cbts

Case Study

Healthcare Provider

Client: Healthcare Provider

Client is a leading healthcare provider in both pediatric and adult healthcare. Consisting of clinics and hospitals supported by over 20,000 healthcare workers, the client provides inpatient and outpatient general care as well as specialty care including heart, neuroscience, cancer, orthopedic, women's and pediatric services.

Challenge	CBTS solution	Results
• Poor performance on existing infrastructure because of increased demand resulting in dropped connections on critical applications.	• Full technology refresh with Aruba ClearPass and integrated Bluetooth beacons.	• Increased wireless coverage to 30 devices to 1 patient room, reducing need for physical cable upgrades and tethered devices.
• No network segmentation for credit card processing, device profiling, or sensitive data.	• Fortinet firewalls to drive security policy, enforcement and deep network monitoring.	• Limited potential attack vectors to minimized threats and malware introduced by individual users and bad actors.
• Functionality limitations on existing load balancing would not scale to meet new environment requirements.	• F5 physical Big IP load balancing with access policy management.	• Scalable, secure application delivery across all network segmentations.

Security, covered.

Security challenge

With the growing use of IoT devices in the healthcare field, the existing network environment was not able to meet the connectivity demands brought on by new technology. This was felt most by the existing voice infrastructure, which was dropping calls at an unacceptable rate.

The existing network had no LAN segmentation which prevented the isolation of clients for PCI requirements, sensitive data, biomedical hardware or the ability to qualify or disqualify devices based on roles, device type or credentials. The management of the network required complex configurations using manual modifications creating a burden on network operations staff for MAC-D, deployments and break-fix replacements.

CBTS security solution

CBTS designed and installed a full technology refresh for secure network access control using Aruba APs and Bluetooth beacons along with ClearPass Policy Manager giving agentless visibility and dynamic role-based access control for security enforcement and response. ClearPass Policy Manager became the central nervous system for both the wired and wireless network. Standard configurations were developed to simplify network administration and service while providing a consistent user experience throughout the network.

To solve the problem of no LAN segmentation between hospitals, CBTS provided, installed, and configured 30 Fortinet firewalls at 13 locations. This allows client high performance, multilayered security and deep visibility for end-to-end protection across the enterprise network, offering scalable performance and low latency. The Fortinet firewalls also provide reporting to help meet PCI and HIPPA compliance

Knowing the current load balancer could not scale to meet the demands required by the new network, a redundant and highly available physical F5 Big IP environment was installed and configured by CBTS. This enabled a resilient and secure application delivery across the network as well as an additional layer of security on all the segments.

At the time there was a sudden shift to work from home and the client needed to quickly increase their VPN licensing for secure remote access. CBTS was able to provide additional Pulse Secure licensing needed for a seamless transition.

Results

The client has future-proofed their organization by establishing a secure wireless network that can handle the advances of technology. By upgrading their wireless coverage throughout the hospital, client was able to minimize cable upgrades and tethered devices. Utilizing the new wireless technology for voice provides secure, stable connectivity for more effective communication between staff and patients and improving patient quality of care. Integrated Bluetooth beacons supplemented by stand-alone beacons created location services and push-notification such as way-finding throughout the hospital, alert notification and integration of healthcare management systems for a seamless user experience.

With the deployment of ClearPass and Fortinet the client now has secure dynamic segmentation based on device profile type, automatic assignment of vLANs for segmentation and isolation for sensitive data. Automation of on-netting new devices within predefined device profiles as well as vLAN segmentation eliminates the complex configurations using manual modifications allowing more time for network operations staff to focus on business priorities.

Optimized application speed, reliability and security with F5 supports the greater demand the new network enabled, put the finishing touch on creating a network that is secure, reliable, meets compliance, and provides greater business benefits with reduced costs.

cbts

Security, covered.