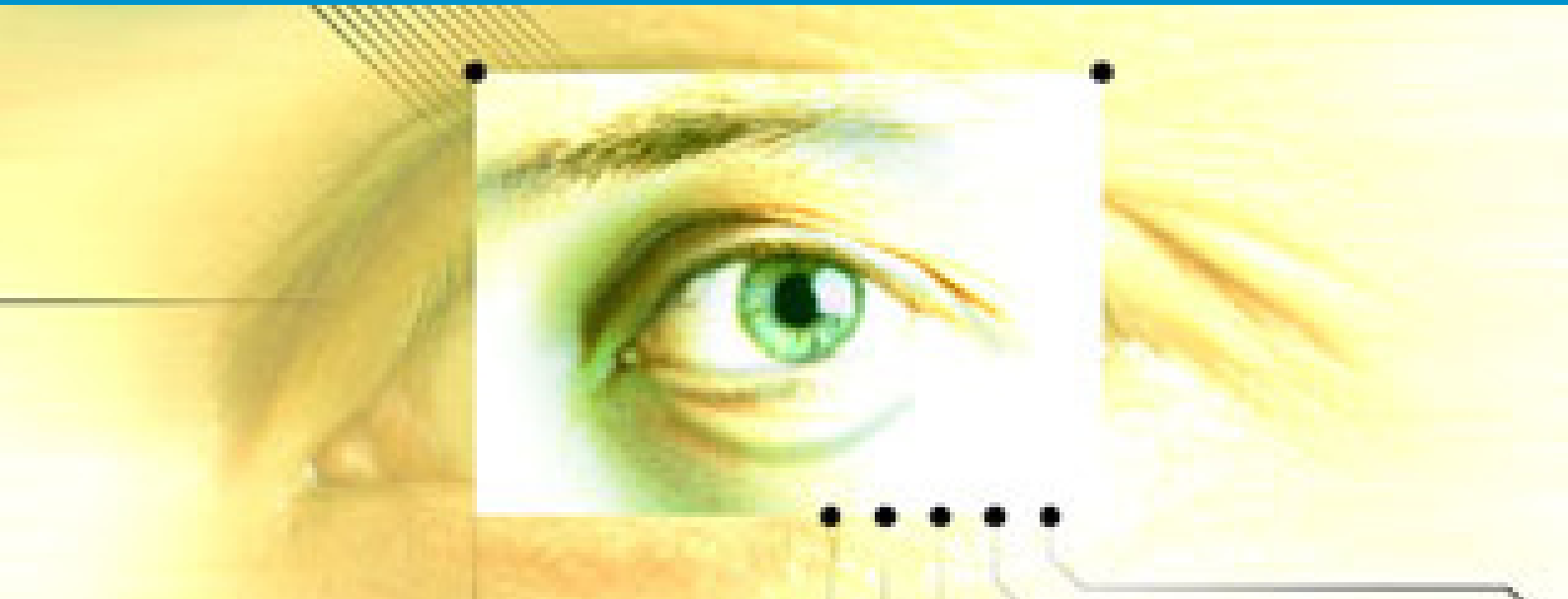


# Bullseye



## Enterprise Data Protection

A Bullseye Report by Bloor Research  
Author : Nigel Stanley  
Publish date : April 2008

Having Enterprise Data  
Protection as an objective is a  
worthy goal for any organisation

Nigel Stanley

## Executive summary and conclusions

Enterprise Data Protection is an umbrella term used to describe the coming together of data leak prevention technologies with encryption (often referred to as data loss prevention) technologies.

The reason for the coming together of two different security technologies is the natural synergy they share. By stopping data leaks in the first instance an organisation will achieve a high level of protection but, accepting that no organisation can ever prevent all data from leaking, it makes sense to secure sensitive data further using encryption.

This combined approach delivers a comprehensive, robust and practical response to the data loss problem.

For the purposes of this Bullseye report an ideal but mythical Enterprise Data Protection product has been created by the Bullseye committee combining the best known features of data leak and data encryption products. This “perfect product” does not currently exist; instead it represents a vision of what could be developed in the future. A list of attributes has then been created from this perfect product that has enabled the Bullseye committee, formed in support of this project, to review current vendors and their products against such a perfect benchmark using an open methodology.

The relative scores of the vendors and their products, measured against the perfect product have been turned into the Bullseye landscape diagram (Figure 1).

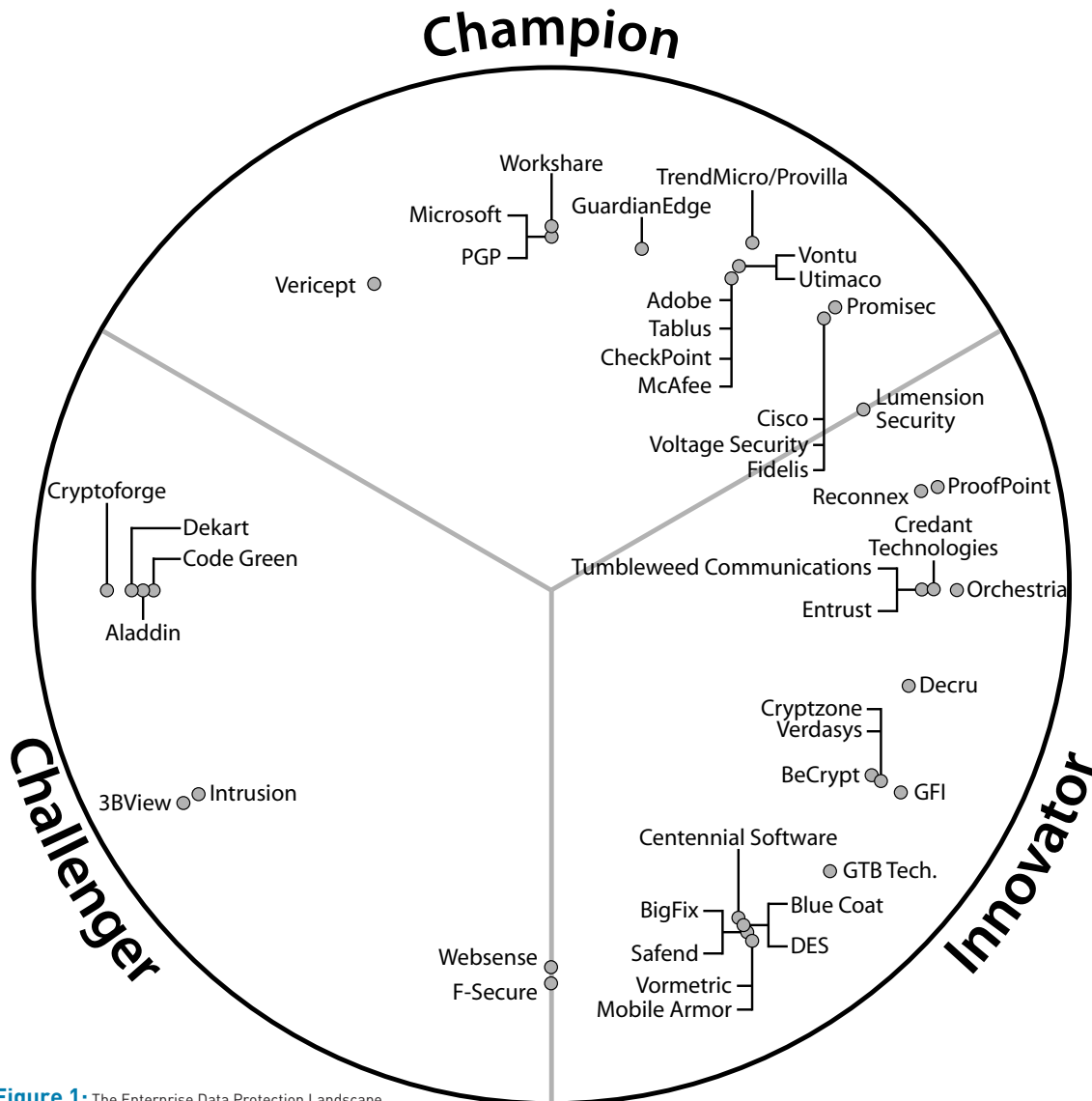


Figure 1: The Enterprise Data Protection Landscape

**Executive summary and conclusions**

To ensure this report is relevant and useful today Figures 2 and 3 produce a similar view but of the data encryption and data leak prevention vendors with products available now. These vendors and products were compared to each other rather than a "perfect product" to produce two easy to use landscape diagrams.

In practice, the Enterprise Data Protection domain has been proven as a desirable objective for vendors as they seek partnerships and acquisitions to complement their own solutions in this area. New and emerging Digital Rights Management products continue to cross over into what was considered the data loss prevention marketplace at the same time as data encryption vendors look at ways of complementing their products.

End user organisations need to be reviewing their data loss and encryption strategies as a matter of urgency to prevent expensive and reputation-damaging incidents. This needs to be approached from a strategic viewpoint so that best use is made of budgets, personnel and systems.

Having Enterprise Data Protection as an objective is a worthy goal for any organisation.

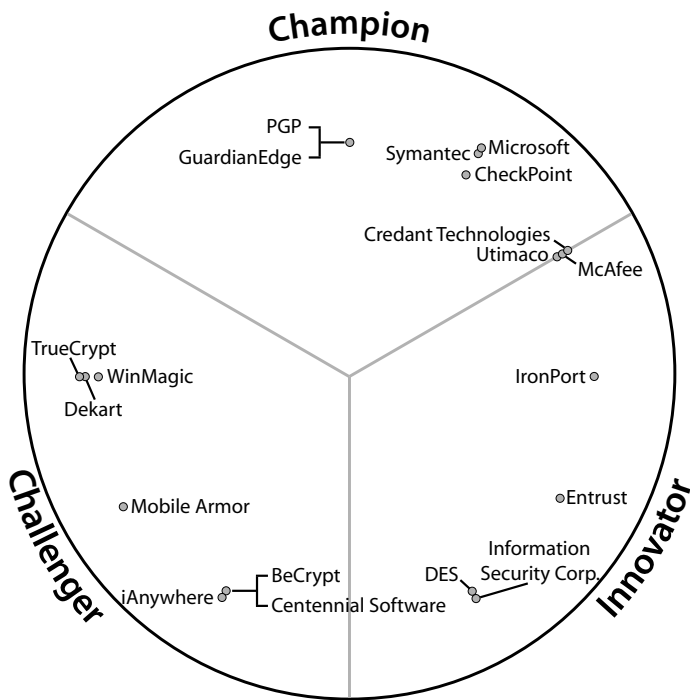


Figure 2: The Data Encryption Landscape

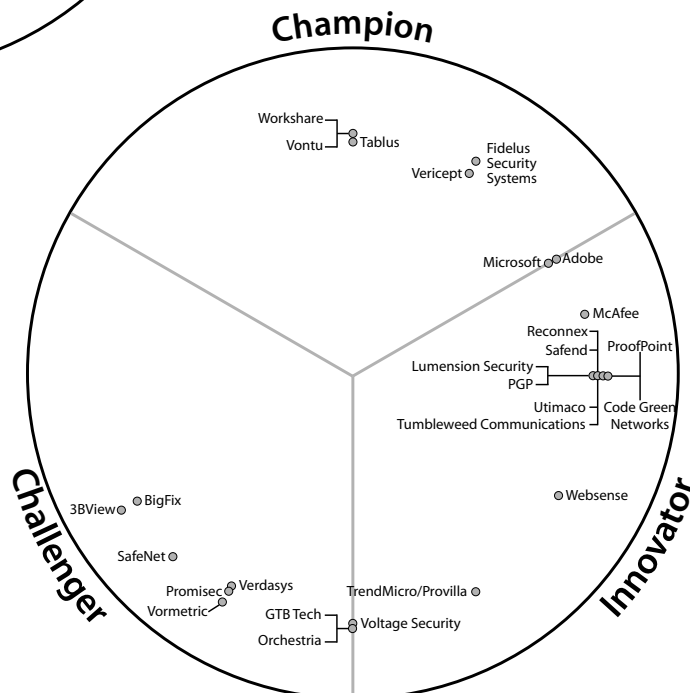


Figure 3: The Data Leak Prevention Landscape

## The IT security domain

IT security is a complex and time-consuming area that is constantly evolving as new threats emerge. IT security solutions fall into complimentary activity categories:

- Policy management**  
 Policies and procedures need to be created and then enforced across the business. These policies need to fit with corporate objectives and facilitate the success of the business and not be seen to be unreasonable or impractical. Users should be given the tools and flexibility to do their jobs but, in turn, must be educated in the risks associated with using IT in a connected world. Areas of policy management inevitably fall into domains other than IT security, as they require business-led input as well.
- Access control and identity management**  
 This important area enables the business to work with IT to determine who should access which systems or applications, the provisioning of accounts and a number of other functions concerned with the correct access to the correct systems at the right time. Good access control and identity management will enable the delivery of better foundational IT security.
- Unified threat management**  
 Security technologies need to be intelligently implemented so that the business achieves maximum security for a reasonable budget. There are a set of threat management technologies such as anti-malware, intrusion prevention and firewalls, which are put in place by most organisations. Other technologies may only be implemented if the business considers themselves to be at particular risk, for example advanced attack detection tools. It is recognised that Enterprise Data Protection, as described in this paper, will become part of Unified Threat Management as it becomes more mainstream and available.
- New, emerging and refocused IT security**  
 New threats emerge on a regular basis and existing threats become the object of renewed attention, often fuelled by governance and regulatory concerns or a general maturing of products in the market place. In parallel, vendors produce innovative solutions to combat these new, emerging or refocused threats, which eventually become subsumed as part of foundational IT security systems.
- Enterprise Data Protection**  
 The coming together of data loss prevention and data encryption and the purpose of this Bullseye report.

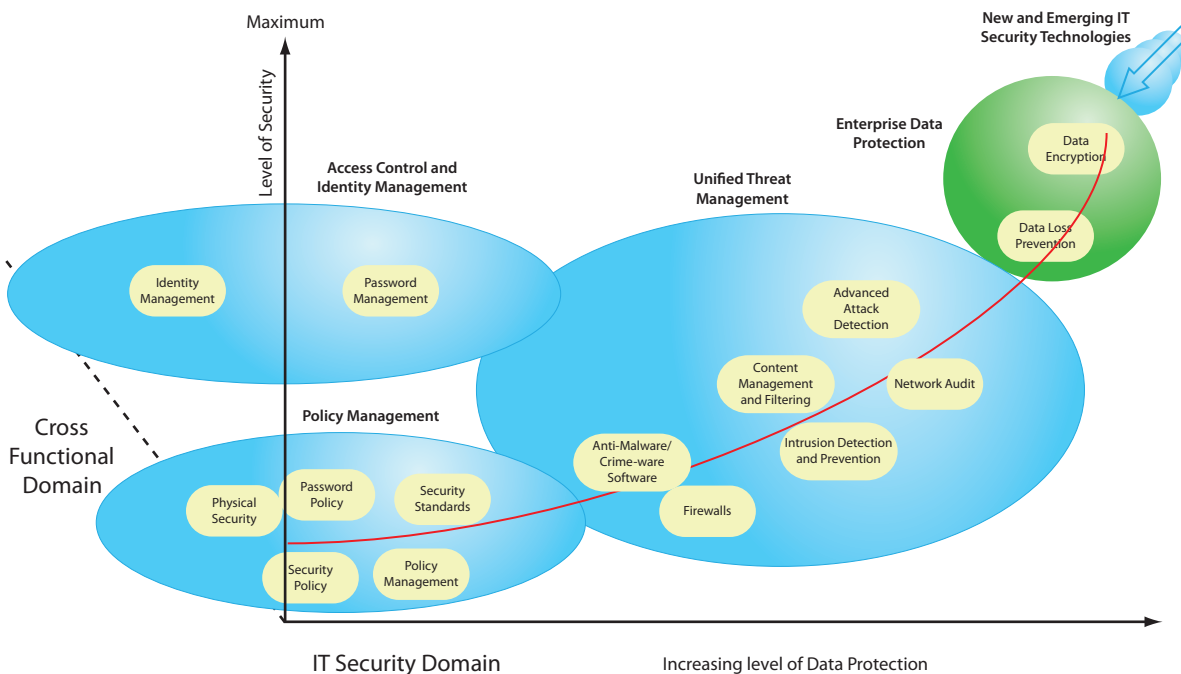


Figure 4: The IT Security Domain

## Introduction to Enterprise Data Protection

In the past, IT security had been focused on securing organisational perimeters until it was realised that these were quickly breaking down due to the increasing demands of mobile workers, closer business relationships, outsourcing and other organisational challenges.

This led to what is now known as IT security de-perimeterisation.

At the same time, public awareness and the global regulatory environment have made the consequences of data breaches a significant business issue. Quickly, attention has moved to securing data itself by focusing on detecting and protecting data at risk.

This data security is delivered via two technologies:

- *Leak prevention* solutions, which are used to detect if data is at risk of leaving an organisation's control, for example via email or a USB drive.
- *Loss protection* using encryption to protect individual data whilst, for example, on laptops or in email.

Enterprise Data Protection is a new and evolving market place that represents the coming together of leak and loss prevention technologies.

### Components of Enterprise Data Protection

Despite having in place good security policies and technologies, ultimately the data still remains at risk unless two actions are taken:

Data is monitored by smart tools to prevent data leakage

Data is protected with encryption to ensure any data actually lost would have minimal business impact

By combining these two areas of IT security in combination with foundational security technologies a business can be assured that it is as secure as possible.

Technologies that comprise the Enterprise Data Protection domain include:

- Data leak prevention
  - » Endpoint level data leak prevention
  - » Network level data leak prevention
- Data loss protection
- Data encryption
- Digital rights management
- Email encryption
- Data loss prevention
- Mobile encryption
- End point encryption
- Network server encryption
- Document security
- Server/mainframe encryption

## Introduction to Enterprise Data Protection

### Enterprise Data Protection—the perfect product benchmark

Part of the Bullseye process is the creation of a mythical perfect product that will achieve a 100% Bullseye score. It is accepted that this perfect product may be some time away, but the description provides a benchmark against which current and existing products can be evaluated.

### Enterprise Data Protection—description of the perfect product

The product would be able to detect and prevent data leaks across email, print, CD/DVD, copy to USB, IM and FTP sources, print screen and any other new and emerging data leak vectors. If data does leak by mistake, it would be encrypted so that no clear text data ever leaves an organisation inappropriately.

The product will support industry standards, as appropriate, and have published interfaces for third party integration. It will support proprietary as well as open source operating systems. Data leak prevention rules could easily be implemented by business users who can adapt the rules in line with business requirements and policies. As business policies evolve any changes can easily be reflected back into the data leak detection mechanism.

Monitoring of attempted data leak violations will be undertaken by the business and will not need the input of IT specialists. The setup and configuration of the product would be straightforward for a reasonably experienced computer user and leak monitoring will be fully customisable, with log files auditable for any subsequent investigations. These log files will be able to provide evidentially robust reports for forensic investigations.

Smart ways of preventing data leaks will include the use of heuristics and file fingerprinting to determine if data has been manipulated prior to possible removal as well as more conventional keyword/attribute based data analysis. It will not be possible to circumvent the data leak detection capability by adapting, changing, manipulating or otherwise corrupting the data.

As well as leak prevention, data will be automatically encrypted at all stages, so that any data that should leave the business is in an encrypted form. Users will not be expected to manually encrypt data as all decisions concerning when and how to protect data by encryption will be undertaken for them by the product.

At no time will data “in the clear” be visible to any unauthorised persons inside or outside the organisation. It will not be possible for recipients of encrypted data to unencrypt the data and forward it on as plain text.

There will be support for a range of encryption standards including X.509 and Open PGP with the ability to integrate into other standard encryption technologies. The robustness of the encryption algorithms used must grow in line with new and emerging threats.

Products used to backup data, including disk drives and tape backup systems, will have integrated encryption and data leak prevention capabilities.

Effective and efficient encryption key management will come as standard and support facilities such as key issue, distribution and escrow. Key management will be straightforward and any complexities hidden from users and administrators.

Full disk encryption will come as standard, as will encryption of data across folders, email, removable media, mainframe systems and network file servers. There will be tight integration with email systems and implementation of the product will support both end-to-end and gateway-based encryption models, based on requirements of the business. Support for encryption on mobile/handheld devices is a standard feature as is the ability to remediate files across the deployed solution.

Dynamic, real time encryption of data will be a fast process that will not be obvious to any user and will not have any detrimental affect on any system performance.

File and data discovery is supported at the end point, network and gateway level and all data in transit will be dynamically monitored to ensure that it is protected as appropriate. If there is no direct support for data leak prevention or data loss protection then the product must easily integrate into a partner’s solution such that a seamless single product is produced, with all of the attributes of the perfect product. The product will scale both up and down to support the requirements of medium and enterprise deployments and there will be no performance degradation visible to users where this solution has been implemented. This will be evidenced in case studies.

Full support will be implemented for remote or disconnected users, such that any data used off line is as protected as it would be when connected to the monitored network. This will extend to the use of handheld devices, smart phones and any other device capable of carrying sensitive data.

End user training will not be necessary as any data protection/leak prevention will be automatic. IT department training will be minimal and business user training will also be minimal. Product pricing will be in the average range for such a product, as measured by its nearest competing solutions. Technical support will be made available at standard industry pricing and the quality of service will remain good to excellent as measured by regular customer feedback.

## Introduction to Enterprise Data Protection

### Criteria for vendor inclusion

Like many markets, IT security contains hundreds of products many of which have overlapping or multiple features in one solution.

A market review was undertaken and vendors were selected who actively marketed their solutions as data encryption, data leak or other associated technologies.

Once an initial set of vendors was selected the list was reviewed to ensure that the following conditions applied:

- Product was targeted across most if not all market sectors
- Product was available on the general market
- Product had been available for more than 1 year

Vendors that listed a feature relevant to the Enterprise Data Protection domain but could not significantly evidence this were excluded.

The following were also excluded:

- Software source code security and auditing tools
- Pure digital rights management (DRM) vendors
- Document management tools
- Application-specific security tools
- Appliances or software designed to secure one particular element of a solution, for example a relational database

During the research it was evident that there were some vendors that still had a firm North American approach to their sales, and had very little or any presence in EMEA or other international markets. This did not result in them being excluded from the report, but their scores were similarly reduced in areas of geographical coverage. In some instances this did make data collection more difficult.

In some instances the inclusion of a vendor was a difficult decision as their solution may have been on the margins of the accepted criteria. As this is the first report into the Enterprise Data Protection domain it was decided to include more vendors initially on the basis that subsequent reports may see them excluded. If a vendor was included in these circumstances it is accepted that they would score in the lower range against the ideal product benchmark.

One technology area that did require special attention was that of digital rights management (DRM). Whilst taking a slightly different approach to solving the data leak problem, DRM is still a valid strategy and, on that basis, some major vendors in the DRM market were rated in this report. This was conditional on them actively marketing and selling their DRM product as a way of managing data leaks otherwise a complete new vendor sector would have required analysis.

Some vendors were excluded even though they appeared to have an interesting solution. These were mainly very small companies with little or no direct market presence and with no auditable third party product endorsement.

## The Bullseye open research framework

The Bullseye open research framework is an independent multi-dimensional model for the comparative analysis of IT products. It provides end users with greater depth, more dimensions, and is readily configurable to reflect user priorities but still visually simple to assimilate and use.

Bullseye measures both the technology and business to provide a set of weighted attribute scores that enables buyers to make the best decision.

There are 3 elements to the production of a Bullseye: the core methodology, the domain schema, and the evaluation process. The Bullseye method uses seven primary criteria for evaluating vendor/product solutions, each of which is made up from various lower level generic and specific attributes, to which weightings are applied to calculate the total for that criteria. These are:

- Stability and risk
- Performance
- Architecture
- Fit for purpose
- Ease of use
- Support and coverage
- Value

The domain schemas are created and approved by an independent committee of end users, analysts, vendors, consultants and trade associations based on 5 primary steps:

- Define the domain: what is the area (referred to as the sandbox) you are assessing and what other domains does it interact with.
- Define the optimal product: what would/could you build if there was no limit on money, time or expertise.
- Define the specific attributes that will be used to assess the technologies and their relationships to the generic attributes.
- Define the scoring criteria: how does each attribute get scored on a scale of 0-5.
- Define the weightings for each attribute (specific, generic and master).

There are 2 specific graphical views of the high level data of which the first is used within our Bullseye reports and the second within our individual product/company reviews. These are:

1. *The landscape Bullseye*, which provides a high level view of all the appropriate players in a domain. You can define the domain you wish to view dynamically. This is split into 3 sectors:
  - » Champions: generally large stable organisations with a strong overall solution and vision.
  - » Innovators: smaller companies or new products from larger companies that are very strong at the technology level.
  - » Challengers: valid solutions that should be considered based on more personal criteria, like existing legacy investments or integration requirements.

The primary Bullseye graphic presents the products or companies in 2 dimensions. Nearest the centre (bull) has the highest rating and the positions around the circle show a holistic view of the type of solution for a generic buyer.

2. *The solution view* gives a picture of the overall solution based in its commercial, technical and function fit. The end result is like a shooting target where the smaller the shaded area of coverage the better the solution.

Further information regarding the Bullseye framework and the schema for the Enterprise Data Protection domain can be found at [www.bullseyefoundation.org](http://www.bullseyefoundation.org).

## Market Overview

The volatile nature of the Enterprise Data Protection market was ably demonstrated by the number of partnerships and acquisitions announced over the course of this research program. Many of these partnerships appear to be more like courtships as vendors explore the technical and cultural matches of other suppliers.

In November 2007, Symantec purchased the data leak prevention company Vontu and McAfee purchased SafeBoot giving both of these well respected security vendors a foothold in the Enterprise Data Protection market.

IBM announced partnerships in November 2007 with a number of security vendors including Fidelis Security Systems and Verdasys on the data leak prevention side and PGP for data encryption. Yet another announcement in November 2007 saw Utimaco, a data security company, announce a partnership with Safend, a data leak prevention supplier.

Lumension Security, previously known as Patchlink, purchased Securewave in July 2007. In February 2008, PGP announced a partnership with Lumension to provide the ex-Securewave Sanctuary product as part of PGP Endpoint, an Enterprise Data Protection offering.

Workshare is another company that actively works with partners such as Utimaco, PGP and Voltage to provide a broader offering.

In some quarters, data leak prevention is still seen as a shelfware solution with little track record of success. This view is increasingly challenged as larger vendors such as IBM consolidate data leak prevention technologies into their mainstream offerings.

Many smaller vendors are generating new and innovative ways of detecting signs of an impending data loss incident using complex algorithms and detection mechanisms. In addition, all vendors have to play catch up with the myriad of new end user devices, all of which can download significant amounts of corporate data.

Demand for Enterprise Data Protection has grown in the end user community, fuelled by many very public losses of confidential data. The reputational damage following on from such losses can be extremely costly, along with the expense of repairing customer and partner relationships. End users are starting to realise that not only should data be prevented from leaving an organisation in the first place the same data must be encrypted. This way, any data that does go missing will be protected.

Practical issues surrounding the management of data encryption keys still arise despite the relative maturity of the encryption market. For vendors to be successful in building an Enterprise Data Protection solution consideration needs to be given to making key management far easier.

The legal aspects of data loss incidents are also acting as a catalyst to product adoption. Specific loss disclosure laws are yet to be enacted in all international markets but US-based legislation is having a ripple affect as other markets realise that local laws may soon be introduced.

Digital rights management (DRM) vendors continue to offer a slightly different approach to data loss prevention. With the growth in digital download technologies, DRM is becoming increasingly important and the lines between it and more conventional data leak prevention technologies are starting to disappear.

### Actions today

It is fully accepted that this Bullseye report represents a forward looking view of products and technologies, and no one vendor is able to produce the perfect product today.

On that basis, organisations still need to be protecting themselves and ensuring that data does not leak from their systems and if it does it remains securely encrypted. Whilst waiting for the perfect product, vendor solutions available today should be assessed and partnerships created with the best vendor able to supply an Enterprise Data Protection product set in a realistic time frame that suits your particular organisation.

That way, existing products could be implemented knowing that when they are updated in the medium term that you will be moving closer to the goal of Enterprise Data Protection.

### Acknowledgments

Bloor Research would like to thank the committee members that have supported this Bullseye.

### Further information

For additional information relating to this subject visit <http://www.bloor-research.com/update/944>

Bloor Research has spent the last decade developing what is recognised as Europe's leading independent IT research organisation. With its core research activities underpinning a range of services, from research and consulting to events and publishing, Bloor Research is committed to turning knowledge into client value across all of its products and engagements. Our objectives are:

- Save clients' time by providing comparison and analysis that is clear and succinct.
- Update clients' expertise, enabling them to have a clear understanding of IT issues and facts and validate existing technology strategies.
- Bring an independent perspective, minimising the inherent risks of product selection and decision-making.
- Communicate our visionary perspective of the future of IT.

Founded in 1989, Bloor Research is one of the world's leading IT research, analysis and consultancy organisations—distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services and consultancy projects.



### Nigel Stanley Practice Leader—Security

Nigel Stanley is a specialist in business technology and IT security.

For a number of years Nigel was Technical Director of a leading UK Microsoft partner where he led a team of consultants and engineers providing secure business IT solutions. This included data warehouses, client server applications and intelligent web based solutions. Many of these solutions required additional security due to their sensitive nature.

From 1995 until 2003 Nigel was a Microsoft Regional Director, an advisory role to Microsoft Corporation in Redmond in recognition of his expertise in Microsoft technologies and software development tools.

Nigel had previously worked for Microsoft as a systems engineer and product manager specialising in databases and developer technologies. He was active throughout Europe as a leading expert on database design and implementation.

Nigel has written three books on database and development technologies including Microsoft .NET. He is working on a number of business-led IT assignments and is an executive board member of a number of privately held companies. He has significant experience in security and related activities and is practice leader for security at Bloor Research.

## Copyright & disclaimer

This document is copyright © 2008 Bloor Research. No part of this publication may be reproduced by any method whatsoever without the prior consent of Bloor Research.

Due to the nature of this material, numerous hardware and software products have been mentioned by name. In the majority, if not all, of the cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not Bloor Research's intent to claim these names or trademarks as our own. Likewise, company logos, graphics or screen shots have been reproduced with the consent of the owner and are subject to that owner's copyright.

Whilst every care has been taken in the preparation of this document to ensure that the information is correct, the publishers cannot accept responsibility for any errors or omissions.



Suite 4, Town Hall,  
86 Watling Street East  
TOWCESTER,  
Northamptonshire,  
NN12 6BS, United Kingdom

Tel: +44 (0)870 345 9911  
Fax: +44 (0)870 345 9922  
Web: [www.bloor-research.com](http://www.bloor-research.com)  
email: [info@bloor-research.com](mailto:info@bloor-research.com)