

Information Assurance

Removable Media and Mass Storage Protection Technologies

In-Depth Research report version 1.0 / October 2009

www.secproof.com

Author

Mikko Jakonen (Information Assurance & Technology)

Co-Authors

Antti Hemminki (Risk Management)

Hannu Kasanen (Identity & Access Management)

Analysis

By Mikko Jakonen

This in-depth research report assesses the maturity and capabilities of leading removable media and mass storage protection technologies and applications against the Information Assurance needs of medium-to-large organizations.

The current situation is that none of the technologies and the implementations available Commercial-Off-The-Shelf (COTS) delivers full factor functionality for enterprise Information Assurance needs. All of them are lacking at least in integration capabilities or in supporting off-line use cases. All the applications seem to be point solutions. Point solutions are accepted, but they should have real integration interfaces available. Currently Envault and IronKey seem to go furthest with the functional integration and utilization of existing infrastructure.

Our research approach has been simple – we wanted to find out which applications could deliver the most suitable implementation based our vision of Information Assurance. Based on our findings and arguments, the tone of analysis is heavy and may sound negative. However, some of the techniques introduced and walked through delivered at least potential for good Information Assurance management practices. Then it is up to the user organization to select which is worse – shortcomings in management framework or loss of data.

The analysis was done by applying scenario analysis to selected technologies with different use-cases and requirements faced by private enterprises, public sector organizations and government institutions in path to secure their valuable information. The research base was conducted during May – August 2009.

The selected approach allowed us to demonstrate the potential bottlenecks of different, highly proprietary implementations regarding specific Information Assurance requirements.

Some technologies are more mature than others, some are pure software, some rely heavily on hardware, and some even reside on hardware – there are a variety of differences, making some of the selected solutions ill suitable for serious enterprise-wide usage.



About

Secproof is a consulting company specialized in development and assurance of operations, competitive edge, and security through ensuring operational resilience & continuity.

Secproof is recognized among large and medium-sized international organizations as a reliable partner committed to sustainable co-operation. We are involved in development and assurance in all areas of business operations.

Our core practices are Risk, Continuity and Security management, ICT Architecture consulting, including Identity and Access Management, and a variety of Technology services. Being the leading and renowned specialist in its core areas, Secproof is delivering Excellence, Assurance, and Training services with a proven delivery model guaranteeing best possible results and goal efficiency.

Secproof is formed by specialists with over 10 decades of professional experience in our core operating areas. Utilizing our in-depth technology knowledge, we continuously deliver security research reports and technology recommendations for government institutions and private companies alike.

Authors

Mikko Jakonen (mikkoj@secproof.com)

Antti Hemminki (anttih@secproof.com) and Hannu Kasanen (hannuk@secproof.com)

Trademarks

All trademarks, product names and registered trademarks are the property of their respective owners. Any third-party trademarks, service marks and logos are the property of their respective owners

Terms of use

This research documentation may contain proprietary information including trademarks, service marks and patents protected by intellectual property laws and international intellectual property treaties. Secproof authorizes you to view and make a single copy of its content for offline use. The content may not be sold, reproduced, or distributed without our written permission. Any further rights not specifically granted herein are reserved.

This document can be freely copied and printed for customer's internal use. Customers can also excerpt material from this document provided that they label the document as Proprietary and add the copyright notice in the document stating: Copyright © Secproof Finland 2009 - Used with the permission of the copyright holder. Contains previously developed intellectual property and methodologies to which Secproof retains rights.

TABLE OF CONTENTS

1. RESEARCH	5
1.1. SYNOPSIS.....	5
1.2. STATE OF THE REMOVABLE MEDIA PROTECTION FIELD.....	6
1.3. INFORMATION ASSURANCE (IA) LANDSCAPE	7
1.3.1. <i>Suppliers</i>	7
1.3.2. <i>What to expect – the big player buyouts</i>	7
1.3.3. <i>Techniques</i>	7
1.3.4. <i>Threats and risks</i>	8
2. THE BIG PICTURE	9
2.1. ABOUT:PROTECTION	9
2.2. DATA PROTECTION INITIATIVES.....	9
2.3. THE AAA AND INFORMATION ASSURANCE – COMBINED TRUTH?	9
3. THE VISION	10
4. TARGET OF EVALUATION (TOE)	12
4.1. FORMING THE BASIS.....	12
4.2. APPLICATIONS	12
4.3. CAPABILITIES	13
4.3.1. <i>Encryption strategy</i>	13
4.3.2. <i>Alignment</i>	14
4.3.3. <i>Use-cases</i>	15
4.3.4. <i>Use-case support per application</i>	15
4.4. FEATURES, CAPABILITY AND IA PERSPECTIVE	16
4.4.1. <i>Comparison table</i>	17
5. SYNTHESIS OF FEATURES	18
5.1.1. <i>The near perfect match?</i>	19
6. TECHNOLOGIES	20
6.1. KINGSTON (DTV)	20
6.2. IRONKEY (ENTERPRISE).....	21
6.3. CHECKPOINT (MEDIA ENCRYPTION)	22
6.4. UTMACO/SOPHOS (SAFE GUARD DEVICE ENCRYPTION).....	23
6.5. ENVULT (REMOVABLE MEDIA PROTECTION)	24
6.6. MICROSOFT (BITLOCKER TO GO)	25
6.7. TRUECRYPT	26
6.8. PGP (ENDPOINT DEVICE CONTROL).....	27
6.9. GFI (ENDPOINT SECURITY).....	28
6.10. DEVICELOCK.....	29
6.11. MCAFEE	30
6.12. SYMANTEC	31
7. APPENDICES	32
7.1. APPENDIX A - BUYING A REMOVABLE MEDIA & MASS STORAGE PROTECTION TECHNOLOGY.....	32

1. Research

1.1. Synopsis

Summary

The lack of mature security technology interoperability and frameworks for such interoperability is vertically distressing the currently available removable media and mass storage protection technologies and applications. The applications provide varying levels of data protection functionality, but do not provide full end-to-end manageability.

As long as Microsoft is a key player in the field, other major vendors of endpoint security applications and technology, such as Checkpoint, are not making serious changes in approaches toward management infrastructure. The vendors are still creating the point solution implementations for endpoint security management. However, Windows 7 with the BitLocker technology is still lacking real enterprise functionality, remote auditing capabilities and strong information protection scheme.

However, organizations must either implement some form of protection or risk leaking valuable business information – and currently the basic choice is to implement the point solutions. Interestingly, Microsoft has announced its “ForeFront” framework that could give a glimpse of hope to the playfield in terms of interoperability, but not going further into Information Protection itself. But that is just for Microsoft Windows based environments – whatever happens on the Mac and *NIX side will be totally different game.

During 2009 and 2010, it is unlikely that there would be any Commercial Off The Shelf (COTS) application suites available that would deliver all required endpoint protection and security integration capabilities for organizations’ Information Assurance needs.

It seems that two most promising new technologies covered in this research, IronKey and Envault, are able to reach the IA plateau at some level; many of the advanced functionalities required by customers are currently being developed and built into the applications by these innovative newcomers. But at the moment, we don’t see that they would support the full end-to-end Information Assurance scheme either. It will take time, but we predict that information protection techniques will see similar evolution as the World Wide Web services have: Innovative new technologies and companies bringing us “Security 2.0”.

This research focuses on the Information Assurance needs of organizations. With Information Assurance, we mean everything related to the information management in organizations; it is a practice of managing information-related risks. More specifically: The practice to protect and defend information systems by assuring the confidentiality, integrity, authentication, availability and non-repudiation.

That is also what a removable media and mass storage protection application should ultimately manage, access control beyond “my own domain” and the basic encryption functionality.

1.2. State of the removable media protection field

<p>The current technologies</p> <ul style="list-style-type: none"> • Are immature or under development for Information Assurance use. • Focus on resolving one key issue, either data confidentiality or access – not both. • Should NOT raise questions like “how strong is the encryption?”, but they do, due to the poor understanding of Enterprise Architecture or ICT management. • Require end-user knowledge or interaction, have a non-transparent approach, excluding Envault. • Have poor integration capabilities with systems management and other security applications. • Have poor cost/threat-mitigation ratio and cannot protect information based on role/compartment. 	<p>Justification</p> <ul style="list-style-type: none"> • Organizations need to protect confidential information available on various resources. • Removable media form a potential threat to an organization’s valuable or critical information. • Moving and storing vast amounts of data using mass storage devices has become a common practice. • Organizations must fulfill external requirements such as data protection regulation and standards. • Irregular or non-existing practice for removable media management lowers the operational efficiency of ICT. • The decision whether to protect information should not be left to end-users – automation and transparency is a must.
<p>Implementations</p> <ul style="list-style-type: none"> • The “triple-A”, or “AAA”, has been mostly forgotten in end-to-end use-case scenarios, excluding those directly supporting existing infrastructure. • May limit the availability of information off-line or off-site. • Poor access federation and collaborative use-case capabilities. • Do not support existing security infrastructure, such as fingerprint readers in laptops. • Should have data recovery available as well, either directly tied with the protection system or as a integral part with laptop data protection. • Extended Enterprise – scenario support is mostly missing. 	<p>Organizations should</p> <ul style="list-style-type: none"> • Form an Information Assurance (IA) framework, based on solid information security practices and risk management disciplines. • As part of the IA framework, define clear classifications and handling rules for data. • Decide who owns the information and who are the policy associates – form a vision about the Extended Enterprise. • Define proper end-point security management principles and policies. • Create a threat model for end-point security. • Define requirements for end-to-end use-cases where secured information flow is analyzed. • Implement protection measures with end-point removable media encryption. • Implement protection measures with end-point device management capability. • Implement a proper Identity & Access Management system. • Not rely solely on MS Active Directory, as certain data may need to be used off-line or delivered to a third party. • Potentially implement federation techniques for user authentication in foreign identity domain. • Follow the Information Assurance field on technical side and push suppliers to support better integration of technologies. • Together with other security infrastructure technologies, form scenario-driven Defense-In-Depth and Defense-In-Information (DII) strategies.

1.3. Information Assurance (IA) landscape

1.3.1. Suppliers

The removable media and mass storage protection is a relatively new field with many small and medium-sized suppliers providing point solutions. We can expect some consolidation to take place as the industry matures, possibly bringing a more holistic approach as the point solution is integrated to a broader application suite.

1.3.2. What to expect – the big player buyouts

During 2006-2009 for example the EMC Corporation bought some major houses that have traditionally provided information security applications. RSA is a well known purchase, but less known is that EMC acquired Authentica, a leading enterprise rights management software. This gives a glimpse of the idea what might come to the table during the next two to three years.

In the light of the EMC example, it looks like the EMC and some others, including Microsoft, are interested in building an end-to-end solution for the Information Assurance "market". Microsoft already has its Office Sharepoint product with some Information Rights Management capabilities.

1.3.3. Techniques

Inside the organization, it is currently possible to create a technical Information Assurance framework that is built upon proprietary (closed) technologies and has some limited set of IA functionality.

However, as we expand the organization's boundaries outside the LAN (e.g. Extended Enterprise), we find that there is no common and open technology available that could integrate external collaborators seamlessly in. Some proprietary federation techniques have been introduced and tried over the years, but the results have been poor.

Current removable media protection applications approach the IA needs by providing data protection and Information Rights Management features such as:

- Persistent protection of data
- Dynamic policy control
- Data expiration
- Mobile user support
- Audit trail
- Transparency for end user
- Tight data integration

1.3.4. Threats and risks

It's all about risk management; the need for any removable media protection must be assessed against potential business risks and threats the organization faces. To give some perspectives and potential use-cases, we present a few selected examples of threats. Each of the perspectives has their own special needs on top of the common IA requirements.

- **Industrial espionage**

Especially in knowledge-based businesses with large R&D stakes, information about new designs, pilot production results, and details of new endeavours are pure money. Same holds true for government institutions with national intelligence objectives.

The target of removable media and mass storage protection practices should be, in addition to the general IA targets, to be able to track and potentially follow the misuse of information. This is a valid argument, since it is still very hard to determine from the "noise" whether the use is legitimate or not. Solid data handling policies are needed, and very hard to maintain and enforce in a networked, collaborative, and multi-actor environment.

- **Regulatory non-compliance**

Data protection regulation in many parts of the western world imposes penalties for careless handling of personal information such as medical records or banking details. The motivation for such regulation is clear: Losing a USB drive containing personal records can expose the private individuals to identity theft and other misuse of their information. However, the major problem in achieving regulatory compliance regarding the handling of removable media and mass storages is that the practices and proper guidance for executing the tasks in detail do not exist.

- **IT administration/insider threat**

Any organization's IT administration has access to valuable information in forms of passwords, designs, disaster recovery plans, process charts, role and access information, etc. The need to protect such information is obvious. An attack to the heart of information resources and systems managing the information itself will collapse the whole deck.

But not only IT administration has access to valuable information. In fact, any employee may be able to copy large amounts of data on removable media or mass storages, for example customer records. The risk of disgruntled ex-employees stealing confidential data and taking it to competitors, or setting up a new competing business, is elevated during economic downturn.

- **Uncontrolled collaboration**

Collaboration is a must for many organizations working with their customers or external partners. If the collaboration is left uncontrolled, confidential information may end up to unauthorized parties. The tricky part in building a protected collaboration environment is how to manage the collaboration entities so that they are able to access the protected information on-demand and role-based. Collaboration frameworks can also change rapidly, so the protection technology should be able to adapt as well. Role-based access control, or RBAC in short, with access federation capabilities might respond to this requirement.

2. The big picture

2.1. About:protection

There are removable media and mass storage protection technologies and there are not. The large variety of the technologies and their integration capabilities makes things complex. Some of the technologies seem to be unusable for organizations larger than 20 people, some are lacking basic details that are required by regulation, policies or other demand, and some require too much effort, skills or knowledge from the end-users.

There are no absolute right answers for “how to protect removable media”. There are a couple of good methods for doing it – which in front require both technology solutions and management disciplines in forms of policies to be followed. The enforcement of disciplines and policies requires the management interface to be in correct shape. Most of the technologies support only partially the management frameworks available or commonly found for example in certain antivirus or firewall products.

2.2. Data protection initiatives

But what data to protect and when - the current models of protection do not yet qualify for information management, as too much life cycle or labeling details are missing. If we count for example iPods or other music/media players as removable media as well, then we have serious issues with the protection of data, as making a clear distinction between allowed and disallowed data in removable media is unmanageable. In classifying data, the ladders should lead to the root, to the creation of data.

Moreover, the technologies should be as invisible as possible for end users, and still deliver a state of knowing that my data is securely stored on my USB memory. Not all technologies provide a successful approach for this.

2.3. The AAA and Information Assurance – combined truth?

AAA stands for Authentication, Authorization and Accounting. For proper AAA in an organization the typically needed key elements are:

- Identity Management system (IdM)
- Access Management system (IAM)
- Ability to authorize a user, which sums that the user must have proper rights or permissions granted to the information he or she needs.
- Ability to record and audit the usage of information resources based on the authorizations and user actions.
- Life cycle information of user identities, usage of the permissions and authorizations.

Well, how this sums up with removable media and mass storage protection? The integration between AAA and the Information Assurance “field” is vague at the moment even with the best applications.

3. The vision

The willing state

Our vision of the world of data protection is quite different from the one we have today. Let's face it: None of the removable media protection technologies covers the actual "willing state" of information assurance needed by organizations. **We are not there yet.**

To open the rough statement a bit, let's walk through the willing state principles.

What do we want? We want the data to be continuously secured from the moment of its creation and throughout all latter stages of its life-cycle. The information may end up to a removable media or mass storage for transportation and then again be available for users that have privileges to the information granted by an authorization process. All this needs to be done securely, yet it must not disturb the end user too much. And we want the information to be under continuous monitoring, creating a log of authorizations and user actions - with various memory appliances you may have to be able to stand in a court of law to tell what really happened with that data from beginning.

The above basically delivers the "military grade", "lower-upper systems", and "data labelling" in common environments. Such functionality should already be there. But many organizations are spending big sums of money to integrate all the technologies together without still being able to provide real end-to-end information assurance.

Our current systems have weak protections, and even if the data is protected outside the system, there may still be a hole on the system side. Eventually someone will squeeze from the right place and be able to get the information without proper, approved authorization to it.

Assumptions in background

First; let's skip the common Joe away and concentrate on organizations, enterprises and government institutions – folks that really need to protect their valuable information.

Second; you need to have a reason to protect data – and all data is not the same. Well – now comes the tricky part: Different data has different value. For consulting and healthcare companies, customer data is vital to keep secure. For a technology company, new designs are critical. Especially organizations under a legislation or compliance regulations, defense- and military or organizations working with classified business secrets are somewhat forced protect their information going in and out through the house. Some legislation requirements or policy enforcements require organizations to handle their information in certain way. Basically, to define how the IA framework has been built.

Third: Management of the IA is the key to successful data protection, even with the removable media and mass storages. To properly adjust the management practices over the use-cases that need to be supported is a demanding task. In most cases, the interoperability with different tools that IT managers may have for infrastructure management is missing IA requirements totally or in many aspects. Even handling the basic authentication seems to be an issue for most organizations with current tools.

Demands

We could invent more demands set by angles we have established with Information Assurance practice. The truth is that most of the enterprises still need good information management disciplines and assurance, so that information does not leak from the organization. Most enterprises should take care of the basic assumptions first, and understand that they indeed are "an enterprise", not just a group of people and resources creating and utilizing information. Most notably, the information used in enterprises is **business** information, and it would be a perfect time to start acting like an enterprise as well and taking the necessary information assurance steps.

Implementations: Distinction of user and system

Some of the suppliers of the studied removable media / mass storage protection applications have made a self-aware distinction between the system and user – which seems to be wise. This gives a basis for protection against misbehavior from both the user-side and the infrastructure side, for example if operating system or domain gets under malicious influence.

However, even the suppliers that made the distinction are lacking in the end-to-end integration between user and data.

There are pros and cons in this approach. Either you utilize the existing enterprise infrastructure, such as Microsoft AD, and trust it for authentication and authorization – or – you take the long road to build a totally separate security infrastructure for access control. The first integrates without problems and scales well; the latter is more complex to implement and manage, but may in some cases be more trustworthy than the AD domain.

Implementations: Protection during the whole life-cycle of data

With some applications supporting the relevant use cases used in this research, we can know that data has been transferred to a removable media, we are even able to protect it, but still we are not able to track the data from its origin and through the triple "A", or enforce policies needed by the information itself – from creation of the data to the end of its life-cycle.

Let's combine the real needs for information protection, and we can see that a user must be enrolled or granted permissions to certain confidential information, and the information must be available and hold its integrity in end-to-end usage pipe. That pipe includes the removable media.

Implementations: Integration and interoperability

Like said - the integration and interoperability is missing. We are keeping our faith that someday, there will be software implemented in devices (pc/laptop/mobile) that responds to web services' calls for easy management, and mass storages that have capabilities to work over organization boundaries, securely, keeping the policies and labeling set to the DATA itself, not just with the hardware chip or an additional tool on workstation.

4. Target of Evaluation (ToE)

4.1. Forming the basis

The operability, management and protection strategy or technique of removable media and mass storage protection applications is the target of this evaluation.

Primarily, we want to know how suitable the application is for organizations, what are the prerequisites for an organization to adopt the application, how the application should be used and managed, and what are the advantages of the approach the supplier has selected, if any.

Secondarily, we are interested in central manageability of application, suitability for securing organization's data, the approach the supplier has selected for information assurance, potential weaknesses of the approach and so on.

Third, with less weight, we cover how the actual data encryption capability is implemented and how the management framework works.

It is a narrow line basically – either you have a hardware-based or a software-based encryption approach. Yet we did not want to narrow the ToE field too much, and therefore we included the port blocking applications in the research as well.

4.2. Applications

The suppliers and/or applications pointed for evaluation are as follows:

- Kingston (DTV), www.kingston.com
- IronKey (Enterprise), www.ironkey.com
- CheckPoint Software Technologies, www.checkpoint.com
- Utimaco/Sophos, www.sophos.com
- Envault Corporation, www.envaultcorp.com
- Microsoft, www.microsoft.com
- TrueCrypt, www.truecrypt.com
- PGP, www.pgp.com
- GFI (EndPointSecurity), www.gfi.com
- DeviceLock, www.devicelock.com
- McAfee, www.mcafee.com
- Symantec, www.symantec.com

4.3. Capabilities

4.3.1. Encryption strategy

The research found four different encryption strategies:

- Hardware (chip on token)
- Software (on token)
- Software (on workstation)
- Software- distributed/vaulted encryption.

The **hardware model** works by having a dedicated encryption chip on the mass storage itself. This enables the possibility to implement read/write operations independently of the host operating system. Offline use is also always possible - yet at the same time the security is hampered by having the data on token behind a simple, stand-alone user-password - and the end-user's willingness to use the hardware token in the first place.

However, there are different approaches to manage the off-site access of hardware encrypted USB drives, including limiting user rights to access data depending on the authentication method and host environment. IronKey is implementing this approach with its "IronKey Enterprise" offering that provides central management capabilities that make it suitable for enterprise use, even when it is a point solution.

The **"software on token"** model works by having a piece of software on the removable media itself that is run by the host computer. The software allows setting password-protection for data. This approach is the cheapest, because simple encryption applications often come with even cheapest USB drives, or can be freely downloaded from the Internet. Downside is the total lack of enterprise features such as enforced data protection, accounting, central management and policy control.

The **"software on workstation"** model delivers capability to protect the data on-site or with the computer. The upside is that software applications are more versatile than hardware, since they can protect many kinds of removable media and mass storages. The end-user interaction and transparency of the protection, as well as central manageability of the software, determine how well the protection performs. Most problems come with off-site use – lack of off-site auditing, access control other than simple user-password, and in some cases even missing write capability hinder the usability of current solutions. Some applications such as MS Bitlocker only work in Windows environments.

The **"software-distributed/vaulted"** model is a novel approach pioneered by Envault Corporation. In this model, data is first encrypted and then cut into two asymmetric pieces (99:1 ratio). The small part is stored in a secure network server, and the large part on the removable media. This way the access control is fully integrated with the existing enterprise infrastructure and authentication, and the system is capable of full audit trail and remote suspend/kill for data and removable media in real-time. On-site use is fully transparent for end-users and best in this research. The same versatility applies to Envault as for normal software on workstation applications. An interesting feature of the distributed model is that it is file-based, not container-based – this allows Envault to uniquely integrate with data labeling solutions such as MS SharePoint for policy-based protection. The drawback is that the distributed method requires accessing the server occasionally and is therefore not fully offline/off-site capable alone.

To enable offline/off-site use, both Envault and IronKey have specific modules in their application. For offline use Envault can use workstation-side buffering of the 1% pieces, allowing work to continue e.g. in an airplane, and for off-site/3rd party computer use Envault is utilizing its Airlock, which works basically as a software on token approach with some advanced functionality such as accounting, data expiration and passphrase protection and passphrase complexity management. The cost of the offline use is a weaker protection strategy and it may require more IT management overhead, but on the other hand, it delivers certain (not full!) possibility to extend the data protection scheme outside the organization perimeter.

Port blocking is omitted from this list because it is not encryption at all, and it focuses on securing the ports where mass storage devices are attached and collect information about what data has been transferred through the interface(s).

4.3.2. Alignment

The following table shows the application alignment towards each other in capabilities of system management (own system), encryption, integration and device/port management.

The smaller number the application has, the better it performs.

<p>MANAGEMENT</p> <ol style="list-style-type: none"> 1. IronKey 2. Microsoft, Envault, CheckPoint 3. Utimaco 4. McAfee, Symantec, GFI, DeviceLock 5. Kingston, TrueCrypt 	<p>ENCRYPTION</p> <ol style="list-style-type: none"> 1. IronKey, Envault 2. Utimaco, TrueCrypt 3. Microsoft 4. Kingston
<p>INTEGRATION</p> <ol style="list-style-type: none"> 1. CheckPoint 2. Microsoft 3. IronKey, Envault, GFI, DeviceLock 4. Utimaco, McAfee 5. Symantec, PGP, TrueCrypt 	<p>DEVICE/PORT SECURITY</p> <ol style="list-style-type: none"> 1. GFI, DeviceLock 2. CheckPoint, Symantec 3. Utimaco, McAfee, Envault 4. PGP 5. TrueCrypt <p>Microsoft is delivering Operating System level port/device security</p>

The criteria used for evaluating the applications are as follows:

- Technical architecture compatibility with the infrastructure utilized by the most Enterprises. End-user interaction, transparency, usability and needs for user training.
- Support for Enterprise security policies.
- Capabilities for the end-to-end Information Assurance methods and models.
- Enterprise class management capabilities.

4.3.3. Use-cases

We defined the following six use-cases to simulate the real-world scenarios and needs regarding the use of protected removable media in an organization setting:

- (UC1) Use case 1 – off-line user, occasional connection with corporate network, with legitimate needs to deliver data to a 3rd party (off-site).
- (UC2) Use case 2 – off-line user, occasional visits locally on the corporate LAN, with legitimate needs to deliver data to a 3rd party (off-site).
- (UC3) Use case 3 – on-line user, working most of the time on corporate LAN, occasional legitimate needs to deliver data to a 3rd party (off-site).
- (UC4) Use case 4 – on-line user, working most of the time on corporate LAN, no legitimate needs to deliver data to a 3rd party (off-site).
- (UC5) Use case 5 – off-line user, no connection to the corporate network of any kind, no legitimate needs to deliver data to a 3rd party (off-site).
- (UC6) Use case 6 – off-line user, no network connections of any kind, standalone workstation with legitimate needs to deliver data to a 3rd party (off-site).

In this analysis, any other use cases beyond these are considered irrelevant or illegitimate scenarios.

4.3.4. Use-case support per application

	UC1	UC2	UC3	UC4	UC5	UC6
Kingston	X	X	X			X
IronKey	X*	X*	X*	X	X	X*
CheckPoint	X	X	X	X		X
Utimaco	X	X	X	X		X
Envault	X*	X*	X*	X	X	X*
Microsoft	X	X	X	X		
TrueCrypt					X	
PGP					X	X
GFI					X	
Devicelock					X	
McAfee					X	
Symantec					X	

The table shows some applications are able to work on several different use scenarios simultaneously, thus providing a transparent utilization and real enterprise-grade protection.

* IronKey and Envault allow also protected writing in off-site/3rd party computers for return-trip data protection.

4.4. Features, capability and IA perspective

The following table establishes a basic view of the features and capabilities offered by the applications analyzed in this research.

The table is divided on distinct parts, where

- 1st section concentrates on the encryption as focus area
- 2nd section shows available management features
- 3rd section introduces additional security features
- 4th section reveals an application's potential for Information Assurance

4.4.1. Comparison table

	Kingston	IronKey	Checkpoint	Utmaco	Envault	Microsoft	TrueCrypt	PGP	GFI	DeviceLock	MCAfee	Symantec
Encryption strategy	X	X										
<i>Hardware (on-token)</i>												
<i>Hardware (off-token)</i>												
<i>Software on workstation</i>	S		X	X		X	X	X			X	X
<i>Software-Distributed/vaulted</i>					X							
<i>Needs end user application</i>	S		X	X	X	X	X	X		X	X	X
End user interface	X	X	X	X	X/T	X	X/T	X			X	X
<i>UI & usage through application</i>												
Management	S		X	X	X	X	S	X	X	X	X	X
<i>Application is manageable</i>												
<i>Remote management</i>		X	X	P	X	E		P	X	X	X	X
<i>Security Management integration**</i>		X	X	P	P	E			P	P		
Additional Security Features*		E	X	P	X	E		X	X	X	P	X
<i>Port/device blocking</i>												
<i>Endpoint security integration</i>			X	X		P		X			X	X
Information Assurance capabilities		X										
<i>Compartments/role based data access</i>					P	P	E					
<i>IRM or DRM integration</i>							E					
<i>Data labeling</i>					E	E						
<i>Policy driven management</i>		X	P	P	P	X		P	X	X	P	P
<i>Multiple privilege levels for data</i>		X			P	P	X					
<i>Remote management (non-LAN or WAN)</i>		X										
<i>Remote lock/delete data</i>		X		X	X	X						
<i>Logging (remote)</i>		X		P	X							

grayed – feature not available

X – functionality exists “out-of-the-box”, **E** – with extendable module or/and additional application.

S – Some – basic management/data handling locally, **P** – Partial – not all important functions are available or can be managed remotely.

T – End user experience of the application is mostly or totally transparent.

*Additional Security Features are add-on/options that enhance the actual encryption/protection scheme. Therefore f.ex. logging is not part of the additional features.

**Ability to directly integrate with 3rd party security solutions or “AAA” technologies.

5. Synthesis of Features

The analyzed applications and technologies provide varying combinations of IA related features. Some features are rather common: Write enabled/read-only rules, varying capabilities with different authorization sets, and capabilities to log transferred data. The greatest differences come are in the policy enforcement and remote management features. Most of the technologies seem to paint a strict line between hardware and software.

Each of the technologies provides some sort of management capability, even the Kingston drive, but seriously speaking there are only a few of the many to fulfill the basic enterprise needs for removable media information protection.

Still, none of the technologies provided the perfect set of ultimately needed features for Information Assurance in the way it should be. They are more or less point solutions.

The fact is that **"you are not going to get all the features in single pack"** – having said that, it seems that Envault and IronKey are listening to their customers and adding functionalities that are needed for real enterprise-grade use, and performed best in the use case comparison.

What one application has on hardware, another provides with software and vice-versa. And the best data protection technologies lack features in port blocking, whereas a good port blocking software fails to protect data. There is no direct winner.

The tools

IronKey Enterprise comes very close with the fine tuned model of integrating the authorization with 3rd party utilities, such as PKI or RSA SecurID. It delivers the encryption capabilities and certain logging capabilities as well management features. The downside is real off-line usage, while there are good features for doing that on some extend.). IronKey does not require anything on workstation side and lowers the management barrier with the model that everything is on hardware. The price and lack of port protection are the ultimate cons that you have to sacrifice in tolerance of information assurance needs. IronKey lacks many advantages and ideas that Envault has implemented with software. The integration with other systems, such as Active Directory could be handy in most of the environments, but as there is no software for IronKey installed on workstation – for example automatic sign-on is not directly possible.

Envault lacks with the 3rd party integration, but works great together with Active Directory and Group Policies, which extends the usability in organizations. It provides a unique approach for distributing the encrypted data to maintain its security and make it usable under the management domain established. Unlike any other encryption technology, Envault's distributed encryption does not use end-user passwords at all – the technology works over the existing Windows authorization and authentication infrastructure of the organization. This combined with very transparent way of protecting data, it is the easiest product to use for end-users. And, much like IronKey, it delivers off-line and off-site usage of the data with Airlock mechanism, however not sharing the same management capabilities of data.

Envault's biggest advantage could be the capability to use any normal memory sticks and external hard disks and other removable media without potentially expensive encryption chips. As Envault's Removable Media Protection is still a quite new product, it lacks fine-grained authorization methods that can be found in IronKey. Envault's encryption and data protection side on the other hand is very advanced. The management is somewhat easy, and even end users have their own optional management interface and the deployment is easy as long as the initial implementation is done through the AD.

Both Envault and IronKey could find the "logging only" feature handy as well, i.e. writing data without protection but logging the transfer - currently everything put to the removable media is encrypted. Envault's material however states that the file-based approach allows integration with data

labeling such as MS SharePoint, creating a policy-based model for file protection. A major upside of Envault against Microsoft Bitlocker is that protected data can be accessed with Mac and Linux based computers.

IronKey lacks the capabilities of **GFI or DeviceLock** on the port management side – users can still use any unprotected removable media. GFI and DeviceLock on the other hand do not provide media encryption. Envault combines data protection and port blocking features, but the port blocking is currently limited to USB and FireWire mass storages and CD/DVD media.

However, it truly looks like that GFI is missing the point while Windows Vista and now Windows 7 are both capable to manage the port side as well.

5.1.1. The near perfect match?

Based on analysis, it looks like there is a *near* perfect match in applications available while considering the IA objective. This is, however, when we combine the functionalities of 2 or 3 different applications.

Such combination delivers a strict, manageable and secure enough approach for an organization's removable mass storage protection. However, buying 3 distinct products can be costly. Our recommended applications are:

- **IronKey** HW based application and Enterprise server for device management, data protection and secure application delivery use with strong authentication and key generation when compliance requirements are high.
- **Envault** Removable Media Protection for securing the data in distributed manner, transparently to end-users, with Active Directory integration and usage logging. Most secure approach when combined with HW based application protection.
- Utilize **Windows built-in port** security and AD (GPO) management.

Information Assurance support

To combine the capabilities of each application introduced here you'll get the best of breed, but still no integration with the data itself, e.g. data labeling and tracking on life-cycle based is missing. Envault's stated support for data labeling and according protection policies in coming releases may well put Envault to a league of its own considering enterprise IA requirements.

6. Technologies

The following technical information is mostly based on the publicly available research papers, whitepapers and vendor information found on their respective web sites. The conclusions and details to support this research document is done by the research team, by testing the technologies as described in chapter 4.3.2

6.1. Kingston (DTV)

INTRODUCTION

[1] **Kingston DataTraveler** High Speed 2.0 USB Flash drive delivers a 256-bit hardware based AES encryption capabilities on DataTraveler Vault – Privacy Edition; which encrypts 100% of data. Use of an enforced complex password mechanism is available.

The other model – DataTraveler Vault (DTV) delivers same 256-bit hardware based AES encryption capabilities as Privacy Edition. It is waterproof and TAA compliant.

The main difference between the DTV edition and Privacy Edition is the 'Two Partitions' – model. The public and encrypted zones are separated and encrypted zone is accessible with *DTVaultLock security software for Windows*. The zone size is customizable.

The DTVaultLock delivers an UI to support the encryption and management of encrypted zone. It allows user to change the size of encrypted partition and set/change password. There is no user management or administrative/centralized management available for the DTVaultLock nor different privilege levels for the data. If user password is lost, the only way recover from situation is to format the privacy zone and re-setup it. The data recovery is not possible.

The DTVaultLock works only with Kingston brand memory stick/USB Flash drive.

Data encryption is not supported in Mac OS or with Linux (Mac OS status subject to change in later versions).

The DTV speeds up to 24MB/sec for reading and 10MB/sec for writing in encryption mode.

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Quick & dirty + Cheap 	<ul style="list-style-type: none"> - Un-secure & un-manageable in enterprise

6.2. IronKey (Enterprise)

INTRODUCTION

[3] **IronKey Enterprise** – is self-defending secure storage, as the web pages are telling you. The application is hardware based USB memory/token with capacities ranging from 1 GB to 8 GB. The approach is hardware-based. The read speed for encrypted content is 30 MB per second and write speed 20 MB per second. The token conforms to the military standard MIL-STD-810F waterproof and is able to work on 16G rms operating shock. The application include PKCS #11 digital certificate interface that can be used to integrate into enterprise authentication systems. The system allows two factor authentication with RSA SecurID or with certificates (PKCS #15, with #11 interface).

The application encrypts all the data on storage and there is no software or drivers to install. The storage is remotely manageable through the IronKey Enterprise server. The system was designed to separate the user and the system. The management application allows device-specific policies and enforcement on and off the enterprise network.

IronKey allows defining policies for management and permissions or revocation by administrative authorization. Application allows tracking the devices and remotely delete or deny the access to the data in case of compromise or theft.

The management application is delivered as a software appliance on an IronKey flash drive.

Data encryption is based on AES (CBC mode) encryption and key creation is done on hardware and is conforming to FIPS 140-2. PKI is 2048-bit RSA and hash algorithm 256-bit SHA. Encryption key's protection is done with 128-bit DRNG.

In addition, IronKey is providing a device security utility to lock down the USB ports on PC. The authentication can be as well two-factor or PKI based.

However, the IronKey Enterprise is not providing authorized 'whitelisting' of allowed tokens in organization's environment, or integration with the USB locking mechanism and USB encryption dongle.

Can be viewed as the ultimate point solution that does one thing well, or as the most secure USB drive ever made as the vendor says.

SUMMARY

Pros	Cons
+ Enterprise product.	- On USB-token only, based on vendor-specific hardware.
+ Integration capabilities and management model.	- Integration still limited and no Microsoft AD integration directly available.
+ System independence; separation of user and system.	- Users can still lose data with regular USB drives, CDs etc.
+ Secure application delivery.	- Expensive.
+ Secure platform, no software installation necessary.	

6.3. Checkpoint (Media Encryption)

INTRODUCTION

[4] **CheckPoint Media Encryption** “prevents unauthorized copying of sensitive data by combining port and device management, content filtering and centralized auditing with robust media encryption. Based on market-leading Pointsec technologies, CheckPoint Media Encryption plugs potential leak points and logs data movement to and from any plug and play devices, providing comprehensive control of security policies.”

The application is manageable with CheckPoint Secure Client utilities. Features include:

- “Deploys quickly, which meets compliance objectives and conserves resources.
- Controls input and output on all connection ports.
- Centrally manages devices individually by type, brand, or model.
- Provides complete audit of device usage.
- Integrates with Windows 2000/2003 Active Directory and Novell eDirectory.
- Application runs transparently to users. ”

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Integration with existing security infra (if Checkpoint) + Transparent + Microsoft AD integration 	<ul style="list-style-type: none"> - Problematic management. - Collaboration cases are difficult - Off-site logging. - May be difficult to justify extra costs versus added benefits over MS Bitlocker to go and Windows port control (Windows 7)

6.4. Utimaco/Sophos (SafeGuard Device Encryption)

INTRODUCTION

[5] "Prevent unauthorized access to mobile and stationary endpoint devices by encrypting fixed and external hard disks and removable media easily and transparently with SafeGuard Device Encryption. If a device falls into the wrong hands, the data is unreadable, even if the hard disk is removed."

"SafeGuard Device Encryption is the only solution in the world whose Smart Media Encryption allows sector- or file-based encryption of entire exchangeable data media in a single product. This unique ability allows a mix of unencrypted or encrypted data to be stored and managed on any media at the same time. Data exchange between employees and business partners has never been this easy or so secure."

- Offers transparent multi-platform hard disk encryption, laptop encryption, and file encryption for PDAs, smart phones, and removable media that does not impact productivity
- Easy to use with single-sign on and password recovery functionality
- Share data easily through automated personal keyring sets, enhancing productivity
- Monitor compliance with detailed logs and reports of client activities from a central console
- Powerful administration and deployment options offer flexibility to organizations with centrally managed and non-centrally managed users

"SafeGuard Device Encryption is a module of SafeGuard Enterprise, the comprehensive data security suite of Utimaco for managing information protection in mixed IT environments. It is centrally managed by SafeGuard Management Center module to deliver the highest levels of data security and performance available today."

SUMMARY

Pros	Cons
+ Transparent and support of multiple media platforms.	- Problematic management
+ Pre-filled regulation support	- Requires Safeguard DLP in junction to provide balance.
+ Full support for Vista BitLocker and AD	- Collaboration cases are difficult
	- May be difficult to justify extra costs versus added benefits over MS Bitlocker to go and Windows port control (Windows 7)

6.5. Envault (Removable Media Protection)

INTRODUCTION

Envault Removable Media Protection (previously Envault USB Storage Protection) protects the contents of your organization's all existing and future USB drives and other removable media against data leakage and theft. Plus it gives a full audit trail and remote suspend/kill capability over organization's data on any removable media in real time.

With the unique Envaulting technology, your organization gets to control the data availability dynamically – you decide who can access company data, and where and when. All data copied from a workstation to removable media/storage is automatically protected, without the need for any user action, passwords, or other user-based security decisions.

Deploying Envault is a breeze: Define your security policies through AD console, install a management server, and distribute the workstation driver as an MSI package to your workstations. End-users' removable media become protected through self-provisioning as they utilize them, so there is no need for any roll-out projects."

Envault's vaulted/distributed encryption model is a new approach to protecting enterprise data. It consists of a workstation driver software and a central management server, and utilizes the existing enterprise network infrastructure to provide single-sign-on authentication. The driver software integrates seamlessly with the operating system to provide transparent user experience. Envault uses AD for centralized policy management and provides a management interface for remote management and auditing of protected data/mass storages. The application can enforce protection or allow read-only access for unprotected media. Includes port control capability through AD template.

Data protection utilizes AES-256 (FIPS 140-2) and communication between central management and protection server is protected with PKI mechanism and SSLv3.

Envault was remarkably easy to deploy, but the actual utilization could be a bit faster when inserting and protecting a large hard disk that is full of data for the first time. However, previously empty or lightly filled media were ready to use in seconds. We believe that this is because the system protects data file-by-file, instead of encrypting the whole volume/container.

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Enterprise product. + Transparent user experience and tight OS integration. + AD Group Policy based management for user privileges and data availability. + Offline/off-site access and logging features. + Remote suspend/kill for all media. + Works with Mac OS and Linux. + Possibility for data labeling support / strong roadmap. 	<ul style="list-style-type: none"> - No integration with 3rd party authentication tools. - Distributed encryption technology requires occasional network connectivity. - New technology, maturity as small question mark.

6.6. Microsoft (BitLocker to go)

BitLocker to Go "extends BitLocker data protection to USB storage devices, enabling them to be restricted with a passphrase. In addition to having control over passphrase length and complexity, IT administrators can set a policy that requires users to apply BitLocker protection to removable drives before being able to write to them."

Microsoft brings BitLocker to go with Windows 7. It delivers basic encryption and password-protection for USB connected mass storages. Together with Windows 7's port control features it delivers some manageability for USB storages." BitLocker enables possibility to integrate 3rd party protection techniques with it.

Possibility to recover lost encryption keys from AD (however seems to be plainly sending the user's password to AD).

Specifications may be subject to change, please refer to Microsoft documentation.

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Quick and dirty + Comes with Windows 7 ultimate + Transparent operation 	<ul style="list-style-type: none"> - MS environment only, and protected writing not possible with legacy systems (Windows XP) - Only user-password authentication. - No real enterprise features such as auditing or remote management - missing IA features and has poor enterprise use case support

6.7. TrueCrypt

INTRODUCTION

TrueCrypt "is an Open Source, free cryptographic engine for various operating systems. The main features include:

- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encrypts a partition or drive where Windows is installed (pre-boot authentication).
- Encryption is automatic, real-time (on-the-fly) and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Provides plausible deniability, in case an adversary forces you to reveal the password: Hidden volume (steganography) and hidden operating system."

Encryption algorithms: AES-256, Serpent, and Twofish. Mode of operation: XTS.

SUMMARY

Pros	Cons
+ Free	- No central manageability
+ Quick to implement	- Lacking nearly all IA features
+ Unique features towards the plausible deniability	- Cryptographic verification un-sure per build.

6.8. PGP (Endpoint Device Control)

INTRODUCTION

PGP Endpoint Device Control “provides built-in security that detects, authorizes, and secures removable storage devices and media (such as USB drives, CDs, and DVDs).

- Easy, automatic operation—Permits safe and authorized removable storage use, without changing the user experience or reducing productivity.
- Enforced security policies—Enforces policies for device usage via USB, FireWire, Wi-Fi, and Bluetooth connections; automatically encrypts removable storage based on policy; can also log usage and demonstrate compliance to auditors.”

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Integrated approach. + Device protection. + Integrates to the existing security infra (if PGP present). 	<ul style="list-style-type: none"> - Device security product, encryption complicated due the nature of application. - Microsoft integration lacks important features. - Complicated management. - Off-line usage scenarios complicated. - Information Assurance forgotten? - No DLP features.

6.9. GFI (EndPointSecurity)

INTRODUCTION

GFI EndPointSecurity "controls Portable Device Access to your Network. Basically, it allows the control of Floppy disks, CD/DVDs, iPods, Storage devices, Printers, PDAs, Network adapters, Modems, Imaging devices etc."

"The GFI EndPointSecurity does not encrypt the data on removable media, it basically allows the efficient security management of the end-point technology."

"GFI EndPointSecurity integrates to Microsoft AD to request authorization information group based towards the policy set. The pros are definitely the tight integration with Active Directory capabilities, Group Policies etc., - cons are the requirement to be connected with AD directly or over the SSL-VPN, IPSec and with the management server when updates are needed. This creates potential problem for those whom travel a lot and are not frequently visiting the AD domain either locally or remotely."

However, it truly looks like that GFI is missing the point while Windows Vista and now Windows 7 are both capable to manage the port side as well – with the Domain architecture provided by Microsoft.

The GFI EndPointSecurity does not encrypt the data on removable media, it basically allows the efficient security management of the end-point technology.

Application allows prevention of data copying to the removable media or copying unwanted data to the corporate network.

The agent application that resides on target computer is tamperproof and retains to block mode if agent is attempted to tamper with malicious code or activity.

The application categorizes computer to the protection groups and allows individual setting of protection configuration.

The logging is based on SQL server and the application allows real-time status monitoring and alerting of pre-set actions. The ReportBack application is requires to gather detailed reporting of utilization and potential breach attempts. ReportBack is free (per 05/2009).

Other features include:

- Scan and detect a list of devices that have been used or are currently in use
- Set up custom popup messages for users when they are blocked from using a device
- Support for operating systems in any Unicode compliant language

SUMMARY

Pros	Cons
+ Large option base.	- Point-solution supplier.
+ Tight Microsoft integration.	- No encryption.
+ Extensive logging features.	- Microsoft integration too tight?
	- Transportability issue?

6.10. DeviceLock

INTRODUCTION

DeviceLock "provides access controlled management and utilization of computer interfaces. The main features includes:"

- "Access Control. Control which users or groups can access USB, FireWire, Infrared...ports. It's possible to set devices in read-only mode and control access to them depending on the time of day and day of the week."
- "Tamper Protection. Configurable DeviceLock Administrators feature prevents anyone from tampering with DeviceLock settings locally..."
- "Content-Aware Rules. Administrators can now selectively grant or deny access to certain true file types for removable media..."
- "USB White List. Allows you to authorize a specific model of device to access the USB port, while locking out all others..."
- "Media White List. Allows to authorize access to specific DVD/CD-ROM disks, uniquely identified by data signature..."
- "Temporary White List. Allows granting temporary access to a USB-connected device by the issuing of an access code, rather than through regular DeviceLock permission setting/editing procedures..."
- "Auditing. DeviceLock's auditing capability tracks user and file activity for specified device types and ports on a local computer..."
- "Mobile Device Data Leakage Prevention. With DeviceLock, you can set granular access control, auditing, and shadowing rules for mobile devices that use Windows Mobile or Palm OS ..."
- "Network-Awareness. Administrators can define different online vs. offline security policies for the same user account. A reasonable and often necessary setting on a mobile user's laptop, for example, is to disable WiFi when docked to the corporate network and enable it when undocked."
- "TrueCrypt & PGP® Whole Disk Encryption Integration. DeviceLock can detect encrypted PGP® and TrueCrypt disks (USB flash drives and other removable media) and apply special "encrypted" permissions to them..."
- "Lexar® SAFE PSD Integration. DeviceLock detects hardware-encrypted Lexar® SAFE PSD S1100 USB drives and applies special "encrypted" permissions to them."

SUMMARY

Pros	Cons
+ Large option and feature base.	- No encryption.
+ Tight Microsoft integration.	- Microsoft integration too tight?
+ Extensive logging features.	- LAN is must!
+ Data shadowing.	- Transportability issue?
+ Possibility to integrate with PGP, Lexar or TrueCrypt to provide encryption.	

6.11. McAfee

INTRODUCTION

McAfee has actually 2 different utilities to suggest for the requested functionality. Another one is the System Protection and the other is McAfee encrypted USB/EndPoint Encryption (former SafeBoot).

Features include:

- "Protect a broad range of data on all devices
Provide consistent protection for data on desktops, laptops, mobile devices, removable media and portable storage devices; secure a broad range of information including customer data, intellectual property, legal and financial records, and employee records.
- Seamlessly integrate with existing infrastructure
Integrate with other McAfee security products and synchronize with Active Directory, LDAP, PKI, and others; support all Windows operating systems and common languages.
- Track and manage encrypted USB storage devices company-wide using McAfee ePolicy Orchestrator® (McAfee ePO™) for automated security reporting, auditing, monitoring, and policy administration
- Ensure compliance with corporate security policies, data privacy legislation, and industry regulations through use of encrypted USB devices
Implement and enforce company-wide security polices that ensure data stored on devices is protected.
- Provide data mobility without compromising security policies
Use McAfee Encrypted USB storage devices to help avoid brand damage, customer distrust, noncompliance penalties, competitive disadvantage, and financial losses by securing data no matter where it travels.
- Control data access with strong, two-factor authentication
Use built-in user access control to restrict and authorize who can read data stored on McAfee Encrypted USB storage devices.
- Secure data with industry-leading encryption algorithms and certifications for strong protection
Protect data stored on McAfee Encrypted USB storage devices with automated, transparent AES-256 encryption and FIPS-140-2 certification"

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Broad range of supported functions. + Microsoft Integration (AD). + Hardware tokens reliability and integration. 	<ul style="list-style-type: none"> - Information Assurance complicated and management tied down to proprietary tools. - PKI support is "bogus". - Off-line logging virtually useless.

6.12. Symantec

INTRODUCTION

Symantec Endpoint Protection delivers the following features for the removable mass media protection:

- "Device Control Controls which peripherals can be connected to a machine and how the peripherals are used. It locks down an endpoints to prevent connections from thumb drives, CD burners, printers, and other USB devices.
- Prevents sensitive and confidential data from being extracted or stolen from endpoints (data leakage).
- Prevents endpoints from being infected by viruses spread from peripheral devices."

SUMMARY

Pros	Cons
<ul style="list-style-type: none"> + Integrated "suite" with Symantec AV/FW product. + One agent & console approach. + Application control mechanisms. 	<ul style="list-style-type: none"> - Endpoint security focused more to the malware protection than to information assurance. - Sensitive data leakage prevention (DLP) is "bogus", the information assurance rests on file specifications. - Slow.

7. APPENDICES

7.1. APPENDIX A - Buying a removable media & mass storage protection technology

IT can be difficult. Now it is said. There are a couple of things to consider among the well established IA requirements and management scenarios. We've collected some notes regarding obtaining such technology.

1. Enterprise Architecture ("readiness")

A big theme to look for, but highly important in scenarios regarding how Information Assurance is utilized by the organization; who are the actors inside the organization as well as outside the organization (Extended Enterprise), and what are the processes between the actors and the technology platforms utilized by the organization and the Extended Enterprise.

2. Requirement management

To what kind of organization and required technical state the protection technology is being considered? Now beware – this is a tricky thing, the most requirements will need iteration since you will have to make sacrifices due to technological limitations or not supporting point number three – use cases.

3. What use-cases need to be supported?

Various use-cases bring various obstacles that must be overcome. The obstacles vary between scenarios: Some use cases are online, some are offline/off-site, and the type of information being transferred can be different in each case, and may therefore require different kind of protection or access capabilities.

Some of the users may reside in "hostile" environments, such as agencies or schools, where data transferred from the media to the network can be malicious. This creates an additional element for the use-case support as well.

4. What are the environmental needs? Or infra?

Remember the IA-based perspectives of threats? Consider the actual threat model you have against the environment to which you are building the protection.

5. What kind of feedback or reporting capabilities are required?

Do you have solid security architecture in place (which supports the Enterprise Architecture)? How about legislation or compliance?

6. "Who do you work with"? – The Extended Enterprise itself

Do you have the thing that requires multiple people to transfer data outside the organization perimeter with a USB dongle? Any better ideas to combine Information Assurance principles and ease of use? Invent better ways to collaborate.

Other questions: Interoperability and integration with applications already in your environment, Suite approaches, licensing model/SaaS/Clouding etc.

Alternatively, you could wait a couple of years so that interoperability would be stronger than now. However, that might rule out the advantages of having the protection – **right?**