WHITEPAPER

PERIMETRIX SAFESPACE™

FULL-SPECTRUM CONFIDENTIALITY PROTECTION AND DATA INTEGRITY

KEEPING SECRETS SAFE

PERIMETRIX

1. INTRODUCTION

By implementing Perimetrix SafeSpace™ any organisation of any size can build a simple, reliable and convenient system of defence against internal violations.

Every organisation has to protect its corporate secrets: its confidential information, intellectual property, and personnel and client data. But this vital data has to be protected not only from without, but also from within.

Managers fully understand that a leak of corporate secrets reduces competitiveness, spoils relationships with customers, partners and investors and attracts the attention of state and regulatory watchdogs.

However, many companies and state organisations today do not use leakage-protection systems. The fault lies with the inefficiency of the solutions on the market which are either able to prevent only chance leaks, or are so complicated and bureaucratic that they bring work to a standstill.

In addition, the available products do not provide full-range solutions to the issue of leaks. Instead, they concentrate on one aspect, for example: blocking a workstation's ports or filtering outgoing traffic. Everything else is left to the company, such as dealing with the theft and loss of laptops and mobile devices containing confidential information, or preventing leaks via printers.

Companies are simply afraid to invest in leakage-prevention systems since they need a full solution. But what they are offered simply papers over the cracks. And let's not forget the price. These dubious technologies which are often obsolete in no time are big-ticket items.

Company managers clearly understand that the problems enumerated above result from the immaturity of leak-protection technology. Top managers are simply waiting for an effective, full-spectrum solution to come onto the horizon.

This paper looks at just such a product. Perimetrix SafeSpace™ is free of the limitations inherent in the standard technology to date. At the core of the product is the unique Secret Documents Lifecycle™ technology. Using this, developers have been able to transfer into electronic form all the principles of high-security document usage which have proved their effectiveness over decades of use in highly confidential organisations.

By implementing Perimetrix SafeSpace™ any organisation of any size can build a simple, reliable and convenient system of defence against internal violations of document procedures and solve the problem of protecting confidentiality and data integrity once and for all.

PERIMETRIX

2. OUTDATED APPROACHES TO DATA INTEGRITY

Gartner shows that the available products on the market do not provide dependable defence.

Why is it that the majority of solutions on offer to date have not hit home? Gartner – one of the world's top IT consulting companies – has an answer. In its latest research entitled Hype Cycle for Information Security, 2007 analysts clearly report that leak-prevention technology is yet to reach maturity. According to Gartner, this will occur in the next 2-5 years, and for now the implementation of the solutions on offer offers "limited" benefits to business.

Although leak-protection technology is usually regarded as an effective means of protecting intellectual property, Gartner shows that in practice, the technology is far more useful in identifying faulty business processes – and only finds the occasional leak. While the majority of incidents results from unintentional leaks, data modifications and file destruction, the technology available thus far has been able to offer little to guard against a motivated insider.

Gartner shows that the available products on the market do not provide dependable defence. In addition, their effectiveness reaches a mere 80%. And the less said about so-called full-spectrum solutions, the better.

PERIMETRIX

Leak occurs only when confidential information goes beyond the corporate perimeter.

2.1. REASONS FOR FAILURE

The key failing of the solutions which exist today is the very way they approach the task. Although developers are absolutely right to consider that a leak occurs only when confidential information goes beyond the corporate perimeter, they incorrectly consider their remit only the channels by which data can leave: email, Internet, mobile devices and printers.

As a result, many aspects of the problem remain unsolved. For example, there is nothing to prevent an employee from copying data onto his laptop and then pretending it was stolen. Moreover, leak protection on workstations usually works on the basis of permit-or-deny, and does not take into account the confidentiality level of the content which is being copied, for example, onto a USB device. Thus, an employee with the right clearance to secret data is removed from the area of control and, potentially, could misuse his clearance for nefarious purposes.

However, even these problems are insignificant when compared to the low effectiveness of the products on the market.

2.2. PAST IMMATURE TECHNOLOGIES

The low effectiveness of the technologies used is, then, explained primarily by their lack of maturity. Although methods of identifying confidential information have already passed through two levels of evolution, they either provide only 80% effectiveness, or are so unwieldy that they cause bottlenecks in business processes.

The first generation of technology came in the form of various forms of probabilistic analysis. This included linguistic and signature analysis (Digital Fingerprints). The 80% effectiveness which Gartner indicates in its research come the very best which the above methods can provide in terms of filtering outgoing traffic to distinguish a confidential document from a non-confidential one. Even considering key words found in context, and even using a content filtration database which takes client-specific terms into consideration, the effectiveness of probabilistic analysis is generally less than 80%.

We should understand that if instead of using linguistic analysis to identify confidential content digital markers or labels are used instead, it makes no real difference since digital labels are easily circumnavigated. There is nothing to stop an insider from using steganography or simply encoding a communication to stop it from being picked up (by using a different code, changing letters to numbers and other such standard tricks).

The second generation of technology saw deterministic methods using a special marker for all confidential documents. This allows 100% protection of secret files identified as such at the classification stage. However, there arises an entire range of issues, for example: what should be done with new documents users create once the system has been implemented? The problem is that the product is unable to deal with classifying data on an on-going basis.

Moreover, such solutions are usually complicated to implement, and at the business end, we find a system which is highly inflexible. Its usage leads to increasing organisational bureaucracy which creates conflict between the information security department and other departments.[1]

2.3. CONCLUSIONS

The technology which has been on the market up to now simply defeats any desire to invest properly in systems which protect corporate secrets. However, a new generation of leak-prevention systems which protects confidentiality and data integrity – Perimetrix SafeSpace™ – and applies the revolutionary concept found in Secret Documents Lifecycle™, overcomes all the limitations described above, protects investment, and creates a flexible and effective system of internal and informational security.

1 More information about the evolution of leak-protection technologies can be found in the Secret Documents Lifecycle™: The New Generation of Corporate Secrets Protection Technology

PERIMETRIX

3. INTRODUCING PERIMETRIX SAFESPACE™

Perimetrix approached the whole issue of protecting data in the way trusted for decades by high-security organisations tasked with protecting state secrets.

Instead of concentrating on leakage channels and falling into the trap of the previous generations, Perimetrix approached the whole issue of protecting data in the way trusted for decades by high-security organisations tasked with protecting state secrets. Out of this came a new generation of technologies which protects secret documents at all points in the lifecycle – Secret Documents Lifecycle™ (hereafter: SDL).

3.1. SECRET DOCUMENTS LIFECYCLE™

The central concept behind SDL is the creation of a safe space in which users can work with secret documents under the control of a protection system. In every secure organisation there is a secret compartment or department where employees go to get access to secret documents.

To begin, he signs into a registry where he states who he is and what he wants with the document he is signing out. Then another employee – the secret-document archive keeper and, as it were, librarian – finds the necessary document using the inventory number and hands it over.

Having received the document, the employee may not leave. He may only work with secret papers only within a designated area. That is, the employee has to use a reading room attached to the secret-documents section where he may sit and read the document.

During this process, all work with the document is fully controlled. He may not modify the document (that is, change the content in any way, destroy it or copy it). Of course, if the employee has the required clearance, he may do so, but in that case a record of what he has done remains in a separate journal stating what changes were made, when, and by whom in the said document. This means that in the event of an investigation, it is possible to identify anyone who has broken policy rules.

When using such an approach with a document, both reliable auditing of secret document integrity and the protection of its confidentiality against the most extreme eventualities due to unsanctioned access are assured. For example, let's say an employee is unable to leave a designated area with a secret document and then lose it or have it stolen. In this case, the space in which the document is used and stored is under total control and full safety may be assured.

PERIMETRIX

Of course, this method of working with documents is associated with increasing formal procedures and bureaucracy. However, all these failings are removed by the transposition all operations and events journals into the electronic realm. Here, the protection system itself will automatically maintain an account file and keep tabs on all changes to documents as well as keep a copy of different versions in the archive.

However, SDL technology is able to control not only the use of secret documents. It covers all other stages in the document lifecycle: the creation, storage, archiving, and deletion of documents, as well as less common actions such as reducing the confidentiality level of a document and moving it to another storage facility.

Thus, SDL technology creates a secure space in which documents are stored, used, moved and, ultimately, live and die. This is a key part of the Perimetrix SafeSpace™ full-spectrum solution.

3.2. PERIMETRIX SAFESPACE™

Perimetrix SafeSpace™ comprises three key components, each of which can be implemented as a standalone product (see Fig. 1):

- **Perimetrix SafeStore™** is a system of initial document classification which incorporates multiple levels of confidentiality and then stores secret documents in SafeHouse™, a distributed storage facility. This product ensures the safety of confidential data at rest.
- **Perimetrix SafeUse™** is a system of control over the use of classified secret documents by authorised employees. This product ensures the protection of information in use, the automatic classification of new documents, the integrity audit of secret documents and retrospective analysis via ShadowCore™, the central archive.
- **Perimetrix SafeEdge™** is a real-time monitoring system for all documents leaving the network (SMTP, HTTP, printer, IM, FTP, P2P) which automatically classifies incoming documents. This product ensures the protection of data in motion.

Although any one of the three Perimetrix products can be implemented as a standalone solution, the synergistic advantages of using all three products together are compelling: an organisation can create a reliable leak-prevention system which covers data issues in all three states: data at rest, data in use, and data in motion – as well as provide integrity audit.

3.3. PERIMETRIX SAFESTORE™

Of course, when creating a protection system for confidentiality and data integrity, a huge volume of documents already exists in an organisation. So, the first stage in implementing the system is to classify and categorise of all that information. This process is significantly simpler than with the products of previous generations since Perimetrix Ready-Compliance™ integrated technology allows even large amounts of data to be categorised in a matter of hours.

Once it has been established how confidential a particular document is, Perimetrix SafeStore™ apportions it a level of secrecy and level of access. The label itself is incorporated into the document in such a way as to be invisible to users and not open to modification or deletion.

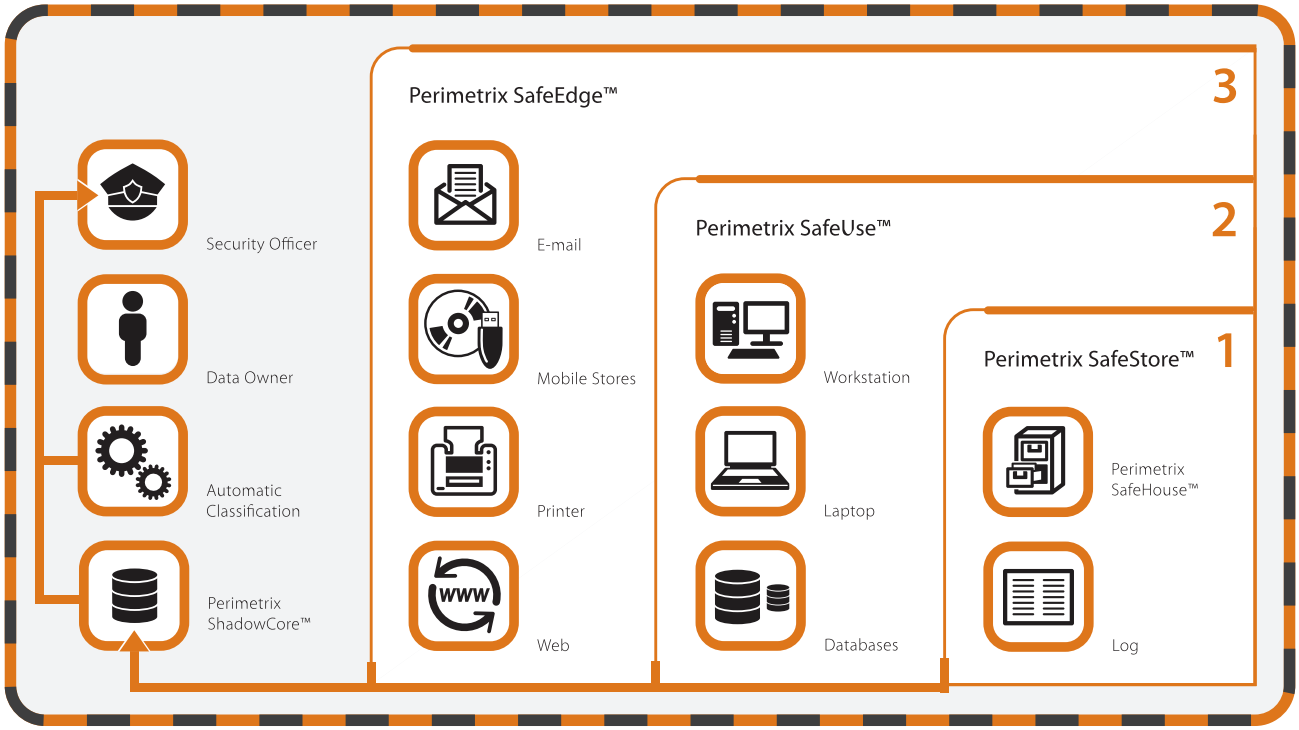

Fig. 1. Outline of Perimetrix SafeSpace™

PERIMETRIX

This label contains information on the owner and the class of the document. Thanks to multiple levels of confidentiality, the class itself can have multiple aspects. For example, a class can include:

- The nature (category) of information held in the document (financial and personal data, intellectual property, etc.)
- Relation to a particular department (finance, marketing, production, etc.)
- Level of confidentiality (for in-house use, secret, top secret, etc.)

When Perimetrix SafeStore™ has labelled all classified documents they are send to a special storage facility: Perimetrix SafeHouse™ where they are held in encrypted form.

This storage can be implemented either as a centralised or distributed system. In the latter case, documents physically remain on users' workstations, but in encrypted form and with embedded labels. The result: a protected storage facility which reliably safeguards the confidentiality and integrity of secret documents even in the event of the loss or theft of hardware – including laptops – or any other form of attack.

It makes no difference to the protected storage facility what form data is stored in: text documents, tables, pictures, multimedia or even database content. In the case of database content, the database itself does not reside in the storage facility – but users work only with the secure storage via which all data passes before reaching the user.

Perimetrix SafeStore™ also provides protection for secret documents on laptops and mobile devices. If an employee's mobile device is lost, confidential documents will be still be encrypted and absolutely unusable to anyone else.

3.4. PERIMETRIX SAFEUSE™

When all relevant documents are in Perimetrix SafeHouse™, the working process may begin. Users work with documents which are already classified, of course, but they may also need to create new documents. All related operations are controlled by Perimetrix SafeUse™.

Work with classified, labelled documents is controlled by the policies the company has opted for. This means that employees are not able to perform operations with classes of information they do not have sufficient security clearance for. For example, the policy may forbid any employee from copying of even a part of a top-secret document with the exception of a small group of users. In this case, employees without the right clearance cannot print, copy to USB storage devices, or send top-secret documents by email or Internet. They also cannot even buffer any of the text of such documents. But if a forbidden action is attempted, the Security Officer will receive the appropriate notification.

As mentioned, while working, employees not only use classified documents but also create new ones. In this case, if an employee uses an existing document to create a new one, then the confidentiality labels from the original document automatically transfers to the new document. Thus, all new documents are classified automatically (with the exception of those created from scratch, without the use of existing documents or templates).

In this way, Perimetrix SafeUse™ does not guess whether a document is secret or not and whether it can be released from the corporate network. The product always knows exactly what class of confidentiality a document relates to ahead of time and, therefore, maintains 100% effectiveness and reliability.

Of course, Perimetrix SafeUse™ is equally effective on mobile computers used outside the corporate network. As noted above, Perimetrix SafeStore™ protects secret documents from unauthorised access in the event of theft or loss of a mobile device. However, Perimetrix SafeUse™ substantially increases this level of protection, providing control over user actions by means of several policies of working with classified documents outside the office.

Below is a example of the sort of policies which the system can opt for:

- **Restricted use.** In this case, the employee on a business trip can get access to documents by using a personal key; for example, by using strong authentication or a password. At this level of access, there is no control over how the employee uses the document.
- **Secret.** This access level uses authentication and further control over secret documents which is just the same as control insider the network. At the same time, document actions are logged for audit and integrity control. Once the mobile computer is plugged back into the corporate network, all events journals and audit databases are transferred to the central archive.[1]
- **Top secret.** Here, to gain access to a document, one has to go through both the authentification process and as well as set up a VPN connection with the corporate network. Only then is it possible to work with a top secret document. Naturally, all actions are controlled and recorded for later auditing purposes. Moreover, notification of any violations are provided in real time so, should it become necessary, the security officer can deprive the remote employee of access to top secret documents.

We have already mentioned the Perimetrix ShadowCore™ central archive, a key component of Perimetrix SafeUse™, which effectively solves the issue of auditing the integrity of secret documents.

All events (who did what and when to which document) are stored in the Perimetrix ShadowCore™ central database along with shadow copies of the documents themselves (both those circulating within the network as well as those which go outside it). This way, a powerful foundation is created for integrity audit, retrospective analysis and incident investigation.

By using this database, security officers can collect and analyse statistics, and construct graphs and reports. Using this information, one can ascertain how effectively the organisation's information resources are being used, and balance and optimise data streams and internal communications processes.

1 See Audit at all points in the lifecycle for more details

Importantly, Perimetrix SafeUse™ contains an inbuilt single system of user identification. This means that by using the central database, it is always possible to identify which employee performed any action. Also, it means it is now possible to get beyond the key limitation of piecemeal leak-protection systems which consist of several non-integrated components. Such systems trace Internet channel actions by identifying users only by faceless IP-addresses (which may be dynamic), email channels – by email address (which is easily falsified) – and external-device channels by users' account names. Such a piecemeal approach is inefficient and creates data which it is hard or impossible to merge and use across the datasphere to track perpetrators of violations.

By analysing the central database and investigating an event, it is possible to identify what chain of events preceded an attempted leak or other violation. By accumulating such information, it is possible to handle internal threats proactively, heading off potential attempts by employees to leak data before they happen.

The audit of secret documents integrity it is a key requirement for a whole range of industry legislation, standards and directives. In particularly, SOX pays special attention to the integrity of financial documents – which has become the defacto standard in the sphere of corporate management. In addition, an audit of secret documents integrity is the cornerstone of any standard relating to information security or risk management, etc.

An audit of integrity requires that each sensitive document be protected from modification (up to and including document destruction). To this end, means of internal control are created which, in general terms, cannot stop the modification of important documents by those employees who have the right clearance levels. However, the means of internal control result in always being able to identify who made what changes to a document as well as restore important files to their original state (including after destruction).

Perimetrix SafeUse™ and ShadowCore™ fully address the issue of audit of integrity and protection from the distortion or destruction of documents. The central archive contains all the necessary data for an audit: various document versions as well as records of who changed what, when and how. If necessary, it is easy to bring up the history of any document and trace its entire lifecycle to find the moment when an offender distorted the record, and find out when and how he did it and then roll back the changes by simply restoring the document to an earlier version.

Underpinning Perimetrix SafeEdge™ are three probabilistic protection methods: Digital Fingerprints, linguistic, and signature analysis.

3.5. PERIMETRIX SAFEEDGE™

Perimetrix SafeUse™ provides 100% protection for classified documents. However, if a user creates a new document without using an existing document or a template, such a new document will not be classified automatically.

Research conducted by Perimetrix shows that workers very rarely create documents from scratch using their own content. As a rule, such documents only occasionally exceed 0.5% of all documents created. So, only a very small percentage of the new documents created in a company cannot be accommodated by automatic classification. Nevertheless, they need to be protected, and this is the main role of Perimetrix SafeEdge™.

Underpinning Perimetrix SafeEdge™ are three probabilistic protection methods: Digital Fingerprints, linguistic, and signature analysis. We earlier cited the effectiveness of such methods as 80%. Here, however, total percentage of unclassified files these methods are being called upon to protect is around only 0.5% of the total.

Thus, according to the theory of probability, the proportion of false positives or missed secret documents is around 0.005 x 0.8 = 0.004. In other words, total technology effectiveness is 99.6% – more than sufficient for risk assessment and threat analysis. And at such levels, the question of false positives does not even enter the frame.

At the same time, protection of unclassified documents is provided even if they leave the network not via a network gateway (such as email, Internet, printer, etc.) but via a workstation port; for example, when files are copied to a USB device. Here, the file is still sent to the filtration server for real-time classification. This creates no noticeable burden on the workstation or company network since the number of such files is extremely small.

Of course, unclassified documents can be stored and mount up on users' workstations if users do not attempt to send them beyond the network, which would result in their automatic classification. However, Perimetrix SafeStore™ can be set up to conduct a regular document inventory of such documents at times when the network is less heavily used, such as at night or at weekends when all new documents are automatically classified as such and place in the SafeHouse™ storage facility.

In closing, Perimetrix SafeEdge™ provides protection for data in motion. If a secret document leaves the corporate network and is sent, for example, to a partner, then encryption will be applied automatically in accordance with the policy, completely transparently.

3.6. PUBLICATION OF SECRET DOCUMENTS

When either using standalone products or the full-spectrum solution Perimetrix SafeSpace™ a company may need to transfer a secret document to a non-secure environment. To facilitate this, there is a procedure of lowering the confidentiality level of a document.

Of course, when copying data from a secret document, an employee could create a public file intended for further use, or to be sent outside the company. In such a case, the employee could initiate a procedure of lowering the secrecy level. This requires the participation of another one or even two colleagues, depending on the security police in operation. For example, a security office, line manager or person with unrestricted access.

For users who regularly create public documents there are templates which allow the immediate creation of non-secure documents. However, during this process, the user is prevented from working with confidential information in other documents – which is a logical consequence.

The high output of Perimetrix SafeSpace™ is provided by a unique load-balancing system.

3.7. PRODUCTION CAPACITY AND SCALABILITY

Perimetrix SafeSpace™ is created to protect secret documents in large organisations – where there are upwards of 500 workstations. The main requirement of such clients are high output and ease of scalability.

The high output of Perimetrix SafeSpace™ is provided by a unique load-balancing system which finds the quickest way to process each request and adjust the load in the event any imbalance in the process.

High scalability results from the cluster structure of the solution which allows new elements to be added easily. Practically all Perimetrix SafeSpace™ elements are capable of being clustered. Therefore, any bottleneck is simple to turn into a cluster. And by adding a new node, the cluster solves the output issue.

Perimetrix SafeSpace™ components are completely platform-independent and can work on Windows, Linux or Unix.

3.8. CONCLUSIONS

Unlike standard and out-of-date approaches which use deterministic and probabilistic methods, SDL technology provides an extremely high level of security (over 99%) and protects data at rest, data in use and data in motion.

The key advantage of the SDL concept is the fact that this approach solves the issue fully and right across the board. Even if an employee loses a laptop with secret documents or tries to copy confidential information to a USB drive, no leak will occur. By implementing the SDL concept, an organisation is free of the issue of leaks once and for all.

4. ABOUT PERIMETRIX

Perimetrix develops third-generation corporate secret defense systems. Thanks to the Secret Documents Lifecycle™ revolutionary concept, our solutions deliver 100% secret document protection – guaranteed; plus: complete control over communications channels and full audit of electronic operations.

Unlike the competition, Perimetrix concentrates all its technological prowess, innovative approach and unique experience on solving a vital task for clients: the safe storage of corporate secrets to raise competitiveness, promotion of good relations with investors and compliance with government requirements.

Perimetrix was founded in October 2007, by an innovative group of security professionals at the cutting edge of modern internal IT-threat defense systems. Perimetrix is a member of the CompuLink group of companies – the leading alliance on the Russian IT market. The CompuLink's robust financial position, unique experience and expertise, and impressive client base provide Perimetrix with a solid foundation for development. Thanks to this powerful support, Perimetrix is able to provide wide-ranging internal-threat IT projects, come out as the Russian market's leader and create a convincing basis for international expansion.

PERIMETRIX

Perimetrix Headquarters

45 Michurinskiy av.
Moscow, 119607
Russian Federation

Phone: +7 495 737 99 91
Fax: +7 495 737 99 92

info@perimetrix.com
www.perimetrix.com

KEEPING SECRETS SAFE

PERIMETRIX