INTERFAITH MEDICAL CENTER BOLSTERS APPLICATION AND NETWORK SECURITY TO BETTER SAFEGUARD PATIENT DATA

Interfaith Medical Center

INDUSTRY

HEALTHCARE

LOCATION

BROOKLYN, NEW YORK

KEY CHALLENGES

- Enhance security, compliance, and mobility with limited resources
- Reduce the risk of threats coming in from endpoints and IoT devices
- Improve IT efficiency to direct more funds to patient care

SOLUTION

Interfaith Medical Center utilized VMware NSX® Data Center for micro-segmentation and VMware AppDefense™ to protect applications on its virtual infrastructure. Integrated with VMware vSphere®, the combination delivers complete app-level segmentation for an advanced, least privilege security posture. The emphasis on security extends to the end user with solutions for virtual desktops and mobile device management.

BUSINESS BENEFITS

- Defends hospital systems against emerging threats
- Enables a small team to manage powerful patient data protections
- Saves more than $2 Million by achieving nearly 100% virtualization

Protecting patient data is paramount for Interfaith Medical Center (IMC). The hospital wanted to share medical information via a patient portal while meeting compliance regulations and improving security for connected medical devices as the Internet of Things (IoT) transforms healthcare. IMC is solving these challenges with help from VMware, enhancing its VMware vSphere infrastructure with a zero-trust security model that uses VMware NSX Data Center and VMware AppDefense to protect its applications and data. With this combination, the hospital's small security team can more effectively defend against emerging threats, leveraging network micro-segmentation in addition to application control and behavioral monitoring. With VMware Horizon®, the hospital extends secure virtual desktops to clinicians' own mobile devices, and locks down hospital-issued devices with VMware Workspace ONE™.

Interfaith Medical Center 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.

The Challenge

IMC is always striving to provide patients with the highest quality healthcare experiences while staying ahead of the security curve to maintain patient safety and trust. When IMC began offering patients access to their healthcare information via an online portal so they could take a more active role in their care, it needed to enhance network security and prevent unauthorized access to electronic health records. One goal was to have more automated and adaptive security tools, so they can be managed by a small staff of security engineers.

The hospital also needed to comply with the U.S. National Institute of Standards and Technology (NIST) and Meaningful Use guidelines for securing virtualized workloads, while supporting increased clinical mobility and the influx of Internet-enabled medical devices. Application security was also a focus: Even on a fully patched VM, a vulnerable web application could still be targeted for attack.

"We want to do more than just be compliant," says Christopher Frenz, Assistant Vice President of Information Security and Infrastructure, Interfaith Medical Center, who oversees the hospital's security operations. "We want to do everything we can to protect our network and our patient data from being compromised. That's always a challenge with a small IT team, so we wanted to use software and automation to be more efficient."

> "With AppDefense and NSX Data Center bolstering our vSphere foundation, we can mitigate risk by extending a zero-trust model across the network, all the way to the endpoints. It's a powerful combination."
>
> CHRISTOPHER FRENZ
> ASSISTANT VICE PRESIDENT
> OF IT INFRASTRUCTURE
> INTERFAITH MEDICAL CENTER

VMWARE FOOTPRINT

- VMware AppDefense
- VMware NSX Data Center for vSphere 6.3 Advanced
- VMware vSphere 6.5 Enterprise
- VMware Horizon 7.1 Advanced
- VMware Workspace ONE, powered by AirWatch® technology
- VMware vRealize® Suite Standard

The Solution

Like most enterprise application environments, the hospital's Meditech electronic health records (EHR) system runs on vSphere, previously with relatively little network segmentation or firewalling between workloads. To prevent threats from moving laterally from server to server within the environment, IMC deployed NSX Data Center and used micro-segmentation to lock down communications and isolate public-facing systems such as its patient portal. With NSX Data Center, the hospital can tie automated, fine-grained security policies to individual virtual machines, increasing flexibility and efficiency.

"VMware NSX Data Center has helped make securely deploying our patient portal possible, allowing us to meet Meaningful Use requirements in a virtualized environment," says Frenz. "That's a huge benefit to our patients and our hospital."

IMC also upgraded to vSphere 6.5 due to its enhanced capabilities for encryption of VMs and encrypted vMotion®, protecting data both at rest and in motion. The hospital was an early adopter of AppDefense, a data center security product that protects applications running in virtualized environments. AppDefense leverages vSphere 6.5 to secure the environment from a protected position, without any additional agent deployment.

Integrated together, vSphere, AppDefense, and NSX make up a powerful solution for protecting applications called Adaptive Micro-segmentation. Adaptive Micro-segmentation extends the power of network micro-segmentation with NSX to the workloads that comprise the application. AppDefense gathers a holistic understanding of every workload's intended state and behavior as part of an application and leverages vSphere and NSX to enforce the workload's intended state. When the runtime state of the workload deviates unexpectedly, AppDefense orchestrates a response automatically to prevent the unexpected behavior from executing in the environment.

"We set up a web server with a fully patched OS and known application vulnerabilities, and we watched VMware AppDefense stop them," says Frenz. "It was great to be part of the beta testing process for AppDefense because we could see for ourselves how effective it is."

AppDefense is now an essential layer of security for IMC, protecting critical VMs such as domain controllers, system interfaces for medical devices, and data archiving systems. If a virtual machine becomes infected, an automated response action takes place to either block the behavior or remediate the problem. And because AppDefense leverages components within the vSphere hypervisor, it is isolated from the attack surface, in addition to being easier to deploy and manage than traditional agents.

"AppDefense complements our other security solutions very nicely by filling a gap that we didn't have covered before," says Frenz. "Ransomware attacks against hospitals do happen, and you can lose thousands of computers in minutes. With AppDefense and NSX Data Center bolstering our vSphere foundation, we can mitigate risk by extending a zero-trust model across the network, all the way to the endpoints. It's a powerful combination."

IMC is using Workspace ONE to ensure that around 200 hospital-issued phones and mobile devices are encrypted and to enforce strong passwords. Workspace ONE also provides the ability to remotely wipe a device if it's lost or stolen.

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

Dell, Windows

Horizon provides virtual desktops to clinicians who want to bring their own smartphones or tablets to work. “Wherever they go in the hospital, whichever client they’re using, the desktop is available,” said Frenz. “They can sit down at a hospital computer, then pick up the work on their personal device. This gives them faster access to medical information, which makes for more responsive care.” Security is enhanced because hospital data only exists within the virtual desktop. “As soon as they leave the hospital, the network connection breaks and the VM is gone. We don’t have to worry about a device being stolen because there’s no actual hospital data on it.”

Business Results & Benefits

By enabling IMC to cost-effectively scale its data center and empowering a small team to implement and manage a least privilege security posture, VMware is helping the hospital better safeguard patient data and applications. IMC has successfully avoided any data breaches and is detecting and responding to advanced threats before they impact privacy or operations.

“The potential that AppDefense offers to trigger vSphere and NSX Data Center automation of precise security responses is a game changer,” says Frenz. “It’s much faster than a person could respond, even if the threat was detected right away—and by then, as any security professional knows, it’s often too late.”

Deploying NSX Data Center helped IMC qualify for Meaningful Use Stages 1 and 2, earning incentive payments to re-invest in new healthcare technology. The hospital is now in the process of completing Meaningful Use Stage 3 qualification, which includes the Protected Patient Health Information and Health Information Exchange objectives for which NSX Data Center was critical.

“NSX Data Center helped us meet Meaningful Use objectives by providing an extra layer of security 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. “We can 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.”

The hospital is also reducing data center costs, even as it expands patient offerings and empowers patients to be more proactive about their care by checking their medical records and prescriptions from home. “Virtualizing our servers with vSphere saved us more than $2 Million over a seven-year period, and we achieved 100% payback on vSphere in half that time,” says Frenz.

Looking Ahead

As the use of Internet-enabled medical devices explodes and network micro-segmentation becomes a prerequisite for secure medical device deployment, IMC will be ready.

“Anything we do to improve security ultimately impacts patient safety, and we trust VMware to provide us with effective tools for securing virtual environments,” says Frenz. “If we didn’t have solutions that work together so effectively such as AppDefense, vSphere, and NSX Data Center, it would be far more difficult and more expensive for us to keep patients and data safe and secure.”

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

Item No: 186143wf-vmw-cs-Interfaith Med Ctr-uslet-101c
11/18