



ALTERNATIVE SOLUTIONS

Who is Looking at Your Client Data?

The latest major leak of information, whether you call it the Paradise Papers or the Stolen Papers, is a serious concern to any company that holds private data about individuals. Regulations exist on how you hold and process data and we are all aware that these regulations will be stricter with the introduction of GDPR.

Whatever regulations are implemented, the potential damage to your organisation's reputation from a security breach is incalculable.

Appleby have stated that the breach was the result of a hacker, which is a third party who has gained access to and removed data from their systems. Whether a breach is due to a hacker or a disgruntled employee, the result is the same and private data is in the public domain.

Access Monitoring

Modern day applications have the capability to provide very detailed logging information. This data can prove useful in many scenarios and it is relatively simple to enable the capture of this information but making sense of the output can be very challenging - for example a server with verbose logging can generate a colossal amount of data in small amount of time.

Alerting and Reporting

Properly managed all of this data can be used to alert you about a wide range of potential threats where a user may be accessing data and could be vital in a legal case. Shown below are two sample reports that can alert you to such threats. The user could be an employee or it could be a third party who has gained access and is using a genuine account to attempt to steal information. By sending these alerts by email you can take immediate action to prevent a breach.

Excessive Access Permissions

Shows accounts with permissions for infrequently accessed files and folders. Use this report for spotting unnecessary permissions and preventing data leaks. Track permissions assigned to accounts directly or by group membership.

Object: \\fs1\Accounting (Permissions: Different from parent)

Account	Permissions	Means Granted	Times Accessed
ENTERPRISE\N.Key	Full Control	Directly	0
ENTERPRISE\T.Simpson	Full Control	Group	0
ENTERPRISE\P.Anderson	Full Control	Group	0
ENTERPRISE\K.Miller	Write and list folder content	Directly	0
ENTERPRISE\T.Allen	Read (Execute, List folder content)	Group	0

Establish proper control over access rights assignment

Ensure that regulated personal data is not made accessible to unauthorized employees by enabling strict control over access permissions.

Alternative Solutions Limited
PO Box 176, Cirrus House
Garenne Park, Rue de la Cache
St Sampson, Guernsey, GY1 3LQ

T: 01481 701234 F: 01481 715718
W: www.asl.gg E: info@asl.gg

Registered in Guernsey 16421



ALTERNATIVE SOLUTIONS

Stay informed about anomalous or patently illicit user behavior

Monitor user behavior for indications of a potentially malicious intent to unlawfully access or modify data.

Data Access Surges

Shows users who have accessed sensitive data they almost never accessed before (by default, the inactivity threshold is set to 2 actions). The report highlights previously inactive users who performed more actions within a short period of time (by default, 7 days) than during a considerably longer preceding period (by default, 30 days).

Path	User Name	Attempts
\\fs1\Office\Finance\Cardholders.xlsx	ENTERPRISE\J.Smith	19
http://spenterprise/Documents/Legal/Social Security Numbers.xlsx	ENTERPRISE\G.Johnson	11
\\vmcfs2\Office\Accounting\Budget2016.xlsx	ENTERPRISE\J.Rosenberg	6
http://spenterprise/Documents/Accounting/Budget2016.docx	ENTERPRISE\J.Rosenberg	3
\\nf1\Marketing\Backup\Passwords.txt	ENTERPRISE\D.Harris	2

In addition to the alerts, regular reports show that you are meeting the necessary regulations for protecting data. Reports can cover any area of the business, but typically relate to the following areas:

- Board level summary of threats and remediation
- GDPR reporting
- Compliance audits

Visibility Platforms

A visibility platform gives you the confidence that you are undertaking user behaviour analysis, mitigating risk and protecting your client data.

About the Author

Matthew Neville has worked in the IT industry for 20 years. He has extensive knowledge of IT infrastructure and runs a team of people who provide complete system support. As security of both systems and information has become more critical he has focused more on this area and has qualified as a Certified Information Systems Security Professional (CISSP). Matthew can be contacted on 01481 701234 or by emailing matthew@asl.gg.

Alternative Solutions Limited
PO Box 176, Cirrus House
Garenne Park, Rue de la Cache
St Sampson, Guernsey, GY1 3LQ

T: 01481 701234 F: 01481 715718
W: www.asl.gg E: info@asl.gg

Registered in Guernsey 16421