POINT OF VIEW

Data Loss Prevention (DLP) Pre-Implementation – GAVS Approach

Hariharan Madhavan
GAVS Security Operations Centre

To discover how GAVS can help you innovate and bring greater value to your business, write to inquiry@gavstech.com or visit www.gavstech.com.

Introduction

DLP implementation requires some preparation from the organization before choosing a product or proceeding with an implementation. This paper seeks to throw light on such considerations to help a client organization choose both the right product and partner for implementation.

What is to be protected?

The answer to the above question will differ for every organization. Right from trade secrets to patents, to classified corporate documents to PII, PHI or card- holder information, the needs are to be assessed and documented as part of the initial study. Organizations who jump into a DLP implementation without doing this basic study will not get ROI from a DLP implementation. Once this is documented clearly, it will help to a great deal during implementation and configuration of DLP rules.

Where is the information to be protected?

The second question to be answered is where the information to be protected is. Classified information could be present in file servers, FTP servers, document management systems, emails, mobile devices, virtual machines, cloud storage, external drives, printers, and chat logs. This list is to be made ready, since the DLP product should address transfers to and from all these mediums of information storage. If this list is unavailable, we might end up buying the cheapest DLP product in the market, not the one which addresses the mediums in which we have classified information.

Where is the information to be protected?

Products in the market have the capability to discover and index classified information in your file servers and selected destinations. The discovery capability should clearly be enquired with the product vendor as to what the targets are on which discovery will be supported. At a minimum, file servers are definitely supported, anything beyond that up to cloud storage is different for each product. For example, one may be using box storage in his/her organization, whether the DLP product would support discovery there, is something one needs to clearly ask the product vendor.

The best thing to do is to actually get data classification done without relying completely on product's discovery capability. For example, if the target organization has 4 classifications, an implementation vendor can help run automated classification scripts in the file shares based on certain criteria or business rules in the documents. Affixing the classification henceforth can also establish document classification awareness among employees. Once documents are classified, excessive reliance on discovery can be minimised and even simple DLP products can be subscribed. This is very crucial to DLP environments with a large endpoint footprint where the DLP total cost of ownership can literally run into millions of dollars per annum as licensing cost.

Workflows for Incidents

When an incident is triggered, it is usually mined by a DLP incident analyst and forwarded through the relevant workflow for the concerned department manager or head to decide on the infraction, and whether it requires any initiation of sanctions against the concerned employee. The workflows and the incident responses vary from each organization and it is important to understand whether the client requires a simple workflow as described above or a more detailed workflow such that no manager is able to simply accept a violation and collude on the security incident. Depending on the requirements of the client, the product needs to support essential features to make the solution functional and effective, and the implementation vendor needs to customize the features in the product to make the solution functional and effective.

Incident Tuning

During the initial 3-4 month of the implementation cycle, the DLP incident management team would have to find means of reducing noise without suppressing material incidents. This is definitely a balance between reducing noisy incidents and without nullifying the purpose of DLP deployment. Optimization of DLP rules come only through experience and the DLP vendor's support during this period defines how effective the solution is going to be post the 4th month. Choosing the right vendor can help a client organization during this phase, as most vendors are keen to get the solution up and running and leave the client organization to some professional services group during optimization stage. Improper optimization can lead to extremely noisy DLP environment leading to oversight of security incidents or neglect also if there is no dedicated DLP monitoring team.

Conclusion

Based on the considerations and analysis as stated in the paper, product selection is to be made on a basis that will fulfil all the requirements, constraints and criteria as defined in the beginning of the solution requirement identification. There have been more1 failed DLP implementations than successful ones for the reasons stated above and hence appropriate caution is to be exercised before finalizing the implementation vendor and purchasing the product licenses.

References:

- Top 6 Reasons Why Data Loss Prevention(DLP) Implementation Fails retrieved 31th July 2016 from CISO Platform http://www.cisoplatform.com/profiles/blogs/top-6-reasons-why-datalossprevention-implementation-fails
- Symantec Administration Guide 14.5 retrieved from Symantec Partner Library
- Websense Data Security Deployment guide retrieved from http://www.websense.com/content/support/library/data/v78/deploy/deploy_dss.pdf

About GAVS

GAVS Technologies (GAVS) is a global IT services & solutions provider enabling enterprises in their digital transformation journey through infrastructure solutions. GAVS services and solutions are aligned with strategic technology trends to enable enterprises take advantage of Bimodal IT trend managing current operations, transforming them through IT Operation analytics, automation, cloud orchestration and DevOps.

GAVS has been recognized as a Cool Vendor by Gartner in Cool Vendors in ITSM 2.0, 2016 and positioned as an Aspirant in Everest Group PEAK Matrix ™ for Healthcare Provider IT Services. GAVS was also rated as a prominent India-based Remote Infrastructure Management player & one of the key small players serving the mid-market & enterprise clients in North America by Gartner.

USA

GAVS Technologies N.A., Inc
10901 W 120th Avenue,
Suite 110,
Broomfield CO 80021, USA
Tel: +1 303 782 0402
Fax: +1 303 782 0403

GAVS Technologies N.A., Inc
116 Village Blvd, Suite 200,
Princeton, New Jersey 08540, USA
Tel: +1 609 951 2256/7
Fax: +1 609 520 1702

GAVS Technologies N.A., Inc
50 S Main Street, Suite 200,
Naperville, IL 60540, USA
Tel: +1 630 352 2255
Fax: +1 630 352 2301

UK

GAVS Technologies (Europe) Ltd.
3000 Hillswood Drive,
Hillswood Business Park,
Chertsey KT16 ORS,
United Kingdom
Tel: + 44 (0) 1932 796564

INDIA

GAVS Technologies Pvt. Ltd.
No.11, Old Mahabalipuram Road,
Sholinganallur, Chennai,
India - 600 119
Tel: +91 44 6669 4287

Middle East

GAVS Technologies LLC
Office No. 11, 5th floor,
Building No. 4,
Knowledge Oasis Muscat,
Rusayl, Sultanate of Oman
Tel: +968 24170606
Fax: +968 24166255

GAVS Technologies
P.O. Box: 124195, Office No 202,
Al Thuraiya Tower 1
Dubai Internet City
Dubai, UAE
Tel: +971 4 4541234

For more information on how GAVS can help solve your business problems, write to inquiry@gavstech.com.