

Case Study

NHS's cybersecurity strategy on the advent of the COVID-19 pandemic



Company: East Coast Community Healthcare | Industry: Healthcare | Location: United Kingdom

About East Coast Community Healthcare

The East Coast Community Healthcare CIC (ECCH) is a staff-owned social enterprise, providing community-based NHS and social care in Norfolk & Suffolk. The National Health Service is the publicly funded healthcare system in England, and one of the four National Health Service systems in the United Kingdom. It is also the second largest single-payer healthcare system in the world. The staff strength of ECCH is as high as 700 and comprises 6 sites.

Business challenges

Andrew Webster, a third line IT support Engineer, has seen an increase in the number of remote employees due to the COVID-19 nationwide lockdown. The single AD domain structure's data security risk is at an all time high, with sensitive medical files being accessed by remote workers from different locations. Some of the main challenges they faced were difficulties to monitor their AD, keep track of account usage, account lockouts and audit file servers containing sensitive data. With an influx in patients during this COVID-19 pandemic, the cyber space of East Coast Community Healthcare could not risk a data loss or downtime in network.



AD360 is very good for managing and tracking use of resources. It's very intuitive and easy to use.



Andrew Webster,

IT support engineer, East Coast Community Healthcare.

How AD360 helped secure sensitive medical data of NHS

Auditing the file servers containing sensitive files with medical data was their top priority. AD360's comprehensive auditing capabilities helped them track all file accesses, modifications, and deletions. All file and folder movements captured accurately by AD360 helped them track files that went missing and investigate unwarranted and accidental deletions. Other capabilities of AD360's file auditing include monitoring permission changes, file integrity monitoring, folder owner changes, failed attempts to access or modify files and more.



Fairly easy to use and very intuitive, AD360 is very good for managing and tracking resources.

- Andrew Webster, IT support engineer

Andrew tells us that ECCH has been using other ManageEngine products which has helped them manage, track and secure their network resources. This prompted them to choose AD360 for their security and auditing needs. Calling it easy and intuitive to use, he's glad he chose AD360 to be part of their cybersecurity solutions suite. He also stated that the support team of AD360 is very knowledgeable and thanks them for getting their setup working exactly as needed. He appreciates them for providing a beneficial and informative session on the capabilities of AD360.

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine AD360

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps you perform all your IAM tasks with a simple, easy-to-use interface.

AD360 provides all these functionalities for Windows Active Directory, Exchange Servers, and Office 365. With AD360, you can just choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from within a single console.

[\\$ Get Quote](#)

[↓ Download](#)