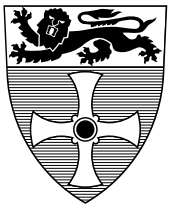
UNIVERSITY OF
NEWCASTLE



University of Newcastle upon Tyne

COMPUTING SCIENCE

A Trust-economic Perspective on Information Security Technologies

S. E. Parkin and A. van Moorsel

TECHNICAL REPORT SERIES

No. CS-TR-1056 October, 2007

TECHNICAL REPORT SERIES

No. CS-TR-1056 October, 2007

A Trust-economic Perspective on Information Security Technologies

Simon Edward Parkin and Aad van Moorsel

Abstract

This report surveys existing enterprise technologies and products available to control access to confidential digital data. We survey USB access control solutions, digital rights management software, disk encryption techniques and operating system solutions. We compare the various technologies with respect to granularity and extent of administrative control, platform coverage, user education features, and accommodation of data use outside the boundaries of the company network. The researched technologies allow restrictions to be placed on copying, editing, viewing and printing from within various software applications, provide auditing options and prevent outsider access through encryption. Several of the mentioned technologies offer training and education options, informing users as to the reasoning of access control events as they occur and educating them about the permissions that apply to them. A serious drawback of many of the technologies is the central administration it requires. We are interested in cost trade-off, to be able to make trust-economic decisions. The cost of software deployment is linked to the features that each product provides, where finer granularity of device and file content control, encryption and user education implies that per-user purchase cost increases.

Printed and published by the University of Newcastle upon Tyne,
Computing Science, Claremont Tower, Claremont Road,
Newcastle upon Tyne, NE1 7RU, England.

Bibliographical details

PARKIN, S. E, VAN MOORSEL, A..

A Trust-economic Perspective on Information Security Technologies
[By] S. E. Parkin, A. van Moorsel.

Newcastle upon Tyne: University of Newcastle upon Tyne: Computing Science, 2007.

(University of Newcastle upon Tyne, Computing Science, Technical Report Series, No. CS-TR-1056)

Added entries

UNIVERSITY OF NEWCASTLE UPON TYNE
Computing Science. Technical Report Series. CS-TR-1056

Abstract

This report surveys existing enterprise technologies and products available to control access to confidential digital data. We survey USB access control solutions, digital rights management software, disk encryption techniques and operating system solutions. We compare the various technologies with respect to granularity and extent of administrative control, platform coverage, user education features, and accommodation of data use outside the boundaries of the company network. The researched technologies allow restrictions to be placed on copying, editing, viewing and printing from within various software applications, provide auditing options and prevent outsider access through encryption. Several of the mentioned technologies offer training and education options, informing users as to the reasoning of access control events as they occur and educating them about the permissions that apply to them. A serious drawback of many of the technologies is the central administration it requires. We are interested in cost trade-off, to be able to make trust-economic decisions. The cost of software deployment is linked to the features that each product provides, where finer granularity of device and file content control, encryption and user education implies that per-user purchase cost increases.

About the author

Aad van Moorsel joined the University of Newcastle in 2004. He worked in industry from 1996 until 2003, first as a researcher at Bell Labs/Lucent Technologies in Murray Hill and then as a research manager at Hewlett-Packard Labs in Palo Alto, both in the United States. Aad got his PhD in computer science from Universiteit Twente in The Netherlands (1993) and has a Masters in mathematics from Universiteit Leiden, also in The Netherlands. After finishing his PhD he was a postdoc at the University of Illinois at Urbana-Champaign, Illinois, USA, for two years. Aad has worked in a variety of areas, from performance modelling to systems management, web services and grid computing. Most recently, he was responsible for HP's research in web and grid services, and worked on the software strategy of the company. Aad is Deputy Director of the North-East Regional e-Science Center. His research agenda is in the area of self-managing systems.

Simon Parkin completed a BSc Computing Science degree in 2002 and an Advanced Masters degree in System Design for Internet Applications (SDIA) in 2003, both at Newcastle University. Between 2003 and 2007 Simon studied a PhD under the supervision of Dr. Graham Morgan. Research subjects covered during this period included E-Commerce, Service Level Agreements (SLAs) and Distributed Virtual Environments (DVEs). Simon also contributed to the EU-funded "Trusted and QoS-Aware Provision of Application Services" (TAPAS) project during this time.
Simon is currently working with Dr. Aad van Moorsel.

Suggested keywords

USB ACCESS CONTROL,
DIGITAL RIGHTS MANAGEMENT,
DISK ENCRYPTION,
TRUST ECONOMICS

A Trust-economic Perspective on Information Security Technologies

Simon Edward Parkin, Aad van Moorsel

School of Computing

Newcastle University

{s.e.parkin, aad.vanmoorsel}@newcastle.ac.uk

Abstract

This report surveys existing enterprise technologies and products available to control access to confidential digital data. We survey USB access control solutions, digital rights management software, disk encryption techniques and operating system solutions. We compare the various technologies with respect to granularity and extent of administrative control, platform coverage, user education features, and accommodation of data use outside the boundaries of the company network. The researched technologies allow restrictions to be placed on copying, editing, viewing and printing from within various software applications, provide auditing options and prevent outsider access through encryption. Several of the mentioned technologies offer training and education options, informing users as to the reasoning of access control events as they occur and educating them about the permissions that apply to them. A serious drawback of many of the technologies is the central administration it requires. We are interested in cost trade-off, to be able to make trust-economic decisions. The cost of software deployment is linked to the features that each product provides, where finer granularity of device and file content control, encryption and user education implies that per-user purchase cost increases.

Contents

1. Introduction

1.1 Introduction

Recently published data[1] suggests that some of the greatest IT threats an organisation faces are data and information theft and employee negligence with respect to data and information. In particular, [Infowatch] reports that the greatest information security threats within an organisation are the leakage of confidential information and the distortion of sensitive information. Such threats are believed to have the potential to damage company reputations (thereby impacting on the potential of the customer base) [Infowatch], and may lead to sanctions imposed by industrial regulatory bodies (who should be made aware of data breaches) [Infowatch].

To illustrate the scale of the problem, at least two-third of office workers own a removable storage device (e.g. USB memory sticks, media players etc.) [Centennial, Charlesworth]. Furthermore, 70% of workers connect some form of removable storage device to a company PC on a daily basis [Centennial]. The latter fact becomes a problem when considering that it has been found that 60% of office workers in the UK have created personal copies of electronic company documents within the workplace (such as confidential records and customer databases) [Fisher]. It is speculated that within the workplace "many employees do not see company theft as stealing and do not apply any 'moral brakes' to such activities" [Charlesworth]. All in all portable storage devices are one of the major conduits of data leakage within Europe [Infowatch], and even more so within smaller firms.

The above mentioned 'human vulnerabilities' related to data and information are an example of a larger security problem faced by enterprises. 70% of all security breaches originate from inside company networks [Centennial], although research shows that 60% of security incidents are actually caused by human error [Centennial]. With regards to the latter, two-thirds of USB sticks are lost by their owners, with 20% of these devices having sensitive information stored on them [Centennial].

In addition to company or business-sensitive data, companies may also own customer and other personal information of individuals. Over 50% of IT professionals feel that EU legislation should require businesses to protect the personal data it holds from threats posed from inside. Proposed solutions include the deployment of software to prevent the leakage of data from within the control of the enterprise, and with this the deployment of consistent internal security policies. This encompasses control of external network access points, and training staff to adhere to company-wide data management policies.

Despite these proposed initiatives, an estimated 55% of companies have made no attempts to protect themselves from the threats posed by removable media devices [DTI2006]. Furthermore, a reported 62% of all UK companies had an IT security incident in the last year, and this rises to 87% amongst larger organisations (which also tend to suffer incidents with greater regularity). The average cost of a UK company's worst incident is £12,000, and for larger businesses this is closer to £90,000.

In this paper we address the data and information security from a `trust-economic' perspective. That is, we are interested in solutions in relation to their impact on the enterprise, in terms of employee behaviour, enterprise policies and financial costs and risks. This document surveys technologies in four categories:

- USB Access Control Solutions (Section 3)
- Digital Rights Management Solutions (Section 4)
- Disk Encryption Solutions (Section 5)

[1] We note that some of the discussed data refers to marketing or popular scientific articles, and we do not know the scientific basis behind some of the presented numbers. However, we have chosen to use them, in the belief they indicate a growing concern and problem.

- Operating System Solutions (Section 6)

Section 6 then discusses remaining open technology issues we have identified.

1.2 Illustrative Scenario

The following example of an employee using a removable USB storage device illustrates key points relating to the figures outlined in Section 1.1:

There is a need to consider "the use, by operations staff (e.g., within Merrill Lynch or, perhaps, HP), of USB memory sticks to store company/confidential data whilst outside of the company's environment. A typical problem might be that a staff member buys a memory stick from a high-street store, saves confidential data onto it on Friday afternoon, and reloads the data to the system on Monday morning. Over the week-end, the stick may have been exposed to a range of highly insecure, potentially corrupted environments. The question is to understand the trade-offs (including effectiveness, inhibition of business operations, and cost) between policy- and technology-based strategies for managing the risks."

This scenario encompasses a number of user actions:

- Copying potentially confidential data to an external data-storage device (in this case a USB memory stick).
- Positioning confidential data outside of the workplace within which its confidentiality would otherwise be secured.
- Exposing confidential data to an insecure operating environment.

- Exposing a potentially insecure external data-storage device (which may nonetheless contain confidential company data) to a secure enterprise network. This also raises the threat of reducing the integrity of the company file-system by injecting corrupted data into it (should the data stored on the data-storage device have been exposed to unknown applications and subsequently copied to the company file-system).

1.3 Requirements

The use case defined in Section 1.2 alludes to a number of requirements both within and outside the associated working environment:

1) Data must be secured without adversely inhibiting employee productivity or behaviour

If any access control services prove to be less than transparent, they may influence the behavioural patterns of those users directly affected by them. For example, if a software application is distributed to user machines to manage data transfer to external devices, it may require that the entire contents of an external USB device be scanned every time such a device is connected. If the process of scanning the device takes time (an amount of time noticeable to the computer user), users may be unwilling to store their data in this way.

As a further example, a user may copy data to a USB device from a computer running dedicated access-control software (i.e. an application that controls the transfer of data to external devices based upon a corporate policy). With this, there would be a need to allow access to that data only within environments that operate the same file control software, without prohibiting access to other files stored upon the USB device (e.g. if a family member shares an employee's personal USB device).

In both cases, it may be that an alternative form of data storage would have to be provided.

2) *Clear and exercisable definitions must be presented to describe what constitutes 'confidential' data and how it can be accessed*

There would be a requirement to not only identify which data individual users can access within the company network, but also what data a user can copy to a personal storage device for removal from the site – these two sets of data may not necessarily be identical. This poses problems relating to dynamic file creation e.g. whether a user must attach appropriate security classifications to a file as it is created, and in fact who has the authority to determine the classification of a file.

3) *Only permitted users should be able to access confidential data*

If an employee connects a USB device to their personal computer (which it may be assumed has a direct connection to the Internet), it is wholly conceivable that – in an insecure environment as described in the Use Case of Section 1.2 – an unknown person may attempt to gain access to the data contained within the USB device. As such, there is a need to at the very least restrict access to any critical data contained on the USB device to only the permitted user (and not necessarily simply the account they hold on their respective home computer). This suggests that software may need to be installed upon the USB device itself in order to provide consistent data access permissions, or alternatively that the same software application (e.g. access-control software) is used to access the device from any computer (much in the same way that dedicated music applications restrict access to the contents of copy-protected CDs e.g. [Mediamax]). The latter solution could result in inappropriate manipulation of the working environment in order to guarantee compliance, as found in [SonyXCP].

Similarly, if a USB device is taken outside of the work environment and is subsequently lost, there should be guarantees that any critical company data is not viewable by unknown persons. With this there is a need to provide encryption of data that does not overly inhibit the use of the enterprise computer environment or the USB device itself. The loss of a USB device also raises the possibility of loss of availability to the company of important information which may only have been stored on the device alone. This suggests that data-mirroring capabilities should be provided within the workplace.

4) *The financial cost of any measures taken to maintain the integrity of confidential company data must not exceed the potential costs associated with loss of data integrity*

If additional software and/or hardware is installed within the organisation, its financial cost to the company must not exceed the cost that would otherwise be associated with the consequences of losing critical or confidential company data. That is to say if it is envisaged that confidential documents could become corrupted beyond use or otherwise fall into the wrong hands (to then be potentially manipulated by criminal elements), the cost of preventing such an incident must not exceed the potential losses suffered by the company if such an event occurred. Such judgement would however require informed financial models to be developed in order to determine the necessary spending model to employ.

2. USB Access Control Solutions

The software products described in this section are primarily concerned with how removable data-storage devices interact with the computer network operated by an organisation, and how the associated physical connection endpoints can be secured and brought under the control of the organisation. The basic principle behind these products is that users of an enterprise network and the enclosed company data should be made to adhere to a unified device access policy dictated from within the organisation itself (thereby achieving predictable, manageable behaviour amongst the associated workforce). A device access policy then applies either to individual machines or individual users (thereby constituting a data confidentiality policy). The products in this section ensure that data within an enterprise network remains under the control of the organisation, and at the same time that only those persons permitted to access particular files are able to do so.

The products examined here are:

- 'DeviceLock' from Smartline Inc. [DeviceLock];
- 'DeviceShield' from Layton Technology [DeviceShield];
- 'DeviceWall' from Centennial Software [DeviceWall];
- 'Disknet Pro' from Reflex Magnetics [Disknet];
- 'McAfee Data Loss Prevention' from McAfee Inc. [McAfee];
- 'Pointsec Protector' from Check Point Software Technologies Inc. [Pointsec];
- 'Safend Protector' from Safend Ltd. [Safend];
- 'Sanctuary Device Control' from SecureWave [SecureWave]

Many of these products illustrate similar capabilities, evidencing how such capabilities are standard expectations within the target domain of enterprise network control. Conversely, there are differences between the products which reflect their differing motivational factors – these will be investigated in order to determine how they can best be exploited in practice.

2.1 Platform Support

	Windows 98	Windows NT4	Windows 2000	Windows 2003	Windows XP	Windows Vista	Macintosh OS	Linux
DeviceLock		✓	✓	✓	✓			
DeviceShield		✓	✓		✓			
DeviceWall		✓	✓	✓	✓			
Disknet Pro		✓	✓	✓	✓			
McAfee				✓	✓			
Pointsec			✓	✓	✓			
Safend			✓	✓	✓	✓		
SecureWave			✓	✓	✓	✓		

Figure 1 Platform support provided by USB access control solutions

The USB access-control products reviewed in this section only provide support for the Microsoft Windows family of operating systems (generally the 2000/XP range, and the NT4/2003 Server derivations). There is no support for the Macintosh OS or Linux platforms, and no access-control products could be found for the latter platforms that offered similar functionality to the products described here. There is also no support for older versions of the Windows operating system, such as Windows 98. However [Safend] and [SecureWave] can be deployed within the Microsoft Windows Vista platform.

Where products have been aimed at the Windows platform, efforts have been made to provide seamless integration with the operating system by extending existing functionality. In most cases products integrate

directly with Windows Active Directory [Active2003], so as to provide a link between access rights and enterprise roles. In addition [Disknet], [Pointsec] and [SecureWave] provide support for Novell eDirectory, thereby expanding the applicability beyond that of the standard Windows applications. [SecureWave] also offers support for Windows Embedded Point of Service and Windows XP Tablet PC Edition, extending its applicability to retail environments and palm devices respectively.

Amongst many (if not all) of the product developers there appears to be an assumption that auxiliary Microsoft applications are available for use. For example, [DeviceShield] requires Microsoft SQL server to store recorded data, and [McAfee] requires .NET Framework components to provide functionality.

2.2 Product Motivations

The products considered in this section are motivated by a number of factors. The principal driving factor is prevention of internal data theft from within an organisation (e.g. [DeviceLock], [Pointsec], [Safend]). This is closely coupled with the prevention of corruption of secured data through the injection of unsolicited content into the network (as promoted by [GFI]). All products are primarily concerned with endpoint security within enterprise network domains. Products such as [SecureWave] and [Safend] also highlight the need to comply with regulatory standards (e.g. preventing users from uploading copyright-controlled entertainment content to an enterprise computer network).

As well as preventing data leakage and corruption of the enterprise network, [Disknet] places importance on the adherence of employees to dictated working practices – attention is given to the apparent need to prevent users from transporting games and other "inappropriate material" to their workstations (i.e. material that contravenes law, or copyright-controlled material e.g. music, games, confidential competitor material, pornography). [DeviceShield] also supports endpoint access control as a means of reducing the potential maintenance overhead that unauthorised devices introduce.

[Safend] provides workstation installations that cannot be tampered with by non-authorised members of staff, which places a degree of suspicion firmly with employees within the organisation. The latter point highlights the focus which all of the products place upon suspicion or monitoring of employee behaviour. There is a risk that in providing functionality that concentrates on the needs of the organisation over the capabilities of the individual, that the motivations (or freedoms) of the end-user are potentially inhibited. However, some products acknowledge this by attempting to educate users as to their capabilities within the company domain under the governance of device access policies (e.g. [DeviceWall], [Safend]).

2.3 Sample Product Pricing Structures

The most fully-featured access control solutions ([DeviceWall], [Disknet], [McAfee], [Safend], [SecureWave]) only provide pricing information upon direct consultation with the providers. Particular products (e.g. [SecureWave]) can only be priced once the target network configuration is known. Also, [Pointsec] for example prices deployments based on the merits of the purchasing company and their specific requirements. However, the other products described in this section offer pricing information based upon the number of machines in an organisational network – these costs are represented as cost-per-workstation, as shown in Figure 2.

(Where Applicable) Currency Exchange Rate USD to GBP: $1 = £0.50487, as referenced 02/06/07 [XE]

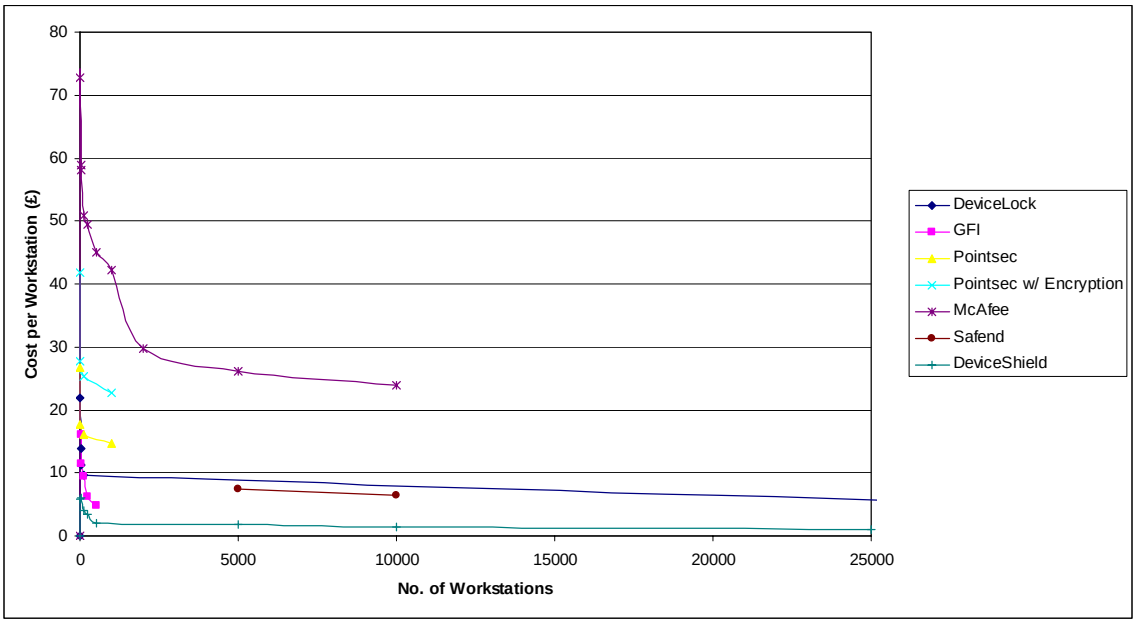


Figure 2 Sample pricing structures of USB access control solutions

As can be seen in Figure 2 [DeviceLock] and [GFI] have somewhat similar pricing structures, and offer greater value for money than the options presented for [Pointsec] with respect to basic USB access control. This is compounded by the fact that [Pointsec] requires prospective clients to purchase a license for the 'Smartcenter for Pointsec' [SmartCenter] (a centralised management suite), which incurs a further cost of between £2524 and £7573 for between 1000 and 3000 users respectively.
The [McAfee] prices include technical support and consideration for discounts on any further licences that are required.
[Safend] requires that the 'Safend Auditor' product also be purchased, which can cost £1766.75 for a 5000 user licence, and £2473.45 for a 10000 user licence. Maintenance contracts are sold separately, for example £1.57 for each seat in a 5000 seat licence.

2.4 Administrative Models

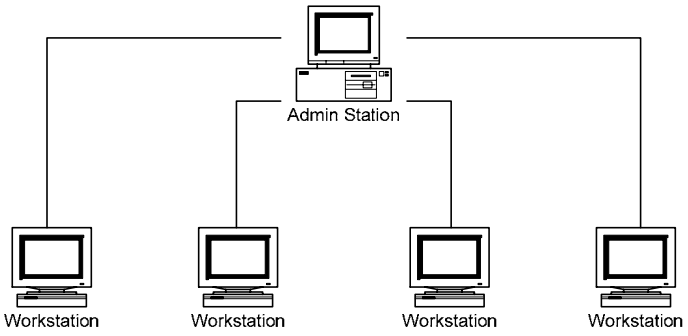


Figure 3 Centralised administration of end-user workstations

Many USB access control products install from a centralised security station, sending client-side installations directly to user workstations without the need for employee cooperation or for the administrator to

leave their station. This assumes that all of the computers that are connected to an organisation network are centrally managed, which may not always be the case (the creators of these products could however be expected to argue that fragmented network management is a poor model to follow).

The more comprehensive access control products appear to be aimed at corporations that have dedicated IT security staff available at all times. Control of access permissions is centralised (typically through a dedicated software-based management console), and the timely deployment of per-user or per-device access controls relies upon the availability of the appropriate staff members. Infrastructure such as this may require additional funds for IT security staff should they not already be available within the organisation. Redundancy may be required both within the computer network directly connecting the IT security staff, and within the security team itself (i.e. additional members of staff available to cover staff illnesses, lunch breaks etc.). [DeviceWall] acknowledges the power given to administrators, consequently recording the actions of administrative staff. It is then assumed that auditing of the administrators themselves is governed by, for instance, a dedicated audit department.

Countering the reliance on centralised IT administrative staff is the capability of products to maintain access policies according to groups of users and known device types. This then means that during common (i.e. predictable) working practices, user permissions can be managed without intervention from administrative staff.

Having adopted centralised control models, there is little accompanying discussion in the product information provided as to how such management schemes scale to serve a large number of workstations and portable storage devices. Most of the products suggest that they actively attempt to deploy as little logic as possible upon user workstations (e.g. [DeviceShield, DeviceWall, GFI]). The use of role- and group-based access control and re-usable device profiles also provides the capacity to deploy identical device access rights in similar working environments, without the need to duplicate redundant information. These capabilities could be interpreted as attempts to provide scalable infrastructure, but also an exercise in simplifying system deployment and maintenance.

All of the products described in this section aim to provide transparent installation and operation (thereby reducing the interference in user productivity that may otherwise be experienced), although the localised resource demands of device inspection and the need to effectively inform users of events pertinent to device usage are issues that need further investigation.

2.5 Device Coverage & Device Access Management Policies

Most products secure all access points in a corporate network. They provide coverage of USB endpoints as well as other device connection technologies such as Firewire and writeable CD drives, and remote-communication channels such as WiFi and Bluetooth. [GFI] concerns itself exclusively with types of removable storage media (including iPods), whereas [Pointsec] concentrates solely upon securing USB device access.

The more comprehensive products provide explicit blocking of access to specific categories, brands or even models of USB device, and unique CDs/DVDs (through serial number recognition, as available in [DeviceLock], [McAfee] and [Safend]). [DeviceLock] provides the capacity to control access to specific USB devices, provided the manufacturer has supplied unique identifiers for individual devices that can be recorded by the software. [Disknet] also extends the range of access modes by providing access schemes that forcibly require employees to encrypt data held on removable devices (thereby guaranteeing restrictions upon who can access the data on the device once it has been removed from the company network).

A few products also accommodate situations such as allowing users to read CDs such as training packs without necessarily allowing them to also write data to writeable data CDs. [Safend] and [DeviceLock] for instance provide the capacity to recognise the ‘data signature’ of an individual CD or DVD, so that only legitimate media will be accepted at network endpoints.

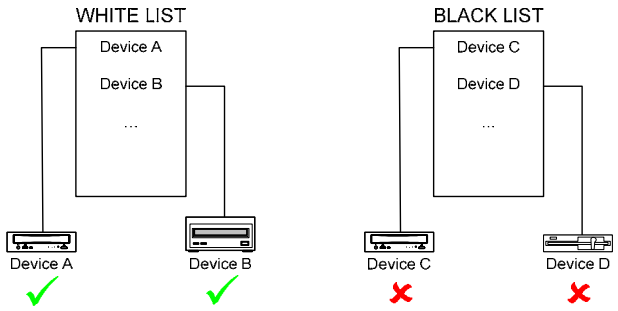


Figure 4 'White list' and 'black list' device access control

Many products employ 'white-list' and 'black-list' approaches to device access. Respectively in these cases devices can be explicitly included or excluded from an organisation's device access schemes. This allows structured access policies to be re-used across different end-user accounts, or across entire user groups, without undue replication of device information.

2.6 File Access Management Policies

A number of USB access control solutions (e.g. [DeviceShield], [Disknet], [Pointsec], [Safend], [SecureWave]) incorporate file-type filtering techniques to limit the types of files that users can transfer to removable media devices. [McAfee] goes one step further and allows filters to be applied to the contents of files (so that, for instance, files containing details such as credit card numbers can be prevented from leaving the company network). Filtering schemes are defined by administrators, and then enacted at the client-side (i.e. at user workstations where the access endpoints are found).

[Safend] can completely prevent access to U3 devices [U3], which are capable of acting as self-enclosed operating environments. Similarly, there is the capacity in most products to prevent executable files or 'autorun' programs from being copied to or executed from removable storage devices. Such precautions are prudent in the face of threats to the company network from malicious software. [Disknet] and [Safend] again highlight the consideration of improper behaviour on the part of company employees, whether this manifests itself either maliciously through the deliberate modification of specific file types (even directly within file headers), or through the accidental deletion of groups of files. Simpler approaches to data theft prevention (or at least, end-user control) are also exhibited; [SecureWave] provides the capacity to limit the amount of data that users are permitted to transfer to removable storage devices, while with [DeviceLock] access periods can be designated so as to control when end-users can utilise devices.

[McAfee] can be used to define complex rules that dictate automated responses to prohibited behaviour. For example, it can be permitted to copy only three files containing number patterns similar to those of credit card numbers to an external storage device before the activity is completely stopped.

2.7 User Monitoring

Many USB access control solutions are driven by the expectation that employees will try to corrupt the enterprise network from within, or otherwise attempt to gain access to company data for which they do not hold the appropriate permissions. It is worth remembering also that end-users can sometimes unintentionally gain access to files that they shouldn't have been able to, and such occurrences would need to be studied and rectified to prevent them from happening again.

In light of these precursors, all of the products provide audit trails of device and file access (i.e. which devices were connected to which ports, and which files were accessed by which specific users), supported with recorded duplicates of any copied data which are then retained by administrators (for instance should there be a need to produce evidence against employees in the expectation of subsequent legal action against them). For instance, [DeviceShield], [Disknet] and [SecureWave] provide records of both authorised and unauthorised access events (including those initiated by unauthorised code acting on workstations). [Safend] even provides auditing information relating to usage of protected devices outside of the company network.

[Disknet] encrypts and filters audit information on end-user workstations before delivering it to the administrators (which again assumes malicious intent amongst employees, but also provides scalable auditing through the reduction of audit data). [DeviceWall] records individual device connections and the names of those files that are accessed most regularly from device endpoints, and notably provides a full audit trail of the behaviour of the security administrators themselves. [DeviceWall] also considers the need to inform less computer-literate staff of network behaviour, providing as it does options to present audit data in customisable reports, graphs and charts (e.g. pie charts illustrating types of device access). [SecureWave] exhibits similar behaviour, in that audit data can be presented in reports, but also saved to file formats including XML and HTML, potentially for further processing in other applications.

The auditing of copied data raises the issue of employee privacy – for example, if an employee copies personal details (such as bank account information) to a USB device, this information may then be copied to the centralised administration centre, thereby providing access to individuals (specifically administrators) who should not otherwise be privy to such information. The providers of these products could however counter this with the argument that personal information has no place in the work environment.
Numerous products ([DeviceLock], [Safend], [SecureWave]) have the value-added feature of preventing the insertion of key-logging software within the PS2 or USB device connection chain on individual workstations. This does not directly tie in with the main motivation of endpoint device access control, but rather reflects the assumption of malicious intent on the part of employees.

2.8 Data Encryption

The access control solutions that are primarily targeted at large corporations provide facilities to encrypt data before it is stored on removable media devices (either automatically or after prompting end-users), and purport to even facilitate access to encrypted data outside of the work environment (e.g. [DeviceWall, Disknet, Pointsec, SecureWave]). These measures essentially extend the reach of the enterprise, by securing the data in such a way that at any time it can only be accessed in accordance with the data access policies of the organisation at any time. [DeviceWall] installs an applet on each workstation that allows staff to create encrypted devices and set personal passwords themselves (which empowers the user and actively involves them in the encryption process). Devices with contents encrypted by [DeviceWall] cannot be accessed outside of the enterprise network, which although beneficial to the security of company data, brings into question the usefulness of said devices as personal belongings (as in the Use Case in Section 1.2). If secured data is destined for use outside of the company domain, [Disknet] can configure password-only access to encrypted devices, through installation of a file-reader program on external machines.
In those cases where encryption features are provided, it is unclear whether the entire contents of a particular device are encrypted, or whether unprotected (i.e. personal) files can be co-located on the same device as encrypted data. However, [DeviceShield] can accommodate comprehensive encryption configurations, allowing access passwords to be defined for individual encrypted files. It can also manage selective automated encryption, so that only sensitive files are encrypted when copied to an external device.

2.9 Atypical Access

Most of the products examined in this section provide for employees needing to either gain temporary (but legitimate) device access that is otherwise prohibited by their assigned access rights, or gain access to a protected device on a machine that is outside of the control of the organisation. In the case of the latter, it is assumed that there is some network connectivity, and that the centralised policy server can be contacted from whichever machine a device is connected to.

Offline access to secured devices is achieved in different ways depending upon the access control solution that is employed. When using [DeviceWall] for example, temporary access is permitted to any device of a type already recorded in a user's access policy. Furthermore when temporary access is granted, a time-stamped log is created recording who was given access privilege, the specification of the device they used, and why access to the device was permitted. Alternatively, [DeviceLock] and [DeviceWall] permit temporary access to devices through phone conversations with IT administrators (as a means of obtaining an access code for the device). This process, although secure, relies heavily on the availability of administrative staff, and provides a solution that is technically not integrated with the enterprise-wide access solution (i.e. it is not clear whether the details of phone conversations between administrators and end-users are forcibly recorded and synchronised with the automated access logs). Users of the [Safend] solution achieve offline device access through a specialised utility that is carried with data whenever a device is encrypted, thereby essentially re-appropriating USB devices as self-enclosed encrypted storage devices. Products such as [DeviceLock] and [SecureWave] limit temporary access to a secured device to within a pre-defined timeframe.

2.10 User Education

Focus is primarily on securing data within an enterprise network, with any resulting effects upon the behaviour of company employees acting as a secondary concern. However, a number of products actively aim to educate end-users as to their access rights, informing users of whether they are able to transfer specific files to a particular device, and in some cases going so far as to describe the levels of access that the user has, and the levels of access they require in order to use a particular device. If end-users are fully aware of the permissions they have, it could be envisaged that they will be less likely to (at least unknowingly) infringe them.

[DeviceWall] provides options to inform users of their access rights (both upon use of a device and every time they log onto the company network). Reasons can also be provided as to why unauthorised file transfers may have been prohibited. Features such as these act to involve employees in the process of securing company data, thereby encouraging regulated access to protected files without generating unwelcome confusion amongst the affected staff. [Safend] provides a client-side application that guides the user while initialising new devices, including configuration of offline access passwords and device encryption states, thereby again maintaining the involvement of the user. [Disknet] involves users in the enforced scanning of devices for viruses and spyware, making them aware of the process before it commences.

Many products provide visual notification of access rights, with varying degrees of information. For instance, [GFI] will inform users if access to a particular device drive is prohibited, whereas [Disknet] utilises the Windows XP notification balloon device to inform end-users of prevented actions. [DeviceLock], [McAfee] and [SecureWave] can present context-sensitive information to users, such as references to specific kinds of devices not being permitted for use, or specific actions being blocked (e.g. [McAfee] may state that sending a file to a printer is blocked).

3. Digital Rights Management (DRM) Solutions

The products described in this section are concerned with enforcing data-management and intellectual property policies, so as to maintain lawful business practices and structured data control. The focus is less on how the devices containing company data are managed, and more so on how company data is secured in a manner which is both logical and can be persisted for as long as the data that it is associated with exists. As such, these products may be employed to create rigorous frameworks that describe levels of access to sensitive and protected enterprise data, with these levels then corresponding to the access rights of individual members or groups of staff.

These products are aimed at securing specific types of electronic documents, and as such are meant in this case for those subsets of organisations (such as legal departments) that deal with mainly word-processor or spreadsheet documents.

The products described herein are:

- 'Liquid Machines Document Control' from Liquid Machines [LiquidMachines];
- 'Information Rights Management' framework from Oracle Corporation [Oracle];
- 'Secure2Trust' from Avoco Secure Limited [Secure2Trust];
- 'Workshare Protect' from Workshare Inc [Workshare]

3.1 Platform Support

	Windows 98	Windows NT	Windows 2000	Windows 2003	Windows XP	Windows Vista	Macintosh OS	Linux
LiquidMachines			✓	✓	✓			
Oracle			✓	✓	✓			
Secure2Trust			✓		✓			
Workshare			✓	✓	✓			

Figure 5 Platform support provided by Digital Rights Management solutions

	Application Support
LiquidMachines	Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Visio, Adobe PDF, HTML, GIF, JPEG, TXT, RTF, XML, CSV, CUB
Oracle	Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Lotus Notes
Secure2Trust	Microsoft Word, Rich Text Format, Microsoft Excel, Microsoft Powerpoint, Adobe Acrobat Reader
Workshare	Microsoft Word, Microsoft Excel, Microsoft PowerPoint

Figure 6 Application support provided by Digital Rights Management solutions

With [Oracle] although the framework itself only supports the Microsoft Windows platform, the associated file-access program is available for Macintosh OS so as to allow users of the platform to access encrypted documents (although they cannot create protected files). [Oracle] can also be integrated with Microsoft Sharepoint (Microsoft's solution for inter-networked collaboration), but requires Microsoft SQL server when installed as a standalone application.

All products maintain the security of file contents even as they are passed between supported applications of different types. [LiquidMachines] supports over 65 applications and file formats, and can be integrated

into enterprise directories such as Microsoft Active Directory and SunONE LDAP. Support is also provided for multiple policy servers including Microsoft Rights Management System (RMS).

The makers of both [LiquidMachines] and [Secure2Trust] claim that support for other applications above the basic provisions can be provided by arrangement.

3.2 Sample Product Pricing Structures

Most of the software products in this category provide pricing information only upon consultation when the requirements of the purchaser are known (e.g. [LiquidMachines], [Oracle], [Secure2Trust]). However, pricing information for [Workshare] is illustrated in Figure 7:

(Where Applicable) Currency Exchange Rate USD to GBP: $1 = £0.50487, as referenced 02/06/07 [XE]

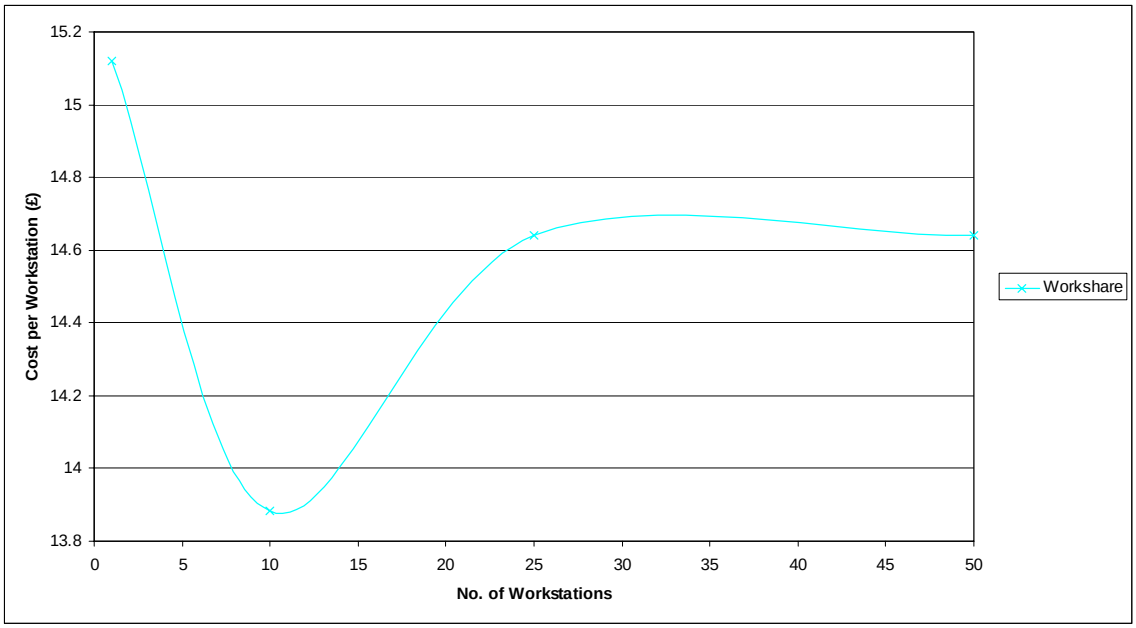


Figure 7 Sample pricing information for Digital Rights Management (DRM) products

It must be noted however that the pricing details for [Workshare] apply to a 1-year licence (which presumably would require renewal for each subsequent year of use).

3.3 Product Motivations

The products in this section aim to ensure that the content of confidential files is only available to those persons that have the correct privileges. As such, centralised access rights are associated with company files, and access schemes for individual files persist with those files regardless of whether they reside within the enterprise network, on a removable data storage device, or on a computer that is not controlled by the organisation. [Workshare] takes information control a step further by also considering the consequences of private notes and comments that are inadvertently embedded in documents even after they have left the control of their authors. In a similar vein, [Oracle] extends the concept of securing electronic documents by including capabilities to track the use of sensitive enterprise data both within and outside the company network, while also providing features that prevent users from side-stepping these measures (qualities that assume malicious intent on the part of the workforce). [Secure2Trust] views issues of content integrity with the purpose of providing manageability within intellectual property. This includes the aforementioned data access control features, as well as document signing and watermarking capabilities.

[LiquidMachines] provides support for enterprise content management systems such as EMC and Veritas.

3.4 Administrative Models

As with the USB access control solutions, all of the products described in this section are centrally managed i.e. all of the permissions associated with a particular document are stored in a centralised location within the organisation. This is prudent from a practical perspective considering that all of the products endeavour to provide manageable and consistent data access schemes amongst enterprise employees (with the latter represented through individual user roles or as part of a user group).

Content control products aim to operate transparently to the end-user. Furthermore, some consideration has been given to how a centrally-managed model can be maintained in practice; [Oracle] purports to be able to support 50000 users with a single server machine.

3.5 User Monitoring & Education

With an emphasis on data security [Oracle] and [Workshare] audit how end-users access protected files. In the case of [Oracle] efforts have been made to ensure that the capability to log user behaviour persists both within and outside its domain of control. Audited information includes details of successful and attempted file access events, including the identified user, the time of the event, the application that was used, and the location of the accessed file. Such information can assist an administrator in determining whether access was deliberate or unintentional and, in the case of the latter, can inform measures to ensure that similar events do not occur in the future.

All of the content control applications integrate directly into the toolbar menus of the targeted applications, so that they can be accessed and remain active while users work with their files. [Oracle] and [Secure2Trust] add additional information and options to the file management system; the former adds a 'SealedMedia' tab to file property displays, while the latter adds options to the file context menu.
With [Oracle] efforts are made to inform end-users about their personal access permissions. For instance, when a user attempts to access a secured file for which they do not have adequate access rights, they are automatically directed to an enterprise-managed web page that can be configured to provide context-sensitive information such as instructions for proper file use and e-mail links to any staff assigned to help with such matters. [Workshare] keeps users informed as to whether they have access to the files they are working with, and involves them in the process of removing personalised metadata and sensitive information from documents (such as comments in word processor files, or passwords and credit card numbers in e-mails) and during the application of access rights to individual documents.

[LiquidMachines] actively informs application users of access policy information e.g. data lifetime, and what actions (such as printing and editing a file), are permissible. [Oracle] disables menu/toolbar options that aren't permitted to be used by a user's access rights, and for instance notifies users if they try to retrieve content from a sealed document. [Secure2Trust] automatically prompts users to configure file access permissions when files are saved.

3.6 Data Encryption & Data Access Management Policies

Content control products are primarily concerned with restricting the editing, copying, and printing (either to a hard copy or the Windows clipboard) of protected file contents. All of the products provide role-based access schemes, and incorporate encryption into their operation as a means of securing the contents of confidential files. [Oracle] requires users to 'log in' to protected files, either with a dedicated password or automatically with their Windows user account information. [Oracle] is also capable of destroying files that are deemed to have expired, while also redirecting users to more up-to-date content. This then keeps documents consistent as they are propagated within and beyond an organisational boundary.

[Secure2Trust] provides extensive data security capabilities, including the ability to associate digital certificates or watermarking attributes to encrypted files (thereby closely identifying who is associated with a file within a particular usage context). Furthermore, access can be restricted by passwords and through access from specific secure locations. An emphasis is placed on how per-file security policies remain associated with the subject file, with an expectation that files will be transferred between secure and insecure locations. A number of content control features are also provided (e.g. screen capture prevention, viewing and printing restrictions, scheduled access). [Workshare] provides basic features to control the transfer of secured files to removable media such as USB devices and CDs, or as attachments within e-mails.

3.7 Offline Data Access

With [Oracle], access identities have configurable and enforceable offline periods, thereby acknowledging the mobility of employees. Sealed documents can be created and accessed through use of dedicated creation and reader applications. In addition, all actions pertinent to document security are logged locally on the active machine (with such information then being transferred back to the centralised administration site upon re-connection to the controlled network). This acts to create a complete picture of user activity. [Secure2Trust] integrates authentication measures directly into a protected document, with the expectation that secured files may be transferred across different storage devices and across different realms of authority. [Secure2Trust] can also be used to create 'secure teams' of employees, thereby encrypting files in such a way as to allow collaboration with external companies. [LiquidMachines] purports to offer offline users full functionality and zero latency while still maintaining policy restrictions.

4. 5. Disk Encryption Solutions

Disk encryption solutions exist which protect the contents of hard drives from unauthorised users while also ensuring that the transport of data to external storage devices such as USB devices does not compromise this protection. The following products are examined here:

- 'PrivateDisk' from Dekart [PrivateDisk];
- 'ProtectPack' from SafeNet Inc. [ProtectPack];
- 'TrueCrypt' from the TrueCrypt Foundation [Truecrypt]

4.1 Platform Support

	Windows 98	Windows NT	Windows 2000	Windows 2003	Windows XP	Windows Vista	Macintosh OS	Linux
PrivateDisk				✓	✓			
ProtectPack		✓	✓		✓			
TrueCrypt			✓	✓	✓	✓		✓

Figure 8 Platform support provided by Disk Encryption solutions

In addition [PrivateDisk] also provides support for Microsoft Windows 95.

4.2 Sample Product Pricing Structures

Prices for [ProtectPack] are provided upon consultation with the developer. [TrueCrypt] is a free, open-source encryption solution. Pricing information for [PrivateDisk] is provided in Figure 9. Prices include technical support and free minor upgrades.

(Where Applicable) Currency Exchange Rate USD to GBP: $1 = £0.50487, as referenced 02/06/07 [XE]

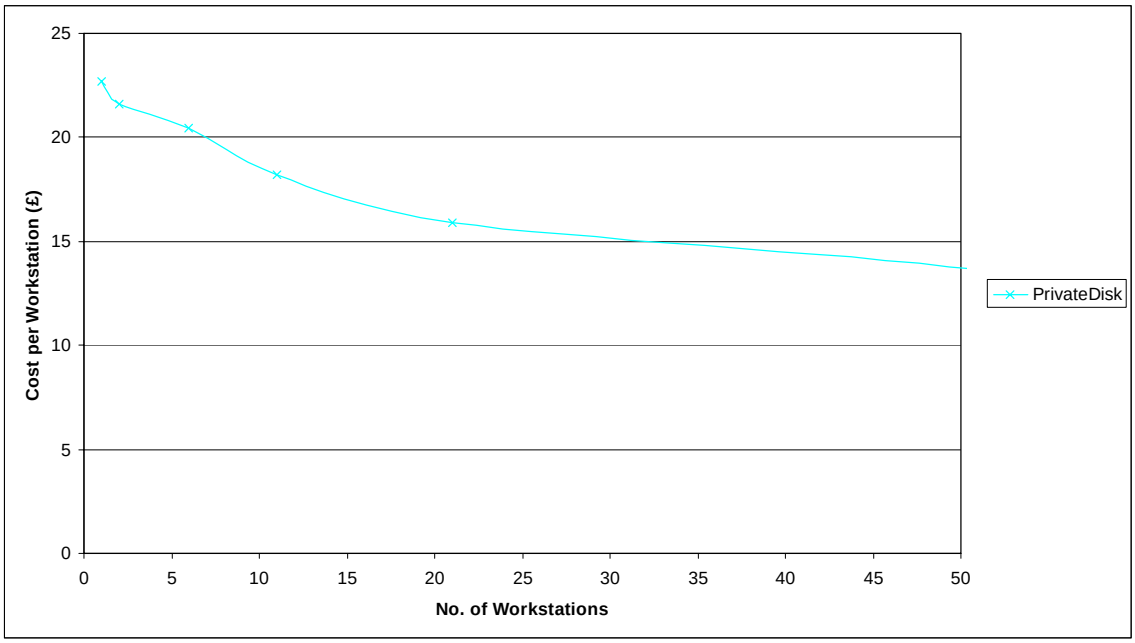


Figure 9 Sample pricing information for Disk Encryption solutions

4.3 Product Motivations

[TrueCrypt] is a disk-encryption solution for the maintenance of virtual encrypted disks which can be used like real hard drives. Capabilities are provided to encrypt an entire hard disk partition or a storage device such as a USB flash drive. [TrueCrypt] is also interesting in that it incorporates the concept of 'plausible deniability': if an unknown party forces a user to reveal their access password for instance, TrueCrypt provides and supports two kinds of plausible deniability. Firstly using hidden volumes (steganography), and also through measures that ensure that it is impossible to identify a TrueCrypt volume within a hard drive. As such, a TrueCrypt volume appears to consist of random data, making it impossible to prove that an encrypted volume exists. This premise highlights the seating of the product in encryption theory. None of the data stored on an encrypted volume can be read without adequate decryption criteria. As such the entire file system is encrypted (including file and folder names, unused storage space, and file meta data).
[PrivateDisk] is a hard-disk encryption application which automatically encrypts and decrypts data as it moves to and from an encrypted drive. It incorporates a white-list permissions policy that controls which applications are allowed to access an encrypted drive, while also providing additional features such as data backup & recovery and compression facilities.

[ProtectPack] is more pragmatic in its design, concentrating as it does on how confidential data is secured as it travels between individuals. The argument here is that data is only at risk when it is being transported, be that via removable media (such as USB storage devices or CDs) or e-mails. As such, persistent, practical encryption of data is the core goal of [ProtectPack].

4.4 Data Encryption & Data Access Management Policies

[PrivateDisk] and [ProtectPack] provide role-based access schemes, whereas with [TrueCrypt] users are prompted for access passwords or keyfiles whenever they wish to mount a protected drive.

[ProtectPack] is notable in that as well as wrapping files within its own protected file format, encrypted files become self-contained to the point that no additional software is required to access the file at a later date. These self-describing archives can then be compressed automatically to reduce storage requirements, and subsequently attached to e-mails or transferred to USB devices or CDs.

[PrivateDisk] incorporates features such as secure data wiping, automatic disconnection of encrypted disks (after defined inactivity periods), and encrypted backup facilities. Also, CD/DVD encryption is enforced; only the applications that are stored within the encrypted disk are allowed to run, which guarantees that distributed files cannot be copied or modified. Also, employees can be permitted to access confidential data, but without being able to run file-copying programs to capture information.

With [Truecrypt] if there is a need to access a single TrueCrypt volume simultaneously from multiple operating systems, an encrypted volume can either be mounted or dismounted on a single computer (e.g. a server), allowing decrypted or encrypted shared access to drive contents respectively.

4.5 Offline Data Access

With [ProtectPack], options are available to create self-extracting documents, which are then associated with an integrated application for accessing the original file contents in a secure manner (provided the user has the appropriate password). [TrueCrypt] can run in so-called 'traveller' mode, which means that it does not have to be installed on the operating system under which it is run. There are two ways to achieve this: after unpacking the binary distribution archive an associated executable can be run, or alternatively a dedicated 'traveller' disk can be created and used to launch TrueCrypt.

[PrivateDisk] provides USB disk portability, in that it can be used with USB storage drives, DVDs, portable media players etc. The disk encryption software footprint is deliberately small, and can be launched directly from the removable media.

5. Operating System Solutions

It is worth investigating whether any of the functionality recommended for the control of removable devices and management of confidential content in an enterprise setting is available within current operating systems. If this is the case, it would provide distinct advantages over third-party solutions, as the requisite features would already be integrated directly into the operating system, and it would not require the purchase and maintenance of additional applications.

5.1 Microsoft Windows Vista

The latest version of the Microsoft Windows Operating System, Windows Vista [Vista], provides additional functionality for the control of both copyrighted material and stored data. In addition, there are features to the control device access through user account management.

5.1.1.1 Digital Rights Management (DRM) Content Protection

It is the belief of Microsoft that next-generation multimedia content such as HD-DVD and BluRay will see greater adoption over the next few years [Russinovich]. Windows Vista incorporates what is called the Protected Media Path (PMP) to ensure that protected content can be accessed correctly. The PMP includes Protected User-Mode Audio (PUMA) and the Protected Video Path (PVP), which provide mechanisms for device drivers, media player applications and hardware to prevent unauthorised software or hardware from capturing high-definition content. The PVP is split into further sub-components [VistaProtection], namely the Output Protection Management (PVP-OPM), which ensures that PC video outputs have the level of protection required by content, and the User-Accessible Bus (PVP-UAB), which provides encryption of premium content across those components bridging the motherboard and the graphics adapter.

The PMP relies on a kernel mechanism introduced in Windows Vista called a ‘protected process’. As well as the running executable, associated process threads and security privileges associated with a system user, protected processes incorporate additional restraints to control access to content. All executable code loaded into a protected process must essentially be granted explicit permission to operate from Microsoft, typically by having the code signed (i.e. approved). Only if no unsigned code is found in the kernel-mode environment will the code then be loaded.

The ‘protected environment’ provided within Windows Vista combines with the components of the PMP to constitute a protection mechanism to prohibit access to copyright-controlled media content by unauthorised parties. In Windows Vista, the protected environment provides process isolation and continually monitors the state of kernel-mode software.

The documentation states that high-definition content is “valuable content that needs to be protected from stealing”, and that as such “each content type has its own particular policy that defines what the user can and cannot do with it”. In [McKenzie], it is speculated that Microsoft may re-appropriate the Digital Rights Management (DRM) technology that has thus far been reserved for high-definition media content towards other enterprises. That is, that the DRM constructs of Windows Vista could be utilised in the future to provide content-protection for any electronic data artefacts that must be protected against theft and loss. [White] also talks of the potential for such features to be appropriated for other types of content by stating that “while [high-definition] content has some unique content protection requirements, many of the requirements apply to commercial content generally, independent of resolution”.

Some critics have raised concerns about the costs of supporting the Windows Vista protected environment and the protection of premium content. [Gutmann] suggests that as a result of these additional features, hardware costs will increase, a claim which is not necessarily denied by the graphics hardware manufacturers, such as ATI [Levinthal]. It is also suggested that these costs will be passed onto purchasers of multimedia PCs.

Windows Vista requires that devices notify the operating system if they detect anything unusual during their operation. Gutmann suggests that this change in approach with regards to error-handling would mean that any normally unnoticeable glitches in system behaviour would be observed as a potential malicious attack. In the event of such an observation, the graphics subsystem within Windows Vista will be re-started. Although Microsoft state that this would only take a few seconds, Gutmann speculates that systems with high availability requirements may not tolerate the overhead of periodic soft-reboots of the graphics subsystem.

A further demand of Windows Vista is that device drivers poll the underlying hardware regularly as a means of detecting attacks. Further device-specific polling is also carried out, for example when devices are examined for signs of unusual behaviour as described above. Gutmann suggests that these practices constitute unnecessary CPU resource consumption.

5.1.1.2 USB Device Control

Windows Vista and Windows Server "Longhorn" provide Group Policy settings for removable storage access devices to control the permissible actions of end-users within an organisation [VistaControllingDevice]. An administrator can apply policies to control whether users are able to read from or write to removable storage devices. Such policies can be applied at the computer level (thereby restricting everyone that uses a particular computer), or to individual users or groups of users (associating access rights with specific user accounts). Access to specific types of devices can be controlled, such as USB and other removable media, CD/DVD drives (including USB-connected devices), and ‘smart’ devices such as media players, mobile phones and Windows CE devices.

Windows Vista Group Policy also describes ‘device identification strings’. When the Windows operating system detects a device that has not been previously installed on the computer, the operating system queries the device to retrieve its list of device identification strings (assigned by the device manufacturer). These identifiers can vary, potentially matching a single make and model of a device, or applying only to a general class of devices. The identifiers are used to determine which device drivers to install for a particular device, but can also be used to identify individual devices during future use. As such these identifiers allow administrators to restrict access to a particular device.

There are a number of different device control settings that can be applied to removable USB devices [VistaSecurity]. These include options to delegate device installation to administrators only, and prevent or allow device installation based upon certain identifiers (constituting black- and white-list access policies respectively). There is also the capacity to prevent the installation of any devices that are not known to the system administrators. It is notable that these features allow for the customisation of text presented to end-users if they should trigger associated events; this could be used as a means of educating users or re-directing them to further explanatory material.

5.1.1.3 Data Security & Encryption

Microsoft Windows Vista Enterprise and Ultimate editions include BitLocker Drive Encryption [VistaSecurity]. The entire Windows volume is encrypted to help prevent unauthorised users from gaining access to the contents of a hard drive. When Windows starts up BitLocker evaluates the integrity of a machine’s software and hardware. If it is determined that an attempt has been made to tamper with any contents of the drive, the startup process will be halted. BitLocker then eliminates bypassing of the Windows Vista protection mechanisms and offline access of a protected volume as means of accessing protected data. To unlock a halted boot sequence a user can be prompted to produce a personal identification code or a USB flash drive containing decryption keys. This then guarantees that only authorised users gain access to protected data.

The Encrypting File System (EFS) provided by Windows can be used to encrypt files and folders to help protect data from unauthorised access. EFS operates transparently – when an application accesses an encrypted file, the operating system automatically attempts to acquire a decryption key for the content, silently encrypting and decrypting files on the user's behalf.

5.1.1.4 Information Rights Management (IRM)

Although not a part of the Windows Vista operating system, the Microsoft Windows Office 2003 suite of applications provides features for Information Rights Management (IRM) [OfficeRights]. These features prevent sensitive information from being accessed by unauthorised persons, whether by accident or maliciously. Office 2003 documents (files created in Microsoft Word 2003, Microsoft Excel 2003 or Microsoft Powerpoint 2003) can have restrictions associated with them to specifically control the actions that particular users are permitted to enact. Permissions can be applied either to a specific document, or to individual users or groups of users, and include permission to view a document (but not edit, print or copy any of its content) or change a document (i.e. edit a file, but not print it). Full control of a document can also be granted, allowing control of the permissions associated with the document, including document expiry dates etc.

5.2 Microsoft Windows XP

Although Microsoft Windows XP does not offer functionality similar to that of Vista with respect to Digital Rights Management (DRM) and BitLocker, it does incorporate Encrypting File System (EFS) (as described in Section 5.1.1.3). Windows XP can also be augmented with the Windows Rights Management Service (RMS), thereby allowing users to associate permissions with Microsoft Office documents which can then be centrally managed.

5.3 Other Operating Platforms

Similar functionality to that described as in Microsoft Windows Vista (i.e. centralised document access control, device access control, offline drive protection etc.) is not found in the Macintosh OS or Linux platforms.

6. Requirements of a Complete Solution

The software solutions described in this document purport to solve a variety of data protection problems in the workplace. These include prohibiting improper use of USB (and other device) access points, protecting confidential document content, and securing data at rest within the company network. If an organisation is to consider purchasing products to resolve the described issues, there are other associated factors that must be assessed. These factors have the potential to contribute to the financial cost of adopting a given software solution.

Deployment Costs

If a particular software solution is adopted, it may take time to deploy across an entire organisation network. There may be differences in machine configurations that hinder deployment and take time to resolve. There may also be machines that are not already under central access control. Furthermore, whenever new machines are added to the network they will have to be brought under the influence of the any data protection product being used.

An organisation may find itself tied to a particular software product if migration to other products in the future is not immediately viable. For instance, if access definitions particular to the adopted product cannot be migrated to another product with similar functionality, the same or similar access definitions will have to be created from scratch with any new software used in the future. This would result in time being spent re-defining access definitions in the future having already created adequate definitions previously, or otherwise that an organisation may evaluate this extra effort and be put off seeking other solutions in the future and may choose to remain with the same software solution.

Once a solution is deployed, it will have to be maintained. Software patches issued to resolve faults or deficiencies in the product may take time to deploy correctly, or may cause unexpected behaviour in machines with differing configurations which would themselves need to be resolved.
Upgrades may be offered over time that an organisation may have to purchase. These may be required to provide up-to-date functionality or to maintain compatibility with the software used by business partners (should they be using the same software solutions).
Product upgrades may add extra features. These extra features could add to the resource requirements of the software, potentially requiring upgrades to the hardware or operating system platforms upon which they are used. For example, a new feature may be available that a company feels it needs, but may only be accessible from a newer operating system. This would require the company to upgrade the entire operating system deployment across the network to use the new feature. A more subtle situation is one wherein successive upgrades steadily add complexity to the software, and with this a slight increase in resource demands. Eventually the organisation will find that it has to upgrade all of its hardware to support a product that company machines were able to sustain with an earlier version.

It is shown that in most cases the greater the purchase order, the lower the per-workstation/per-licence cost to the purchasing organisation (as shown in Figure 2 & Figure 9 for USB Access Control and Data Encryption solutions respectively). However, the pricing data for [Workshare] (Figure 7) suggests that per-unit costs may be governed by demand for specific order sizes. As such, with some products there may in fact be ‘optimum’ order sizes which do not necessarily follow a linear pattern.

With regards to USB Access Control solutions (Section 2), it may be necessary for the company to provide employees with external data devices (should they have reasonable grounds to use one during their work). This could require a great number of devices be purchased, monitored and replaced over time. Accounting for device use and maintaining the devices themselves would require man-hours and money.

Administrative Costs

The great majority of the software solutions discussed in this report require or expect that a company network is centrally managed i.e. that all user access roles are kept consistent and managed from one location, such as a database of user profiles. In order to ensure timely deployment and use of access

permissions amongst employees, it is necessary to dedicate IT staff to the tasks of defining user permissions and regulating access to new and differing forms of media or file content. If IT personnel are already available within the company, such tasks may add to their workload. Alternatively, if such staff are not already present, new employees must be sought to maintain the software, and will in turn require time to familiarise themselves with the company network.

To further ensure that a centrally administrated system is kept functional and responsive, it may be necessary to incorporate some level of redundancy into the company network. That is to say, if the medium connecting administrators to vital parts of the network is damaged or develops a fault of some sort, an alternate route must be provided. Without this, parts of the network may cease to function correctly, potentially limiting employee productivity or introducing inconsistency into the access control scheme deployed across the network.

In the case of Digital Rights Management (DRM) solutions (Section 3), it may be necessary to arrange closer ties between staff and legal representatives. A legal team may need to review each company document to determine if content is being properly and consistently controlled. For instance, an employee may write a document from scratch and may indirectly cite content found within an already protected document without an awareness of the legal ramifications. To prevent the accidental introduction of data control inconsistencies such as this each new document may need the approval of an individual qualified in the legalities of data use and creation. Re-deployment or hiring of staff for these purposes would require both time and money, consistently and over for the duration of the use of the software product.

Productivity Costs

Employee productivity may be hindered during deployment of a chosen software solution. End-users may find that their normal work routines need to altered, or that completely new ways of interacting with the network need to be developed. For example, where a user would have transferred data to an external drive, they may find that they have to set a password for the device or obtain permission from the central IT administration body. Adapting to new network procedures may take time away from other areas of work, or could potentially sway employees away from their normal work routines entirely.

To ensure consistent use of a new software solution, company-wide education programs may be required. Such programs would be used to train end-users on proper working practices and how best to use the new software. Stand-alone educational documentation or websites would take time to develop, and could potentially require the efforts of a professional training body or representative from the developers of the software itself (whose time may have to be paid for as well). If group tutorials are chosen as a means to educate employees, this would place demands upon the time of numerous employees at any one time, as well as requiring staff to lead the tutorials.

Existing inconsistencies may be inadvertently uncovered after deployment of a software product. For example an employee may be informed by the new software that they have insufficient rights to access a document. The employee in question may be unsure as to why access has been denied and may in turn contact an administrator to resolve the issue. It may then be found that the employee was not properly informed of their access rights prior to deployment, or that access rights have been managed incorrectly upon deployment, inappropriately restricting the capabilities of the employee. Both of these could potentially be attributed to human error. Time would be required by both employees and administrative staff to resolve such issues should they arise, immediately after deployment of a software solution. This would distract both parties from other tasks (although in the case of administrative staff it could be regarded as part of their job). However it is worth remembering that the deployment of an adequate solution may at least prevent accidental or malicious abuse of company data, thereby maintaining adherence to data protection and usage laws, and reducing the chances of penalties to the company or loss of company data.

7. Remaining Vulnerabilities & Potential Research Directions

With respect to the products that have been examined in this document, a number of shortcomings are evident, both in the requirements detailed in Section 1.3 that the products have not addressed, and complications that may arise from their integration into an enterprise network. These factors have the potential to restrict employee productivity or otherwise leave existing vulnerabilities in conventional working practices unresolved.
Potential avenues for future work based upon the findings of this report are also described here.

Centralised Administration
All of the access control solutions that were examined follow a model of centralised control, wherein access policies are recorded at a single location from which they are pushed to end-users whenever they interact with the network. This approach is practical in terms of providing a means of maintaining consistent, manageable security policies, but in itself creates problems of its own. Firstly, it is assumed that all of the workstations that have access to confidential company data are in turn accessible from any location within the company network. Where employees are working with sensitive files, it is assumed that a channel exists through which those files can be secured from a remote location without the need to directly consult the end-user.

To guarantee the operation of a central point of administration, there would be a requirement to provide redundant data stores and network connections. This would then ensure that enterprise security policies and connectivity with the managed network persist. The matter of redundancy also encompasses the team charged with managing and propagating access rights. Administrative staff would be expected to manage temporary (and in some cases offline) access to devices and data in a timely manner.

Insecure Offline File Access
In the case of offline file access, the perimeter of the data security controls on insecure machines is unclear. For instance, an employee may choose to work from home on a computer that does not have adequate security protection (and as such may have been infiltrated by active criminal elements through virus software etc.). A situation could materialise wherein the owner of the home computer has legitimately gained access to secured data but at the same time malicious software has been able to access the same data on behalf of unauthorised persons. With this and similar scenarios, there is a need to determine how tightly-coupled role-based access is with company files stored on removable media, or even the physical storage devices themselves.

There is another issue associated with offline file access. Where products permit offline access to secured files the solutions range from passwords obtained through direct communication with administrative staff, to having a reader program bound with protected files or devices. It may be worthwhile investigating which strategy works best, and how such processes can best be automated.

Offline Productivity
Many products detail procedures for transferring files from a company network for further use elsewhere, including the subsequent return of files to the controlled network domain. It is however necessary to determine how files destined for the company network but originally created outside of its reach can be secured i.e. whether data-encryption features are bidirectional or whether a user must synchronise with the access control framework during file creation in order to guarantee that any such files are secured. As an example, an employee may be working on location at a site that does not provide adequate options for remotely connecting to the company network, yet they may be generating documents that are known in advance to be destined for stringent access control once they enter the company domain (e.g. on-site reports, customer-oriented data-gathering exercises).

Financial Costs of User Education
It may be worth investigating the costs of producing educational material that informs end-users of how to interact with the enterprise network once control applications have been installed. It may be that an access control/DRM application impacts so heavily upon end-user productivity that educating them about new

working practices costs the organisation more than they may have lost without having adopted the application. Although the latter is an extreme example, it does highlight the need to be able to objectively observe user behaviour and be aware of the processes necessary to alter such behaviour in accordance with the adoption of a particular software application.

Centralised Policy Creation

The products investigated herein all assume that there is a clear, centralised corporate policy towards data confidentiality and device access. Questions may be raised as to who within the organisation is best qualified to determine what the policy should be, and whether there are ways to make the definition of such policies easier. This is even more important when considering that more organisations are expected to make attempts to secure their networks, and as such will undergo the process of applying global policies to their networks.

Furthermore, those within the organisation that understand which information should be controlled (e.g. legal and human resources divisions) should be able to inform the unambiguous definition of corporate data security policies by enterprise IT administrative staff without requiring knowledge of how any adopted data security solutions work.

Intuitive Data Control

Digital Rights Management (DRM) products seem to dictate the processes that inform users of their permissions, based upon the hosting operating system (e.g. using notification balloons within the Windows XP system tray, or positioning drop-down menus into application toolbars). Research could be conducted into how best to integrate additional data security features into applications. Many of the DRM products only consider how to prevent improper access to protected data, and not necessarily how best to inform users of such events.

As an example, an employee may attempt to select and copy text from an Adobe Acrobat PDF file. Instead of notifying the employee that they are not permitted to copy the text only when they try to paste it into another file or application, they could be informed of this lack of correct permissions during the act of selecting text to copy. The intuitiveness of content permission and the associated process logic could be investigated, as well as how intuitive data control can be applied unilaterally across different applications without necessarily shoe-horning the associated functionality into existing application layouts.

Unified Access Policy Specifications

With the growing number of application features aimed at restricting access to confidential data (e.g. time constraints, passwords, user names, group names etc.) there are a great number of DRM applications that despite having similar features are incompatible with each other. If a general standard of permission definitions could be devised that does not limit the usability of basic file formats or require additional operating platform features to accommodate such definitions, inter-DRM application file control could be accommodated. At present, there is no discussion in any product literature about integrating DRM products with each other. It is assumed that either there was no existing DRM application within an enterprise, or that where organisations are working together they are using the same DRM software. As an example, if two companies rigorously define DRM policies using different products, and one company takes over the other, they may then wish to unify the DRM policies of the two previously separate companies. There are then issues relating to the criteria that dictate which DRM product to retain, and whether there is any means of transferring pre-defined access policies to a superseding DRM product.

Research also shows that a major factor preventing organisations from adopting data security applications is a lack of standards with regards to how data protection is defined [Infowatch].

Open Source USB Access Control Solution

No open-source USB access control solutions currently exist. Such an application could be developed and deployed (or adapted) to then provide USB access control on Linux & Macintosh OS operating platforms.

8. Conclusions

The great majority of the products examined in this document use centralised administration models to consistently manage role- and group-based access to critical company data, wherein a single server application communicates with comparatively small workstation installations. Where files are transferred beyond the control of the company administration, data encryption techniques provide a means of securing data and preventing unauthorised persons from accessing critical information. With respect to the dedicated device access control solutions, there is the capacity to control a range of network endpoints beyond USB devices (including CD drives and remote communication ports such as WiFi). File-filtering can also be employed to prevent malicious software from entering the network while also providing for more complex access restrictions.

Digital Rights Management (DRM) solutions provide approaches to achieving file content protection, through close integration of access rights with company documents (e.g. with use of file encryption and digital signatures). Techniques are also applied that build up a complete picture of data access events amongst the employees of an organisation (both within and outside the company domain).

File encryption solutions visited in this report provide secured access to data at rest, while also accommodating passage of encrypted content from protected hard drives to portable storage devices.

In terms of the financial costs of adopting any of the solutions that have been described, there are a number of factors that must be considered beyond the cost of the product software itself. It is necessary to have a reliable server machine (or machines) to support the core access management application. From this there is then a requirement for dedicated IT personnel to be made available that are capable of authorising networked and offline access whenever required. Where it is relevant, client-side applications can be deployed and managed automatically from the centralised server without intervention from either administrators or end-users. The latter can also be said of access permission policies (for instance where the same rights are applicable to a group of users).

There is also the need to consider how staff should be educated to adopt such additional software in their working practices, and how costly this may be both financially and with respect to productivity.

Acknowledgements

This work was conducted in the ‘Trust Economics’ project, funded through the UK Department of Trade and Industry, grant nr. P0007E, under the ‘Human Vulnerabilities in Network Security’ innovation platform. Comments and feedback from our project partners has substantially improved this document.

9. References

[Active2003] Microsoft Corporation, “Windows Server 2003 Active Directory”, http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx, as viewed 02/06/07

[Charlesworth] Andrew Charlesworth, “Data theft by employees 'commonplace'”, http://www.vnunet.com/vnunet/news/2165309/theft-employees-commonplace, as viewed 29/07/07

[Centennial] Centennial Software, “Gone in Sixty Seconds: The Executive Guide to Internal Data Theft”, 2006, http://www.centennial-software.com/resources/whitepapers/?product=2, as viewed 29/07/07

[DeviceLock] Smartline Inc., “DeviceLock”, http://www.protect-me.com/dl/, as viewed 09/05/07

[DeviceShield] Layton Technology, “DeviceShield”, http://www.laytontechnology.com/pages/deviceshield.asp, as viewed 20/06/07

[DeviceWall] Centennial Software, “DeviceWall Product Info”, http://www.devicewall.com/pro/, as viewed 09/05/07

[Disknet] Reflex Magnetics, “Reflex Magnetics Disknet Pro”, http://www.reflex-magnetics.co.uk/products/disknetpro/, as viewed 09/05/07

[DTI2006] Department of Trade and Industry, “Information Security Breaches Survey 2006”, April 2006, http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults_execsum06.pdf, as viewed 29/07/07

[Fisher] Matt Fisher, “UK data theft culture - managers burying heads in the sand?”, http://www.watchyourend.com/2006/11/20/uk-data-theft-culture-managers-burying-heads-in-the-sand/, as viewed 29/07/07

[GFI] GFI Software, “GFI EndPoint Security”, http://www.gfi.com/endpointsecurity/, as viewed 09/05/07

[Gutmann] Peter Gutmann, “A Cost Analysis of Windows Vista Content Protection“, http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html, as viewed 20/06/07

[Infowatch] Infowatch, “Internal IT Threats in Europe 2006”, http://www.infowatch.com/threats?chapter=162971949&id=207784668, as viewed 29/07/07

[Levinthal] Pete Levinthal, “Digital Media Content Protection”, http://download.microsoft.com/download/9/8/f/98f3fe47-dfc3-4e74-92a3-088782200fe7/TWEN05002_WinHEC05.ppt, as viewed 13/07/07

[LiquidMachines] Liquid Machines, “Liquid Machines Document Control”, http://www.liquidmachines.com/content1063.html, as viewed 20/06/07

[McAfee] McAfee Inc., “McAfee Data Loss Prevention”, http://www.mcafee.com/us/enterprise/products/data_loss_prevention/data_loss_prevention.html, as viewed 20/06/07

[McKenzie] Matt McKenzie, “Vista and More: Piecing Together Microsoft's DRM Puzzle”, http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9005047, as viewed 20/06/07

[Mediamax] Mediamax Technology, “Mediamax Technology”, http://www.mediamaxtechnologies.com, as viewed 08/05/07

[OfficeRights] Microsoft Corporation, “About Information Rights Management”, http://office.microsoft.com/en-us/help/HP062208591033.aspx, as viewed 20/06/07

[Oracle] Oracle Corporation, “Oracle Information Rights Management”, http://www.oracle.com/products/middleware/content-management/information-rights-management.html, as viewed 09/05/07

[Pointsec] Check Point Software Technologies Inc., “Pointsec Protector”, http://www.checkpoint.com/products/datasecurity/protector/index.html, as viewed 10/05/07

[PrivateDisk] Dekart, “Private Disk”, http://www.dekart.com/products/encryption/private_disk/, as viewed 20/06/07

[ProtectPack] SafeNet Inc., “SafeNet ProtectPack”, http://www.safenet-inc.com/products/data_at_rest_protection/ProtectPack.asp, as viewed 09/05/07

[RDT] RDT, Deutschland, “HDGuard”, http://www.hdguard.com/, as viewed 16/05/07

[Russinovich] Mark Russinovich, “Windows Administration: Inside the Windows Vista Kernel: Part 3”, http://www.microsoft.com/technet/technetmag/issues/2007/04/VistaKernel/default.aspx, as viewed 18/07/07

[Safend] Safend Ltd., “Safend Protector”, http://www.safend.com/65-en/Safend%20Protector.aspx, as viewed 10/05/07

[SecureWave] SecureWave, “SecureWave Sanctuary Device Control”, http://www.securewave.com/usb_security.jsp, as viewed 09/05/07

[Secure2Trust] Avoco Secure Limited, “Secure2Trust”, http://www.avocosecure.com/html_pages/products/secure2trust.html, as viewed 09/05/07

[SmartCenter] Check Point Software Technologies Inc., “SmartCenter”, http://www.checkpoint.com/products/smartcenter/index.html, as viewed 02/06/07

[SonyXCP] “2005 Sony BMG CD copy protection scandal”, http://en.wikipedia.org/wiki/2005_Sony_BMG_CD_copy_protection_scandal, as viewed 08/05/07

[TrueCrypt] TrueCrypt Foundation, “TrueCrypt”, http://www.truecrypt.org/, as viewed 20/06/07

[U3] U3 LLC., “U3”, http://www.u3.com/, as viewed 02/06/07

[Vista] Microsoft Corporation, “Windows Vista Home Page”, http://www.microsoft.com/windows/products/windowsvista/default.mspx, as viewed 18/07/07

[VistaControllingDevice] Microsoft Corporation, “Step-By-Step Guide to Controlling Device Installation and Usage with Group Policy”, http://www.microsoft.com/technet/windowsvista/library/9fe5bf05-a4a9-44e2-a0c3-b4b4eaaa37f3.mspx, as viewed 20/06/07

[VistaProtection] Microsoft Corporation, “Output Content Protection and Windows Vista”, http://download.microsoft.com/download/5/D/6/5D6EAF2B-7DDF-476B-93DC-7CF0072878E6/output_protect.doc, as viewed 20/06/07

[VistaSecurity] Microsoft Corporation, “Windows Vista Security Guide Chapter 3: Protect Sensitive Data”, http://www.microsoft.com/technet/windowsvista/security/protect_sensitive_data.mspx, as viewed 20/06/07

[White] Nick White, “Windows Vista Content Protection - Twenty Questions (and Answers)”, http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/20/windows-vista-content-protection-twenty-questions-and-answers.aspx, as viewed 20/06/07

[WindowsRMS] Microsoft Corporation, “Windows Server 2003 Rights Management Service”, http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx, as viewed 29/07/07

[Workshare] Workshare Inc., “Workshare Protect”, http://www.workshare.com/products/wsprotect/default.aspx, as viewed 09/05/07