IMC ELEVATES SECURITY POSTURE WITH VMWARE NSX, MEETS COMPLIANCE AND PROTECTS PATIENT DATA

Interfaith Medical Center

INDUSTRY
HEALTHCARE

LOCATION
BROOKLYN, NEW YORK

KEY CHALLENGES
- Improve the privacy and security of patient health information
- Securely share patient data to qualify for Meaningful Use programs
- Comply with NIST Cybersecurity Framework requirements for network security

SOLUTION
Interfaith Medical Center utilized VMware vSphere combined with VMware NSX to provide the most advanced security posture for the hospital to share medical information via a patient portal, meet NIST compliance regulations, and prepare for the increasing use of the Internet of Things to enable connected medical devices.

BUSINESS BENEFITS
- Qualified for Meaningful Use guidelines and compliance with NIST standards
- Reduced risk of moving patient data on Internet-enabled devices
- Saved USD $2.03 Million by achieving nearly 100% virtualization
- Lowered CapEx costs

Interfaith Medical Center (IMC) is a critical safety-net hospital for the Central Brooklyn communities of Crown Heights and Bedford-Stuyvesant. The 287-bed nonprofit teaching hospital and its network of ambulatory care clinics treat more than 250,000 patients every year.

IMC is embracing the industry directives, participating in Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs and solving data security, compliance, and privacy challenges. The hospital recently launched an online portal that allows patients to view information about their treatment and prescriptions and become more involved in their care. To improve efficiency, IMC virtualized nearly 100% of its server environment with VMware vSphere® and relies on VMware vRealize® Operations Management™ Enterprise for valuable insights on workload capacity and health. To improve security and meet compliance, the medical center is protecting virtual servers with micro-segmentation using VMware NSX®.

The Challenge

Most of IMC's critical applications run in a VMware vSphere Enterprise Plus environment, including Meditech EHR, glucometer software to help treat diabetes patients, and EndoWorks for gastrointestinal screenings. When IMC began offering patients access to healthcare information via an online portal to improve patient communication, satisfaction, and turnaround times while qualifying for Meaningful Use incentive programs, it introduced new security concerns. IMC also needed to make sure that its environment would comply with cybersecurity guidelines set by the National Institute of Standards and Technology (NIST).

"If security is poorly implemented, a patient portal could become a big problem—especially in a virtualized environment where traffic doesn't always leave the host to go through traditional network appliances," says Christopher Frenz, Director of IT Infrastructure, Interfaith Medical Center. "To expand online information access for patients, we needed a more secure data center to prevent unauthorized access to medical records, so we selected VMware NSX."

In addition to enabling more secure sharing of patient data, the hospital needed to segment its network to properly prepare to support the influx of Internet-enabled devices. "With the increasing number of IoT devices, the more segmented our network is, the better off we are," says Frenz. "That way, threats can't move laterally within the data center."

"With VMware NSX, we now make critical patient data more readily available to hospital medical professionals and to patients while keeping it segmented and secure."

CHRISTOPHER FRENZ
DIRECTOR OF IT INFRASTRUCTURE
INTERFAITH MEDICAL CENTER

The Solution

To address its business needs in a rapidly changing industry, IMC found VMware to offer the best security solution. With VMware NSX, the hospital can tie automated, fine-grained security policies to individual virtual machines, as well as isolate legacy systems on the network. The hospital easily self-deployed VMware NSX with micro-segmentation controlling its entire on-premises VMware vSphere environment in just a few days.

"We recognized that a virtualized environment requires a different approach to security, as outlined in the NIST Cybersecurity Framework," says Frenz. "To secure our patient portal and enhance compliance, we need to provide the same level of network segmentation to virtual machines that we traditionally applied to our physical machines. With VMware NSX, it's easy to lock down communications between virtual servers. It goes beyond a traditional firewall or DMZ-type setup—we can take network security a step further, down to the individual virtual machine."

Even in an unlikely scenario where attackers managed to get through the hospital's perimeter defenses, they still wouldn't be able to jump from machine to machine and access data. "We can isolate the threat, respond immediately, and minimize any impact," says Frenz. "VMware NSX Guest Introspection allows us to quickly identify any service or guest with personal information on it, giving us the visibility we need if such an event were to occur."

Business Results & Benefits

With a fully virtualized data center and granular security enabled by VMware NSX, the hospital is reducing costs while expanding its patient offerings and empowering patients to be more proactive about their care.

"Virtualizing our servers with VMware saved us approximately $2.03 Million over a seven-year period, and we achieved 100% payback on vSphere in half that time," says Frenz. "Virtualization simplifies management and allows us to deploy new systems a lot faster, without buying and standing up new infrastructure. It's also easier to upgrade applications and guard against downtime, because we can use vMotion to move virtual machines between physical hosts. Upgrading to vSphere 6 has made a big difference, giving us an improved web-based interface that makes it easier to configure load balancing and other features."

Since deploying VMware NSX over a year ago, IMC is securely and successfully enabling patients to check their medical records and prescriptions from home. IMC qualified for Meaningful Use Stages 1 and 2, earning incentive payments to reinvest in new healthcare technology. As the hospital pursues Meaningful Use Stage 3 (MU3) qualification, which is required for all hospitals by 2018, VMware NSX will be critical in meeting all the objectives.

Two MU3 objectives in particular—Protected Patient Health Information and Health Information Exchange—were much easier to achieve. "VMware NSX helped us meet both MU3 objectives by providing an extra layer of security around our virtual machines to better protect patient health information and by providing a more flexible network via its software-defined network feature set, which provides greater flexibility to securely set up the exchange of data with third parties," says Frenz. "VMware NSX has helped make securely deploying our patient portal possible, allowing us to meet Meaningful Use requirements in a virtualized environment. That's a huge benefit to our patients and our hospital."

"Virtualizing our servers with VMware saved us approximately $2.03 million over a seven-year period, and we achieved 100% payback on vSphere in half that time."

CHRISTOPHER FRENZ
DIRECTOR OF IT INFRASTRUCTURE
INTERFAITH MEDICAL CENTER

VMWARE FOOTPRINT

- VMware vSphere 6 with Operations Management Enterprise
- VMware NSX Advanced
- VMware vCloud® Air™ Disaster Recovery
- VMware Horizon® Advanced 6.1
- VMware AirWatch Green Management Suite™
- VMware vRealize Suite Standard Edition

APPLICATIONS VIRTUALIZED

- Meditech EHR, EndoWorks, e-prescribing and medical coding systems, radiology/cardiology picture archiving communications systems (PACS), glucometer software, X-ray and EKG systems

PLATFORM

- Windows

The micro-segmentation provided by VMware NSX maps directly to the recommendations made by NIST for securing virtualized workloads[1], helping IMC stay secure and compliant. It's also reducing CapEx costs even further, allowing the hospital to isolate and secure legacy systems to extend their useful life and defer hardware refreshes.

Looking Ahead

As the healthcare industry adopts the Internet of Things at an increasing pace, IMC plans to use VMware NSX and VMware AirWatch® to manage network security and endpoint devices. "Every day, more and more medical equipment is becoming network-enabled," says Frenz. "With VMware NSX, we now make critical patient data more readily available to hospital medical professionals and to patients while keeping it segmented and secure. It's a huge advantage that allows us to deliver more innovative treatments, empower patients to take a more active role in their own care, improve and meet healthcare outcomes, and meet compliance requirements."

[1]. NIST Special Publication 800-125B, "Secure Virtual Network Configuration for Virtual Machine (VM) Protection"

vmware®

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