SECURE EHR WITH VMWARE NSX

ePHI is a Prime Target for Attack

A recent study by the Ponemon Institute and IBM shows that the cost of a security breach and exposure of a patient health record is now averaging $355 USD per record. The average annual total cost to an organization in the US is $7.01 million USD and the average number of records breached is around 29,000 . The security of electronic Protected Health Information (ePHI) has never been a higher priority for healthcare organizations.

The Expansive EHR Attack Surface

Electronic Health Record (EHR) systems are mission-critical applications for the 21st century healthcare organization. As the central location of all ePHI within a hospital, these systems are an enormous target for attackers.

EHR systems require anywhere from tens to hundreds of servers to run the application and are tightly integrated into a number of other tools used across the organization. Ideally, IT organizations would deploy a firewall to protect each individual server that makes up the EHR system, to enforce the appropriate security controls required to protect such a mission critical workload.

Unfortunately, deploying a traditional firewall for every server in an EHR environment is prohibitively expensive and would be nearly impossible to manage. Therefore, healthcare IT organizations have relied on perimeter firewalls alone to protect their systems, leaving them vulnerable to security breaches. The problem with this perimeter-centric approach is that attackers still find their way around perimeter defenses, often targeting less critical systems (such as the mobile device of a practitioner) and moving laterally through the data center, until they find the valuable information they are looking for (Figure 1). This technique has proven effective in many of the data breaches that have made headlines in recent years.

"IT security threats are more numerous than ever, and a micro-segmentation approach is going to be our next line of defense"

JOEL VENGCO
CHIEF INFORMATION OFFICER
BAYSTATE HEALTH

KEY HIGHLIGHTS

- Health records are extremely valuable, making EHR systems prime targets for attack.
- Perimeter firewalls alone are insufficient as they are unable stop attackers from moving laterally within the network.
- VMware NSX® enables micro-segmentation and prevents the lateral movement of attackers, protecting electronic Protected Health Information (ePHI) from the inside out.

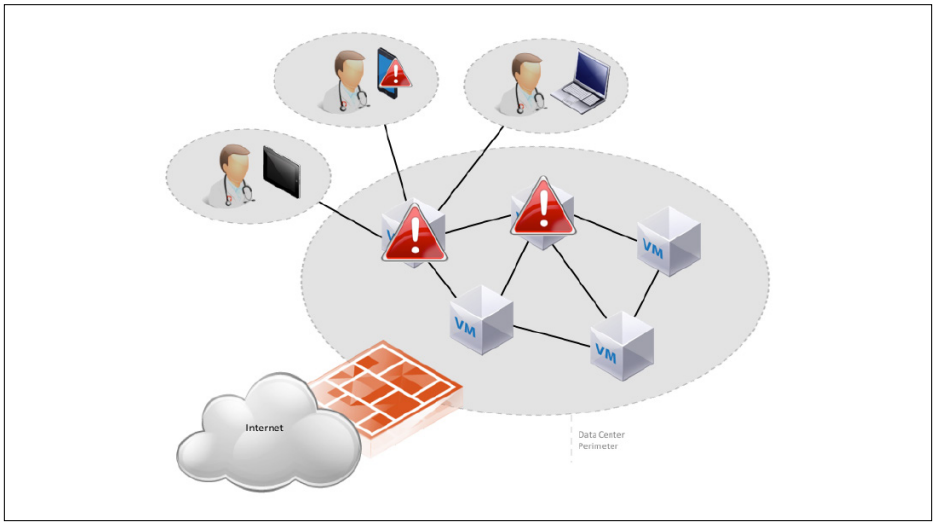

Figure 1

KEY STATISTIC:

89% of healthcare organizations had at least 1 data breach involving the loss or theft of patient data in the past 2 years. 45% had more than 5 breaches. – Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data (Ponemon Institute, May 2016)

LEARN MORE

For more information, visit VMware Solutions for Healthcare.

Secure EHR with VMware NSX

VMware NSX is the only security solution that enables the firewalling and segmentation of a data center network down to the individual VM level, a concept known as micro-segmentation (Figure 2). This effectively gives each workload its own firewall, which is dynamically provisioned, changed, moved, and de-provisioned in conjunction with the workload to which it is attached, making micro-segmentation operationally feasible for the first time.

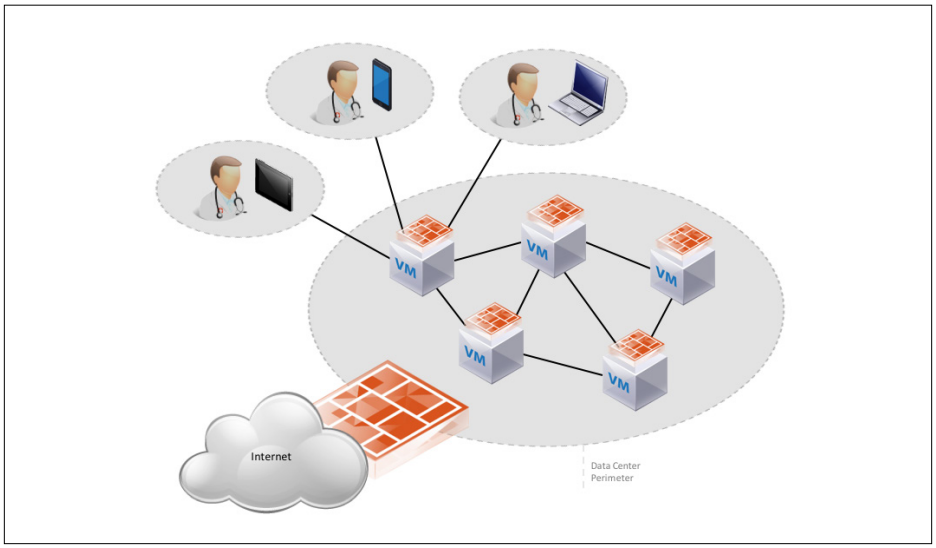

Figure 2

The result for healthcare IT organizations is that their EHR environments can finally be secured from the inside out. Critical ePHI is protected from within the data center, at the virtual server level where the data is stored, instead of relying on endpoint protection and traditional perimeter firewalls that have proven ineffective in stopping modern threats.

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

12/16