rubrik

Cranfield University Implements Rubrik Sensitive Data Discovery for Proactive Data Governance

INDUSTRY

Education

RESULTS

- Significantly faster time to address search questions (1 day vs. days to weeks)
- Identified and mitigated thousands of at-risk data for credit card and national insurance numbers
- No production impact

THE CHALLENGE

- Reactive approach to identifying and addressing risks due to lack of visibility
- Previous blind spots in what types of sensitive data exists where
- Increase in ransomware and security attacks calls for proactive mitigation measures

Cranfield University, a British postgraduate university, is a global leader for education and transformational research in technology and management. Every year, Cranfield University delivers academic courses in 50 countries outside of the UK and executive development to over 15,000 people. Cranfield is one of the UK's top five commercial research-intensive universities.

Matthew Verrier, Systems Manager at Cranfield University, manages the underlying infrastructure and core applications for the university, which includes ensuring data security. "Following the General Data Protection Regulation (GDPR), data governance and compliance has been brought to the fore. At the university, we created various new roles to ensure we are effectively managing data security. Sensitive Data Discovery will play its part in our overall strategy to discover what and where personally identifiable information (PII) is stored in order to improve processes," said Verrier.

POLICY-DRIVEN AUTOMATION TO ASSIST WITH REGULATORY COMPLIANCE

Cranfield University is currently using Sensitive Data Discovery to discover and report on Payment Card Industry Data Security Standard (PCI-DSS) data and United Kingdom PII across our virtual server estate. "When we first ran Sensitive Data Discovery, we detected thousands of hits that included credit card information, national insurance numbers, or user's tax references that needed mitigation efforts. We were able to quickly address which information was acceptable, what needed actioning and importantly, where individuals stored sensitive information in inappropriate locations."

With Sensitive Data Discovery in place, Verrier and team can now build repeatable processes to ensure the organization is meeting data governance policies. "We can now mark files that require further investigation and take action, such as removing or move data to the right locations. Similarly, we can add them to our exclusion/allow list so they are no longer flagged in future scans. If we identify where improvements can be made, we can approach the owners of the data sets directly in order to manage sensitive data more effectively," said Verrier.

For Verrier and team, it is critical to meet compliance requirements in order to avoid potential costly GDPR and Information Commissioner's Office (ICO) fines. Verrier said, "A major business consequence for non-compliance is brand damage and loss of reputation. Our university has numerous high-profile partnerships with global businesses. If sensitive data was exposed, it could put those relationships at risk. Our

team must ensure we meet not only our own, but also our partners' IT and security requirements with confidence."

FASTER CUSTOM SEARCH TO MEET ACCESS REQUESTS

In the United Kingdom, the Freedom of Information Act (FOI) entitles members of the public to request information from public authorities, similar to Subject Access Requests (SAR) under GDPR. Cranfield University must be able to address these types of requests within the time limit required. "In the past, a custom search could have taken days to weeks, especially if we were looking blind. With Sensitive Data Discovery, we can search across all our 400 virtual machines for a specific keyword or phrase within one day without impacting our business operations."

Additional benefits include:

- **Easy to set up and manage**: "Configuring was so easy. It just required implementing pre-built policies."
- **No production impact**: "Other data classification solutions would tax our production environment. With Rubrik, the advantage is it leverages our existing backup data and has no production impact."
- **Anomaly detection with Ransomware Investigation**: "We implemented Rubrik Ransomware Investigation to continuously monitor and alert us to suspicious or malicious activity. While we have not had a ransomware attack in the past, Ransomware Investigation makes us aware of any large- scale changes at a file system level to our virtual machines and allows us to investigate quickly."

rubrik

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

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

20220119_v1