

DLP TAGGER

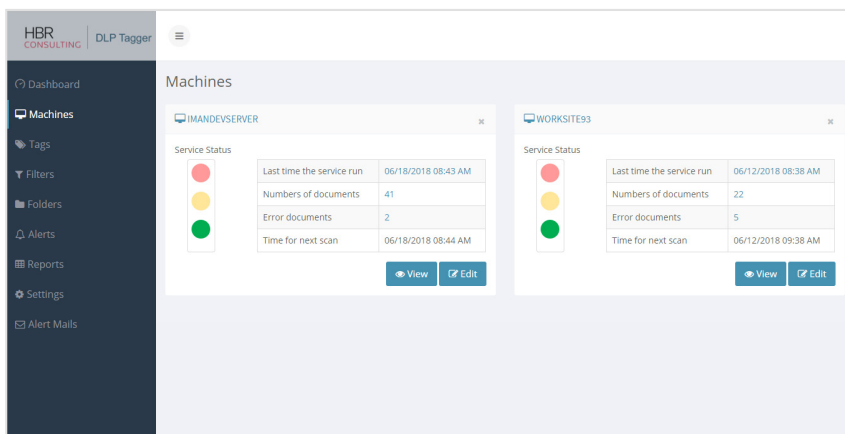
TECHNOLOGY SOLUTIONS MUST KEEP PACE WITH INCREASING SECURITY DEMANDS

It is critical for law firms to comply with client-directed rules to prevent all data leakage. Unfortunately for information security executives and IT buyers, traditional data loss prevention (DLP) solutions fall short. They are too broad and inflexible. Because these solutions were not designed for the legal industry, their filters rely on Personally Identifiable Information (PII) or account strings that are not relevant to the Matter.

HBR DLP Tagger is a data loss prevention utility specifically designed to close this gap and make existing systems more effective at preventing data leakage. DLP Tagger is unique in its ability to integrate with industry leading document management systems (DMS). As a flexible, configurable and lightweight add-on, the utility automatically tags responsive documents with custom attributes such as client and matter numbers. DLP systems can then use these attributes to filter appropriately.

KEY FEATURES

- Scalable to multi-servers at no additional cost
- Optional web-based UI provides dashboard reporting and proactive email alerts
- Natively apply tags for the following: client, matter, author, and document type
- Create and apply custom tag sets to documents
- Filter to apply tags only to specific clients and/or workspaces
- Supports hash tagging for performance and scalability



In addition to its comprehensive dashboard, DLP Tagger includes a customizable reporting feature. Create detailed reports based on specific date ranges, machine names, client matter or document number as well as status.

TECHNICAL SPECIFICATIONS

HBR DLP Tagger was designed to work seamlessly with your existing DMS systems, making them more successful at preventing data loss.

Setup is simple – a one-time configuration and then let it run. With DLP Tagger, you can reduce the risk of data leaks and prevent documents from unexpectedly being sent outside your network.

Supported platforms currently include:

- iManage (on-premises and cloud)
- NetDocuments
- Windows folders (file shares)

The following file types are supported:

- .doc, .docx
- .msg
- .pdf
- .ppt, .pptx
- .xls, .xlsx

Known DLP endpoint compatibility:

- Workshare Secure
- Proofpoint
- Forcepoint

“With cyber threats like email phishing schemes on the rise, email security is more paramount than ever. Because DLP Tagger applies tags like client, matter or security classification to DMS documents, law firms can finally leverage DLP solutions to comply with outside counsel guidelines and other client-driven data security requirements.”

– Scott Springer, Senior Director
HBR's Software Solutions practice