

Data Leak Prevention

Introduction

The current stress in the worldwide economy has manifested itself in many ways. As well as macro economic upheaval and the challenges it presents the public and private sector, more practical and localised issues are appearing, including the increase risk to businesses of data loss.

Previous work at Bloor Research has underpinned the significance of the inside threat to data loss. Whilst this problem has often been attributed to the “incompetent and non-malicious” user releasing data by mistake the increasing numbers of disaffected white-collar knowledge workers being made redundant is seeing an increase in “competent and malicious” data loss incidents.

Publicity surrounding significant data loss incidents over the past year has brought the issue to the fore. Senior politicians have become embroiled in public sector episodes as much as private sector company directors. Clearly data loss can be summarised in one word—risk—and it is up to security professionals to work with the business to mitigate this risk, be it to shareholder value, reputation or personal embarrassment.

Data protection often starts with the creation of IT security policies through to user education and the deployment of supporting technology.

Data leak prevention can play a significant part in this data protection as it prevents unauthorised data leaving an organisation’s endpoints. It does this using a variety of techniques, including key word matching, traffic pattern analysis, network monitoring and file tracking. Although no data leak prevention vendor would ever guarantee 100% of all leaks would be prevented, a solution such as this can form a major part of an organisation’s security strategy.

Many organisations are combining data leak prevention with data encryption so that if any significant data does leave the organisation it will remain encrypted and therefore unusable to anyone other than an authorised recipient. This combined approach of leak prevention

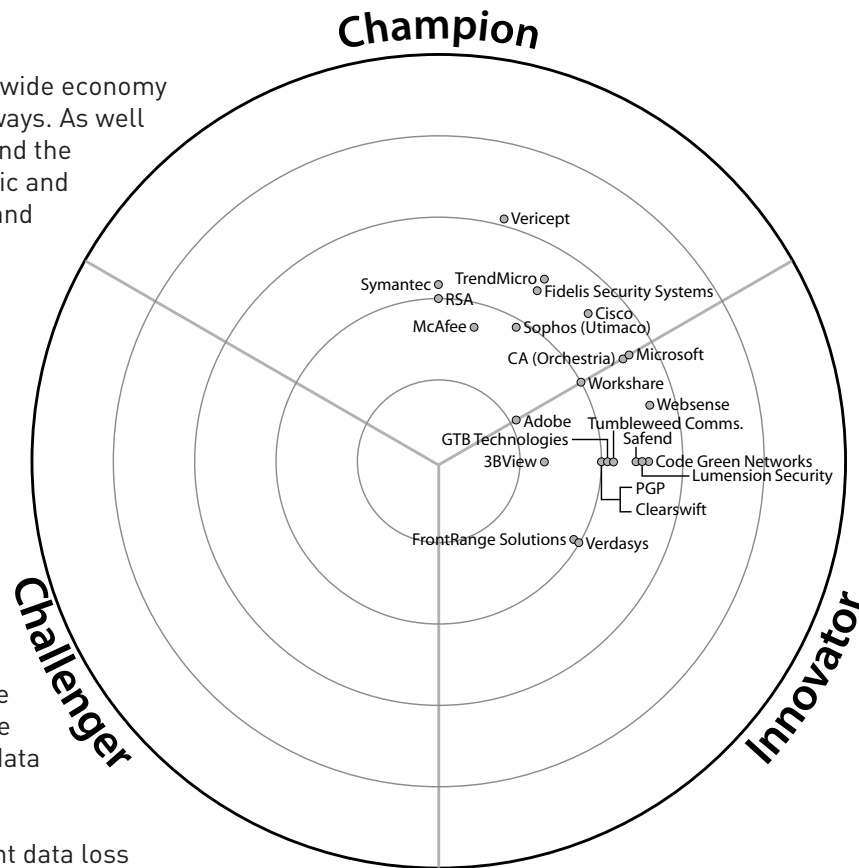


Figure 1: The highest scoring companies are nearest the centre. The analyst then defines a benchmark score for a domain leading company from their overall ratings and all those above that are in the champions segment. Those that remain are placed in the Innovator segment if their innovation rating is over 2.5 and Challenger if it is less than 2.5. The exact position in each segment is calculated based on their combined innovation and overall score.

and encryption is referred to as Enterprise Data Protection and is the subject of another Market Update from Bloor Research.

Data leak prevention and data loss prevention are generally synonymous terms but data loss prevention has also been used to describe data encryption. The term ‘extrusion prevention’ is also used by some vendors to describe data leak prevention.

Data leak prevention technologies can be quite advanced as they need to determine the validity of a piece of data being moved from one place to another without stopping legitimate business access to the data.

In some systems analysis is undertaken of the data traffic pattern over a period of time to determine where data tends to originate and terminate and which users are involved in the process. It will also look at the mechanism used to transfer the data such as email, USB, CD/DVD or any one of the many other data transmission mechanisms. Data leak prevention systems

will often detect the use of keywords during the attempted data transmission, picking up on obvious candidate terms such as “confidential” and “executive” to indicate a potential leak.

Some solutions act at the network packet level reviewing data as it passes through the network. These systems will analyse a particular file or set of data and determine if its use is appropriate rather than examining explicit user behaviour. Over time a data leak prevention solution will often build up a comprehensive map of data movements and be able to flag potential violations. This flagging will often be in the form of a message to the user telling them that the data movement they are attempting may be in violation of the data leak rules for an organisation. The user may then be given an opportunity to justify their action, sometimes by typing into a suitable dialog box, which can then be sent to a line manager for review. Of critical importance to users is that the system does not become a burden and an obstruction to their normal work. In many cases the number of false positive or false negative activations may change over a period of time as the data leak prevention system learns what is acceptable behaviour for particular users or data sets.

Digital rights management (DRM) is starting to be used as a way of preventing data leaks. Often with a DRM solution meta data is carried with a piece of data describing who may or may not have access to it. Using this technique some vendors promote the notion of security travelling with a set of data wherever it goes. An analysis of DRM vendors is outside the scope of this Market Update but some have been included where they have a complementary data leak prevention offering.

A number of vendors also provide content inspection appliances to monitor data as it passes through a network. Where appropriate, these have also been included in this report when complemented by a data leak prevention offering.

Key market issues

The data leak prevention market has a number of vendors with different approaches to preventing data leaks. Terminology will often differ as vendors attempt to differentiate their product set from others. Of interest is the move by both data leak prevention and encryption vendors to form partnerships, or to become acquired, to provide a broader product offering. This is probably in recognition of the fact that data leak prevention will never be 100% successful so it makes sense to protect data using encryption as well.

There is also considerable discussion about the viability of data leak prevention solutions in general as a number of customers are reporting they have been oversold on a particular solution. Data leak prevention has been referred to as shelfware by some detractors.

For the purposes of this market update the following product areas have been covered:

- Data leak prevention
- Endpoint level data leak prevention
- Network level data leak prevention
- Data loss protection
- Digital rights management
- Data loss prevention

Vendor landscape

In January 2009, CA announced that it was to acquire data loss prevention vendor Orchestria.

In December 2008, Microsoft announced that it was integrating Data Loss Prevention (DLP) technologies from RSA into its platform and future information protection products. EMC has engineered RSA DLP Suite 6.5 to integrate with Microsoft Active Directory Rights Management Services.

In October 2008, Symantec announced it was to purchase messaging security firm MessageLabs for \$695m in cash. The company said it will merge MessageLabs with its own Symantec Protection Network for a software-as-a-service offering. This will incorporate Symantec technology in data loss prevention, compliance, endpoint security and archiving.

In September 2008, Sophos announced that it had purchased Utimaco, a data security company with a range of encryption and data loss prevention products that would become a new business unit within Sophos responsible for information and data protection

In August 2008, McAfee said it had agreed to pay \$46m to buy data loss prevention firm Reconnex.

In June 2008, Symantec Corp. announced that an updated version of Vontu Data Loss Prevention was being released featuring enhanced management and support of native SQL database scanning. This was the second DLP product release since Symantec's acquisition of Vontu in December 2007.

Summary and conclusions

Data loss events have a higher profile now than ever before. Coupled with widespread uncertainty about corporate stability and the consequential removal of data by staff around a downsizing, organisations face more challenges to their data than maybe ever on the past.

There is no doubt that a properly configured data leak prevention product can be a significant part of an organisation's security strategy. This Market Update has highlighted how vendors in this area are constantly striving to create new and innovative ways to detect and prevent data leaks using some very smart techniques.

Some potential customers remain unconvinced as to the benefits of data leak prevention and even describe it as shelfware. This is an ill-considered judgement and demonstrates a lack of understanding of the available technology and the benefits it can bring to many organisations, even if it is found unsuitable in their particular circumstances.

The future of data leak prevention appears to be more and more entwined with that of data encryption as vendors form partnerships, alliances and make outright purchases. This may indicate a general feeling that any data leak prevention deployment should be paired with complimentary technologies to help ensure its success. Ultimately it is up to end users to determine if data leak prevention will work in their organisation and, if not, what alternative steps they see themselves taking to prevent data escaping their control. In reality there are few options currently available.

In the current uncertain times, not having a data loss prevention strategy could be seen by many as recklessness.

Nigel Stanley
Data Leak Prevention
March 2009

The logo for Bloor, featuring a stylized 'B' icon followed by the word 'Bloor' in a bold, sans-serif font.

2nd Floor
145–157 St John Street
London, EC1V 4PY
United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748

Web: www.BloorResearch.com
email: info@BloorResearch.com