CompTIA

Data Loss Prevention: A Step-by-Step Guide to Blocking Leaks

Industry analysts report that of all the active DLP installations, over 90% are running in 'monitoring only' mode. This means they notify an organization when data has been leaked but they do not stop it. You have to question why these DLP solutions are not being deployed to proactively prevent the leakage of data, a function they were supposed to be designed for. It appears that this is down to the impact the DLP technology can have on an organization's day to day business. The solutions can have high false positive rates which means a lot of false triggers that have to be looked at. If the solution was active, a false positive means you just prevented an employee from doing their work. Tuning the current solutions for lower false positives typically raises false negatives which means you could be missing instances of data leakage. To make these solutions more effective and accurate you need to spend time training them with each type of confidential content which can be very time consuming.

So the approach to deploying DLP solutions needs to be carefully thought through and planned. To assist you in this task here are the key steps that you should consider to ensure you implement a successful DLP strategy:

Step 1: Do You Really Need a DLP Solution at the Moment?

The first question to ask, believe it or not, is actually whether you really need a DLP solution at the moment. The reason for this question is that the technology and capability of DLP solutions is improving all the time, so the longer you can delay the implementation, then the better the product – so the theory goes. I am not advocating putting your organization at risk, but DLP is a strategy that needs careful planning.

Step 2: What Type of Solution Do You Require?

There are many different types of products on the market that promise to solve DLP such as hard drive encryption products or endpoint port control solutions. While they may address one of the ways that data loss can occur they do not address the issue as a Content-aware DLP solution will. Content-aware DLP solutions focus on controlling the content or data itself.

There are two different types of Content Aware solutions:

1. **Single Channel solutions** – Focuses on just the data loss channel you want to address such as email or Web.

2. **Enterprise DLP solutions** – Involves lengthy implementations and big budgets. It can also be very disruptive to the organization but delivers much more coverage.

However, just because you are an enterprise don't assume you need an Enterprise DLP solution. Don't think automatically that you will need to go out and buy a new product. You might find that your incumbent vendors for email or Web might have a good enough range of products to meet your current needs and a solid roadmap to ensure they will continue to meet your needs in the future.

Step 3: Identify What You Want to Protect

If you know exactly where all the content is that needs to be protected, then you are well on your way. If you don't, then you will need to consider using a data discovery solution to answer this question first and also make sure that you address this issue by ensuring you have control over where what types of content are saved. This will pay dividends in the future.

Step 4: Establish Why the Content Needs to Be Protected

Is it for compliance reasons or for protection of Intellectual Property? This could change not only how the content is identified but also how it is reported on. For compliance, you will need to ensure that you meet not only the data coverage required, like credit card numbers and other personally identifying information (PII) as required for PCI DSS compliance, but also the reporting requirements for the auditing process. For IP control, perhaps the solution has to recognize source code, or perhaps cad files? Ensure the solution you select has the coverage and is easy to teach for your required data types. Don't take the vendor's word for it. Try the solutions out against your data and compare different solutions. This is going to be a critical step in the success of your DLP solution, so you need to give it the time it deserves.

Step 5: Identify How Data is Currently Lost

This will help you determine the type of product to use. Is it through email? Is it being uploaded to websites such as Web email or blog sites? Is it the usage of USB sticks on your endpoints? The most important advice here is not to try to solve all possibilities that you can think of for data loss. You have to remember that what you are trying to stop is the accidental loss of data. If you are trying to stop the deliberate loss of data, then that is significantly more difficult and will quite definitely have a serious impact on your business. If the user is resourceful and knowledgeable enough they will find ways to do it. An audience that many companies forget about is the remote user and the devices they use off-site. People will be more bold and daring if they are not in the office of their organization.

Step 6: Policy Creation

This is where we get down to the implementation. Once the solution is installed we now look at how we can create policy that recognizes the actual content we want to control and then how it will be controlled. The above steps that you have gone through will help you what should be in the policy and how you can prevent the information from leaking out of your organization.

Step 7: Testing

Like any other IT implementation testing is a major factor for ensuring success. You need to do a significant amount of testing with this, always better to be run initially in monitoring only mode to gauge the impact while you are tuning the controls. The testing will help you to fine tune the policy and how it is enforced in the future.

Step 8: Policy Communication

A step many miss. Employees need to be brought into the project to guarantee success. It will impact their day-to-day functions, so you need to be certain they understand why these controls are in place and support its use. This can be as simple as explaining why you are implementing such a control and what could happen if you didn’t. Obtain their feedback on the controls and how you might minimize the impact on their work.

Step 9: Policy Enforcement

Now that we have created the policy, tested it and communicated it, time has come to throw the big switch between just monitoring controls to actively implementing them. Don’t turn them all on at once. Prioritize them and release the most important and critical ones first. Ensure you have plenty of coverage to rectify any issues not found in testing as they arise, as this will impact the employees who are trying to do their job. If you are not helpful or responsive, your employees’ support will vanish!

Step 10: Future Proof Your Organization

You have taken the first steps here, but don’t assume your job is done. Look for better ways of classifying content or where different types of content are saved. When new applications or systems are installed, consider how you can implement them to simplify the DLP controls required. Also continue to pay attention to the evolution of your DLP product. Keep it up to date as there will be newer and better ways of implementing the controls you have in place.