Demystifying Data Leakage Protection (DLP) Technology

By Michael Gabriel, Senior Partner & Data Protection Leader

Data Leakage Prevention **(DLP)** software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).

It was originally intended to prevent unintended sensitive data leakage, which happens all the time and goes mostly unnoticed until it has been determined to be the cause of a data breach. For example, when I was a Chief Information Security Officer (CISO) for a Fortune 1000 educational organization, an admin at one of our ground schools in Colorado created a report of all students enrolled to attend that school for the next two semesters. When the admin went to save the report, she accidently clicked the name of an existing file called “Fall Schedule”, and that file was overwritten by the new report containing student records. Later that week, she went to send out the schedule to a large list of prospective students, sending the inadvertently renamed “Fall Schedule” file containing about 1200 existing student records, including their SSN’s. This was not a large data breach as data breaches go, but still cost the organization over $500,000 to resolve.

DLP software can monitor sensitive data on the network, endpoint, or in storage using a variety of detection mechanisms (e.g. regular expression matching, data fingerprinting) to identify sensitive data and can apply workflow to activities involving sensitive data (e.g. asking for management approval or blocking a transmission). DLP can be used to enforce a data architecture that segments sensitive data in particular protected environments, and can also be used to create a smaller sensitive data footprint in the organization, making your sensitive data a smaller target for attackers.

In the past, DLP has been seen primarily as a large, enterprise security solution due to its prohibitive cost. A large component of that cost is associated with the professional services required to integrate the technology into the organization’s critical business processes. Organizations that tried to cut corners, or implement DLP as a purely IT initiative (without business involvement), quickly found that DLP can also be a powerful business disruption tool. As I like to explain to people unfamiliar with DLP technology, its power lies in the fact that it works at the data layer (unlike most security technology), with the ability to block or redirect sensitive data transmissions. ***Because data is the lifeblood of any business, preventing legitimate data from flowing where it was intended to go is the equivalent of inducing a stroke in the organization’s business processes.***

The good news is that a new generation of DLP software is being rolled out that aims to automate a good percentage of the implementation activities that previously required highly-skilled professional services staff. Products like GhangorCloud DLP (www.ghangorcloud.com) now provide automation around setting up access control profiles, classifying the organization’s data, and produce DLP rule sets to provide protection around where sensitive data can be sent, where it can be stored, and how it can be used within the organization.

Coupled with lower licensing fees than traditional DLP software, this results in a powerful data protection tool that is solidly within the reach of most mid-tier organizations. This will be particularly appealing to mid-tiers who are also migrate3d part of all of their infrastructure to the cloud, as DLP remains a key cloud control for determining which information can be sent and stored in cloud applications like Box.

DLP is a technology that, while largely adopted in the enterprise space, has received a less-than-stellar reputation for its high costs and its reliance on a highly-skilled workforce. When implemented improperly, it has resulted in business disruption and promptly turned off. But the new generation of DLP products (like GhangorCloud DLP) is changing that perception and bringing a powerful data protection tool to the mid-tier, just in the nick of time.