Canterbury Christ Church University Uses Rubrik Sensitive Data Discovery and Ransomware Investigation to Identify and Mitigate Data Risk

INDUSTRY

Education

RESULTS

- 6x faster time to complete searches for Freedom of Information (FOI) and Subject Access Requests (SAR) (12 hrs. vs. 3 days)
- Significant full-time employee (FTE) productivity savings with automated search
- No production impact or additional infrastructure required

THE CHALLENGE

- Limited visibility into sensitive data exposure risk for breaches, audits, or ransomware
- Significant FTE time required to adhere to FOI and SAR requests
- Increased complexity to adhere to current and future data privacy regulations

Canterbury Christ Church University is a public university located in Canterbury, Kent, England. Since its inception in 1962, the university has developed rapidly with over 15,000 students based at locations across Kent in Canterbury, Medway, and Tunbridge Wells. It is Kent's largest center of higher education for the public services and also offers academic and professional programs in various fields.

For Andy Powell, Head of Infrastructure at Canterbury Christ Church University, sensitive data discovery and management is top of mind, especially given the increase in ransomware attacks during the COVID-19 pandemic. "Prior to Sensitive Data Discovery, we had limited visibility into potential sensitive data risk, which can lead to hefty non-compliance violations, fines from the Information Commissioner's Office (ICO), and negative brand impact," said Powell. "Rubrik is unique in that it allows us to transform backup data into a strategic business asset that identifies trends or anomalies indicative of potential data security risks, such as compliance violations, data breaches, or ransomware."

STRONGER DEFENSE AGAINST RANSOMWARE AND DATA EXFILTRATION ATTACKS

"A primary driver for looking at Rubrik was ransomware. Since the pandemic began in March, the education sector has been heavily hit with ransomware attacks. For that reason, we wanted to ensure our critical data in Microsoft 365 was protected with Rubrik along with implementing Rubrik's data security products for stronger security posture," said Powell. "We bought Ransomware Investigation to proactively alert us to anomalous events. It continuously monitors our infrastructure for behavioral abnormalities that could indicate a potential security threat, like ransomware. We rest assured that we have best-in-class backup for ransomware remediation with fast recoveries and immutable backups that cannot be modified or deleted."

A new type of ransomware is on the rise where it exfiltrates data and threatens to publicly disclose organizations' sensitive information if they don't pay up. Powell said, "It's already bad enough to have a ransomware attack, and now we have to worry about a breach with sensitive data being potentially exposed. Sensitive Data Discovery helps us proactively secure where our sensitive data resides and who has access as well as can help us identify if data was exposed in a data exfiltration attack."

REDUCED TIME SPENT ON FREEDOM OF INFORMATION AND SUBJECT ACCESS REQUESTS

In the United Kingdom, the Freedom of Information Act entitles members of the public to request information from public authorities. In addition, Right to Access under General Data Protection Regulation (GDPR) allows any individual to obtain records of his or her personal information from an organization. Prior to Sensitive Data Discovery, the process to address FOI or SAR requests was very time-consuming and manual.

"For example, we got an urgent FOI request in the past that was very painful. It required significant infrastructure resources to facilitate this search. In order to not impact production, it would require at least one day to create a new virtual machine and another two days to restore from backups and index that data. This consumed valuable FTE time," said Powell. "Now, with Sensitive Data Discovery, we can create a keyword search and run it across all relevant shares at once. For that same FOI request, we got over 30,000 hits in half a day and could immediately export that information to legal. More importantly, we didn't need additional infrastructure to facilitate the search and it didn't impact production data."

INCREASED COMPLIANCE AND INSTANT VISIBILITY INTO AT-RISK PCI-DSS OR UK PII DATA

Powell and team use Sensitive Data Discovery to help identify potential locations of high sensitive data concentration and non-compliance violations. As a public institution, the university must comply with all relevant legislation in the United Kingdom, including health data for the National Health Service (NHS), credit card data for Payment Card Industry Data Security Standard (PCI-DSS), and general UK personally identifiable information (UK PII). "Given the evolving data regulatory landscape with new risks posed by Brexit, GDPR, and California Consumer Privacy Act (CCPA), sensitive data management is more important than ever. When we first ran Sensitive Data Discovery, we discovered PCI-DSS where it shouldn't be and potentially breaching significant guidelines. Since we were able to identify the root cause, we quickly fixed the issue and implemented new processes to ensure credit card data was being stored correctly," said Powell.

"Part of compliance is periodic cybersecurity audits. We have seen many public institutions face costly breaches. That's why we want to be proactive on how we are managing our sensitive data. Sensitive Data Discovery helps us continuously monitor and manage UK PII, credit card, and health data as well as prove to auditors what types of sensitive data is where," said Powell.

Additional benefits include:

- **Self-service for incident resolution**: "With role-based access controls, we can allow our Data Protection Officer and IT Security teams to effectively manage identified issues completely without further data exposure."
- **Easy to set up and manage**: "Since Sensitive Data Discovery leverages existing Rubrik deployment, it was very easy to turn on the software and get it up and running. It delivered high performance efficiencies leveraging our existing backup investment."
- **Custom patterns for search**: "We were able to define and search for our own regular expressions that are unique to our university, such as student identification numbers.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com