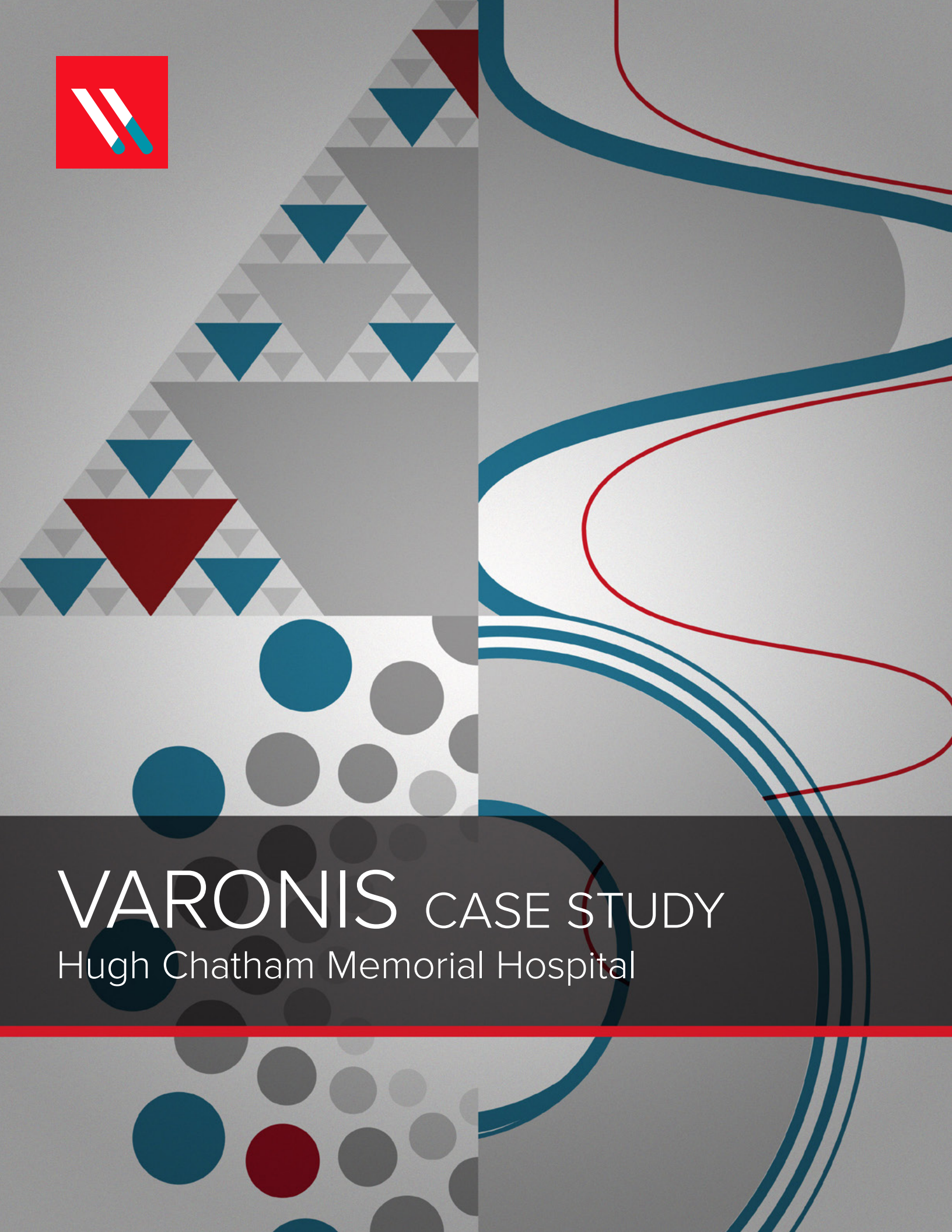

VARONIS CASE STUDY

Hugh Chatham Memorial Hospital

"We completely cleaned up the security of more than a terabyte of network file shares. Seeing the results of the changes was huge. In any organization but specifically in a hospital, the end user's tolerance for change is pretty low. If you have nine hundred or a thousand users and only 5 or 10 of them are actually accessing the data available in an everyone group, it becomes a no-brainer."

— Lee Powe — CIO, Hugh Chatham Memorial Hospital

THE CUSTOMER

Hugh Chatham Memorial Hospital

LOCATION

North Carolina

INDUSTRY

Healthcare

PRODUCTS

Data Classification Framework, DatAdvantage for Exchange and Windows, and DatAlert

Hugh Chatham Memorial Hospital, which serves patients in the Yadkin Valley region of North Carolina and Virginia, employs more than 800 people, provides healthcare services for the community and is served by more than 70 physicians representing 26 specialties and subspecialties.

BUSINESS REQUIREMENTS

MONITORING

Unusual file activity and user behavior.

DATA ACCESS AND CLASSIFICATION

The company needed a solution that could help identify who has access to which files, see who was accessing files, and lock down unnecessary access.

THE VARONIS SOLUTIONS / RESULTS

The Hugh Chatham Memorial Hospital IT team's search for the right solution to control the security of its data led to the evaluation and implementation of Varonis Data Classification Framework, DatAdvantage for Exchange and Windows, and DatAlert.

ALERTING ON RANSOMWARE ATTACKS

Lee Powe, Hugh Chatham Memorial Hospital's CIO, said, *"A week into our implementation we had a brush with ransomware. One of the employees remotely connected and went on a site that started downloading Locky. Luckily the Varonis rules we had in place immediately told me when the individual started encrypting the file, so we disabled the account and restored the files. Without Varonis we would have ended up with a much broader exposure of the breach and the result would have been a lot worse."*

With DatAdvantage and DatAlert in place, Hugh Chatham Memorial Hospital can easily identify who has access to which files, when they access those files and set triggers for any unusual activity, particularly for ransomware threat activity like mass encryptions. By increasing its security and preventing ransomware, Varonis has not only improved the hospital's overall security posture, it also means the IT team doesn't have to spend days recovering data.

IMPLEMENTING A LEAST PRIVILEGE MODEL

With the Data Classification Framework, Varonis was able to help Hugh Chatham Memorial discover sensitive content within its environment, see who had access to what, and help lock down access without interrupting the businesses workflow.

"We completely cleaned up the security of more than a terabyte of network file shares," said Powe. *"Seeing the results of the changes was huge. In any organization but specifically in a hospital, the end user's tolerance for change is pretty low. If you have nine hundred or a thousand users and only 5 or 10 of them are actually accessing the data available in an everyone group, it becomes a no-brainer."*

COMPLIANCE AND E-DISCOVERY REQUESTS

Powe added, *"When I receive a compliance request for a report on a particular user and their file activity over a specific period of time, it takes me less than a minute to run. Before Varonis, it would have taken hours and hours going through log files to try and compile a user's activity in relation to network file shares."*

VARONIS RISK ASSESSMENTS QUICKLY SHOW YOU WHERE YOUR MOST VULNERABLE DATA IS STORED, WHO IS ACCESSING IT, AND WHAT NEEDS TO BE DONE TO SECURE IT. FIND OUT MORE HERE.

ABOUT VARONIS

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis empowers enterprises to stop ransomware in its tracks, discover where sensitive data is overexposed, prioritize vulnerable and stale data, and lock it down without interrupting business. Varonis builds context around the content of data and activity; automates threat detection with predictive threat models built on advanced analytics, user behavior, and machine learning; and monitors critical assets for suspicious activity, including unusual access to sensitive data, abnormal user behavior and file activity to protect against potential exploitation.

All Varonis products are free to try for 30 days. Our systems engineering team will get you up and running in no time.

FAST AND HASSLE FREE

Our dedicated engineer will do all the heavy-lifting for you: setup, configuration, and analysis - with concrete steps to improve your data security.

FIX REAL SECURITY ISSUES

We'll help you fix real production security issues and build a risk report based on your data.

NON-INTRUSIVE

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.

START YOUR FREE TRIAL