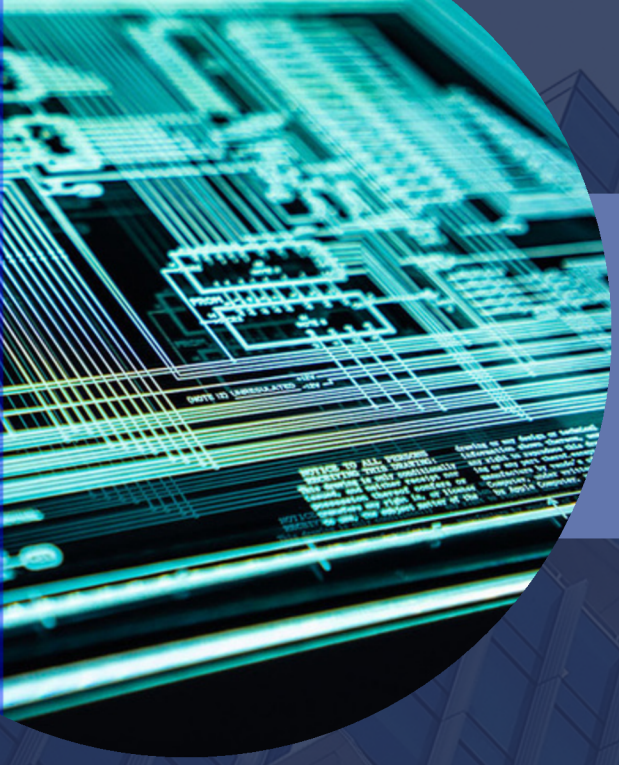

H2 Cyber Risk Advisory Services Ltd

FINANCIAL SERVICES CASE STUDY

Protecting SMEs from Cyber Security threats since 2016.

Background

A financial services company was struggling with data protection compliance and ensuring sensitive client data was properly secured. Some key challenges they faced:

- Large amounts of client financial data that must be retained for 7 years under industry regulations. This included data spread across multiple systems and endpoints.
- Difficulty tracking where all client data resided, especially with remote workers copying files locally. An employee spent 3 weeks trying to compile all data on one client for a subject access request.
- Concern about substantial fines under the Data Protection Act and GDPR if client data was breached. Fines could be upwards of £8.7 million or 2% of global turnover.

At a Glance

Challenges

- Large amounts of data
- Difficulty locating data
- GDPR fines from ICO

Benefits

- Rapid deployment
- Ongoing encryption
- Continuous monitoring

Kevin Hawkins

Director, H2

"Since 2016, H2 have worked with National and International SMEs to secure their data and provide ongoing Cyber Security support"

customersupport@hah2.co.uk www.hah2.co.uk 0800 494 7478

Solution

H2 suggested using the Actifile platform to automatically discover sensitive data across systems, encrypt it, and monitor data flows. Key capabilities:

- Automated discovery of personally identifiable information (PII) stored locally, on servers and in cloud apps used for collaboration. Quickly quantifies data risk exposure.
- Encrypts sensitive files to protect data regardless of where it resides across the hybrid work environment. Encryption causes minimal disruption to users.
- Continuously monitors movement of sensitive data to detect suspicious activity and data exfiltration risks. Detailed audit logs for forensics.
- Lightweight agents on endpoints ensure high adoption by employees. Cloud-based management minimizes ongoing admin workload.

Results

- Actifile deployed in less than 3 days without disrupting employees. Quickly discovered major data risk areas , specifically unprotected cloud storage instances.
- Identifiied and Encrypted over 80% of sensitive files, dramatically improving security posture. Remainder of files were tagged for remediation.
- Implementation of File movement monitoring enabled proactive alerts on suspicious data activities for further investigation. Addressed several risky IT uses.
- Automated subject access requests now possible with detailed data inventories. Access logs in Actifile's system. Report generation was reduced from weeks to minutes.
- With improved data protection controls now in place, the financial services company reduced their regulatory risk and business exposure substantially. Compliance process improvements also resulted.