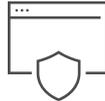




VMware NSX Data Center delivers granular protection for applications via micro-segmentation down to the individual workload



Patient data and TUH's corporate reputation are strengthened due to increased security



The VMware platform creates a stable platform to simplify integration with possible third parties

Data Security Drives Tallaght University Hospital's Digital Transformation

Tallaght University Hospital (TUH) is one of the largest capital investments in healthcare ever undertaken by the Irish Government. Through its engagement with VMware, TUH has strengthened its security, protecting patient data and corporate reputation. It has created a stable platform to add new digital services.

TUH was one of the largest capital investments (€140m) in healthcare ever undertaken by the Irish Government when it opened in 1998.

The site was created from a number of hospitals in the Dublin area moving to one location. In creating this large teaching hospital, management has always been keen to foster the long history of innovation throughout the organization. At the core of its digital transformation the hospital is focusing on keeping data secure, while encouraging greater network connectivity.

Keeping data secure

As healthcare becomes increasingly digital, with patient pathways involving multiple partners, TUH's ICT department wanted to ensure the hospital was the most secure in Ireland. Between ransomware, data breaches and the risks posed by IoT, and consumer access to electronic health information, the healthcare industry is under attack.

"Security is very important to us," says David Wall, director of ICT at TUH. "We work with a great deal of highly personal and organizational information. We take guarding that information extremely seriously."



Tallaght University Hospital

Ospidéal Ollscoile Thamhlachta

An Academic Partner of Trinity College Dublin

TUH is one of Ireland's largest academic teaching hospitals. Research at the hospital is recognized internationally in several areas including irritable bowel disease, vasculitis, carotid artery disease and sarcoidosis. The hospital treats over 52,000 patients each year in the Emergency Department, over 255,000 outpatient appointments, 31,000 day-case admissions, and over 18,000 inpatient admissions.

INDUSTRY

Healthcare

LOCATION

Dublin, Ireland

ABOUT THE PARTNER

PFH Technology Group is a VMware partner providing applications, infrastructure, security, communications and managed services solutions. It has been partnered with VMware for over 15 years, and helps customers manage solutions through lifecycle delivery. Find at more at pfe.ie.

VMWARE FOOTPRINT

VMware NSX Data Center
 VMware vRealize Operations Manager
 VMware vSphere
 VMware vRealize Log Insight

RELATED CONTENT

- [Video](#)
- [Blog article](#)



For Wall, the role of data guardian is to keep data secure, separating different network users where necessary:

“Unfortunately, cybersecurity threats are on the increase in healthcare. It’s very disappointing that criminals are targeting some of the most vulnerable people in the world.”

The recent opening of a new data center and amalgamation of multiple systems has meant that the ICT department must be as innovative as the medical staff. The move represented not only an opportunity to upgrade the ICT infrastructure, but also to establish an ICT platform to support long-term digital transformation. Data, and the security of data, is a priority.

“There were a number of challenges with the previous ICT environment,” explains Ricky McKenna, ICT infrastructure services manager, TUH. “We were running on an aging infrastructure and we did not have enough computer resources. On top of that, we had to physically move our data center in a way that was non-disruptive to the hospital, because we need to keep systems running 24 hours a day, 365 days a year. There is no downtime in healthcare.”

Using micro-segmentation to protect workloads

The new ICT infrastructure is built on VMware solutions.

TUH has deployed VMware NSX® Data Center to operationalize micro-segmentation so, in the event of a cyber-attack, it would prevent its infrastructure from being compromised and protect workloads. NSX Data Center delivers granular protection for applications via micro-segmentation down to the individual workload. It creates context-aware security policies per workload to defend against lateral threats within TUH’s environment.

In addition, TUH uses VMware vRealize® Operations Manager™ for managing and monitoring; VMware vSphere® for virtualizing servers; VMware vRealize® Log Insight™ to log the entire environment.

Local VMware partner PFH Technology Group played a significant role in the design, implementation and delivery of the solution.

“VMware has a good track record in healthcare, so we felt it was a good fit for the hospital,” says Wall. “But it was very important for us that we had a local company that could interface between ourselves and VMware, and PFH provided that service to us. Together with VMware, the hospital and PFH, the project was an overall success.”

From a security perspective, Stephen O’Herlihy, chief technical officer, PFH Technology Group, says the use of NSX Data Center was key: “I use the analogy of a hotel. Yes, a hotel will have security protecting the perimeter, but they don’t leave every guestroom door wide open. VMware NSX Data Center is the same thing: it will lock down every individual VM. Traditionally that has been a huge challenge.”

“VMware NSX Data Center micro-segmentation isolates applications so that if an application does become infected, it won’t be able to infect other hospital applications.”

RICKY MCKENNA
ICT INFRASTRUCTURE SERVICES MANAGER
TALLAGHT UNIVERSITY HOSPITAL

Granular protection through a stable platform

The VMware engagement strengthens TUH’s security posture, protecting patient and organizational data.

“We’ve done a lot of work to ensure that our gateways are secure from a malware perspective but there’s always the risk that we could be unlucky. VMware NSX Data Center micro-segmentation isolates applications so that if an application did become infected, it will not be able to infect other hospital applications,” says McKenna.

Moreover, the VMware platform solution creates a stable platform to add new digital services and simplify integration with possible third parties. The TUH vision for Digitally Enabled Care, says Wall, will involve greater integration between systems, and NSX Data Center enables his team to carefully manage this integration. In recent years TUH has pioneered online bookings, self-service appointment check-in, and digital links between GPs and hospital specialists.

McKenna says the task of managing the ICT infrastructure is greatly reduced, freeing time to focus on deploying new services:

“VMware solutions work very well together. It’s great that you have a single management interface to work on the different components within the VMware solution.”

Looking ahead

The sector is expected to transform over the coming years as the number of connected devices and wearables increase. The goal for healthcare facilities is to harness this data to adopt a more proactive position. The focus will be on maintaining good health, not simply treating poor health. The engagement with VMware leaves TUH well placed to drive greater, more complex connectivity.

“The future’s very exciting,” says Wall. “The hospital is focused on delivering a ‘Hospital without Walls’ and integrating patient care into the community. We will rely heavily on technology to change how we deliver our health services in a more efficient and effective manner across our growing campus and into the community. The use of technology is vital to empower us to deliver and improve the delivery of our services.”



In the modern age, **#healthcare** organizations are plagued by **#datatheft** and **#cybercrime**. We’re protecting Tallaght University Hospital against the increasing threat