

# PHYSICAL SECURITY WITH EMC STORAGE AND VERINT NEXTIVA

EMC VNX, Isilon, and Verint Nextiva

EMC Solutions

September 2014



Copyright © 2010, 2011, 2014 EMC Corporation. All rights reserved.

Published September, 2014

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 H13493

# Table of contents

<b>Reference architecture overview</b> .....	<b>5</b>
Document purpose .....	5
Solution purpose .....	5
The business challenge.....	5
The technology solution .....	6
<b>Solution Architecture</b> .....	<b>8</b>
Architecture diagram.....	8
Digital video streams .....	9
Master Server.....	9
Recorder server.....	9
Environment profile.....	9
Hardware resources .....	9
Software resources .....	10
VNX Video Surveillance Storage (VNX-VSS).....	10
<b>Key components</b> .....	<b>12</b>
Introduction .....	12
EMC VNX platform .....	12
EMC Isilon platform.....	12
VMware vSphere .....	12
VMware Horizon with View .....	12
<b>EMC Technology Overview</b> .....	<b>13</b>
Introduction .....	13
EMC Unisphere .....	13
Block Data Compression .....	13
EMC PowerPath®.....	13
SmartQuotas.....	13
SmartConnect .....	13
<b>Domain secured by EMC RSA</b> .....	<b>14</b>
Overview.....	14
RSA login .....	14
<b>VMware Technology Overview</b> .....	<b>15</b>
Introduction .....	15
VMware View components .....	15
Hypervisor.....	16
VMware View Connection server.....	16

View Security server ..... 16

**Conclusion ..... 17**

Learn More..... 17

**References ..... 18**

EMC documentation..... 18

VMware documentation ..... 18

## Reference architecture overview

**Document purpose** This document provides an architectural overview of the EMC Tiered Storage for Physical Security solution that is enabled by EMC® VNX®, EMC VNXe®, EMC Isilon®, and Verint Nextiva.

This document also includes resource specifications for the solution components and storage arrays. For more detailed information regarding installation and implementation, consult the Proven Solution Guide for Physical Security with Verint Nextiva.

**Solution purpose** The purpose of this solution is to present a reference architecture that provides a general-purpose platform for integrating legacy and state-of-the-art physical security and surveillance infrastructures.

By using the EMC and Verint integrated solution, a security team can view real-time video while also receiving policy-based and anomaly-based alerts. These alerts are generated from sophisticated software analysis of the data from remote locations and historical archives.

This solution is a core reference architecture on which you can build other physical security solutions, including:

- Virtualized infrastructure for physical security that uses VMware vSphere
- RSA SecurID two factor authentication
- Video Security Storage (VNX-VSS100)

### The business challenge

Private businesses and public entities alike have responded to rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. These organizations all need to manage and protect their ever-growing volume of physical security information.

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

- Proprietary software
- Closed hardware platforms
- Lack of manageable archival capabilities
- Data retrieval wait times
- Lost data
- Content authenticity
- Information management limitations

The high expansion costs of legacy video surveillance systems based on CCTV, digital video recorders (DVRs), or networked video recorder (NVR) technologies, and nonintegrated IT and physical security systems amplify these limitations.

Once the information is captured—and throughout the initial response, detection, legal, judicial submission, and the data disposal processes—information management, availability, security, and protection are the core capabilities that are needed for tamper-proof evidence collection, increased conviction rates, and asset protection.

The types of organizations that can benefit from a comprehensive physical security solution include:

- Retailers
- Casinos
- Financial institutions
- Higher education institutions
- Transportation companies
- Law enforcement
- School systems
- Prison systems
- Government agencies

### The technology solution

The EMC Physical Security solution provides the ability to control video surveillance and analyze security incidents in real time from anywhere, while monitoring and collecting evidence faster through real-time data and active archiving capabilities. This solution integrates EMC and Verint technology to help meet the challenges of video surveillance information convergence and management. This enterprise-class solution provides data management in each phase of its lifecycle, including:

- Capturing and monitoring
- Analyzing
- Protecting and securing
- Archiving
- Evidence authentication

Verint Nextiva software aggregates physical security content from multiple sources, and integrates IP networking and a full range of physical security systems, including:

- Video surveillance cameras
- Access control devices and intrusion detection systems
- Information security applications
- Visitor management and identity recognition

- Asset management
- Sensors and alarms
- RFID, biometrics, plus future enhancements and analytics

Verint's Review application is compatible with RSA's SecurID Windows Authentication agent, provides multiple layers of secure access to the physical security infrastructure, and provides authenticated tamper-proof video data for increased conviction rates.

The core storage architecture is based on industry-leading enterprise-class EMC VNX and Isilon storage systems, which can cost-effectively and reliably scale the solution as security requirements.

# Solution Architecture

## Architecture diagram

The physical security components typically comprise legacy analog monitoring capabilities, analog cameras, and IP cameras.

Nextiva encoders convert standard NTSC/PAL video from analog cameras to a digital video stream sent over TCP/IP. Nextiva IP cameras or customer-furnished IP cameras can also be deployed. Each IP camera can produce a digital video stream that is sent over TCP/IP.

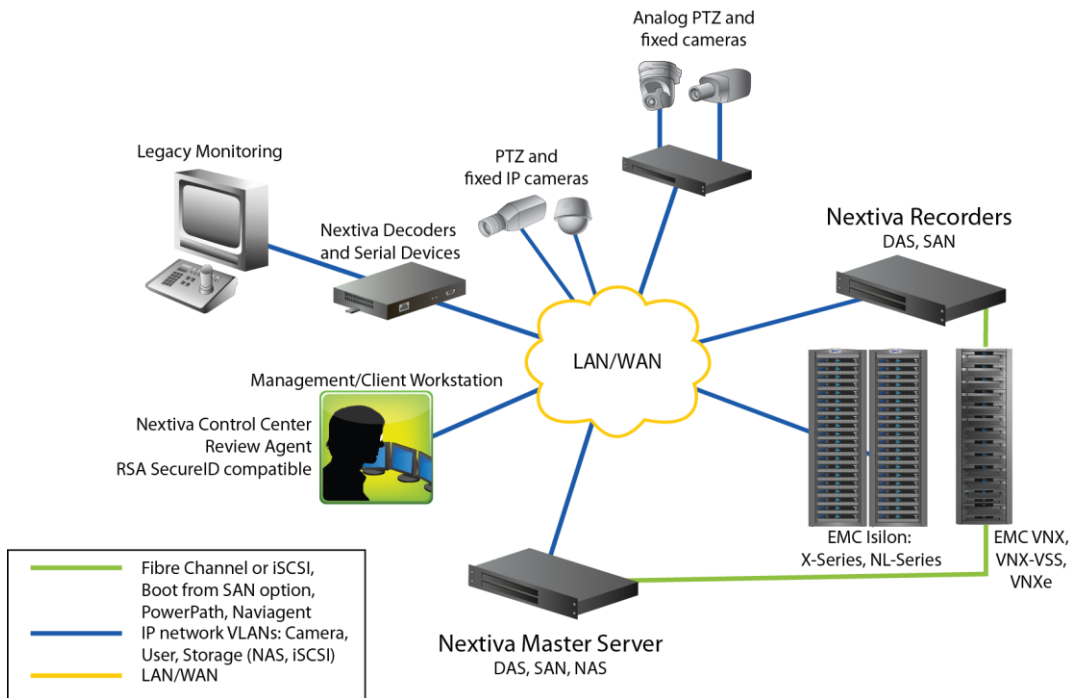
This reference architecture includes EMC VNXe, VNX, VNX-VSS100, and Isilon storage platforms. You can integrate EMC storage platforms and array sizes with Verint Nextiva to provide a physical security solution to meet the requirements of applications of any size.

VNXe and VNX support unified storage solutions. Unified storage topologies include FC, iSCSI, and SMBx (CIFS). The VNXe is a unified only storage platform while the VNX can be configured as block storage only (FC and iSCSI) or unified storage to include SMB protocols.

The VNX-VSS100 is a purpose built Video Surveillance Storage platform. This is an enterprise-class, block-only array that supports FC and iSCSI and is built on the proven VNX platform. As a low cost, high performance and highly available array it is ideally suited for remote locations or smaller centralized sites.

EMC Isilon Scale-Out storage provides enterprise class network attached storage (NAS) for centralized or decentralized enterprise requirements. An Isilon cluster is modularly scalable from terabytes to petabytes of storage.

Figure 1 depicts the overall physical architecture of the solution.





## Figure 1. Solution architecture

### Digital video streams

The Nextiva recorder server application captures digital video streams over TCP/IP and writes them to EMC VNX, EMC VNXe, or EMC Isilon storage solutions.

---

**Note:** The Nextiva recorder application supports only the EMC E-Lab™ Interoperability Navigator SAN and DAS configurations.

---

### Master Server

The Nextiva Master Server application provides access to Nextiva video recordings, authenticates users, and manages events. You can install the master and recorder server applications on a single server as required. This configuration is called a master recorder server.

### Recorder server

The Nextiva recorder server application captures live video streams to storage volumes for archiving. The recorder application keeps a separate index for all captured video and acts as the source for video playback and review requests.

### Environment profile

Table 1 lists the environment profile parameters for this solution.

**Table 1. Environment profile parameters**

Parameter	Value
Nextiva application software	Nextiva 6.1 or later – Windows Server 2008 x32 and x64 (Not 2008 R2) Nextiva 6.3 and 6.4 on Windows Server 2008 R2
Storage topology	SAN, DAS, iSCSI
Number of recorder servers per master recorder	75 with 6.1 and 6.2 with a four-core, 4 GB system running on Windows 2008 x64 (Verint tested)
Isilon NAS Support	Nextiva 6.3 RC2R2 Nextiva 6.4 RC1 or later

### Hardware resources

Table 2 lists the hardware used in this solution.

**Table 2. Solution hardware**

Hardware	Quantity	Configuration
Any 1U, 2U, or blade server on Verint and EMC's supported hardware listing	1	Per master server application Per recorder server application Per Enterprise Storage Manager application
VNX, VNX-VSS100, VNXe, and Isilon	Based on solution requirements	See <i>Configuration and Sizing Guidelines for Verint Nextiva with EMC Storage</i> for more information (restricted to employees only)

Hardware	Quantity	Configuration
Nextiva Review and Nextiva ControlCenter workstations	Minimum of 1; Maximum – Unlimited	Specified in Verint's Nextiva documentation

**Software resources** Table 3 lists the software used in this solution.

**Table 3. Solution software**

Software	Version	Configuration
Windows Server 2008 Windows Server 2012	32/64-bit	Operating system for Nextiva servers and workstations
Nextiva Master Server	6.0 R1 and 6.1	6.0 - Windows Server 2003 R2; Windows Server 2008  6.1/6.2 – Windows 2008 x32 and x64, not R2 (Verint tested)  Local disk drive installation for all nonboot from SAN configurations. Minimum drive specs: C: 35 to 45 GB; D: 10 GB; E: 70 GB
Nextiva recorder server	6.0 R1 and 6.1	Drive specs: C: 35 to 45 GB; D: 10 GB; E: 70 GB
Nextiva ControlCenter	6.0 R1 and 6.1	Administrator interface
Nextiva Review	6.0 R1 and 6.1	User interface
EMC PowerPath	Latest GA version	Installed on Nextiva servers
EMC Naviagent	Latest GA version	Installed on Nextiva servers
Verint Nextiva with NAS support	6.3 RC2 or later 6.4 RC1 or later	Installed on Nextiva servers

### VMX Video Surveillance Storage (VMX-VSS)

The VMX-VSS is a highly available and reliable platform built on the proven EMC VMX family. EMC offers two entry points in the VMX-VSS100 line, the VSS1 with 24 TB minimum raw capacity, and the VSS2 with 120 TB minimum raw capacity.

Both systems are scalable to 344 TB raw capacity, and can handle two 8 GbE Fibre Channel (FC) ports and one 4-port 1 GbE iSCSI adapter per Storage Processor. An additional four 1GbE port for each Storage Processor can be ordered as an upgrade.

### *VSS100 Performance and Capacity considerations*

- VSS1 (24 TB) entry model – Consists of 6 drives that encompassed the vault disks into a RAID group
- VSS2 (120 TB) entry model – Consists of 4 independent vault drives and twenty-four 4 TB drives configured as a storage pool
- Can be expanded using 9-drive and 15-drive expansion packs
- Can hold a maximum of 6 trays (DPE plus 5 DAEs)
- EMC recommends you use vault drives for storage applications of 96 TB or less
- Performance improves with more/smaller RAID groups underlying the Storage Pools
- Capacity improves with larger/fewer RAID groups
- For RAID 6 requirements we recommend the 6+2 RAID group configuration
- For RAID 5 requirements we recommend the 4+1 or the 8+1 configurations
- Maintain at least one hot spare per 30 drives in the array
- Due to limited drive pack options, the final configuration may result in greater than 1 hot spare per 30 drives

## Key components

### Introduction

This section briefly describes the key components used in this solution, including:

- EMC VNX, EMC VSS-100 and Isilon platforms
- VMware vSphere 5.0 or later
- VMware Horizon 6.0 with View or later

### EMC VNX platform

EMC's VNX platform brings flexibility to multiprotocol environments. With EMC unified storage, you can connect to multiple storage networks using NAS, iSCSI, and Fibre Channel SAN. EMC unified storage leverages advanced technologies like EMC FAST VP and EMC FAST Cache on VNX OE for block to optimize performance for the virtual desktop environment, helping support service-level agreements. EMC unified storage supports vStorage APIs for Array Integration (VAAI), which was introduced in VMware vSphere. VAAI enables quicker virtual desktop provisioning and start-up.

### EMC Isilon platform

EMC Isilon scale-out NAS storage increases application performance and improves workflows using a single file system architecture. An Isilon cluster is a storage array made of a minimum of three Isilon nodes. You can use any Isilon cluster capable of supporting the Isilon operating system OneFS 7.0 or later. OneFS 7.0 or later supports Nextiva version 6.3 R2 or later and 6.4 R1 or later.

### VMware vSphere

VMware vSphere is the market-leading virtualization platform that is used across thousands of IT environments around the world. VMware vSphere can transform or virtualize computer hardware resources, including CPU, RAM, hard disk, and network controller, to create a fully functional virtual machine that runs its own operating systems and applications like a physical computer.

The high-availability features of VMware vSphere coupled with Distributed Resource Scheduler and Storage vMotion® enable the seamless migration of virtual desktops from one ESX® server to another with minimal or no impact to the customer's usage.

### VMware Horizon with View

VMware Horizon with View is the leading desktop virtualization solution that enables desktops to deliver cloud computing services to users. VMware Horizon with View integrates effectively with vSphere to provide:

- Network performance optimization—Blast Performance is a comprehensive set of technologies available with Horizon 6 that are designed to ensure that users have a consistently great experience across devices, locations, media, and connections.
- Virtual San—Supports the usage of different tiers of storage to maximize performance and reduce cost.
- Thin provisioning support—Enables efficient allocation of storage resources when virtual desktops are provisioned. This results in better utilization of the storage infrastructure and reduced CAPEX/OPEX.

# EMC Technology Overview

## Introduction

This section identifies and briefly describes the major EMC VNX features used in this solution environment, including:

- EMC Unisphere
- EMC PowerPath
- Block Data Compression
- SmartQuotas
- SmartConnect

## EMC Unisphere

Unisphere provides a flexible, integrated experience for managing and monitoring several VNX and VNX-VSS storage systems through a single pane of glass. You can also access the entire file and block environment with a single sign-in.

## Block Data Compression

EMC unified storage introduces block data compression, which allows customers to save and reclaim space anywhere in their production environment with no restrictions. This capability makes storage even more efficient by compressing data and reclaiming valuable storage capacity. Data compression works as a background task to minimize performance overhead. Block data compression also supports thin LUNs, and automatically migrates thick LUNs to thin during compression, which frees valuable storage capacity.

## EMC PowerPath®

EMC PowerPath® software provides channel failover on all Nextiva application servers for both fiber and iSCSI (with hardware initiators) connectivity options.

## SmartQuotas

SmartQuotas allows administrators to limit the storage used for each Nextiva Recorders and presents the recorder a view of available storage based on the assigned quota. SmartQuotas allows each recorder to calculate its available disk space and react correctly.

## SmartConnect

SmartConnect provides load balancing of connections to the Isilon cluster as well as failover handling of connections. With SmartConnect all Nextiva Recorders use a single fully qualified domain name (FQDN) or universal naming convention (UNC) path for video storage access. Using this network name provides load balancing when the connection to the cluster is made and simplifies installations.

## Domain secured by EMC RSA

### Overview

This Verint solution, installed with EMC RSA's secured domain, increases Windows and Security Center security. RSA authentication, which uses constantly changing RSA tokens, increases the user's Security Center experience by providing a single login structure for accessing multiple Security Center applications.

For more information, refer to the EMC white paper entitled *EMC Physical Security—Enabled By RSA SecurID Two-Factor Authentication with Verint Nextiva Review and ControlCenter Clients*.

### RSA login

In general, the login process for Verint applications consists of the following steps:

1. The login request using RSA authentication (token) sends the request to the EMC RSA SecurID appliance.
2. If the user credentials are correct, the EMC RSA SecurID appliance proxies the login to Active Directory, and Active Directory authenticates the login into the requested Windows domain.
3. The Windows domain server completes the login.
4. The user accesses the requested application. The user may be required to press **Enter** before continuing into the application (this requirement is application-specific).
5. User credentials are verified to ensure that the user has access rights for the requested application.

**Error! Reference source not found.** shows the login process.

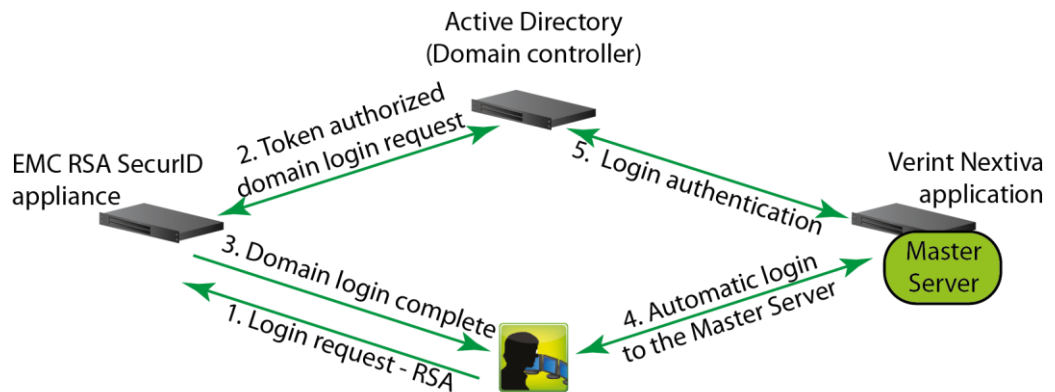


Figure 2. RSA login process

# VMware Technology Overview

## Introduction

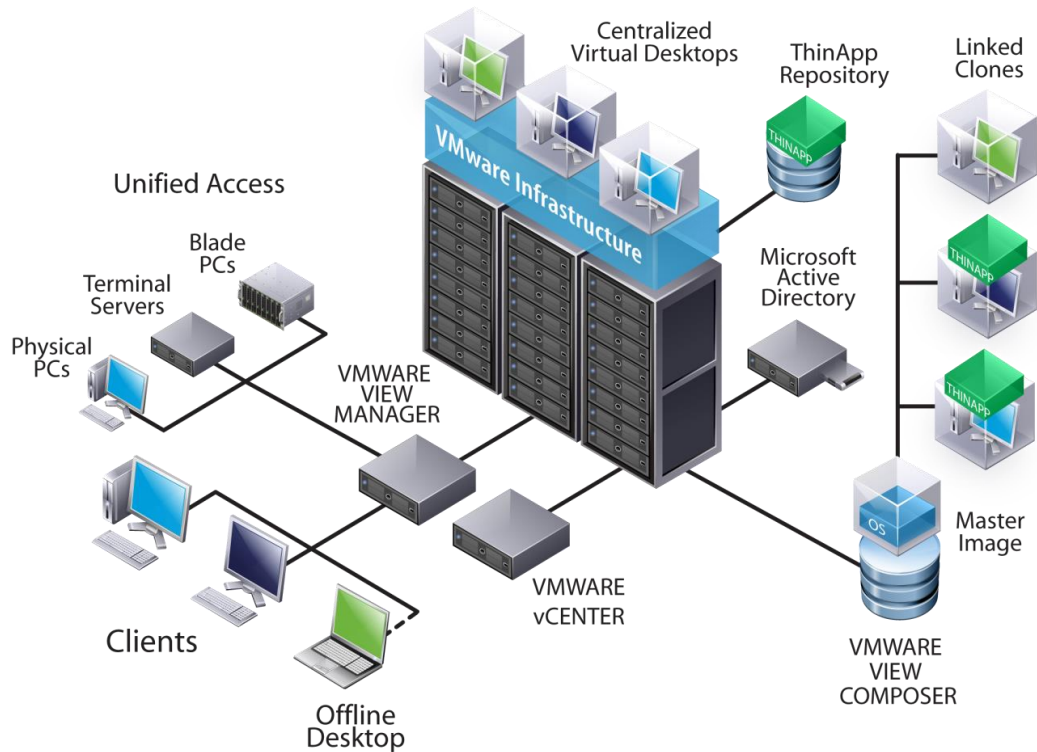
VMware View delivers rich and personalized virtual desktops as a managed service from a virtualization platform built to deliver the entire desktop, including the operating system, applications, and user data. VMware View 4.5 provides centralized automated management of these components with increased control and cost savings. VMware View 4.5 improves business agility while providing a flexible high-performance desktop experience for users across a variety of network conditions.

## VMware View components

To provide a virtual desktop experience, VMware View uses various components, each with its own purpose. The components that make up the View Environment are:

- Hypervisor
- VMware View Connection server
- VMware vSphere vCenter Server/View Composer
- VMware View Security server
- VMware View Transfer server
- Supported database server like Microsoft SQL Server
- VMware View Agent
- VMware View client
- VMware View Admin console
- View PowerCLI
- ThinApp

Figure 3 shows the VMware components described in the following sections.



**Figure 3. VMware components**

### Hypervisor

Hypervisor is used to host the virtual desktops. To get the most out of its features, EMC recommends that you use VMware vSphere 5.0 or greater. The vSphere 5.0 features such as vSphere API for Array Integration (VAAI), Memory Compression, and Ballooning help to host more virtual desktops.

### VMware View Connection server

The VMware View Connection server hosts the LDAP directory and keeps the configuration information for VMware View Desktop Pools, associated virtual desktops, and VMware View. This data can be replicated to other View Connection Replica servers. The Connection server also acts as a connection broker that maintains the desktop assignment. It supports an SSL connection to the desktop using RDP or PCoIP. It also supports RSA® SecurID® two-factor authentication and smart card authentication.

### View Security server

The View Security server is a different type of View Connection server. It supports two network interfaces—one to a private enterprise network and another to the public network. It is typically used in a DMZ and enables users outside the organization to securely connect to their virtual desktops.



## Conclusion

The EMC Storage for Physical Security Solution enabled by Verint's Nextiva products represents an ideal solution for surveillance management and IT infrastructure. The solution provides a flexible and highly scalable infrastructure that can meet a broad range of today's demanding physical security requirements. By leveraging the best-in-class surveillance management software from Verint and advanced IT infrastructure components from EMC, customers can maximize the return on their investment in these crucial platforms.

EMC RSA provides best-in-class user authentication that is compatible with single login domain security. In addition, VMware ESXi reduces the footprint required for our implementation. 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.

### Learn More

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](http://www.EMC.com/solutions/business-need/information-security/physical-security.htm).

## References

### EMC documentation

The following documents, located on the EMC online support website, provide additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your EMC representative:

- *EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series, VMware vSphere 4.1, VMware View 4.5 and VMware View Composer 2.5 — Proven Solution Guide*
- *EMC Infrastructure for Virtual Desktops Enabled by EMC VNX, VMware vSphere 4.1, VMware View 4.5, and VMware View Composer 2.5 — An Architectural Overview*
- *EMC Performance Optimization for Microsoft Windows XP for the Virtual Desktop Infrastructure—Applied Best Practices*
- *Deploying Microsoft Windows 7 Virtual Desktops with VMware View—Applied Best Practices Guide*
- *EMC Infrastructure for Deploying VMware View in the Enterprise EMC Celerra Unified Storage Platforms—Solutions Guide*

### VMware documentation

The following VMware documents, located on the VMware website, also provide useful information:

- *Introduction to VMware View Manager*
- *VMware View Manager Administrator Guide*
- *VMware View Architecture Planning Guide*
- *VMware View Installation Guide*
- *VMware View Integration Guide*
- *VMware View Reference Architecture*
- *Storage Deployment Guide for VMware View*
- *VMware View Windows XP Deployment Guide*
- *VMware View Guide to Profile Virtualization*