

The Who, What, When and Why of Data Leakage Protection/Prevention (DLP)

The digital age has brought about a level of convenience and access to services that were never before imagined. It has also ushered in a whole new set of challenges in privacy and confidentiality. Whether it's through e-health records or online applications for services, governments are collecting and storing ever-increasing amounts of data. What are the critical steps to protecting this data, and ultimately, the privacy of citizens? This session discusses strategies and technologies critical to protecting confidential data.

Presented by: Archie Alimagno
California Department of Insurance

2009 Data Leakage Study

The 2009 Ponemon Institute study notes that data breach incidents cost U.S. companies \$202 per compromised customer record in 2008, compared to \$197 in 2007. The average total per-incident cost in 2008 was \$6.7 million, compared \$6.3 million in 2007.

The Who

The What

The When

The Why

The Who

- Who will sponsor your DLP project?
- Who makes the decision to implement DLP?
- Who implements and monitors the DLP?
- Who secures the resources (not just \$'s)?
- Who will write the policies and procedures?
- Who can help me in this endeavor?

The What

- What different types of data are in your environment?
- I mean, do you really know?
- What protects that data?
- What procedures are you going to have in place to protect the data?
- What are some experts saying?

The What

✓ Mogull says. “While DLP can't solve data security, it's a powerful risk reduction tool,” he says.

✓ “The main driver for this increase, according to Andrew Jaquith, is that organizations want to safeguard crucial corporate and customer information.”

✓ “DLP enables organizations to minimize the threat of misuse or loss of important business data and puts controls in place that help organizations comply with regulations, ensure data privacy and reduce overall business risk,” (Gijo) Mathew says.

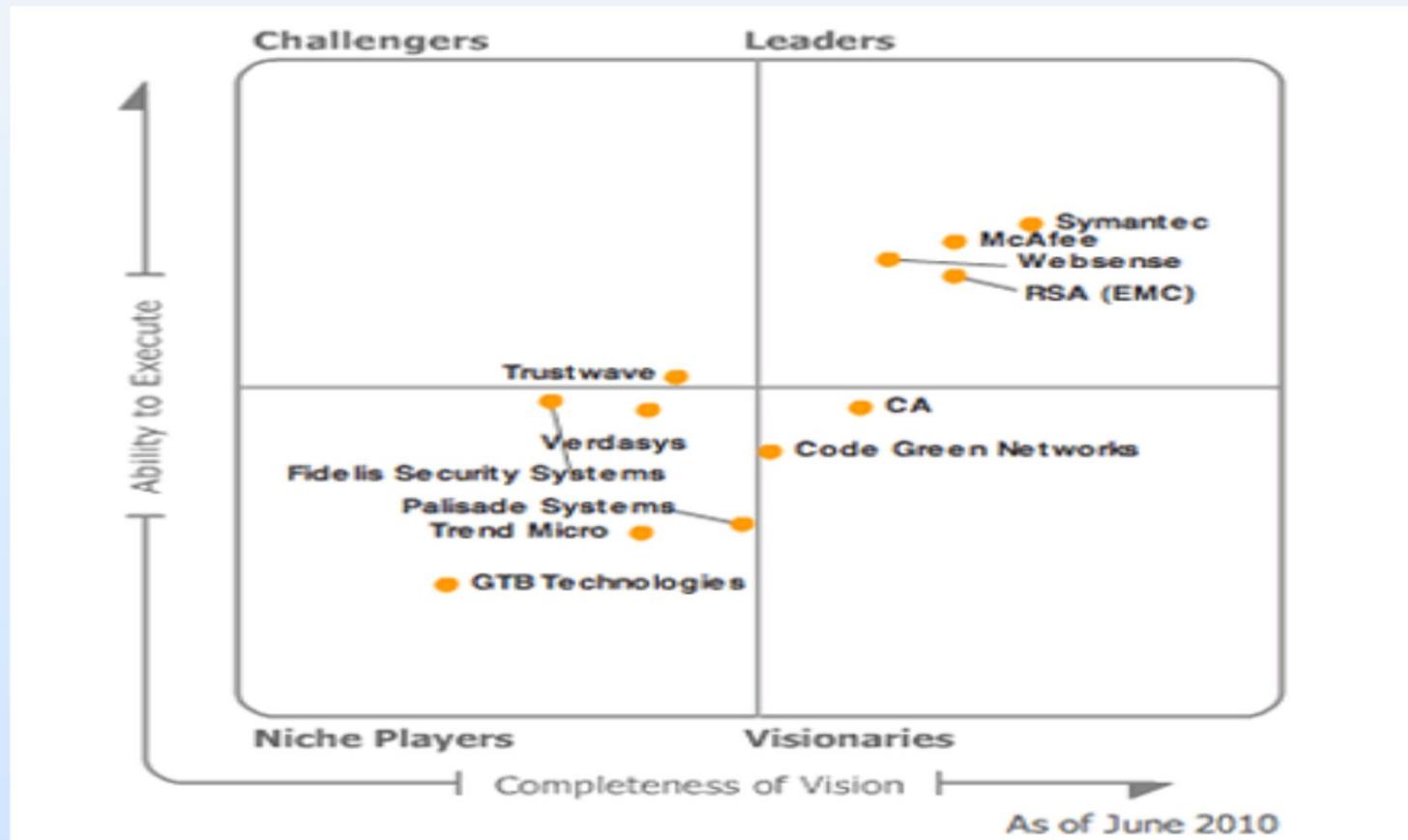
✓ “Unauthorized dissemination of this data, whether it is intentional or not, could substantially harm a company's competitiveness and reputation, and could also get it into hot water from a regulation and compliance perspective,” (Rod) Murchison says.

Source: <http://www.scmagazineus.com/data-leakage-prevention-reducing-risk/article/136039>

The When

- When should DLP be implemented?
- When is the threat to your data real?
- When should I contact vendors; or should I contact vendors?
- Will using the Gartner Magic Quadrant or similar documentation help my department?
Yes, but don't let that be the deciding factor.

The When



The Why

- Why do we need to invest in additional data protection?
- Why is data so hard to protect?
- Why is DLP a potentially resource hungry function?

The next slide provides some insight and answers.

The Why

- ✓ There is a huge misconception that organizations can just add another piece of infrastructure to solve data leakage problems. While securing the network is an important step, of course, but this does not necessarily result in truly improving the overall security of what enterprises care about—PII, PCI, HIPAA, confidential/sensitive data, etc.
- ✓ Today's networks and applications were designed without taking into account the overall security of information. The connectivity of "all" business networks to each other through the Internet was never in fact designed with that in mind--it just happened. **As such, the infrastructure actually has no context for what the exchange of information means leaving many gaps in network security.**

The Why

When you examine your environment, you will see that there are laptops, servers, smart phones, mobile phones, social networks; can you monitor **and** prevent all these potential leakage endpoints? Furthermore, lack of training or awareness by [computer users](#) often results in important information "leaving" the organization.

Compounding this problem is that personal information is usually stored on multiple networks running multiple policies, without any control from the information "owner". Entities that hold consumer information are not necessarily savvy when it comes to IT or to information security issues. Their only objective is to satisfy regulations.

The number of access points is further increased when companies engage in contract work and offshoring activities. The 2009 Ponemon Institute study, third-party organizations accounted for more than 44 percent of data breach cases in 2008, and are also the most costly form of data breaches as a result of additional investigation and consulting fees.

If you need additional information email me
at: Alimagno@Insurance.ca.gov

Q/A Then Demonstration