A New Approach to Healthcare Security

Defense in depth strategy powered by VMware NSX safeguards healthcare infrastructure, applications, and devices

WHITE PAPER

vmware®

Table of Contents

Overview

Electronic patient care and health insurance systems contain millions of valuable records, making them an attractive target for intruders seeking to mine sensitive information. Healthcare providers and payers can be seen as "Information Banks", rich with years of customer data due to Regulatory Compliance requirements of retention and imitate nature of the data itself, rather than with physical cash. This makes them tantalizing targets for the nefarious minded. The FBI estimates that each health record is worth $50. Some sources quote even more, upwards of $200. More than 80 percent of healthcare Chief Information Officers (CIOs), Chief Technology Officers (CTOs), and other security leaders polled by KPMG say their organizations have been victimized by at least one cyber attack in the past two years—and many still feel like sitting ducks. The reality for most healthcare CIOs and Chief Information Security Officers (CISOs) is this: today, it is not a question of if, but rather when, their systems will be attacked.

Advanced intrusion continues to succeed because healthcare IT organizations are meeting mandated requirements—from HIPAA to HITECH*—without taking a defense in depth approach to safeguarding data. They have invested heavily in data center perimeter security but find their solutions falling short when they are asked to address critical business questions such as the following:

- How can we improve our security to effort ratio?
- Is security at the perimeter enough to protect our business from data breaches?
- How can we secure network traffic inside the data center?
- How can we quarantine attacks and limit damage to the rest of network—without incurring huge hardware and firewall costs or an outage?

This paper addresses these questions and more about how healthcare organizations handle breaches, including phishing and malware which operate unfettered internally. It also describes how VMware solutions mitigate risks by delivering the comprehensive protections from breaches that today's security-conscious healthcare organizations require.

Key Insights

- Healthcare organizations are targets of large-scale security breaches.
- Healthcare organizations must advance security postures beyond compliance with regulations—e.g., HIPAA and HITECH.
- Leading HIT teams are adopting software-defined solutions and a layered approach to security that delivers not only protections but also strategic business advantages.
- Six critical capabilities comprise best practices security frameworks and deliver significant ROI.
- Defense in depth strategy powered by VMware NSX safeguards HIT infrastructure, applications, and devices.

Healthcare organizations are targets of large-scale security breaches.

Digital attacks have become so broad and sophisticated that the Ponemon Institute coined "2014: A Year of Mega Breaches," and predicted 2015 to be as bad or worse as more sensitive and confidential information and transactions will be moved to the digital space and become vulnerable to attack.[1]

The healthcare industry is a prime target:

- In the U.S. alone, 100 million healthcare records were compromised in Q1 2015.[2]
- The Identity Theft Resource Center tagged healthcare as the source of 33 percent of all listed incidents

---

* Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act enacted as part of the American Recovery and Reinvestment Act of 2009.

1. Ponemon Institute. "2014: A Year of Mega Breaches," January 28, 2015.
2. U.S. Department of Health and Human Services. 2015

nationwide.

- A full 84 percent of healthcare organizations have been breached in last two years.
- A class-action lawsuit is typically filed only one week after a breach is reported.

"Absolute security will never be a guarantee. Cyber attacks should be considered a constant threat and we need better tools and technologies to mitigate the risk and combat the attacks,"[3] according to Sutter Health CIO John Manis in a recent Scottsdale Institute CIO Summit report.

While 81 percent of those surveyed by KPMG have been recently compromised by malware, botnets, or other cyber-attacks, only 53 percent of providers and 66 percent of payers say they feel adequately prepared for a cyber attack.[4]

Other breaches also concern enterprise leaders, according to the Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, research independently conducted by Ponemon Institute LLC in May 2015. (Figure 1)

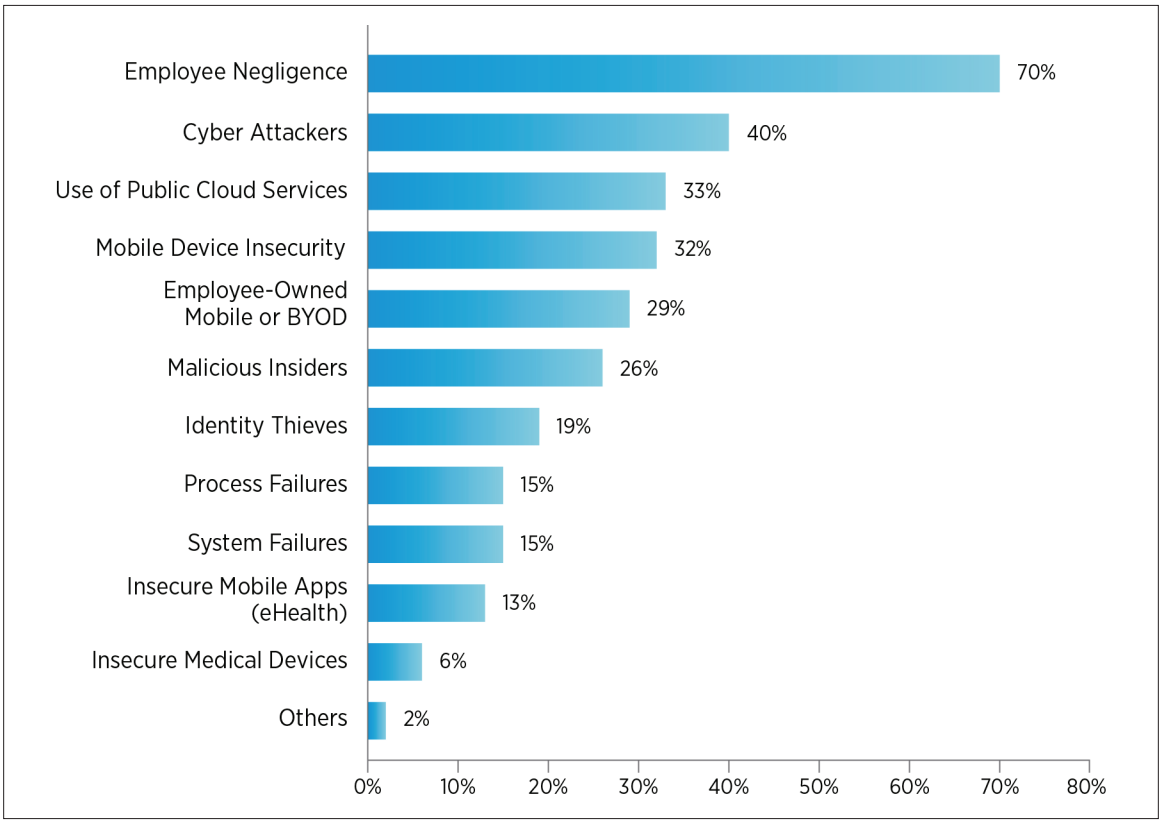

Figure 1. Most Concerning Breaches

Employee negligence, use of public cloud services, malicious insiders, and process failures can be mitigated with strong, auditable user-access controls and micro-segmentation while cyber attackers and identity thieves can be thwarted with strong encryption tied to boundary controls. By using data sovereignty to ensure restricted or regulated data, certain physical areas are protected regardless of who is requesting the data.

Healthcare organizations must advance security postures beyond regulation compliance.

Healthcare organizations working to meet more stringent government and industry requirements cannot predict

3. HealthIT Security. "Why Healthcare Security Must Be Top Priority for CIOs," November 24, 2014.
4. Healthcare IT News. "4 in 5 health orgs hit by cyber crooks." August 27, 2015.

the levels to which cyber criminals will go to breach their systems. VMware and its partners provide proven virtualization solutions that help healthcare organizations address the confidentiality, integrity, and availability requirements in HIPAA and HITECH around personally identifiable information. Beyond compliance, VMware and partners also provide solutions to protect healthcare organizations against today's targeted security threats.

VMware solutions support a defense in depth strategy to combat intrusions. An information assurance concept where multiple layers of security controls are incorporated throughout the IT system, a defense in depth approach helps organizations provide redundancies to prevent vulnerabilities in case one or more controls fail.

Most HIT teams have not integrated a full complement of layered protections for their healthcare infrastructure, applications, and mobile devices, which includes:

Platform security	Distributed firewalls, platform hardening, secure lifecycle development
Secure operations and automation	Enterprise policy controls for security, compliance, configurations, and deployment
Virtualization	Interoperable advanced networking and security services
Compliance guidance	Frameworks, validated reference architectures

Leading HIT teams are adopting software-defined solutions and a layered approach to security that delivers not only protections but also strategic business advantages.

New models of patient care require that systems are highly reliable and that data can be accessed by patients, caregivers, and payers anytime, anywhere. A software-defined strategy coupled with a defense in depth approach is one in which all infrastructure is virtualized and delivered as a service, and where protections are ensured at many layers by interoperable security and compliance frameworks. (Figure 1). When HIT organizations embrace this software-defined approach as the foundation for their IT infrastructure and applications, they can more quickly respond to new demands and their systems become more intelligent, automated, mobile, and secure.

In a software-defined environment with multiple layers of security and compliance, all elements of the infrastructure—compute, network, storage, and security—are virtualized to enable applications to leverage a fully virtualized platform that is completely abstracted from the hardware layer. The environment is safeguarded with protections for infrastructure, applications, and end-point devices. Because environments become more application and service focused, HIT organizations not only improve security and data protection, they increase IT efficiency, agility, flexibility, and control.

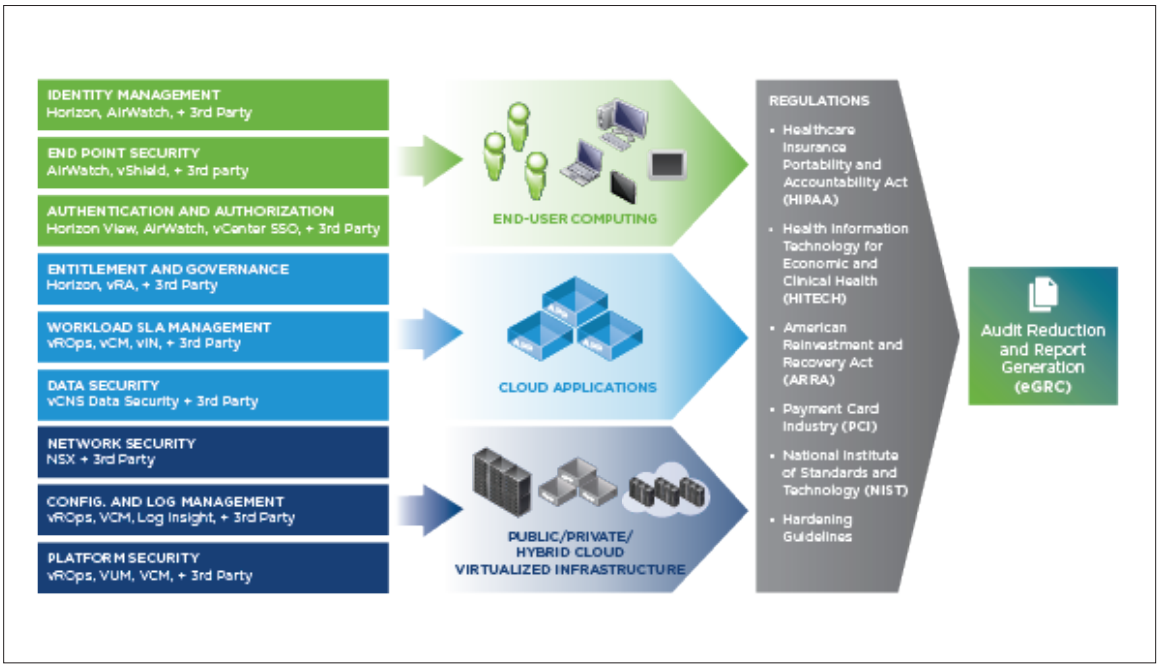

Figure 2: VMare provides an interoperable, multifaceted approach to meet security requirements.

Six critical capabilities comprise best practices security frameworks and deliver significant ROI.

VMware and VMware partner solutions incorporate the six critical capabilities that healthcare organizations need to safeguard their HIT environments. With VMware NSX®, healthcare organizations can define groups (e.g., app) based on things such as OS, workload type (web, app, database) and more. VMware NSX also acts as a platform to deliver best-possible security services, both natively and through more than 30 technology partners. A best practices approach may begin with a passive listener mode to monitor critical activity and determine the status of intra-virtual machine traffic. (Figure 2)

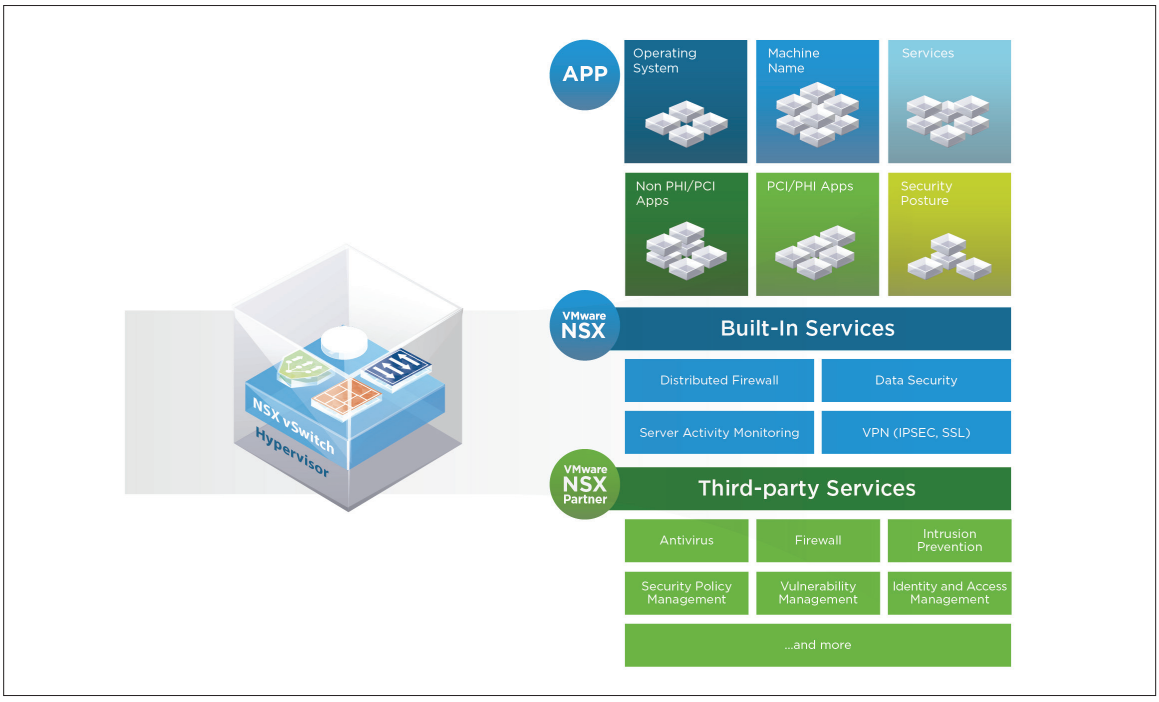

Figure 3: Best-practice, defense in depth security framework enables HIT organizations to remain vigilant by providing proactive protections to address multifaceted challenges

1. Distributed firewalls

The security model that most healthcare organizations use today relies heavily on the border where the network meets the Internet. There are established demilitarized zones with edge firewalls and inspection for systems accessed from outside. Although edge firewall measures protect the systems and can prevent system-level attacks, recent attacks have evolved beyond this method's ability to protect care environments from other methods of breach. Inside the environment is generally considered safe—and most internal systems can talk to just about any other internal system—workstations included, however, this internal openness is now being exploited.

Distributed firewalls are a new approach that brings strength to data center security by tying flexible security policies to individual workloads or workload groups. If a threat gets inside the network, VMware NSX contains and blocks the threat's lateral movement to other servers. This dramatically reduces the attack surface and risk to the business. HIT teams are using distributed firewalls (also known as micro-segmentation) to solve a significant problem that was operationally infeasible with traditional firewalls, and have reported doing so at approximately one-third the cost.

Some examples of workload segmentation include distributed firewall for regulated workloads such as PHI and PCI; managing virtual desktops in groups (e.g., external coders); finance, back-office, clinical or external organizations such as affiliates or recently acquired organizations.

Dynamic and distributed policy enforcement at the virtual-machine level dramatically enhances network security. For healthcare organizations that equates to tighter linkages with third-party solutions that mitigate issues such as misconfigured firewall rules. For example, HIT teams can more effectively monitor ports or establish route-specific traffic to an external solution such as Fortinet and Palo Alto Networks for intelligent inspection. With distributed firewalls, healthcare organizations can speed processes when challenged to react to a problem and remediate it quickly, then audit the results to validate protected workloads are in compliance.

* Network Virtualization and Security with VMware NSX." 2015.

Distributed firewalls increase consistency with streamlined operations and auto-deployment. Because security policies are applied to individual workloads, and travel with the workload as it moves around in the data center, portable policy administration is ensured. Moreover, a distributed firewall can improve performance, simplify operations, and create transparency.

Distributed firewalls help to avoid or minimize the costs of a data breach, including engaging forensic experts, in-house investigations, loss of customers from turnover or diminished acquisition rates, providing free credit or identity monitoring subscriptions, customer communications and outsourcing hotline support, and many other costs that can range from several million to more than one hundred million dollars for a single data breach incident.

Traditionally, deploying firewalls to control an increasing volume of East-West traffic inside the data center has been cost prohibitive for many enterprises. Additionally, the sheer number of devices needed and the effort required to setup and manage a complex matrix of firewall rules has made this approach operationally infeasible.

In addition to making micro-segmentation simpler and more secure, VMware NSX delivers significant CapEx and OpEx reductions for this specific use case. Looking at the capital expense alone, VMware NSX enables enterprises to save upwards of 70 percent over purchasing physical firewalls for micro-segmentation. Following is an analysis of the CapEx savings for a typical enterprise that wants to use micro-segmentation for improved control of server-to-server traffic inside the data center. (Table 1)

Environment & Capacity	
Number of VMs	2,500
VMs per CPU	5
CPUs per server	2
Servers	250
% of VMs requiring firewalling controls	40%
Gbps - Average Application thoughput per host	7
Gbps - Required Firewall throughput in Gbps for all VMs	1,750
Gbps - Effective Required Firewall Throughput	700
Firewalls (20Gbps each x2 for HA)	70
Cost if Hardware	
List cost of each 20Gbps Firewall	$135,000
Total Firewall Cost (But Operationally Infeasible)	$9,450,000
Cost if NSX	
NSX List Cost per CPU	$5,995
NSX Total Cost	$2,997,500
1/19/20161/19/20161/19/20161/19/2016	
CapEx Savings with NSX	**$6,452,500**
	68%

Table 1: Distributed Firewall CapEx Savings

2. Proactive, real-time compliance

Many HIT teams spend time developing manual reports just for audit purposes. However, it is much more effective to rely on built-in, real-time audit capabilities to provide proactive rather than reactive compliance. Organizations using real-time compliance solutions can continuously monitor their infrastructure, looking for

and receiving alerts to any changes. As a result, they can proactively address issues and security gaps as they happen which helps better protect the integrity of HIT resources while keeping the organization in compliance. HIT teams can also provide the critical reports required to meet internal and external audits and quickly remediate compliance issues.

VMware and VMware partners including HyTrust provide solutions that support regulatory requirements and workflows. A real-time, automated compliance checking solution, such as VMware vRealize® Air™ Compliance, automates the detection of non-compliant infrastructure against industry best practices and hardening guidelines—without manual effort or custom scripting.

3. Virtual desktops and mobile device management

Using virtual desktop infrastructure (VDI), HIT teams can segment vulnerable desktops from the rest of the data center and mission-critical server workloads. By integrating third-party solutions, such as Imprivata's Single Sign-On and Tap In/Tap Out, healthcare workflows are even easier to support and optimize. Firewalls can be assigned based on logical groupings while distributed firewalls provide isolation and segmentation of specific workloads (see description of distributed firewalls). In addition, VDI helps secure protected health information (PHI) from becoming lost or stolen when a device is compromised by ensuring data remains in the data center. This is especially important for organizations with caregivers working at patient bedsides, in remote clinics, or even from home or while mobile.

With an enterprise mobility management platform, HIT teams have the flexibility to support the unified management of endpoints, end-to-end security from devices to the data center, and seamless integration across enterprise systems. A single platform can provide HIT teams with powerful automation engines so team members can easily manage a growing number of workstations, PCs, tablets, and mobile devices. Through containerization and context-aware VMware NSX policies, HIT teams can protect sensitive corporate data at the user, application, device, and network levels.

Moreover, HIT teams can manage anti-virus and anti-malware policies for virtualized environments using the same management interfaces they use to secure physical infrastructure. Healthcare organizations gain stronger virtualization security with enhanced end-point protection by offloading anti-virus processing to a secure virtual appliance.

4. Automated security and operations

Automation is critical to a successful security and cloud strategy. Healthcare organizations can proactively monitor, alert, troubleshoot, and resolve performance and operational issues before they affect end users by integrating application and infrastructure performance data for greater visibility into healthcare IT systems. Predictive analytics, powerful visualization, and progressive integration capabilities across physical, virtual, and cloud infrastructures increase the likelihood of finding and resolving issues quickly.

Additionally, HIT teams can develop security policies and blueprints to ensure deployed regulated workloads are always in compliance. Within a single portal, virtual network rules can be created, managed, and automated, and HIT teams can enable self-service with confidence. Troubleshooting and forensics tools aid in management, supporting the virtual network.

Enterprises are using VMware NSX to realize significant operational cost reductions because it dramatically reduces the manual effort and cycle time for networking tasks, including provisioning, change/adaptation, scaling, and troubleshooting/remediation. (Cycle time accounts for delays due to requests, approvals, coordination, handoffs, logistics, downtime windows, etc.)

As the following OpEx analysis shows, VMware NSX dramatically speeds the initial provisioning of a network into production. With traditional hardware, the associated cycle time to provision a network for a new application forces enterprises to wait 23 days. VMware NSX reduces that to minutes – nearly a 100 percent reduction and massive time-to-market win. Likewise, provisioning a network for a new application takes 14 person hours or close to two days of person effort. VMware NSX reduces that to less than 2 person hours—a substantial 87 percent reduction. (Table 2)

	Task Effort (Hours)		Cycle Time (Days)	
	Manual	Automated - NSX	Manual	Automated - NSX
Request & Review Network & Security Resources	1.00	0.00	1	0
Define Network & Security Environment	4.50	1.00	3	0
Determine Changes Required (Capacity Availability)	4.50	0.00	3	0
Review & Approval Process (Change Approval Board)	0.50	0.50	5	0
Change Order Scheduling	0.50	0.00	5	0
Configure the Network (VLAN, Routing)	1.00	0.00	2	0
Configure the Security (Firewall)	1.00	0.00	2	0
Configure the Load Balancer	1.00	0.00	2	0
Provision the Environment	0.30	0.30	0	0
Total	14.30	1.80	23	0
OpEx Savings with NSX	**12.50 Hours**		**23 Days**	
	87%		**100%**	

Table 2: IT Automation OpEx Reduction

5. Network efficiency and asset utilization

Cost and utilization pressures are heating up as healthcare reform funding and reimbursements evolve. HIT teams are becoming frustrated with hardware churn for networking assets because of time and cost replacement demands. When healthcare organizations apply network virtualization, they gain greater flexibility in the hardware layer because features and controls are applied in software. With network virtualization, internal data center traffic is managed between the virtual machines rather than to the physical network and back to servers. By freeing up internal data center traffic, HIT teams can improve the performance of both the network and servers while reducing operational effort.

Specifically, VMware NSX provides the operational model of a VM for networks. HIT teams use VMware NSX to streamline provisioning of network services from weeks to seconds. This removes the manual effort and cycle times associated with procuring, installing, and configuring traditional network hardware. The solution's powerful orchestration capabilities programmatically distribute network services in lock step with virtual machines. Healthcare organizations use VMware NSX to standardize and maintain pre-defined templates that consist of the network topologies and services. The solution's automation capabilities reduce operational expense, accelerate time-to-market, and speed IT service delivery.

NSX also streamlines operations by consolidating configuration state and instrumentation data for all network connections. Administrators have complete operational visibility into what's occurring across the entire network infrastructure. This simplifies traffic management, monitoring, troubleshooting, and remediation.

Enterprises are using VMware NSX to access islands of unused compute capacity inside the data center. In traditional topologies each network cluster has its own compute capacity. IT often over provisions compute because the network re-configuration required to reach available capacity in another cluster takes too long and is prone to error. By many measures, 60 percent or more of a network's total compute capacity remains dormant, which is a waste of resources. HIT teams are using VMware NSX to bridge two or more network clusters and deploy workloads to this unused capacity. As a result, they are saving upwards of 88 percent by using existing server capacity rather than purchasing new physical servers. The following CapEx analysis shows how much enterprise save in annual server expenses by leveraging VMware NSX to use more of its existing compute capacity. (Table 3)

Environment	
Servers	250
Operational VMs	1,000
Current Effective Server Consolidation Ratio	4:1
Design Consolidation Ratio / VMs per host (determined by application performance requirements)	10:1
Annual VM growth rate	30%
VMs per year	300
Compute Asset Utilization	
Current Compute Asset Utilization	40%
Effective Utilized Server Capacity	100
Effective Dark Server Capacity (60% over-provisioned)	150
Target Compute Asset Utilization	85%
Operational VMs with current host capacity at TARGET asset utilization	2,125
Target Effective Server Consolidation Ratio	8.5:1
Effective Utilized Server Capacity at TARGET asset utilization	213
Effective Dark Server Capacity at TARGET asset utilization (15% over-provisioned)	37
Cost Without NSX	
Average Host Cost	$12,000
Annual Server cost (75 servers per year) to support growth at current compute asset utilization	$900,000
Cost With NSX	
Years of planned annual growth, without adding physical host capacity	3.75
CapEx savings with NSX	$3,375,000

Table 3: Server Asset Utilization CapEx Saving

6. Management of multiple-location enterprises

Leveraging network virtualization provides freedom for IP address management through encapsulation. This is particularly relevant for healthcare organizations involved in merger, acquisition, and affiliation activities. The implementation of a merged network may be a major critical path item in the consolidation plan yet risks may exist which could be easily mitigated with segmentation. As acquiring organizations seeks to drive efficiencies and expand business models, they can uncover unknown risks that may exist in their acquired organizations' IT systems. More effective network security can help ensure a successful business relationship from the start.

Moreover, HIT teams are leveraging VMware NSX as a complement to their existing disaster recovery (DR) solutions. The solution is helping them to reduce their recovery time objective (RTO) by upwards of 80 percent, considerably minimizing downtime and cost to the business. HIT teams use VMware NSX to replicate the entire network and its security environment. They periodically snapshot the network construct, along with its applications and services, and maintain it at a recover site. IT does not need to change IP addresses because the virtual network construct is decoupled from the underlying hardware and topology. The disaster recovery site is identical to the primary site, with no tradeoffs in functionality or performance. The copy sits at the recovery site in standby mode for push-button activation in the event of a disaster. Any changes made to the

source network are automatically replicated to the copy at the recovery site.

Defense in depth strategy powered by VMware NSX safeguards HIT infrastructure, applications, and devices.

Now is the time for healthcare organizations to adopt a new model for data center security; one that's defined in software, with native and third-party security controls that allow HIT teams to protect workloads at the virtual level, across private and hybrid cloud infrastructures. VMware vCloud for Healthcare features comprehensive mobility, private cloud, and public cloud services that advance a defense in depth approach by helping HIT teams improve delivery outcomes and address the compounding cost, quality, and delivery challenges of patient care while safeguarding information and systems. (Figure 3)

The vCloud for Healthcare portfolio of solutions includes the following key capabilities:

- Mobility services – VDI, cloud workspaces, and enterprise mobility management
- Private cloud services – Security and compliance, systems analytics, IT financial management, automation, and business continuity
- Public cloud services – Hybrid cloud deployment

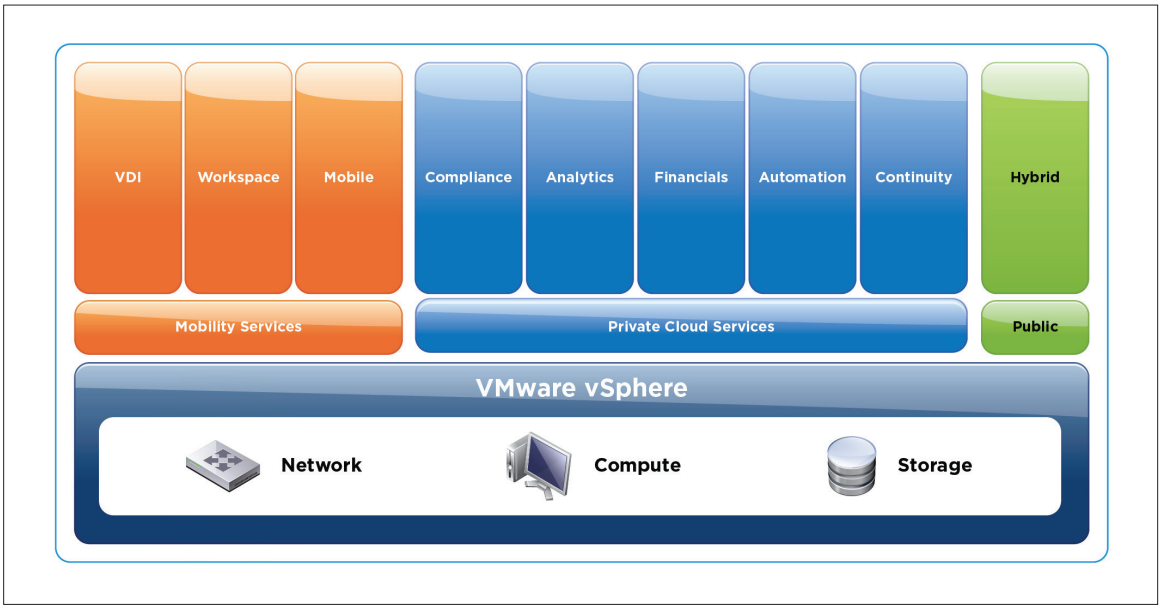

Figure 4: A comprehensive approach to security and compliance

With VMware security and real-time monitoring solutions, healthcare organizations achieve business and IT benefits:

- Network security inside the data center – HIT teams can create fully isolated and protected parallel virtual networks on top of existing physical networks.
- Automated deployments and data center agility – HIT teams can implement powerful security policies that mirror business logic and workflows.
- Integration with leading networking and security infrastructure – HIT teams can continue to use existing security products within a new advanced platform—without the need for extra investment. vCloud for Healthcare has been integrated with and tested by leading healthcare ISVs to ensure it meets healthcare organizations' security and compliance needs.

Learn More

Threats to healthcare IT show no signs of dissipating. Most CIOs and CISOs are choosing to deploy a multifaceted, defense in depth approach to security because it provides their healthcare organizations with best-practices security frameworks. HIT teams are using these frameworks to mitigate and anticipate risks. They are also

integrating frameworks with layered security to increase system uptime and accessibility while improving IT flexibility and agility as they respond to issues.

While the goal of every healthcare organization is to develop a strategy and deploy proven solutions that evolve with increasing threats, only a few technology companies provide comprehensive security and compliance support. VMware and VMware partners deliver the platform security, secure operations, security virtualization, and compliance guidance healthcare HIT teams require, where and when they need protection most.

To learn more about vCloud for Healthcare and how VMware solutions safeguard healthcare infrastructure, applications, and mobile devices, visit http://www.vmware.com/industry/healthcare/overview.

Existing VMware customers may also explore the benefits of vRealize Air Compliance as a service and VMware compliance checkers at http://vrealizeair.vmware.com/compliance or by contacting their account teams for more information.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

 Item No: VMW8856-WP-NEW-APPROACH-HEALTHCARE-SECURITY-USLET-104 1/16