Why EMC for Virtual Desktop (VDI)
TABLE OF CONTENTS

Executive Summary ........................................................................................................................................... 2
Introduction .................................................................................................................................................. 3
Today’s IT challenge – why organizations are transitioning to VDI .......................................................... 3
The Benefits Are Real: Leveraging VDI ........................................................................................................... 5
Technical Considerations for Successful VDI Implementations ............................................................... 6
EMC’s Supporting VDI Technologies and Solutions .................................................................................... 12
EMC VDI Expertise ....................................................................................................................................... 21
EMC References .......................................................................................................................................... 25

LIST OF FIGURES

Figure 1. Virtual Desktop Concept ................................................................................................................. 4
Figure 2. EMC tiered storage technologies minimize the cost of ownership .................................................. 9
Figure 3. Share, access, and relocate virtual desktops between sites over distance ........................................ 11
Figure 4. FAST Suite - FAST VP + FAST Cache ......................................................................................... 15
Figure 5. Global Deduplication with EMC Avamar ....................................................................................... 17
Figure 6. VDI Component protection with EMC Avamar ............................................................................... 18
Figure 7. VPLEX Diagram .............................................................................................................................. 19
Figure 8. Cost-effective Desktop Virtualization Platform ............................................................................... 21
Figure 9. EMC VDI Deployment High-level Architecture .............................................................................. 23
In February 2010, an epic snowstorm struck Washington, D.C., and the surrounding area, virtually shutting down the U.S. capital for four days. The U.S. government lost nearly $70 million a day due to lost productivity. While this number is staggering, it could have been as large as $100 million per day. Fortunately, 30% of government workers were able to telecommute, allowing them to continue working during the storm.

President Obama signed the Telework Enhancement Act of 2010, providing agencies greater flexibility in managing our workforce. The Act provides a framework for agencies to better leverage technology and to maximize the use of flexible work arrangements, which will aid in recruiting new Federal workers, retain valuable talent and allow the Federal government to maintain productivity in various situations -- including those involving national security and other emergency situations.

To maximize the impact of this new law, OPM will be coordinating agency efforts to build effective telework programs with three key objectives in mind:

1. **Improve Continuity of Operations (COOP)** - using telework as a strategy to keep government operational during inclement weather or other emergencies

2. **Promote Management Effectiveness** – using telework to target reductions in management costs related to employee turnover and absenteeism, and to reduce real estate costs and environmental impact and transit costs

3. **Enhance Work-life Balance** – using telework to allow employees to better manage their work and family obligations, retaining a more resilient Federal workforce able to better meet agency goals

Virtual Desktop deployment is a key technology to be compliant with the Telework Enhancement Act.
EXECUTIVE SUMMARY

EMC identifies and discusses several technical considerations with regard to consolidated infrastructure, storage, back-up and recovery, security, and business continuity that will directly impact the successful implementation of a robust, resilient and efficient VDI solution. Although EMC solutions are optimized around VMware and its View technology for VDI, EMC products also support other VDI technologies such as Citrix. This paper is purposefully agnostic toward the virtualization layer of the solution. Additionally, this paper does not attempt to address a comprehensive VDI solution, rather we’ve chosen to identify and discuss important components of an overall solution. EMC has reference architectures for VMware and other VDI solutions available and can provide them to the Government upon request. Finally, this paper response references two highly successful VDI projects that have leveraged EMC technologies and solutions that could be used as a starting point for any subsequent enterprise-wide deployment. The first is a Citrix-based solution developed for the Citrix Executive Briefing Center in Santa Clara, California and the second is EMC IT’s own internal implementation of a VMware-based VDI solution.

EMC solutions and technology provide the foundation for enterprise class and enterprise-wide VDI solutions – proven through hundreds of customer implementations and tested every day in EMC’s own internal IT infrastructure.
INTRODUCTION

In today’s ever changing IT world, organizations are moving to a more flexible, high-demand, end user platforms utilizing thin, “ultra-thin,” and “zero” client end technology. Virtual Desktop Infrastructure (VDI) is widely considered the solution for administrative ease and flexibility to support their end user computing environments. Robust VDI solutions, based upon enterprise-ready virtual infrastructure technologies throughout the IT stack, can ultimately enable the delivery of desired cloud computing services to the end users. VDI deployments offer well-documented benefits, including improved efficiency, dramatic cost(s) reductions, greater data center flexibility, and more efficient and effective delivery of services. As well as provide the infrastructure for today’s teleworker.

Today’s IT challenge – why organizations are transitioning to VDI

Current physical infrastructures lead to burdensome administrative time, lost data and costly repairs. Physical desktop environments typically have vast amounts of decentralized user data, numerous and varied applications installed on desktop/laptops, and many variations of hardware and software for the IT team to support. This creates costly end user downtime and a heavy IT administrative burden. Some additional challenges of physical infrastructures include:

- **IT Management and Support** - Business continuity, desktop backup, application deployment and compatibility are critical. However, these critical functions are complicated by decentralized business role profiles and non-standard desktop images and patches.
- **Performance** - As increasing numbers of users access applications remotely, performance is often degraded. This issue is compounded if users are unable to access mission-critical applications in a timely fashion. In addition, aging physical machines cannot always accommodate sophisticated computing and storage needs or the heavy bandwidth necessary to provide rich media to end users via thin clients.
- **Data Security** - Securing physical machines is always challenging, but with remote and highly dispersed workers, it is an even more complex and costly proposition.
- **User Convenience** - Today’s users demand the capability to work from anywhere and to either use their own machine(s) or to choose their preferred work platform. Cumbersome physical infrastructures are not nimble enough to accommodate this level of flexibility. In addition to addressing those needs, organizations must resolve deployment delays for patches and next-generation applications on these machines to provide users secure access to network resources.
- **Energy Consumption** - Organizations must balance the need for high-end computing capabilities with the increase in power consumption to satisfy the Departments’ efforts to reduce dependence on fossil fuels and become more energy efficient.
VDI has become the leading solution to resolve many of these issues. One such advantage is a hardware agnostic platform. Companies can utilize existing hardware to expand their lifecycle. Thin, ultra-thin, and zero clients give the advantage of a very small footprint that acts as a conduit to the datacenter for the end user’s VDI image and data. Downtime is minimal, as the VDI software agent can be installed on any machine. This significantly reduces end user downtime and lost productivity. Virtual desktop offers end users the ability to access work-related data and applications from anywhere, at any time.

Application virtualization technology provides another key advantage. This technology allows all applications to be centrally located on a shared server, instead of the physical desktop, saving install time, patching and error resolution. Users can be easily added to application profiles with a few, simple administrative keystrokes.

Finally, with proper design and configuration, all user data is centrally located back in the data center. This gives companies both the flexibility and freedom to be able to quickly restore end users within minutes, instead of hours/days depending on the hardware issue.

For large organizations, that are embracing these technologies offers many advantages, including reduced capital expenditures, increased savings, enhanced data security and the ability to harness user’s potential, while offering them a balance in their work and personal lives.

![Virtual Desktop Concept](image-url)
The Benefits Are Real: Leveraging VDI

The administrative ease and flexibility is a dramatic change in the way that addresses the everyday needs of the user. EMC solutions and technology provide the foundation for enterprise class and enterprise-wide VDI solutions – proven through hundreds of customer implementations and tested every day in EMC’s own internal IT infrastructure.
TECHNICAL CONSIDERATIONS FOR SUCCESSFUL VDI IMPLEMENTATIONS

The challenges related to traditional desktop deployment and day-to-day administration include lost laptops containing corporate data, security breaches related to viruses or hackers, and simply ensuring IT resources can maintain the required service level agreements (SLAs). In addition to the challenges of operational management, IT must also consider implications of broader system wide issues such as compliance, corporate governance, and business continuity strategies.

By decoupling the desktop from the underlying hardware and operating system, you will be able to provide users choice and control of the client device used (independent of the hardware operating system). In this section, we discuss several critical technical considerations for designing and deploying successful VDI solutions. Our focus is primarily with respect to the back-end infrastructure and capabilities in the enterprise data center(s) supporting the VDI solution and associated thin, ultra-thin, and zero state clients.

LEVERAGING CONVERGED INFRASTRUCTURE ARCHITECTURE FOR THE VDI

Today, large enterprises are faced with growing costs and security concerns created by the quantity and diversity of personal computers can deploy a secure, cost effective, and flexible virtual desktop environment as a converged infrastructure. A converged infrastructure, by definition, leverages pooled IT resources to provide flexible IT capacity, enabling the seamless, real-time allocation of IT resources in line with demand from business processes. This is achieved by using server virtualization technology to pool computing resources wherever possible, and allocating these resources on-demand using automated tools. Converged infrastructure enables dynamic load balancing and is a more efficient approach than keeping massive computing resources in reserve to run tasks that take place, for example, once a month, but are otherwise under-utilized.

When considering the consolidation of an enterprise desktop environment into a converged infrastructure architecture, organizations should be aware that converged infrastructures can provide:

- **High Availability** - Deliver an optimized solution to include servers, data storage devices, virtualization, networking equipment and software for IT infrastructure management, automation, and orchestration.
- **Scalability** - Enable modular virtual desktop growth and the ability to scale up resources while keeping hardware changes to a minimum.
- **Performance** - Offer balanced I/O, bandwidth and storage and network capacity and provide a quantifiable set of performance and service standards that can be aggregated in measured increments.
- **Flexibility** - Provide foundation for IT organizations to create service catalogs and templates as a repeatable process, as well as accelerate application traffic over the wide area network from the cloud-hosting data center and deliver the even distribution of workloads across two or more resources in order to obtain optimal performance and utilization while averting overloads.
• **Security** - Securely support various workloads/virtual machines and their corresponding application requirements and optimize resource sharing while providing sufficient levels of Quality of Service (QoS) throughout the shared environment.

• **Management / Orchestration** - Provide an extensible management and orchestration model based on industry-standard tools, APIs, and methods.

• **Data Integrity / Reliability** - Supports multiple Redundant Array of Inexpensive Disks (RAID) levels simultaneously including RAID level 1, 5, 6, 10 and data clustering.

• **Functionality** - Rapidly provision and decommission virtual desktop infrastructures.

• **Environmental** - Capability to deliver efficient power, cooling and footprint profiles.

• **Simplified Management** - Including servers, network, and storage whether co-located or distributed throughout the data center.

A converged infrastructure approach can simplify the management behind the firewall, streamline updates to the operating system and patching of applications, more adequately address compliancy matrix requirements, support more efficient and timely application migrations, and provide support from a central location. By establishing a scalable and flexible, shared pool of pre-configured and integrated computing, networking and storage resources in a virtualized environment, customers can benefit significantly in the following ways:

• **Business Enablement** – Increased business agility and responsiveness to changing priorities; improve speed of deployment and the ability to address the scale of global operations with business innovation.

• **Service-based Business Models** – Ability to operate IT as a service.

• **Facilities Optimization** – Lower energy usage; better (less) use of data center real estate.

• **IT Budget Savings** – Efficient use of resources through consolidation and simplification.

• **Reduction in Complexity** – Moving away from fragmented “accidental architectures” to integrated, optimized technology that lowers risk, increases speed and produces predictable outcomes.

• **Flexibility** – Ability of IT to gain responsiveness and scalability through federation to cloud service providers while maintaining enterprise-required policy and control.

**Enterprise Compute and Network Layer for the VDI**

An effective virtual desktop infrastructure can benefit from a robust enterprise-ready compute and networking architecture that is an integrated, scalable, and manageable platform – one where all resources are managed from a unified management domain. The simplified architecture reduces acquisition costs, enables more efficient power use, increases business agility, and reduces ongoing operational costs. Technical considerations include:
• **Exceptional Control and Security of Centralized Desktops** – Provides visibility and security for the network all the way to the virtual machine. Each virtual machine is configured with the policy, security, network, and application optimization profile specific to that virtual desktop. These profiles stay with the virtual machine and desktop even as the virtualization layer moves it across the data center between virtual machine clusters, helping ensure continuous protection of the desktop and its data and applications.

• **Dynamic VDI Provisioning and Deployment** - Enables rapid provisioning and decommissioning of desktops. The auto-provisioning features built into the converged infrastructure support rapid provisioning and decommissioning of resources, enabling IT administrators to create and provision virtual desktops much faster than traditional VDI environments.

• **Outstanding User Computing Experience** - Provides a lossless 10 Gigabit Ethernet ultra low-latency Ethernet fabric that converge LAN and multiprotocol storage traffic, helping ensure high levels of storage array throughput and IOPS for primary and replicated user desktops, applications, and data.

• **Control Desktop TCO** - A simplified architecture, stateless computing, and service profiles operational model enables drastically reduced cycle time for provisioning of virtual desktops.

**Enterprise Shared Storage for the VDI**

An effective virtual desktop infrastructure requires the right hardware, including a robust enterprise-ready shared storage architecture. Technical considerations for why robust enterprise-ready shared storage should be deployed in a VDI architecture include:

• **Reliability and Redundancy** - Automated services and failover of those services without interruption to the users depends upon highly reliable and redundant storage. Storage hardware should provide the infrastructure to achieve the “five 9s” availability required by most of today’s enterprise VDI-related service level agreements (SLAs).

• **Performance** - Storage performance is vital in a virtual desktop infrastructure. Performance needs to be addressed at all storage tiers. High-performance disks such as, Serial Attached SCSI (SAS) or solid-state Flash storage should be considered for high I/O, disk-bound applications such as databases. Lower-tier storage can benefit from the generous, low-cost space that is available in slower SATA drives. Performance within virtual infrastructures is also improved from advances in storage-related technologies such as automated movement of data between storage tiers, as required, based upon both pre-determined and real-time adjusted policies.
Figure 2. EMC tiered storage technologies minimize the cost of ownership

- **Expandability** - Storage scalability is also very important to virtual desktop infrastructure. A simple flexible and scalable hardware architecture is critical for systems to independently scale up capacity and performance as required. An expandable storage design that also includes a simplified component architecture will minimize failure points and provide transparent, non-disruptive upgrade and component maintenance.

- **Storage Communication Protocols** - Choosing the right storage protocol (i.e., iSCSI, FC, or NFS) is an important consideration for virtual desktop infrastructure. Since requirements change over time, customers should consider expanding their future storage communication protocol options by deploying a storage framework that supports all three protocols by using a unified shared storage platform.

- **Advanced Storage Features** - Storage implementations for VDI deployments should consider leveraging a unified shared storage infrastructure, which is required to take advantage of features such as distributed resource scheduling, live migration of virtual machines from one virtual server to another, high availability, and fault tolerance.

**SECURING THE VIRTUAL DESKTOP ENVIRONMENT**

The hosted virtual desktop environment is a strategic and valuable investment that provides organizations with numerous benefits, including the ability to enhance security. Yet, it is still an investment that needs to be managed and secured. For example, as users gain access and work with sensitive information on a virtual desktop, that information can still be put at risk.

Managing risk associated with information in a virtual desktop environment is just as important as managing risk associated with data anywhere within the IT infrastructure. Without appropriate access and data controls in place, organizations could still expose sensitive information to users who should not have access to it. Organizations that deploy VDI solutions are still confronted with security challenges and need to implement the proper controls to address the following security objectives:

- **User Authentication** - Enterprise VDI solutions should be capable of authenticating users trying to gain access to virtual desktops. Validating the identity of users before allowing them to access information and applications is critical. This is especially true in a hosted virtual desktop environment where
users require access anytime, anywhere, often requested through devices over which the enterprise has little control. Positively establishing the identities of users prior to granting access to a virtual desktop, particularly to those users with administrative access and privileges, is an essential security objective.

- **Data Controls** - Enterprise VDI solutions should ensure that users handle sensitive information appropriately during a virtual desktop session. It is critical that such solutions be able to discover sensitive information, such as regulated information and intellectual property, and apply security policies on end user handling of sensitive data in use during a virtual session.

- **Monitoring and Reporting** - Enterprise VDI solutions should be capable of identifying anomalies and vulnerabilities such as inbound and outbound traffic summaries associated with sensitive assets within the hosted virtual desktop environment. They should also be capable of collecting and correlating security information and event management data from across the VDI architecture, monitoring adherence to policy across the infrastructure, and sending alerts when deviations from baseline activity occur.

- **Security Configuration and Vulnerability Management** - Unplanned change is the leading cause of many IT security and compliance incidents. While centralizing end points as virtual machines in the data center simplifies the process of hardening, antivirus updates and patching, ensuring that these processes are properly functioning and that configurations are not a source of security risk is critical. For many organizations, endpoint change management is a major challenge and having a tool that can automate the process of identifying configuration changes that violate policy can help reduce security risk. Enterprise VDI solutions should be capable of maintaining security configuration of the virtual end points and detecting and remediating vulnerabilities promptly across the VDI architecture.

**Optimizing Backup and Recovery of the Virtual Desktop Environment**

As larger numbers of thin, ultra-thin, and zero client end user devices are deployed in the VDI enterprise and the total amount of data stored on virtual machines and desktops increases, traditional backup approaches quickly become insufficient. Traditional backup solutions require a rotational schedule of full and incremental backups, which move a significant amount of redundant data week over week. Because of the unnecessary movement of data, enterprises are often faced with backup windows that roll into production hours, network constraints, and too much storage under management. Specifically in virtual desktop environments, server consolidation can mean overlapping backup windows and heavy impact on hardware resources.

Over the last decade, disk storage has been used to augment traditional backup approaches, but disk solutions that are designed to replace tape libraries and media solve only a fraction of the data protection challenges faced by enterprises.

An important consideration when deploying enterprise VDI backup and recovery solutions is source-based data deduplication technology. Source-based data deduplication delivers fast and efficient protection for virtual desktop environments. Source-based deduplication protects virtual machines by deduplicating data at the
source, so that only new, unique sub-file variable length data segments are sent during daily full backups. This dramatically reduces the daily impact on the virtual and physical infrastructure by up to 500 times as compared to traditional full-backup methods. While traditional backup software moves upward of 200 percent of the primary backup data on a weekly basis, source-based deduplication moves as little as 2 percent on the same seven-day period, removing backup bottlenecks and enabling even greater levels of physical server consolidation.

ENSURING DISASTER RECOVERY AND BUSINESS CONTINUITY OF THE VIRTUAL DESKTOP ENVIRONMENT

Business continuity and disaster recovery are critical for ensuring VDI service level agreements are met. To ensure uptime and accessibility, the infrastructure, applications, and data associated with virtual desktops must be available 24x7. As server and application virtualization has evolved to allow hardware resources to be pooled into resource groups and dynamically allocated for virtual desktops, storage has also evolved beyond the point of simple consolidation into virtual storage. Customers planning to deploy enterprise-wide VDI solutions should consider implementing storage federation technology.

Storage federation enables IT to quickly and efficiently support the business through pools of resources that can be dynamically allocated, creating active/active storage between data centers. The benefits of storage federation for virtual desktop include:

- Sharing of the same data between data centers
- Relocation of virtual desktops between data centers without downtime
- Improved user response time to changes in configuration and workload
- Automated disaster recovery and disaster avoidance

![Figure 3](image)

**Figure 3.** Share, access, and relocate virtual desktops between sites over distance
EMC’s Supporting VDI Technologies and Solutions

In this section, we provide an overview of EMC’s supporting VDI technologies and solutions, as well as their benefits, with respect to the technical considerations discussed in Section II.

Converged Infrastructure – VCE’s Vblock Infrastructure Platforms

VCE, a joint venture formed between Cisco and EMC, with investments from VMware and Intel, offers a completely integrated solution of pretested, operational systems known as the Vblock Infrastructure Platform. This completely integrated IT offering combines the latest virtualization, networking, computing, storage, security, and management technologies with end-to-end vendor accountability.

Vblock platforms are the industry’s first completely integrated IT offering that combines networking by Cisco switches; computing power by Cisco Unified Computing System (UCS); virtualization by VMware vSphere and vCenter Server; storage by EMC Symmetrix VMAX or EMC Unified VNX; security by RSA enVision and RSA SecurID; and management by EMC Ionix Unified Infrastructure Manager.

Vblock infrastructure platforms are enterprise- and service provider-class IT infrastructure pre-engineered, tested, and validated units to deliver a defined performance, capacity, and availability Service Level Agreement (SLA). Vblock platforms streamline IT infrastructure acquisition, deployment, and operations. This converged infrastructure enables rapid virtualization deployment and offer repeatable units of construction based on matched performance, operational characteristics and discrete requirements of power, space, and cooling. Repeatable design patterns facilitate rapid deployment, integration, and scalability. Vblock platforms offer varying storage capacity options and processing and network performance, and they support such incremental capabilities as enhanced security and business continuity.

Benefits of deploying Virtual Desktop Infrastructure on Vblock Infrastructure Platforms include:

- **Modular Virtual Desktop Growth** - IT managers can easily add more virtual desktops as their needs grow simply moving to larger or adding more Vblock Infrastructure Platforms.
- **Rapid Provisioning and Decommissioning of Desktops** - Deploy and decommission virtual desktops much faster than traditional virtual desktop infrastructure (VDI) environments.
- **Simplified Management** - Enables simplified management of the servers, network and storage whether co-located or distributed around the world.
- **Self-curing Architecture** - Accommodates unplanned events such as spikes and boot storms to ensure a consistent high performance virtual desktop user experience.
Support thousands of Virtual Desktop Users on a Single Vblock - A single Vblock consolidated high-density infrastructure can support thousands of VDI users.

Enhanced Security - All desktops are now centrally located in the datacenter(s) so there is a reduced risk of theft or lost laptops.

Improved Mobility - Users can access their virtual desktop at any time from nearly any device.

Efficient Management - Desktops can now be updated in minutes without affecting user settings, data or preferences; includes an extensible management and orchestration model based on industry-stand tools, APIs and methods.

Failure Scenarios - Able to Contain, Manage and Mitigate Failure Scenarios in hardware and software environment due to the Vblock platform design and integration.

The Vblock Infrastructure Platform heralds the convergence of network and compute layers, which simplifies data center manageability and improves flexibility and utilization. Vblock will allow you to focus more on delivering services to end users, and less on how to piece together disparate IT components in order to deploy a secure, highly available, compliant and scalable VDI environment.

**Enterprise Shared Storage for VDI – EMC’s Unified Storage**

EMC’s Unified VNX family of storage arrays can provide the robust enterprise-ready shared storage foundation necessary for today’s effective and efficient virtual desktop solutions. EMC’s Unified VNX storage platforms can provide the necessary reliability and redundancy, performance, expandability, storage communication protocols, and advanced storage-related technologies.

The EMC VNX family delivers industry-leading innovation and enterprise capabilities for file, block, and object storage in a scalable, easy-to-use solution. This next-generation storage platform combines powerful and flexible hardware with advanced efficiency, management, and protection software to meet the demanding needs of today’s enterprises. All of this is available in a choice of systems ranging from affordable entry-level solutions to high-performance, petabyte-capacity configurations servicing the most demanding application requirements.

The EMC VNX series is architected to provide “5-9s” availability in mission-critical business environments with built-in high availability features such as redundant components with no single point of failure, RAID, multipath data access, mirrored
cache, automated system diagnostics, and global hot spare technology. VNX availability and redundancy features include:

- Up to 12.8 gigabytes of mirrored write cache, where each storage processor contains both primary cached data for its LUNs and a secondary copy of the cache for its peer storage processor.
- Battery backup to allow for an orderly shutdown and cache de-staging to vault disks to ensure data protection in the event of a power failure.
- RAID protection levels 0, 1, 1/0, 3, 5, and 6 - all of which can co-exist in the same array simultaneously to match different protection requirements.
- Proactive hot sparing enhances system robustness and delivers maximum reliability and availability.
- Redundant data paths, power supplies, drive connections, and storage processors—all with non-disruptive field-replacement capabilities.
- Continuous system monitoring, call-home notification, and advanced remote diagnostics.

EMC’s VNX series provides an improved storage performance solution for virtual desktop infrastructure. Performance is maximized by leveraging multiple storage tiers and EMC’s Fully Automated Storage Tiering (FAST) intelligent auto-tiering software. FAST dramatically improves performance and maximizes storage efficiency by leveraging the following:

- **FAST Cache** - An extendable cache of up to 2.1TB, FAST Cache gives a real-time performance boost by ensuring that hot data is served from the highest-performing Flash drives for as long as needed. FAST Cache provides improved performance for most workload types, especially those that experience frequent and unpredictable large increases in IO activity, such as VMware View boot storms, and is a cost effective solution allowing more extensive usage of high capacity NL-SAS drives. FAST Cache improves cache hit rates from the traditional 20-30% up to 60-70%.

- **FAST Virtual Pools (VP)** - As a complement to FAST Cache, FAST VP optimizes storage pools on a regular, scheduled basis. With FAST VP, administrators define how and when data is tiered using policies that dynamically move most active data to high-performance drives (e.g. Flash), and less active data to high-capacity drives, all in one-gigabyte increments for both block and file data. FAST VP is the EMC VNX feature that allows a single LUN to leverage the advantages of Flash, SAS, and Near-line SAS drives through the use of pools.
The EMC VNX storage is based on a multi-node architecture, which enables the systems to independently scale capacity and performance. The EMC VNX is designed with simplified component architecture, minimizing failure points and providing transparent, non-disruptive upgrade and component maintenance, and allowing for storage expansion and capacity to be added non-disruptively.

The EMC VNX storage is a robust, unified platform providing shared storage capabilities. The VNX will enable virtual desktop infrastructures to take advantage of features such as distributed resource scheduling, live migration of virtual machines from one virtual server to another, high availability, and fault tolerance.

**SECURING THE VIRTUAL ENVIRONMENT – RSA SOLUTIONS**

RSA, EMC’s Security Division, has developed security solutions to help organizations reap the security advantages of hosted virtual desktops while addressing the traditional challenges, as discussed in Section II “Securing the Virtual Desktop Environment”, associated with securing user access and data in a virtual desktop environment. These solutions include:

- **User Authentication with RSA SecurID** - RSA SecurID ensures that only trusted identities access virtual sessions and sensitive content. RSA SecurID two-factor authentication generates a new one-time password (OTP) code every 60 seconds making it difficult for anyone other than the genuine user to input the correct token code at any given time. To access their virtual desktop, users simply combine their secret personal identification number (PIN) with the token code that appears on their SecurID authenticator display at that given time. The result is a unique, one-time password that is used to positively assure a user’s identity. RSA SecurID authentication integrates with VDI in two ways: 1) ensuring that only trusted identities access virtual desktop sessions and 2) enforcing user authentication for administrative access to the backend data.
center servers hosting the associated virtual machines. By requiring employees and third parties to use stronger authentication technology, organizations can reduce the risk of exposure in the virtual session by assuring only authorized users gain access to sensitive information through their desktop image.

- **Data Controls with RSA Data Loss Prevention (DLP) Endpoint** - RSA DLP Endpoint discovers sensitive information in VDI deployments, such as regulated information and intellectual property, and applies security policies on end user handling of sensitive data in use during a virtual session. It prevents data leakage by discovering sensitive data and managing how it is used on the virtual desktop through monitoring and controlling actions such as printing, saving, copying, and emailing. RSA DLP Endpoint can be easily deployed and managed, regardless of the geographic location wherever the endpoint device resides. From a centralized location, administrators can configure policies and enforce controls across all devices in the virtual environment. Administrators can determine automated actions to be taken if policies are violated – for example, specific actions can be blocked and policy actions can be created to inform users of corporate policies. RSA DLP Endpoint can also initiate an incident tracking workflow process to log and monitor the data at risk.

- **Monitoring and Reporting with RSA enVision** - The RSA enVision platform is a security information and event management solution that offers a scalable, distributed architecture to collect, store, manage, and correlate event logs generated from the VDI infrastructure including information from the RSA SecurID and RSA DLP Endpoint solutions. With RSA EnVision, customers can:
  - Monitor information security policies across virtual machine operations, cluster and resource management, virtual network infrastructure, storage, users, groups and permissions to assure corporate compliance; user activities on virtual desktops, as well as administrator activities within the VDI environment.
  - Collect, protect and store data in a secure and non-filtered fashion.
  - Establish baseline levels of activity for the entire virtual environment to define “normal activity” and detect “abnormal” or unusual activity.
  - Send alerts when deviations from baseline levels or patterns of malicious activity across multiple, disparate devices are detected.
  - Perform forensic analysis to correct policies and settings on systems and provide a debug-level view of all changes and the effect they have on the environment.
  - Establish a closed-loop, incident management workflow to ensure that incidents are recorded, escalated, and remediated in a timely manner.
  - Gain insight into the traffic and events occurring within the virtual environment from any perspective (including by geography, by users, by system, etc.).
  - Streamline the auditing and reporting process with over 1,400 “out-of-the-box” reports that can be easily customized to meet internal and external compliance requirements.
- **Security Configuration and Vulnerability Management with EMC Ionix SCM**
  - EMC Ionix Server Configuration Manager (SCM) inspects, analyzes and allows remediation of detailed configuration items from servers and workstations, across physical and virtual environments. EMC Ionix SCM monitors virtual desktops, generates automatic alerts when systems need to be fine-tuned to resolve problems or ensure compliance, and can automate common tasks to increase operational efficiency, decrease costs, and ensure secure, compliant and up-to-date configurations. EMC Ionix SCM also offers powerful visibility into the IT infrastructure. High level dashboards provide the right level of information needed to make change, configuration and patch management processes more effective – for example, verifying the deployment of patches and detecting and fixing security threats that arise from incorrect configurations. Organizations can also view details about the changes happening within the virtual environment and track the impact those changes have on service levels and compliance.

Security should never be a hindrance, but rather help organizations accelerate their business initiatives. By deploying the right access and data controls, organizations can unlock the value of their investment in VDI, leverage the full capabilities of operating a virtual environment and effectively manage their configuration and compliance requirements.

**DEDUPICATED BACKUP AND RECOVERY OF THE VIRTUAL ENVIRONMENT — EMC AVAMAR**

EMC’s Backup and Recovery Systems (BRS) division provides solutions which simplify data protection in the VDI environment with proven, flexible, and easy-to-use deduplication backup and recovery solutions such as EMC Avamar and EMC Data Domain. These solutions are far and away the most widely deployed and proven backup recovery solutions.

EMC’s Avamar backup software solves traditional backup challenges in virtual desktop environments by reducing the size of backup data at the source enabling backups to complete well within allotted backup windows, providing for quicker restore times and extending organizations’ data retention period through global deduplication. EMC’s Avamar back-up and recovery solution leverages its patented global source-based data deduplication technology that stores only a single copy of sub-file data segments across all sites and servers. This ensures that each unique data segment is backed up only once across the enterprise.

**Figure 5. Global Deduplication with EMC Avamar**
EMC Avamar software quickly and efficiently protects VDI environments by reducing the size of backup data within and across VDI images — using agents in the individual VDI components such as the VDI management servers and Active Directory Server as well as backing up user data and desktop images from any centralized storage. For VDI backups, Avamar eliminates traditional backup bottlenecks caused by the large amount of data that must pass through the same set of shared resources — the physical server’s CPU, Ethernet adapter, memory, and disk storage. Avamar reduces the traditional backup load — up to 200 percent weekly — to as little as 2 percent weekly, dramatically reducing backup times and resource utilization.

Avamar reduces the required daily network bandwidth by up to 500x, allowing organizations to utilize their existing physical and virtual infrastructure for fast, daily virtual full backups and disaster recovery (despite network congestion and other bottlenecks), while minimizing impact of their business applications. Data can be encrypted both in flight and at rest for added security, and centralized management makes protecting thousands of virtual desktops easy. By storing just a single instance of each sub-file data segment globally, Avamar also reduces total back-end backup storage by up to 50x for cost effective, long-term, disk-based recovery. To protect the integrity of the data, Avamar runs an internal operation, called Avamar Hash Filesystem check, which validates the integrity of a specific checkpoint. This validates the reliability of the backup which can be used for a system rollback if needed.

To protect the Virtual Desktop Clients and user home directories, EMC Avamar utilizes an NDMP Accelerator node, to reduce backup times by performing a level-1, incremental forever approach, after the initial level-0 full backup. These incremental dumps enable Avamar to dramatically reduce backup time and the impact on NAS resources and networks.

Figure 6. VDI Component protection with EMC Avamar
DISASTER RECOVERY AND BUSINESS CONTINUITY OF THE VIRTUAL DESKTOP ENVIRONMENT WITH EMC VPLEX

EMC VPLEX is a SAN-based federation solution that removes physical barriers within a single and multiple virtual data centers. EMC VPLEX is the first platform in the world that delivers both local and distributed federation. VPLEX Local enables cooperation of multiple storage arrays within a single data center. VPLEX Metro and VPLEX Geo extend the federation of data centers across distance.

VPLEX, a solution for federating both EMC and non-EMC storage, resides between the servers and heterogeneous storage assets and introduces a new architecture with unique characteristics:

- Scale-out clustering hardware can start small and grow big enabling predictable service levels and response times for the virtual desktop.
- Federation enables online movement of the virtual desktop between datacenters for ultimate flexibility.
- Advanced data caching utilizing large-scale SDRAM cache to improve performance, reduce I/O latency, and array contention.
- Distributed LUN's for automatic sharing, balancing, and failover of I/O between data centers across the VDI environment.
- A consistent view of one or more LUNs across VPLEX Clusters separated either by a few feet within a data center or across asynchronous distances, enabling new models of high availability and workload relocation.

VPLEX Local is designed for use in a single data center, while VPLEX Metro allows customers to connect two VPLEX clusters together within synchronous distances and move virtual desktops or share data between the data centers. VPLEX Geo increases the distance between data centers to asynchronous distances.

VPLEX is designed as a cluster and two clusters can be connected together federating both data centers together for a VPLEX Metro or a VPLEX Geo configuration. Once this is established, customers can have immediate access to their data, because VPLEX can present the same data at each cluster’s location simultaneously.
Customers can automatically balance loads through VPLEX, using storage and compute resources from either cluster’s location. Also, when combined with server virtualization, VPLEX allows customers to transparently move and relocate virtual machines and their corresponding applications and data over distance. This provides a unique capability that allows customers to relocate, share, and balance virtual desktops between sites—which can be within a campus or between data centers up to 100 kilometers apart with VPLEX Metro, or further apart across asynchronous distances with VPLEX Geo. Note that for VPLEX Geo, the distance supported far exceeds 100 km, up to a 50 millisecond response time.

With VPLEX, customers no longer need to spend significant time and resources preparing to move virtual desktop data. Similarly, with VPLEX, customers don’t have to accept a forced outage and restart the application after the move is completed. Instead, a move can be made instantly between sites, over distance, and the data remains online and available during the move—no outage or downtime is required. VPLEX also provides a single, all-inclusive interface for both EMC and non-EMC arrays. So even if customers have a mixed storage environment, VPLEX still provides an easy, all-encompassing solution. Additionally, although VPLEX works with server virtualization to relocate virtual machines over distance, all VPLEX products can also non-disruptively move and relocate physical application data across heterogeneous back-end arrays.
EMC VDI EXPERTISE

EMC solutions, professional services, and application experts have supported the deployment of numerous and varied enterprise-ready VDI solutions customers across the globe over the past several years. The following background references are provided to highlight how EMC solutions were leveraged to provide robust foundations for successful VDI solutions.

**EXAMPLE 1: A CLOSER LOOK AT ONE OF EMC’s VDI REFERENCE ARCHITECTURES**

As an example, the “Reference Architecture: EMC Infrastructure for Virtual Desktops Enabled by EMC VNX Series (NFS), Cisco UCS, VMware vSphere 4.1, and Citrix XenDesktop 5” document describes the building and demonstration of the functionality, performance, and scalability of virtual desktops enabled by the EMC VNX series, Cisco UCS, VMware vSphere 4.1, and Citrix XenDesktop 5. This solution (logical architecture is shown in the figure below) is built on Machine Creation Services (MCS) in XenDesktop 5, and a VNX5300 platform with multiprotocol support, which provides Network File System (NFS) storage for the VMware datastore, and CIFS-based storage for user data. This reference architecture builds a 1,000-seat Citrix XenDesktop 5 environment on VNX and uses the new features of this platform to provide a compelling, cost-effective desktop virtualization platform.

This solution demonstrates how to use EMC VNX5300 and Cisco UCS B-Series platforms to provide the storage and compute resources for a Citrix XenDesktop 5 environment by using Windows 7 virtual desktops provisioned by Machine Creation Services (MCS).

Planning and designing the storage infrastructure for Citrix XenDesktop environment is a critical step because the shared storage must be able to absorb large bursts of
input/output (I/O) that occur over the course of a workday. These bursts can lead to periods of erratic and unpredictable virtual desktop performance. Users may adapt to slow performance, but unpredictable performance will frustrate them and reduces efficiency.

To provide a predictable performance for a virtual desktop infrastructure, the storage system must be able to handle the peak I/O load from the clients while keeping response time to a minimum. Designing for this workload involves the deployment of many disks to handle brief periods of extreme I/O pressure, which is expensive to implement. This solution uses EMC VNX Fast Cache to reduce the number of disks required.

VNX support for NFS also enables the use of VMware NFS datastores for cost effective, easily deployable storage for the desktop virtualization platform.

This reference architecture, and its associated proven solution document, further describes in detail the recommended best practices (and rationale) with respect to storage layout, network configuration, and high availability and failover aspects, tests specific use cases, and articulates the benefits of such a solution.

**EXAMPLE 2: EMC IT’S OWN JOURNEY TO CLOUD-BASED VDI DEPLOYMENT**

EMC Corporation is a large global enterprise with more than 47,000 employees working across 150 locations in 49 countries. EMC’s internal IT infrastructure and processes play an important role in increasing the productivity of the EMC workforce. As part of its own private cloud strategy, EMC IT has been successfully virtualizing its own servers and storage systems over the past several years. Creating a virtual desktop environment is a natural step in our own ability to deliver services from a cloud environment that will allow EMC IT to better address workforce challenges, improve operational and cost efficiencies, and transform the business. EMC IT is currently in the process of deploying a virtual desktop infrastructure solution using a variety of EMC technologies including EMC storage, VMware and other third party components.

The first production sub-phase began in Q1 2011. EMC IT has developed a comprehensive architecture based on best-in-class EMC and partner technologies for implementation. The architecture includes solutions for centralized, shared storage, security, backup and management. EMC IT is also leveraging deduplication and compression technology to significantly reduce TCO in the areas of primary storage and backup. EMC IT’s production final goals include: centralized management, secure desktop environment, rapid deployment, extended desktop lifecycle, and ROI and cost avoidance. Several of the key technologies leveraged include:

- **Vblock 2 infrastructure architecture** - EMC IT has employed a highly scalable Vblock 2 architecture in its initial production rollout of up to 5,000 task workers. It expects to support another 40,000 users in the coming years.

- **EMC Celerra Home Directory** - EMC IT has provided users with a universally accessible home drive, regardless of whether they are logging in from a virtual desktop or a standard laptop. The Home Directory feature also enables compression on user data, so it saves space. This has enabled EMC IT to reduce total storage consumption by almost 50 percent, as well as significantly
reduce administrative overhead by eliminating manual provisioning and configuration of user profiles.

- **VMware View with PCoIP** - By efficiently adjusting the balance of the workload between the server and client, the PCoIP protocol enables EMC IT to enhance the end-user experience dynamically in response to available bandwidth and communication channel latency.

- **EMC Avamar for online backup of end-user data with a user-initiated restore capability** - Installing Avamar agents on a client image provides end users with the ability to restore missing files themselves, which reduces the number of support calls. To capture the initial snap, EMC IT is using Avamar NDMP accelerators to back up data directly from the Celerra Data Mover. In the case of a full restore, NDMP provides the end user with fast restore capabilities (with the help of a backup administrator). This also reduces the Avamar agent’s task of pushing initial backup data to the grid.

- **RSA technologies such as RSA DLP and RSA SecurBook** - These technologies ensure that information remains secure within the organization’s boundaries.

**EXAMPLE 3: CITRIX EBC: A VDI ENVIRONMENT ENABLED BY EMC UNIFIED STORAGE AND CITRIX XENDESKTOP**

The Citrix Executive Briefing Center (EBC) in Santa Clara, California, supports Citrix’s global sales force, its partners, and hundreds of customer demonstrations each month. Among the many product demos, Citrix displays the production environment of its XenDesktop product that delivers virtual desktops and applications to its top executives. To meet the efficiency, scalability and reliability challenges of this production XenDesktop implementation, Citrix has deployed a shared storage infrastructure that can be optimized for desktop performance, to meet service- level agreements (SLA),
and to ensure a quality experience for Citrix's most demanding virtual desktop users including the company’s top executives.

After reviewing EMC's proven solution and reference architecture for Citrix XenDesktop with EMC Unified storage platforms, and advanced technologies like Flash and FAST Cache, Citrix chose an EMC Unified storage solution to power its own Citrix XenDesktop virtual infrastructure. The EMC Unified storage solution uses advanced technologies such as Fully Automated Storage Tiering (FAST VP), FAST Cache, and Enterprise Flash Drives to deliver a scalable, reliable, and performance-optimized solution that meets the SLAs imposed by its users. Virtual desktop environments increase security and simplify management because the infrastructure is in a firewall protected, centralized datacenter that is easily managed by local resources. The combination of XenDesktop and EMC Unified storage technology enables Citrix to realize a secure desktop infrastructure while reducing operational and capital expenses.
EMC REFERENCES
For more information on EMC and the solutions discussed in this paper, please visit the following pages at EMC.com:

- EMC Storage solutions page  
  http://www.emc.com/products/category/storage.htm
- “Current Capabilities and Future Directions for Fully Automated Storage Tiering” video  
  http://www.emc.com/collateral/demos/microsites/mediaplayer-video/intro-fast.htm
- EMC Virtualization solutions page  
  http://www.emc.com/products/category/virtualization.htm
- VCE’s Vblock Infrastructure Platforms page  
- VNX Unified Storage page  
  http://www.emc.com/products/family/vnx-family.htm
- RSA Solutions page  
  - SecurID page  
    http://www.rsa.com/node.aspx?id=1156
  - DLP Endpoint page  
    http://www.rsa.com/node.aspx?id=3429
  - enVision page  
    http://www.rsa.com/node.aspx?id=3170
- Ionix Server Configuration Manager page  
  http://www.emc.com/products/family/ionix-family.htm
- EMC Backup, Recovery, and Archiving solutions page  
- EMC Avamar page  
  http://www.emc.com/products/detail/software/avamar.htm
- EMC Data Domain page  
- VPLEX page  
  http://www.emc.com/storage/vplex/vplex.htm#