DLP Consulting Services

DLP technology has been around for years but today's high profile data breaches, GDPR regulation and an increasing move to cloud based services is fueling the demand for effective DLP solutions.

The loss of personal data and other forms of enterprise information can lead to significant financial losses and reputational damage. At Adarma, we help our customers manage and reduce these risks.

The range of potential ways in which data can be lost is huge. It can be accidental or deliberate, due to the actions of an employee or external hacker and can come from any device or IT service. Today's leading DLP solutions have broad capabilities to match this wide range of threats.

DLP is not "plug-and-play" technology deployed by IT. It has implications across your business operations and needs to be considered in the context of your regulatory, compliance and privacy management framework.

DLP identifies, monitors and protects data in use, in motion on your network, and at rest in your storage services or on desktops, laptops, mobile phones or tablets. Effective DLP can enforce your data security policies and protect against mistakes that lead to data leaks and intentional misuse by insiders, as well as external attacks aimed at data exfiltration.

Typical DLP Requirements

In our experience many customers have similar overall requirements from DLP but very different priorities based on their current level of maturity of data protection controls and perceived threats.

Typical requirements would include::

- Ensuring regulatory compliance.
- Protecting PII data from mis-use and loss.
- Protecting confidential business data from mis-use and loss.
- Ensuring protection of data extends to all devices including BYOD and mobiles and all services including cloud.
- Protecting against accidental loss by well intentioned users through email and web services.
- Gaining control over data stored in cloud services and storage.
- Ensuring data is stored in the right locations so as to reduce the chance of mis-use and loss.
- Providing evidence for use in internal disciplinary or external legal actions.

Challenges facing a DLP programme?

A DLP programme has a broad technical scope but also a wide impact aross an organisation, affecting end users and business processes. Here are some of the challenges we have identified that businesses face when undertaking a DLP programme:

- There is often a lack of clarity around where confidential data is being stored, where it's being sent and who is accessing it.
- Current efforts are usually focused on protecting PCI and PII data as it is easier to identify this information than commercially sensitive data specific to each customer.
- DLP has often been implemented for privacy or compliance requirements and is not fully leveraged by cyber security teams.
- Often ownership and responsibility for data classification and labelling is not devolved outside of IT or Security teams.
- Getting business engagement (outside of IT Security) to prioritise requirements is often something that companies have never tried to do before.
- Many DLP implementations never move beyond 'monitoring' to 'blocking' mode due to concerns over false positive alerts and interrupting business processes.

What does DLP consultancy from Adarma look like?

We have helped many customers through DLP implementations – from initial strategy, through implementation and into ongoing management. We have used our experiences and insights to create the below set of consultancy offerings that can accelerate customer progress and success by leveraging our pre-defined frameworks, processes and artefacts.

- Assessment and Direction – to understand the requirements for DLP and effecitveness of any current DLP solutions.
- Strategy – to define the people, process and technology strategy for DLP; typically as a overall programme which increases in maturity over multiple phases.
- Architecture and Design – to help customers architect the tools and processes to support their strategy.
- Implementation and Deployment – to implement the DLP technologies but also the required service processes, people training and integrations required for an efficient BAU service.
- Operate and Manage – to support customers in on-going management and continual improvement of their DLP solution.

The Adarma way

Our experienced consultants can help customers drive maximum value from their DLP investments and create a valuable platform that provides insight into data usage and prevents data loss incidents. Typical capabilities of a DLP service developed in conjunction with Adarma include the following:

Low false positives. A thorough understanding of business processes and data types, combined with the best detection technology and a standidised framework for managing the full life-cycle of policies results in low false positives.

Protecting the right data. With our approach to data discovery we ensure that the scope of customer's data protection capabilities go way beyond the obvious compliance based data types such as PCI and PII data.

Integration and Automation. By integrating DLP technology into standard enterprise workflow and service management tools, as well as security monitoring (e.g SIEM) tools customers minimise the management overhead of DLP and maximise the valuable insights and intelligence gained and ensure response actions are consistent and auditable.

Actually reduce data loss. By adopting our DLP frameworks and following a defined process for service management DLP policies can be confidentlty moved to 'blocking mode' to stop data loss without causing inconvenience to the customer.

Extending visibility and control to cloud services. By integrating CASB technology as an integral component of DLP customers get consistent detection and protection regardless of whether services and data are cloud or Data Centre based.

SOC integration. With relevant integration into the SOC (Security Opereations Centre) customers can ensure that cyber anaylsts have access to the additional context and information contained with DLP when investigating possible data exfiltration as a result of a cyber breach.

User education and engagement. User awareness of the principles and best practices of DLP can be massively increased by appropriate engagement and communications as part of the DLP programme. This can significantly reduce the risk of data loss and lessen the dependency on technology solutions to DLP.

Why Adarma?

At Adarma, we are passionate about helping customers to reduce data loss. DLP technology is part of the solution but to be truly effective a DLP programme requires well designed people and process components. DLP needs to take a holistic approach and integrate tighly with existing enterprise tools and systems.

For the past 10 years Adarma has been helping FTSE 100 companies understand their threats and respond with appropriate technology, process and people solutions.

Our DLP consultants hold certifications from industry leading vendors and have unrivalled experience in delivering transformational DLP capabilities for customers.

Adarma are uniquely positioned to help customers ensure their DLP controls interconnect effectively with their SOC and Risk, Compliance and Security Management programs.

We are Adarma, one of the largest independent security services companies in the UK. As a business formed and run by veteran senior security leaders, we know security and how to deliver real value in the real world. This is why our clients are successful FTSE 250 organisations from all industry sectors.

See us as your true partner in security. We have the experience, proven track record and industry recognition, to provide best-of-breed services for all our clients. Our team are specialists in Threat Management including SOC design, build & operation. And we always tailor our cybersecurity services to your needs

Contact us to discuss your DLP requirements enquiries@adarma.com

www.adarma.com