Lexington Medical Center Tackles Ransomware for Improved Cybersecurity

The Customer

Location: West Columbia, SC

Industry: Healthcare

Products: DatAdvantage and DatAlert

Lexington Medical Center is a 438-bed hospital in West Columbia, South Carolina. It anchors a healthcare network comprised of five community medical centers — as well as Vista Clinical Research, a state-of-the-art research facility conducting trials in women's health, general medicine, and surgical devices — making data protection a critical concern for the hospital.

Named one of the "Top 25 Best Hospitals to Work for in the U.S.," Lexington Medical Center employs a staff of more than 6,500 health care professionals and treats nearly 85,000 patients, delivers more than 3,500 babies and performs more than 23,000 surgeries each year. The hospital is currently undergoing the largest hospital expansion in South Carolina history.

A Data Risk Assessment Shines Light on Security

Healthcare providers generate and retain highly sensitive information about their patients' health – making them prime targets of ransomware attacks and data breaches. Lexington Medical Center understood these risks and took action. Security staff focused on building a robust cybersecurity infrastructure from the ground up. With the sensitive data on their network, security staff knew they needed to find a solution for protecting the facility's unstructured data on their main network storage.

"Within healthcare organizations, one of biggest challenges is being able to monitor and govern data," said John Hensley, information security analyst at Lexington Medical Center. "If ransomware is able to get a toehold it then can potentially do a lot of damage. Being able to govern our systems, databases, mobile systems and more is vital. The amount of data generated by medical systems is like drinking from a firehouse — managing that flood of data in a way that keeps information protected and secured is vital."

With so much at stake, security staff at Lexington Medical Center did their homework. They researched how other healthcare institutions handled the issues of data management and protection, and reviewed recommendations from Gartner, a leading analyst firm. Lexington Medical Center decided to meet with Varonis based on its reputation and record of accomplishment in helping organizations protect their data, defend against attacks and automate manual data protection routines.

Varonis performed a complimentary Data Risk Assessment for the hospital to help them gain insight into their at-risk sensitive data. "The Data Risk Assessment provided by Varonis gave keen insight into the growth of our data over the past year, in addition to the number of sensitive and stale files," says Hensley. "It was a highly valuable report to obtain to share with leadership to assist in making strategic decisions. This provided a path for us to zero in on."

Choosing Varonis to Gain Visibility and Guard Against Ransomware

After receiving the results of the Data Risk Assessment, and with ransomware making news headlines, the Lexington Medical Center decided to purchase Varonis. They selected Varonis DatAdvantage to monitor its file access activity and streamline permissions management; DatAlert to alert to suspicious activity and unusual behavior; and Data Classification Engine to discover sensitive content, see where it is exposed and lock it down.

Implementation went quickly and smoothly. With Varonis, security staff gained control of their data to mitigate security risks. According to Hensley, Varonis' ability to defend against ransomware such as Locky played a major role in their decision to select Varonis: "DatAlert's ability to alert on anomalies that indicate a ransomware attack and scan files for possible ransomware infection was a huge selling point for us. In the months following deployment, Varonis alerted us to several ransomware attacks. In each case, we were able to shut down accounts quickly and minimize the impact."

Lexington Medical relies on Varonis to gain visibility into their on-premises data stores down to the file level — including what type of data they have, where it's stored, who owns it, who can access it and more. "You need to know where your data resides and who owns it. That was one of the absolute biggest challenges that we had and that was instrumental in helping us make the decision to buy Varonis," said Hensley.

After the initial deployment, Varonis returned to perform additional Data Risk Assessments to ensure the hospital's enterprise data remains secure to a least-privilege model. Staff presented the results to the Lexington Medical Center CIO to demonstrate the value provided by Varonis.

Future Plans

Looking ahead, Lexington Medical Center plans to expand the storage systems that Varonis monitors. The hospital has a vendor-neutral archive where imaging information — anything that produces a medical image for diagnostic purposes – is saved, and they're in talks to have Varonis monitor the system.

"We've been pleased with our ability to get meaningful data out of the products from Varonis," says Hensley. "Another big benefit of working with Varonis is having a business partner I can count on. I cannot say enough about Varonis support staff — they are top notch. I've had engineers work with me in the middle of the night. I can reach out to them anytime."