The next wave of smart Data Loss Prevention solutions

Roman Foeckl, CEO at CoSoSys May 25, 2016

Data Loss Prevention has evolved beautifully in the last few years. The measure of control that DLP now provides is extremely powerful, and helps organizations from all sectors and of all sizes minimize the risk of data theft and loss, and protect their intellectual property as well as other type of sensitive data.

DLP is divided in several categories: endpoint DLP, gateway DLP and, depending on where data resides and how it is used, there is DLP for data at rest, DLP for data in use and DLP for data in motion.

DLP solutions can detect complex regular expressions, keywords, PII, healthcare data, and other type of data, and can cover a wide range of exit points: removable devices, web browsers, email clients, instant messengers, cloud file sharing apps and other online and cloud services. Besides control, the system also offers detailed reports for increased visibility into data that users are transferring outside the company.

Even false positives rates have decreased. They are now addressed by DLP vendors with solutions like thresholds, whitelists, fingerprinting and other techniques. False positives currently mostly occur if DLP systems are not adequately configured and fine-tuned.

However, there is still room for improvement. We predict that in the next couple of years, Artificial Intelligence (AI) will drive the next wave of smart data leak / loss prevention solutions, impacting detection capabilities at all levels.

Intentional or accidental losses will be prevented, tackled in early stages and stopped by applying intelligent algorithms.

AI will also pave the way for the inclusion of effective learning of data transfer and manipulation patterns as part of the Data Loss Prevention solutions of the future. You can add to this self-repair capabilities and the capability to self-adjust detection and control techniques.

There are two approaches for the implementation of AI:

1. DLP vendors will design their own AI systems based on Big Data leveraged from large installations.

2. AI providers will customize the technology to be used by vendors in different information security categories, including DLP.

We believe there is room for both approaches. On one hand, AI experts will be able to use their extensive knowledge to create efficient and highly intelligent security algorithms. On the other hand, “in-house AI”-based DLP solutions will reshape the market – AI will be molded and shaped according to the DLP needs, making it more efficient for this precise technology.

Another DLP concept that will become really familiar in the near future is that of context-aware protection.

Current DLP methodologies do not consider outside factors and contextual information in the analysis of data. For example, should a Financial Manager have access to the organization’s financial records on his smartphone when he is at lunch? Should he be granted access only based on the trustworthiness his job title implies?

Same as in our daily life, there is no black and white in data security, and contextualization holds the key for identifying the multiple shades of gray of data threats. Process analysis encompassing both data and action, along with a snapshot of the world at the moment the action occurred, will reshape prevention and techniques for

risk handling.

Technologies like beacons and geo-location will contribute to the improvement of DLP and AI, enriching the data set required to detect security violations. To avoid privacy issues, vendors should clearly communicate to businesses what data will be collected by context-aware DLP solutions, and organizations should do the same with their employees, along with informing them about the scope of the implementation. Communication is the key to make sure all stakeholders understand and accept the implementation terms.

There are numerous systems that are crossing the fine line between personal data and business data. But, like containerization in the Mobile Device Management context, context-aware DLP solutions will benefit from technologies that differentiate between appropriate-to-share-sensitive data contexts and those that are quite the opposite.