Imperial War Museums improves visibility and control over its sensitive data

The Customer

Location: London, England

Industry: Arts & Culture

Products: DatAdvantage, DatAlert and GDPR Patterns

Imperial War Museums (IWM) is a British national museum organization, with branches at five locations in England: IWM London, IWM North, IWM Duxford, Churchill War Rooms and HMS Belfast. It was founded on 5th March 1917, to create a national war museum to explore conflict from WW1 to the present day.

The Challenge

Heading up the IT team of 37 staff is Ian Crawford, CIO at IWM: "The IT team provides a range of services to manage the IT and AV across all the museums and galleries. Security and the protection of data is an absolute priority, both from an operational and compliance perspective: this encompasses not only media assets but all sensitive internal data from financial records to employee information. It's important that we have full visibility of where sensitive data is and can protect it accordingly."

Although the team was able to extract file permissions information from Active Directory using Powershell, the existing processes were time consuming and cumbersome. Different scripts had to be run, and the resulting information required considerable fine-tuning to provide meaningful data.

One of the key drivers for improving visibility of data, network privileges and permissions was ensuring compliance with regulations; IWM must meet requirements for PCI DSS and demonstrate it can meet the compliance requirements for the National Audit Office and for its own internal security governance.

Protecting Data Permissions

Mike Simnett, IT Infrastructure Development and Security Manager, takes responsibility for developing security standards and best practices at IWM. He comments: "We really needed a solution which could improve the control, visibility and manageability of our critical data and provide evidence that the file permissions we have are secure and correctly assigned."

This was a particular challenge: in common with many organizations IWM found that permission 'creep' had set in over time, meaning that some staff had access to more data than they needed to do their jobs. As well as permanent staff, IWM works with outsourced partners and volunteers who will quickly need Active Directory accounts to access systems for short periods of time. IWM therefore needed a way to keep up to date with these changes and to revoke any accounts which hadn't been used for some time. Those user accounts that are no longer being used, but still have access to the network can represent a security risk as malicious activity can go unnoticed.

The Solution

In February 2016, following an initial proof of concept, IWM selected Varonis DatAdvantage and DatAlert, as they not only addressed its data security challenges, but also ensured that it could meet, and provide evidence for, regulatory compliance.

This ensured that the team has full visibility of where sensitive data is located, so it can be locked down, and of the file permissions for Active Directory. IWM operates a shared drive structure for each department; each of these has a data owner allocated for their area. On a quarterly basis, the team can run a report to show who has access to their folders and digital assets for projects or exhibitions. This is important not only for internal records, but also for material which is held under copyright and license and needs to be monitored accordingly. This gives IWM full control over access or changes such as when someone moves role or leaves the organization.

Ian Crawford comments: "We weren't aware of anything else in the market that matched the features and capabilities of Varonis. With easily understandable reports, we can now provide evidence that the file permissions we have are secure, and correctly assigned, in a fraction of the time that it took us before."

Business Benefits

IMW can also keep control over its stale user accounts and has fine-tuned its leavers' process to ensure that accounts which are no longer needed can be closed down. IWM now runs reports every month to check against any stale users or accounts which are no longer being used.

One of the main advantages has been the ease of use, as Mike comments: "It is now so simple to manage permissions. I particularly like the fact that I can easily make changes to a group or folder structure and, if you need to, you can quickly undo these. This is particularly important with large scale changes – with just one button these can be rolled back."

The team also has improved visibility into any changes on the network or unusual patterns of behavior with Varonis DatAlert, as Mike Simnett explains: "If, for example, someone is added to an administrator group we will get an immediate alert by email. The alerts will also be triggered if there are unusual patterns of behavior or changes in data usage, which could point towards ransomware or other malicious activity. It would be enormously time consuming to do this through Active Directory

logs. It's also useful from a bandwidth management perspective as it will identify if someone is sending out large files." With Varonis, IWM can now provide an audit trail for forensic investigations into any security issues and prove to regulators.

Compliance and Control

With Varonis, IWM can now provide an audit trail for forensic investigations into any security issues and prove to regulators that it has stringent IT controls in place around its sensitive data, including for PCI DSS. As part of its preparations for the EU General Data Protection Regulation (GDPR) compliance, the team is now planning to use Varonis's GDPR Data Patterns to provide a structured way of automatically identifying files that may contain Personally Identifiable Information (PII); from banking information to National Insurance numbers.

Since its deployment, IWM has been impressed not only by the ease of use, but also the ongoing assistance from Varonis's team, as Ian comments: "We now have a streamlined, manageable and robust way of obtaining information to ensure that we were not exposing data to any vulnerabilities. Coupled with this, the support has been excellent: from implementation to ongoing assistance, we've been really pleased with the team's support. In fact I'd say they have been one of the best we've worked with."