SECURE CLINICIAN ENDPOINT ENVIRONMENTS

Positive Patient Outcomes Through Mobility

From hospital rounds, to home visits, to emergency calls at home – healthcare professionals need access to real-time patient information and medical data from anywhere, at any time. The proliferation of mobile devices, BYOD or hospital-owned programs, and remote access has enabled a level of patient information access not previously possible with paper charts.

Mobility Expands the Attack Surface

As hospitals embrace mobility and virtual desktops to improve clinician efficiency, there are more endpoints than ever connected to their networks. This trend coincides with increasing mobile-specific threats. According to Symantec's 2016 Internet Security Threat Report, 2015 saw a 214% increase in new mobile vulnerabilities.

In a traditional network design, these endpoints have access to nearly everything in the data center. This means that a single compromised endpoint is enough for an attacker to move laterally (east-west) across the environment, increasing their foothold in the network and locating valuable patient information to steal (Figure 1).

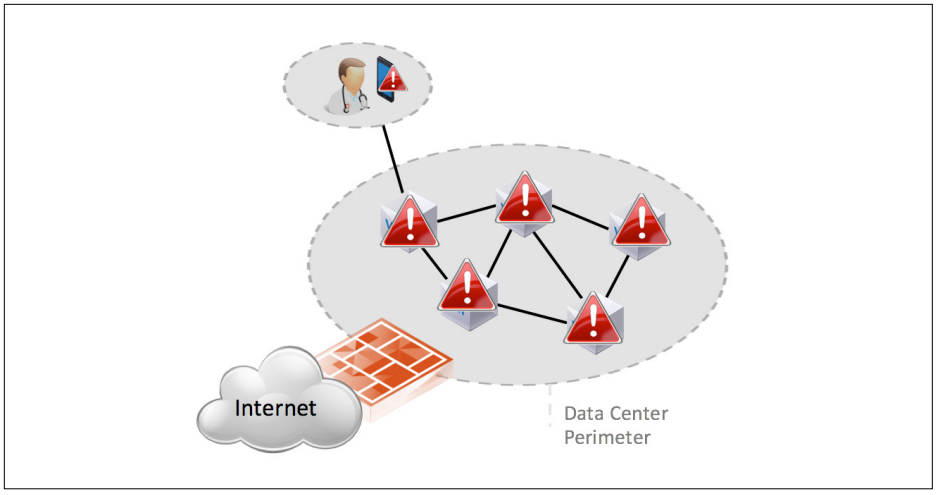

Figure 1

KEY HIGHLIGHTS

- Mobility and VDI are becoming central to driving better patient outcomes and increasing physician efficiency.
- Connecting mobile devices and virtual desktops to the network significantly increases the attack surface.
- VMware NSX prevents threats from expanding from the endpoint into the data center by shrinking the attack surface through micro-segmentation.

KEY STATISTIC:

According to Symantec's 2016 Internet Security Threat Report, 2015 saw a 214% increase in new mobile vulnerabilities. – Internet Security Threat Report (Symantec, April 2016)

"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 OF
BAYSTATE HEALTH

LEARN MORE

For more information, please visit VMware Solutions for Healthcare.

Secure Clinician Endpoint Environments

VMware NSX® enables the segmentation of a network down to the individual VM level, a concept known as micro-segmentation. By applying security policies to individual VMs, NSX reduces east-west traffic within the data center and prevents attackers from moving laterally in search of information.

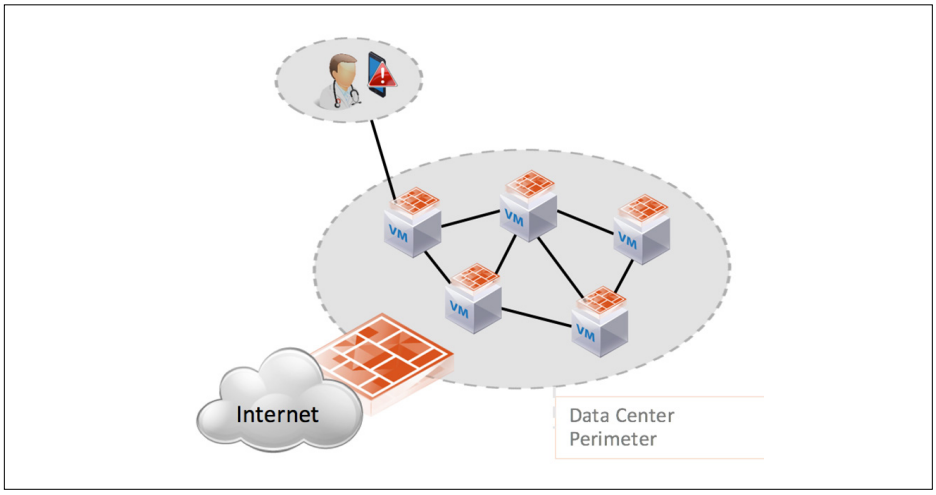

Figure 2

With the help of virtual desktop infrastructure products, such as VMware Horizon®, and mobile device management solutions, such as VMware AirWatch®, NSX can also extend these segments to clinician virtual desktops and mobile devices. This creates a secure tunnel from the application to the server that supports it within the data center.

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