateway server, Omnicast SQL server, Omnicast Directory server, and the Omnicast Archiver server.

Omnicast can take advantage of VMware's High Availability (HA) and Fault Tolerance (FT) features. When vSphere recognizes a failure HA will immediately boot up the same server to a different physical ESX/ESXi host. An FT failover will immediately switch the active server to a second server that has been "shadowing" the instruction execution of the primary.

HA provides:

- Immediate recovery for any Omnicast server

FT provides:

- Near zero downtime for any Omnicast server
- Near zero data loss (data loss is rare)
- Continuous availability

Note

FT is not recommended for Archiver servers (Failover Archivers should be used).

Cisco Unified Computing System (UCS) for vSphere 4 provides a high-performance environment for Genetec Omnicast servers. UCS is also suitable for FT and HA environments.

Key components

Digital video streams

Digital video streams over TCP/IP are captured by the Omnicast Archiver application and written to CLARiiON storage.

Note: Only the EMC E-Lab™ Interoperability Navigator SAN and DAS configurations are supported with the Genetec Omnicast application.

Omnicast Services

For Omnicast Services see the *EMC Storage for Physical Security - Enabled by EMC CLARiiON and Genetec Omnicast Reference Architecture*.

VMware vSphere 4

VMware vSphere 4 is the market-leading virtualization management tool for ESX/ESXi. vSphere 4 combined with ESX/ESXi 4.x turns your infrastructure into an efficient and flexible internal cloud, enabling you to:

- Decrease your capital and operating costs
 - Run a greener data center and reduce energy costs
 - Control your application service levels with advanced availability and security features
 - Streamline IT operations and improve flexibility
-

ESX/ESXi 4.x

ESX and ESXi 4.x both run the same hypervisor. The hypervisor provides a virtual hardware layer forming the basis for server virtualization.

The primary differences between ESX and ESXi 4.x is based on packaging. ESX loads with a running Linux 2.4 kernel. ESXi 4.x uses the Linux loader to install the hypervisor but does not provide the Linux 2.4 kernel.

Compatible vCenter 4.x technologies

Advanced vCenter features include:

vMotion

The capability to move a running virtual machine from one ESX/ESXi host to another.

Storage vMotion

The capability to move a running virtual machine from one storage device to another.

DRS

Dynamic Resource Scheduler – Provides automatic load balancing of an ESX/ESXi cluster using vMotion. DRS can dynamically load balance VM guests between the hosts in the vCenter cluster.

Automatic, dynamic load balancing may be set from conservative to aggressive, depending on how dynamic the movement of VM guests should be for the particular installation.

DRS can also be set for manual load balancing. In manual load-balancing mode, DRS will provide a list of recommendations and the vCenter operator will have the option to accept recommendations.

HA

High Availability – In case of a failure the virtual servers (guest) will automatically restart on another host in the cluster. HA works well for all servers.

FT

Fault Tolerance – Provides a zero downtime failover from the active virtual machine (guest) to a shadow virtual machine (guest) that has been running in lock-synch to the active. FT can protect only VM guests that have a single vCPU requirement.

Note: FT should not be used for Omnicast servers that have the Archiver service running.

Physical architecture

Cisco UCS

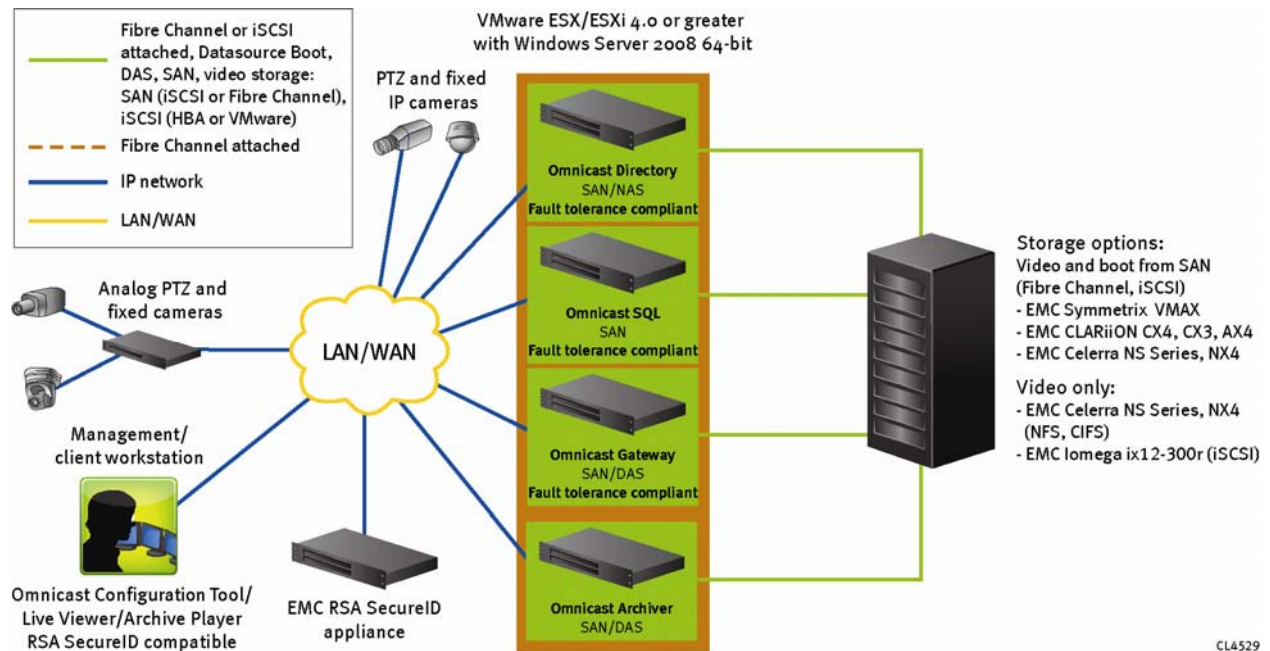
The Cisco UCS is an innovative architecture that integrates computing, networking, and virtualization in a single platform. All Genetec Omnicast servers perform extremely well when installed as ESX VMs on the UCS.

EMC Symmetrix VMAX™ storage, coupled with Cisco UCS and ESX/ESXi 4.0 or later, provides an excellent platform for the demanding installations.

Reference architecture diagram

The following illustration depicts the overall physical architecture of the solution.

See the *EMC Storage for Physical Security - Enabled by EMC CLARiiON and Genetec Omnicast Reference Architecture* for information on Omnicast services placement between VM guests.



**Virtualized
Omnicast
servers**

The reference architecture diagram illustrates the virtualization of Omnicast servers using VMware vSphere 4.

The virtualized infrastructure must use server and storage adapter hardware that is officially validated by VMware and EMC.

Because VMware FT relies on a single processor for all activity such as operating system functions, the Directory, SQL, and Gateway, each of these services should be placed on separate Windows Server 2008 64-bit operating systems. VMware FT provides a full nondisruptive transition for each service, providing no data is lost during failover in most cases. An FT failover is generally not noticeable by the client.

VMware HA allows a virtual machine to be automatically rebooted to a different ESX host in the vSphere cluster. HA may be used for any Omnicast service. HA is not dependent on the CPU having virtualization hardware assist (Intel VT and AMD-V). It may be used when FT is not available.

The database of supported hardware, including fault tolerance, for VMware can be found at:

<http://www.vmware.com/resources/compatibility/search.php>

Minimum virtualized configuration

Note All hardware (processors, Ethernet cards, FC cards, iSCSI cards, and so on) must be supported based on VMware's support matrix.

CPU In the following tables, the Minimum column assumes a system with the directory and Archiver on a single VMware guest. The Recommended Minimum column assumes a configuration with a directory server, and two archive server VMware guests. Both the minimum and recommended minimums include enough processing power for CPU-intense operations such as motion detection and inserting watermarks. The recommended minimum may allow room for minimal expansion.

Minimum	Recommended Minimum
Two 2 GHz cores <ul style="list-style-type: none"> • One socket (quad-core) • Two socket (dual-core) 	Eight 2 GHz cores <ul style="list-style-type: none"> • Two quad-core sockets
<ul style="list-style-type: none"> • Two vCPUs per VM guest running the Archiver service • One vCPU for each guest running directory, vmatrix, and database services. This may be on a single VM guest up to three VM guests. • One vCPU for VM guests running Fault Tolerance (FT) 	

Memory

Minimum	Recommended Minimum
12 GB	16 GB
<ul style="list-style-type: none"> • 2 GB per VM guest plus 2 GB for ESX/ESXi • Allow memory to expand • 64-bit Windows Server 2008 may expand beyond 3 GB per VM guest • VMware memory overloading will occur. This allows VM guests to share common pages of memory thus reducing total memory needs. 	

NIC Ports

Note: In all cases the minimum number of physical NIC ports is two. VLANs may be used on 10 Gb/s NICs to achieve more virtual NIC ports. On a Cisco UCS, the 10 Gb/s ports can be broken many ports using the UCS management utility.

Note: Additional NICs may be required for other functions such as iSCSI.

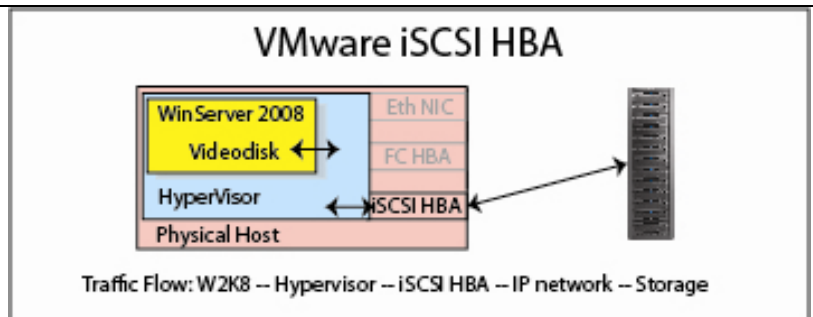
Note: iSCSI NIC may be, through a dedicated NIC, assigned to the ESX/ESXi host or a NIC assigned to an iSCSI-dedicated vSwitch.

Minimum	Recommended Minimum
NIC1 <ul style="list-style-type: none"> • vmconsole (ESX) • VMKernel (ESX/ESXi) • Management network 	NIC1 <ul style="list-style-type: none"> • vmconsole (ESX) • Management network
NIC2 <ul style="list-style-type: none"> • User network 	NIC2 <ul style="list-style-type: none"> • User network1
	NIC3 <ul style="list-style-type: none"> • User network 2
	NIC4 <ul style="list-style-type: none"> • VMKernel (vMotion) • Management network backup
	NIC5 (only needed if FT is active) <ul style="list-style-type: none"> • Fault Tolerance (FT)

Validated environment profile

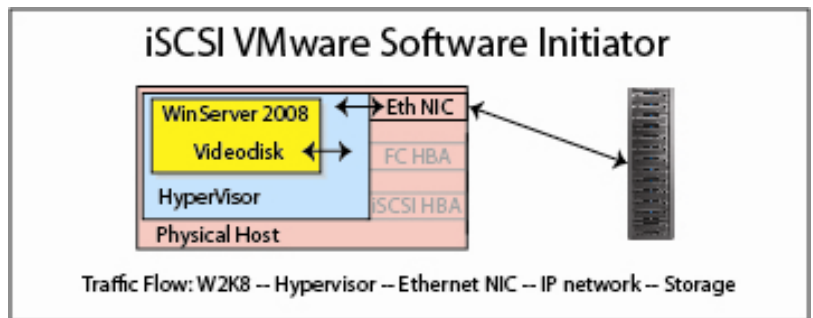
**vCenter/
ESX/ESXi 4.x
storage
topology**

Topology	
<p>FC</p>	<p>Use only VMware- and EMC-approved Fibre Channel (FC) host bus adapter (HBA) cards.</p> <p>The storage area network (SAN) may be either Point-to-Point (FC-P2P) or switched fabric (FC-SW).</p> <p>FC-P2P would connect the storage array directly to a single ESX server. This is a valid solution if the storage array has enough FC ports to accommodate the number of ESX/ESXi hosts.</p> <p>Limitations: VMware ESX/ESXi 4.x limits each LUN to 1.9 TB.</p> <div data-bbox="602 751 1398 1066" style="border: 1px solid black; padding: 10px; text-align: center;"> <p>VMware FC HBA</p> <p>Traffic Flow: W2K8 -- Hypervisor -- iSCSI HBA -- IP network -- Storage</p> </div>
<p>iSCSI</p>	<p>The EMC Physical Security lab has qualified three different implementations of iSCSI:</p> <ul style="list-style-type: none"> • iSCSI HBA • iSCSI VMware software initiators • iSCSI MS Windows Server 2008 software initiators <p>iSCSI (Internet Small Computer System interface) is an Internet Protocol (IP)-based storage network standard. iSCSI uses TCP/IP to allow two hosts to exchange SCSI commands/data.</p> <p>iSCSI is generally considered a SAN protocol, although some consider it a Network Area Storage (NAS) protocol. iSCSI may be considered a SAN/NAS hybrid.</p> <p>iSCSI HBA – The iSCSI HBA is the highest performing iSCSI topology. Because an iSCSI HBA configuration is on the HBA card, booting from an iSCSI-attached EMC storage array is possible.</p> <p>iSCSI HBA increases performance in two ways. First, the server writes to the HBA as if it were a SCSI device, leaving all the IP protocol to the HBA. Secondly, because the HBA is a single-purpose card it handles the iSCSI protocol more efficiently.</p> <p>Limitations: VMware ESX/ESXi 4.x limits each LUN to 1.9 TB.</p>



iSCSI VMware software initiators – The VMware hypervisor has a built-in software iSCSI initiator. The software iSCSI initiator uses software to perform all the IP and SCSI functions performed in the iSCSI HBA as described above.

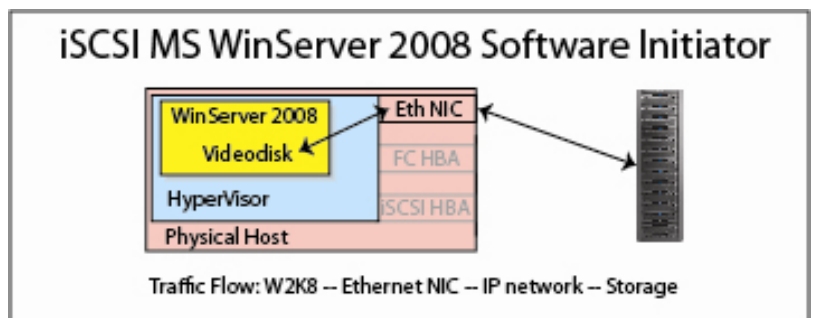
Limitations: VMware ESX/ESXi 4.x limits each LUN to 1.9 TB.



iSCSI Microsoft Server 2008 software initiators – Like iSCSI VMware software initiators, the iSCSI protocol uses software to perform the same functions as an iSCSI HBA. With Microsoft Server 2008 (32- and 64-bit), Microsoft included a high performing iSCSI software initiator in the OS.

The Microsoft Server 2008 software initiator performance is equal to the iSCSI VMware software initiator.

An advantage to using the Microsoft Server 2008 software initiator is that the VMware 1.9 TB LUN size limit is removed.



<p>NFS</p>	<p>Network File System (NFS) is an open standard protocol developed by Sun Microsystems in 1984. NFS allows hosts to access files over a network.</p> <p>NFS is a VMware hypervisor-supported network storage protocol. NFS datastores may be defined as a Windows Server 2008 VM. Genetec can use the datastore as if it is any other disk (for example, \\e:).</p> <p>An advantage to using NFS is that the VMware 1.9 TB LUN size limit is removed.</p> <p>Limitations: NFS is very sensitive to network latency. Ideally the NFS-attached disk array will be co-located within the same room, or connected to the same Ethernet switch as the Genetec Archiver.</p> <p>Note: In most cases it is better to use iSCSI in place of NFS.</p> <div data-bbox="602 800 1398 1108" data-label="Diagram"> <p>The diagram, titled "VMware NFS", illustrates the data path. On the left, a box represents the VM environment containing "WinServer 2008" (with a "Videodisk" icon) and "HyperVisor". Below this is the "Physical Host". On the right, a vertical server rack represents "Storage". Arrows show the flow: from WinServer 2008 to Eth NIC, then from Eth NIC to the Storage rack. Below the diagram, the text reads: "Traffic Flow: W2K8 -- Hypervisor -- Ethernet NIC -- IP network -- Storage".</p> </div>
<p>CIFS</p>	<p>Common Internet File System (CIFS) is use as a shared file access method as well as for communicating to printers, serial, and other miscellaneous objects.</p> <p>Limitations: CIFS is very sensitive to network latency. Ideally the CIFS-attached disk array will be co-located within the same room, or connected to the same Ethernet switch as the Genetec Archiver.</p> <p>Note: In most cases it is better to use iSCSI in place of CIFS.</p> <div data-bbox="602 1461 1398 1770" data-label="Diagram"> <p>The diagram, titled "VMware CIFS", illustrates the data path. On the left, a box represents the VM environment containing "WinServer 2008" (with a "Videodisk" icon) and "HyperVisor". Below this is the "Physical Host". On the right, a vertical server rack represents "Storage". Arrows show the flow: from WinServer 2008 to Eth NIC, then from Eth NIC to the Storage rack. Below the diagram, the text reads: "Traffic Flow: W2K8 -- Ethernet NIC -- IP network -- Storage".</p> </div>

Profile characteristics The solution was validated with the following environment profile.

Profile characteristic	Value
Omnicast application software	The EMC Physical Security lab used Windows Server 2008 64-bit. ESXi 4.0 was used on the Dell servers and ESX 4.0 used on the Cisco UCS.
Storage topology	SAN, NAS iSCSI, and VMware NFS datastores
Bandwidth per archiver	For the EMC Physical Security Lab's LUN throughput test results see the Storage Throughput table in <i>Genetec Configuration Guidelines for EMC CLARiiON Technical Note</i> .

EMC minimum requirements for Genetec on ESX 4.0 or later

Compatible hardware can be found at:

<http://www.vmware.com/resources/compatibility/search.php>

Processor minimum during EMC Physical Security lab tests:

- Quad-core 2 GHz minimum

VMware Fault Tolerance requirements:

- FT requires CPUs to have the virtualization hardware assist feature. Acceptable processors include those with the Intel VT or AMD-V feature sets.

Memory minimums:

- 2 GB per Genetec virtual machine

Storage adapter

- All storage adapters must be VMware certified.
- Fibre Channel adapters must be VMware and EMC certified.

Storage

- Data store
 - Direct attached or SAN devices with unpartitioned space
 - A minimum of 80 GB per VM is required
- Video storage
 - SAN devices with unpartitioned space (that is, VMware RAW attach)
 - FC or iSCSI
 - NAS-attached datastores

Software resources

Software The following table lists the software used to validate the solution.

Software	Version	Configuration
VMware ESX/ESXi 4.0	Update 1	As described in the “Virtual hardware requirements” section.
Windows Server 2008 64-bit		Operating system for Omnicast servers and workstation(s)
Genetec Omnicast	4.4 and 4.6	Windows 2008 64-bit
EMC PowerPath®/VE	Latest GA version	Installed on ESX/ESXi 4.0

Virtual hardware requirements

The following table lists the virtualized hardware requirements for the solution.

Virtual element	Description
vCPU	<ul style="list-style-type: none"> • Two vCPUs per virtualized Omnicast Archiver • One vCPU for non-Archiver VM guests requiring FT
Memory	<ul style="list-style-type: none"> • 2 GB allocated per virtualized Omnicast server • Memory allowed to expand

Conclusion

Summary

The EMC Virtual Infrastructure for Physical Security Enabled by EMC CLARiiON, VMware ESX/ESXi, and Genetec Omnicast represents an ideal solution for surveillance management and IT infrastructure, incorporating virtualization technology that allows increased system performance and maximizes resource utilization.

The solution provides a flexible and highly scalable virtualized infrastructure meeting a broad range of today's demanding physical security requirements. By leveraging the best-in-breed surveillance management software from Genetec and advanced IT infrastructure components from EMC and VMware, customers can maximize the return on investment in these crucial platforms, while optimizing the use of their system infrastructure.

In addition, the solution provides seamless integration with new and legacy infrastructures reducing the total number of physical servers, reducing greenhouse gasses, and more effectively utilizing a physical server's processing capabilities. EMC storage-based functionality also allows customers to nondisruptively back up their primary servers while the system remains online and available to users. As requirements change and become more sophisticated, customers can be assured that the EMC Physical Security Solution's flexibility and modular architecture can be designed to meet their needs.

Next steps

EMC can help to accelerate assessment, design, implementation, and management while lowering the implementation risks and costs of a physical security solution for a VMware environment.

To learn more about this and other solutions contact an EMC representative or visit www.emc.com/solutions/business-need/information-security/physical-security.htm.
