CASE STUDY

PORTSYS®

University Hospital Gets the Most Out of Mobility with Total Access Control

Milton Keynes University Hospital (MKUH) NHS Foundation Trust is a 550-bed hospital operating 50 miles northwest of London. MKUH provides outpatient services to more than 350,000 patients annually, while also managing more than 87,000 emergency department (ED) visits. As a university hospital, Milton Keynes also conducts upwards of 85 research studies on an ongoing basis, involving more than 2,500 research subjects.

To meet its mission for the U. K.'s National Health Service (NHS), the hospital has almost 5,000 employees and volunteers spread across four clinical service units and seven corporate functions with access to resources on its IT network. It also has approximately 1,000 users at partner organizations, the vast majority of whom require remote access to MKUH applications from outside of the hospital.

NHS

Milton Keynes University Hospital
NHS Foundation Trust

When Ollie Chandler, the Head of IT Technical Services at MKUH, arrived in late 2016, he saw there was an urgent need to upgrade the ability of his team to deliver secure remote access to the hospital's resources. At the time, the hospital did not have an adequate access control solution in place to manage personal devices to encourage and enable a BYOD (Bring Your Own Device) approach.

 |

Although the hospital relies on VPN connections for direct access for its Windows 10 corporate devices, only 10 percent of those devices are mobile; the rest are desktop computers. The vast majority of MKUH's staff thus relies on their own personal devices for remote access to hospital applications when they work remotely.

> "The EMB was impressed that we would be able to offer a robust unified remote access solution built with security as its foundation."

"Approximately 80% of the remote access requests we receive don't come from a MKUH corporate device at another location," Chandler said. "They are either coming from the individual's own personal device or a device owned by one of our partners. We needed a solution to enable us to get the most out of mobility, so our users would have access to what they needed to do their jobs wherever they were, as long as they had an internet connection."

Chandler had been a strong proponent of the Microsoft Unified Access Gateway (UAG) solution for remote access at his previous assignment with the Bedford Hospital NHS Trust. However, UAG was reaching the end of life for support as Microsoft continued to mothball that solution.

That led Chandler and his team to begin an extensive search for a remote access control solution – one that would provide not only the high level of security that MKUH's divisions, partners and patients required, but also the remote access capabilities necessary to continue to provide quality patient care. The chosen solution also had to meet strict requirements set forth by the NHS to safeguard patient information.

Ticking Off Every Box for Security

After considering several options, Chandler made a business case to the hospital's Executive Management Board (EMB) for Total Access Control (TAC), an innovative Zero Trust solution from PortSys that provides simpler, stronger and more unified security.

"This was an innovative approach for our EMB to consider, because at the time we only had VPN connections for our own staff's corporate devices, and nothing for BYOD or partners," Chandler said. "The EMB was impressed that we would be able to offer a robust unified remote access solution built with security as its foundation. After the EMB signed off, we were up and running fairly rapidly."

The TAC portal went live with connections to the hospital's applications in less than a day. The solution was first rolled out to a core group of early adopters, before being fully deployed across the enterprise. Early adopters soon found that TAC was easy to use on remote devices, whether they were personal laptops, phones, tablets or desktop computers, and word quickly spread across the organization.

"TAC ticks off every one of our boxes for security," Chandler said. "There are no direct connections to resources. Also, a user's context of access must be authenticated. That includes robust endpoint inspection, verifying the user's credentials, requiring multi-factor authentication, and validating the security status of the device. Each connection to each resource must meet the requirements in our security policies before TAC grants access."

Even then, Chandler added, TAC only provides access to those applications for which a user is authenticated. TAC's function-checking feature enables the use of customized authentication by application, so each resource has its own security policies for access. Extra authentication can be required through TAC for more sensitive applications, eliminating the "all or none" security policies traditionally used by enterprise organizations for remote access.

Chandler was also impressed with TAC's flexibility. MKUH originally decided to present an icon-group Windows desktop through an IDS server, but it soon began adding web links to email and the hospital's Intranet. The addition of more and more web apps soon turned the user interface into a crowded virtual desktop.

> "TAC certainly is worth the payoff since we now have different people with different apps and different icons customized for their unique needs."

"Remote users don't need a full desktop experience for something as simple as reading a policy," Chandler said. "We restructured various groups within Active Directory, and now we can provide the specific applications those groups need through the TAC portal. This made it a lot easier for our service desk to provision access."

"TAC certainly is worth the payoff since we now have different people with different apps and different icons customized for their unique needs," Chandler added. "It is so much easier to give the right people access to the right resources when they need them."

Eliminating Pain Points

The elegant simplicity of TAC's easy-to-use portal eliminates several other pain points as well – for end users and IT security administrators alike.

 | + 1 781-996-4900 | UK: + 44 208 196 2420 | www.portsys.com

TotalAccessControl™
Zero Trust Access

> "TAC enables us to stand out from the crowd and, most importantly, provide better patient care."

"TAC is very intuitive for our end users," Chandler said. "The portal is self-explanatory – nobody needs hours of training in TAC. We regularly add new web applications and IDP server sessions for support companies in minutes. We also copy policies, applications and other things in TAC, which saves us so much time. TAC makes our lives significantly easier."

A huge interoperability benefit for the hospital's IT team was that TAC works in all mainstream browsers, making it much easier for end users with multiple personal and corporate devices.

"When an access request comes in, TAC generates a soft token," Chandler said. "Remote users no longer rely on physical tokens that can easily be lost and were a pain to maintain and manage."

TAC also helps the hospital to meet a large variety of partner missions. Most NHS IT systems are on a national network, but not all of them. TAC is the only way MKUH provides access to its applications for 3rd-party healthcare providers who are not on the national network.

"These partners were onboarded quickly and found out TAC works really well," Chandler said. "They don't have to use our hardware when they are at MKUH – there's a clear demarcation. Also, because it's internet-facing, our applications are available through TAC when partners provide patient care away from the hospital setting."

MKUH also has 3rd-party IT support companies who use TAC from their own offices and on their own devices.

"Third parties come in from a wide variety of Windows devices and Macs," Chandler said. "Regardless of the operating system, we can present any application through a browser with TAC, and it works well."

Enabling Mobility to Improve Patient Care

One of the biggest challenges in access management today is visibility. Chandler said TAC enables MKUH to generate a single report that allows it to answer the critical question for remote access – who accessed what and when?

TAC also allows the IT team to drill down and gain critical insights on any session or remote access activity – including user credentials, the location they access from, the devices used and their status, and what applications were accessed.

"We go into that report regularly to see when people are logging in to TAC and what they are accessing," Chandler said. "That allows us to recognize remote access trends as well as security events that may need additional attention."

Although PortSys has made security a critical component of TAC, Chandler casts the Zero Trust access solution as much more of a total business benefit across the organization – from the IT team to end users and partners, and ultimately, to the patients.

"Total Access Control is much more than just a security solution," Chandler said. "It enables mobility across our entire extended organization. Surrounding hospitals ask what we deliver through TAC today, and they can't deliver the same level of mobility for their users. TAC enables us to stand out from the crowd and, most importantly, provide better patient care."

To learn more, visit https://portsys.com

PORTSYS®

 | + 1 781-996-4900 | UK: + 44 208 196 2420 | www.portsys.com