DLPX
DATA LOSS PREVENTION EXPERTS

A DLP EXPERTS WHITE PAPER
SEPTEMBER 2019

DLP TRUTH AND CONSEQUENCES

HOW VISIBILITY WILL CHANGE YOUR DATA PROTECTION STRATEGY

DLPX
DATA LOSS PREVENTION EXPERTS

DLP TRUTH AND CONSEQUENCES

HOW VISIBILITY WILL CHANGE YOUR DATA PROTECTION STRATEGY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

While the data loss prevention (DLP) vendor landscape has changed over the last decade, the technology approach and architecture largely remain the same. Aside from some minimal feature innovation, by and large, leading DLP vendors still hold to the three-pronged coverage approach of network, discovery and endpoint. The old adage, "If it ain't broke, don't fix it," is the mantra of most DLP vendors and the marketplace doesn't seem to be challenging this mindset. But, if you consider the growing list of recent – and very major – data breaches, it's hard to argue that the traditional DLP approach is working as effectively as expected.

Of course, there will always be some amount of data loss, but with the level of massive data breaches we've seen in recent years, you would expect the marketplace to demand new technologies that can protect data more effectively. DLP vendors and their technologies have reached a level of maturity and there is little room for the innovation required for increased data protection effectiveness.

Over the course of 12 years focused exclusively on DLP and other data protection technologies, we have found the key to improving data protection effectiveness is data activity visibility, as explained further in this paper. Data visibility technologies and services, combined with existing data protection technologies, can be used to drastically increase data protection effectiveness.

FOUR TRUTHS ABOUT DLP

Like most things in life, DLP technologies are not perfect. For the purposes of this paper, we'll review four key truths about DLP that have significant and lasting impact on the technology's capacity to protect data. While these truths are not disputed by DLP vendors, they are certainly areas less-visited by vendor sales teams. Please note that there are some vendors with slightly different approaches to DLP that allow them to avoid some of these challenges.

1. Content-Focused Data Detection

Traditional DLP solutions focus almost exclusively on inspection of textual content. For example, DLP solutions inspect text to detect regular expression pattern matches, such as 555-55-5555 (US social security number) or 4444 4444 4444 4444 (credit card number). Or does the text include identifying keywords like "social security" or "credit card."

Unfortunately, this can be a disadvantage in a number of scenarios. If the file in question includes no textual content, as might be the case with some intellectual property in images or CAD drawings, DLP often has a hard time determining data sensitivity. Some DLP solutions have OCR capabilities, but these work only in select situations can be error-prone. Perhaps more importantly, content can simply be manipulated to hide sensitive data. Defeating content aware sensitive data detection methods can be as simple as adding some X's and O's:

- Changing a last name from "Johnson" to "John**X**son"
- Changing a social security number from "555-55-5555" to "555-5**O**5-5555"

These simple methods can easily avoid sensitive data detection.

We don't want to leave you hanging, so here are the last three of the four truths:

2. DLP Inspects Only on Data Egress Events
3. DLP Requires Known Policies
4. DLP Logs Only Policy Violations

To read more about these DLP truths and how visibility will change your data protection strategy, download the full paper:

https://dlpexperts.com/prove-improve-data-loss-prevention