



SECRET DOCUMENTS LIFECYCLE™

THE NEW GENERATION OF
CORPORATE SECRETS PROTECTION
TECHNOLOGY

KEEPING SECRETS SAFE





1. INTRODUCTION

2. THE EVOLUTION OF APPROACHES IN LEAK PROTECTION

- 2.1. 1ST GENERATION: PROBABILISTIC FILTRATION METHODS
- 2.2. 2ND GENERATION: DETERMINISTIC PROTECTION METHODS
- 2.3. CONCLUSIONS

3. THE SECRET DOCUMENTS LIFECYCLE™ CONCEPT

- 3.1. THE SECRET DOCUMENTS LIFECYCLE CONCEPT
- 3.2. PROTECTION AT ALL POINTS IN THE LIFECYCLE
- 3.3. SECRETS PROTECTION OUT OF THE OFFICE
- 3.4. AUDIT AT ALL POINTS IN THE LIFECYCLE
- 3.5. AUDIT OF SECRET DOCUMENTS INTEGRITY
- 3.6. CONCLUSIONS

4. ABOUT PERIMETRIX



PERIMETRIX

1. INTRODUCTION

According to the Ponemon Institute an average leak costs around 4.7 million USD.

Corporate secrets make up the information a company has which have to be kept confidential. For example: personal data on employees and clients, confidential details on partners, a company's intellectual property, business plans and strategies – all of this is very valuable to a company and must not leak out. If such corporate secrets fall into the hands of competitors, criminals, journalists or leak into the public domain, considerable consequences for investors, management, employees and/or company partners naturally follow.

Such leaks happen all the time and many world famous companies have hit the headlines, including prestigious consulting firms, large industrial producers, and trusted banks. Such occurrences lead to tarnished image, reduced competitiveness and investment attractiveness, as well as unwanted government and regulation watchdog attention arising from failure to comply with legal requirements.

According to Gartner, leaks cost companies far more than implementing prevention solutions.¹ Savings on average are in the order of 500%. Meanwhile, according to the Ponemon Institute an average leak costs around 4.7 million USD.²

There is a whole array of technology on offer which in one way or another protects against leaks and helps secure corporate secrets. This paper will look at and analyse the approaches used today – both their strong and weak points – before turning to the Secret Document Lifecycle™ (hereafter, SDL) – the new generation corporate secrets protection technology developed by Perimetrix.

1 Source: Avivah Litan, vice president and distinguished analyst at Gartner

2 Source: 2006 Ponemon Data Breach Study

2. THE EVOLUTION OF APPROACHES IN LEAK PROTECTION

To date, technologies which identify corporate secrets within the stream of data traffic have gone through two stages of evolution.

Conceptually, a leak occurs at the moment when corporate secrets breach the company's information perimeter. For example: an employee prints off a confidential financial account and takes it out of the office in his case. Of course, instead of the printer, the insider could have used any one of a number of channels to leak the document. This is why developers began with the creation of defence systems which focused on controlling the channels by which information leaves a corporate perimeter.

These channels can be divided into roughly four main groups:

- E-mail
- Internet
- Print devices
- Portable and mobile devices

The idea behind the majority of corporate secrets protection technology is predicated on checking outgoing documents as they exit the company perimeter by means of one of the four channel categories above.

This is why the task for developers became learning how to distinguish secret from non-secret documents and, moreover, to do this automatically with minimum human involvement.

To date, technologies which identify corporate secrets within the stream of data traffic have gone through two stages of evolution. In the first, developers of leak prevention systems concentrated on probabilistic methods which use linguistic analysis or Digital Fingerprints. In the second, providers developed deterministic methods based on branding confidential documents with a unique security label.

We will look at each approach in more detail. However, we may say now that the effectiveness of both probabilistic and deterministic approaches leaves much to be desired. According to Gartner¹, these are highly unreliable technologies which an employee who intentionally wishes to remove confidential information can easily get round, with an effectiveness rate of only 80%. In other words, these approaches are effective only chance leaks arising from mistaken actions, and even then not with complete reliability.

¹ Source: Hype Cycle for Information Security, 2007

Filtration effectiveness using linguistic technologies is only 80%.

2.1. 1ST GENERATION: PROBABILISTIC FILTRATION METHODS

Probabilistic methods of filtering outgoing traffic are the use of linguistic technology or Digital Fingerprints taken from secret documents.

Linguistic analysis methods search outgoing documents for previously determined key phrases and then analyse their context. To do this, the filter learns which documents need to be stopped on the basis of documents already flagged as confidential.

The implementation of a system based on linguistic analysis requires the creation of a content filtration database into which are placed confidential information signature documents of the specific client company. Each signature represents a template or digital fingerprint of a secret document on the basis of its key words and context.

The analysis of outgoing traffic uses this database: the engine scans each document, finds its key words and then analyses the text using the linguistic signature database of digital fingerprints.

The analysis results in a particular rating, for example, from 1 to 10. The higher the rating, the higher the probability that the linguistic filter has engaged a document which is of a confidential nature. This characteristic is why first-generation leak prevention technologies were called probabilistic.

If we turn to table 1, we see that this approach has three main failings. In the first place, this technology provides only a low level of effectiveness. Even with the creation of a content filtration database, filtration effectiveness using linguistic technologies is only 80%. This means that 20% of corporate secrets can make their way out of the company network. Plus, real cases show that the leakage of only 20% of a company's corporate secrets in 60% of cases results in bankruptcy. And one should not forget that one can get round even the most advanced linguistic analysis using simple steganography and communications encryption.

It is worth noting that given intense traffic such a high instance of false positives (20%) would make the lives of information security professionals pure hell. For example, if 100,000 emails go through the email gateway daily, that means security officers will have to process 20,000 communications per day by hand. But this volume of email traffic is modest when compared with the millions of emails some corporations deal with daily.

We should emphasise the fact that effectiveness of 80% is achieved only with the creation of a special content filter based on the characteristics of a concrete company – and to create such a filter requires the classification of all a company's information. Leak-prevention system providers often omit this necessary work, delivering the client nothing more than a standard or default content database. In this case, the product is easily implemented – literally, in a few days – but is plagued by poor effectiveness which falls to around 60%.

Table 1. The main failings of linguistic filtration

| Issue | Description |
|--|---|
| Low effectiveness even in best-case scenario | The best-case scenario is when a content-filtration database is created prior to implementation and is based on the specifics of a particular company. However, even in this case the effectiveness of filtration reaches only 80% which means that 20% of corporate secrets can leave the network without hinderance, added to which 20% false positives can make the lives of security officers extremely difficult. |
| Absence of leak prevention at the level of the workstation | Linguistic filtration is easy to implement for checking network traffic at the gateway level. However, leaks can and do happen via workstations: ports, external devices, mobile devices, wireless networks, etc. However, to achieve real-time analysis of data copied, for example, via a USB port via a separate content-filtration server is technically very difficult. This is why developers prefer not to protect workstations directly, but recommended implementing either administrative or technical protocols to close all open ports. |
| An insider can easily trick the system | The concept of controlling only the four types of communications channel has serious drawbacks. For example, there is nothing to prevent an employee from losing a laptop with corporate secrets – as we see happen repeatedly. Thus, protection systems which are based on linguistic technologies solve only part of the problem and leave clients with their requirement for total leak protection unmet. |

Another problem connected with linguistic filtration is that it is hard to apply it to non-network traffic. It is one thing to analyse email traffic but quite another to analyse files which are copied to external devices.

Attempts to create leak-prevention systems which can conduct linguistic analysis of files copied onto removable devices have not been successful. To do this, all outgoing files have to be routed to a separate server and then control achieved at workstation level with regard to the verdict which the system returns.

It is hard to regard such an approach as integrated as it results in increased loads on the workstation and the network and delivers only low effectiveness. This is why developers who use linguistic analysis either often do not offer protection from leaks at the level of the workstation, or recommend the closing of all open ports by administrative or technical means.

The last main failing of this technology is that an insider can always find a myriad of ways around it, for example: the time-honoured method of leaking via a laptop.

An employee can lose his mobile computer or a thief can steal a laptop he knows to contain secret information. Neither scenario fits with the common concept of four leakage channels which means that providers of a protection system based on linguistic filtration in reality deliver only part of a solution since they do not meet the client's need for total protection from leaks.

2.2. 2ND GENERATION: DETERMINISTIC PROTECTION METHODS

Deterministic technologies require that all confidential files be specially labelled as such. In some products, this means that the label is inserted into the file name. In this case, every file begins, for example, with its confidentiality class or level of secrecy, which leads to the creation of corporate policies on file-naming conventions. Naturally, this is not convenient in practice and far from transparent, creating obstacles to easy workflows for employees.

At the same time, there are more elegant methods of working with documents which do not require the primitive insertion of a special label in the file name. For example, a label can be inserted straight into the file itself, into one of its working titles.

In this case, when a document leaves the corporate network via network channels such as electronic mail, the filter does not have to analyse content. Instead, all it has to do is read the label and apply the appropriate security policy. In other words, by knowing the label, the system can reliably ascertain whether a file is secret or non-secret. From this the second generation of leak-protection systems gets its name: deterministic.

To implement such a system requires the complete classification of all electronic documents in a company and the labelling of all secret files. In this case, the effectiveness of protection of labelled files is 100%.

However, there is a whole range of other problems. In particular, it is not clear what should be done with new documents (of which many are created daily in any organisation). For example, there is nothing to stop an insider from copying a part of a secret document to the clipboard then creating a new file, pasting the text into it and then stealing the new file.

Table 2. The main failings of deterministic methods

| Issue | Description |
|---|---|
| Lack of flexibility | Lack of flexibility is ingrained in the very name and concept behind this technology. The system takes only those decisions which have been foreseen and defined previously. As a result, access to documents on the corporate network is palpably reduced and output is adversely affected, bureaucracy increases and tension appears between business and security interests. |
| Impossibility of providing full-spectrum protection | As usual, there is nothing to prevent an employee from losing a laptop with corporate secrets. Although a security-system agent can enforce the security policy outside the office, it cannot prevent the physical loss of a mobile computer and subsequent unsanctioned access. Thus, deterministic methods do not solve the problem fully, rather they address only a minor part of it. |

All of this leads to a system of protection which works on the level of workstations where clipboard functionality is simply disallowed if the document is marked secret (see Table 2). In addition, the technology has real problems with flexibility which lead to the lowering of document accessibility almost by chain reaction, the reduction of production output and more bureaucracy. If it is possible to regulate the operations of 50-100 employees, then in a large company with a distributed network of branches or even simply 500 or more employees, then the absence of flexibility outweighs the benefits the prevention of leakage delivers.

Moreover, the implementation of such a solution can aggravate internal conflicts within a corporation when the concerns of business diverge from the concerns of security. As a result, the interests of managers can conflict with those of security officers, all of which runs counter to the interests of the company as a whole.

In addition, deterministic methods of leak prevention are just as defenseless against the theft of mobile devices, external devices and laptops. Even if an employee has installed a defence system agent on his laptop, this does nothing to prevent the physical loss or theft of the computer. In other words, this technology addresses only a part of the total problem leaving the rest to the discretion of the company itself.

We may conclude that the use of deterministic systems is an outdated form of linguistic filtration.

The answer to the requirement of complete security for corporate secrets is the development of a new, third-generation technology: Secret Documents Lifecycle™, developed by Perimetrix.

2.3. CONCLUSIONS

Both generations of leak-prevention technology are now out of date. They do not achieve an acceptable level of effectiveness, transparency and accessibility. In addition, neither approach provides a full-spectrum solution. And the requirement of any organisation is the protection of its corporate secrets from leaks no matter where or how they might occur. Thus, investment in these approaches at best results in a partial solution, and that with serious limitations.

The answer to the requirement of complete security for corporate secrets is the development of a new, third-generation technology: Secret Documents Lifecycle™, developed by Perimetrix. Its main advantages are: 100% effectiveness in protecting classified confidential information, a high degree of transparency and accessibility, and a full one-stop solution.



PERIMETRIX

3. THE SECRET DOCUMENTS LIFECYCLE™ CONCEPT

Five base processes of information security: classification, control, monitoring, notification, and audit.

Secret Documents Lifestyle™ (SDL) protects the integrity of confidential data from beginning to end – that is, from the moment a document is created to the moment it is officially deleted. At the core of the concept are the five base processes of information security: classification, control, monitoring, notification, and audit.

1. Classification. The first stage in building a system of leak protection requires the classification and categorisation of information. That is, one has to identify what exactly needs to be protected. Appropriate security access levels are immediately ascribed to existing classified documents and for newly created and incoming documents a document-handling procedure is setup and fine-tuned.

2. Control. The second step entails the protection of secret documents in storage and the allocation of access rights to information on the basis of classes and the access levels defined in the first step. The result is a multi-tiered model of confidential information protection. Moreover, the protection of data in storage includes the use of encryption. This means that corporate secrets are protected against unauthorised access and leaks even in the event of theft or loss of a computer or external device. In addition, at this point the necessary documentation in keeping with the user-access policy with regard to classified data is still maintained.

3. Monitoring. The third step entails the protection of secret documents in use by employees on their computers. At this point, action monitoring of secret document occurs using a combination of both probabilistic and deterministic methods. While this is being done, the protection system always knows who did what and when with this or that confidential file.

4. Notification. The fourth step is the prevention of violations in real time and the notification of the security officer of all incidents, allowing the security service to react quickly in the event of a leak.

5. Audit. The fifth and final step in the creation of a defence system is the archiving of all data circulating on the corporate network and beyond as well as recording the actions users make with that data. Thanks to this archive, organisations can easily perform an audit, conduct a retrospective analysis or investigate an incident. Moreover, such an archive complies with the legislative requirements such as SOX (Sarbanes-Oxley Act) and the Basel II accords.

To understand more fully what SDL technology is it is worth looking at the lifecycle of a typical confidential document.



3.1. THE SECRET DOCUMENTS LIFECYCLE™ CONCEPT

Perimetrix has taken a fresh approach in designing SDL, but not tried to re-invent the wheel. Instead, our developers looked at how secret documents were treated in high-security before the electronic age (Fig. 1).

Document creation. The secret document lifecycle begins with the creation of a new document. An employee who wants to create such a document submits a request in an accepted format and the process of the acceptance and confirmation of this request then begins. The outcome of this procedure is the creation of a blank document which has been accorded a level of secrecy and inventory number. In other words, even before any information appears within a document it is given a secrecy level (which regulates access rights to the document) and an inventory number (indicating the physical whereabouts of the document). It is only then that content is added and it is passed into the workflow or into storage.

Document usage. The place where a document is used as well as the way in which it is used are strictly controlled. In every high-security company there is a secret section (a special department) to which a person turns who wants access to a secret document. To start with, 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 – seeks out the necessary document using the inventory number and hands it over. Of course, types of document access can be many and varied. There will be types of policy: access for normal operations, one-off access, access depending on the document security level, temporary access, etc.

Having received the document, the employee goes nowhere. He may work with secret papers only within a designated area. That is, the employee is 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 he has received (that is, change the content in any way, destroy it or copy it). Of course, if the employee has the required clearance, he may modify the document, 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 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 of 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 such a case, the space in which the document is used and stored is under full control and full safety is assured.

Document destruction. At the end of its lifecycle, any secret document will have to be destroyed, archived or stored elsewhere. Here – just as with the creation of a document – it is necessary to submit a request to destroy, archive or pass on the document elsewhere (i.e. to an agency outside of the company). In the last scenario, not only is the document passed on, but also responsibility for its integrity and confidentiality. Only once a request has been confirmed does the process of document destruction or its secure passage to another storage facility begin. Or a document is archived. We should keep standard document-processing procedure in mind: all actions must be reflected in the appropriate journal, for example: according to the assigned procedure, who destroyed which document and when. Thus, it is always possible to audit past actions, to track the document's history and identify any wrongdoers.

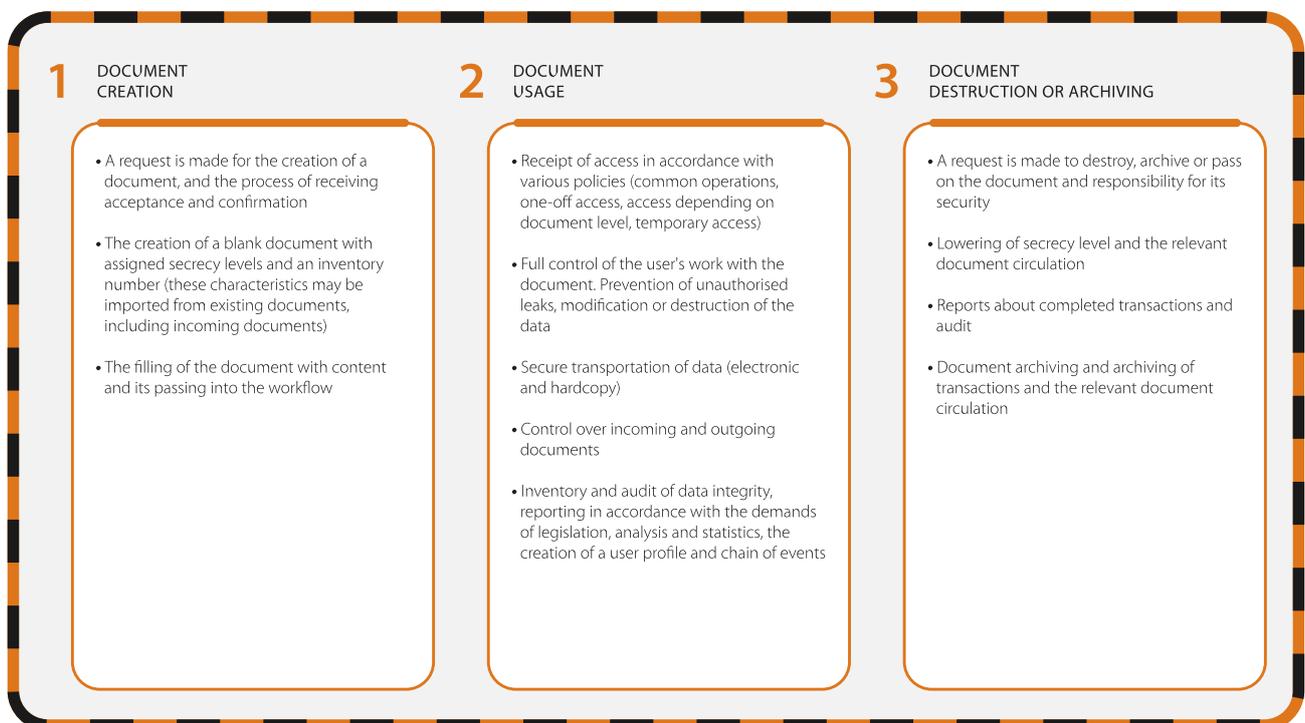


Fig. 1. The lifecycle of a secret document



We should note that the lifecycle can end with the lowering or raising of the secrecy level. In this case, a new document is created with a lower or higher set of rules governing access and usage.

The secret-documents lifecycle we have looked at in high-security organisations is connected with a large number of internal procedures and a lot of bureaucracy. This leads to a slowing of the whole process to the point where ideas about accessibility and transparency become redundant. At the same time, the transfer of the formal work cycle with secret documents described to the electronic sphere allows us to eradicate all the downside. For example, all events journals are filled in automatically and requests are delivered instantaneously.

3.2. PROTECTION AT ALL POINTS IN THE LIFECYCLE

The reason behind SDL technology is to provide secret-document security at all points in the lifecycle. It is obvious that at the time when a leak-prevention system is implemented, there already exists a large volume of documents. Therefore, the first step, as has already been mentioned, is the classification and categorisation of all the information.

When it has been ascertained how confidential a given document is, the following takes place: each document is labelled in accordance with its class of confidentiality or access level. This is achieved by use of a specially developed technology which inserts a label into the document in such a way that is completely invisible to the user and cannot be modified by him. At the same time, in addition to working information, the label contains details about the class of document and access rights to it, as well as about the document owner. Here, the multi-tier confidentiality model already mentioned is used.

Protection of data at rest. The next step is the placing of all classified documents in the special Perimetrix SafeHouse™ storage facility where they are held in encrypted form. This storage can be implemented both as a central depository or as a distributed storage facility. If the second option is chosen, documents are held on users' workstations just as before, but in encrypted form and with embedded labels. This results in a protective storage facility which will reliably secure secret documents from leak and dissemination even in the event of the loss of a laptop or some other form of unauthorised-access attack. In addition, the storage facility makes

no distinction between text documents, tables, graphics, multimedia files and even databases. In the case of a database, the database itself is not placed in the storage facility. Instead, users work with the safe storage and data from the database passes through it before reaching the user.

Protection of data in use. When all documents have been classified and placed in the storage, then the work process begins. Here, all operations with secret documents are controlled by Perimetrix SafeUse™. However, in the course of their duties, employees use not only existing classified documents, but also create new ones. We would expect to see all the problems of deterministic methods arise which were identified earlier, however, our developers have found an elegant solution: on creation of new documents which use content from existing documents, they are “infected” by the confidentiality labels embedded in the prior document. Thus, all new documents are classified automatically (with the exception of those created from scratch).

Research conducted by Perimetrix has shown that workers very rarely create documents from scratch using their own content. As a rule, such documents rarely exceed 0.5% of all documents created. Only in particular circumstances, such as the work of artists, designers, etc., does this figure rise to around 3%. In other words, only a very small percentage of the new documents created in a company cannot be accommodated by automatic classification.

The protection of a confidential and labelled document from theft moves up to 100% effectiveness – which is characteristic for deterministic methods. The system simply knows that a document is secret and so it does not release it to the outside world if the employee does not have the appropriate clearance.

At the same time, an attempt to steal a non-classified document (that is, a document created from scratch and containing the author’s own content) leads us to Perimetrix SafeEdge™ which utilises three probabilistic protection methods: Digital Fingerprints, linguistic, and signature analysis. In this case, the effectiveness of protection rises significantly as against the figures just quoted since the number of unclassified files at any one time will not exceed 0.5% of the total. Thus, the proportion of false positives or missed secret documents according to the theory of probability reaches $0.005 \times 0.8 = 0.004$. In other words, effectiveness of the technology is 99.6% which is more than sufficient for risk assessment and threat analysis. And at such levels, it is not even worth talking about false positives.



PERIMETRIX

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. In this case, the file is still sent to the filtration server for classification in real time. This creates no noticeable extra load 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 the automatic classification of the documents. However, in this case the SDL system conducts a regular document inventory 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 storage facility.

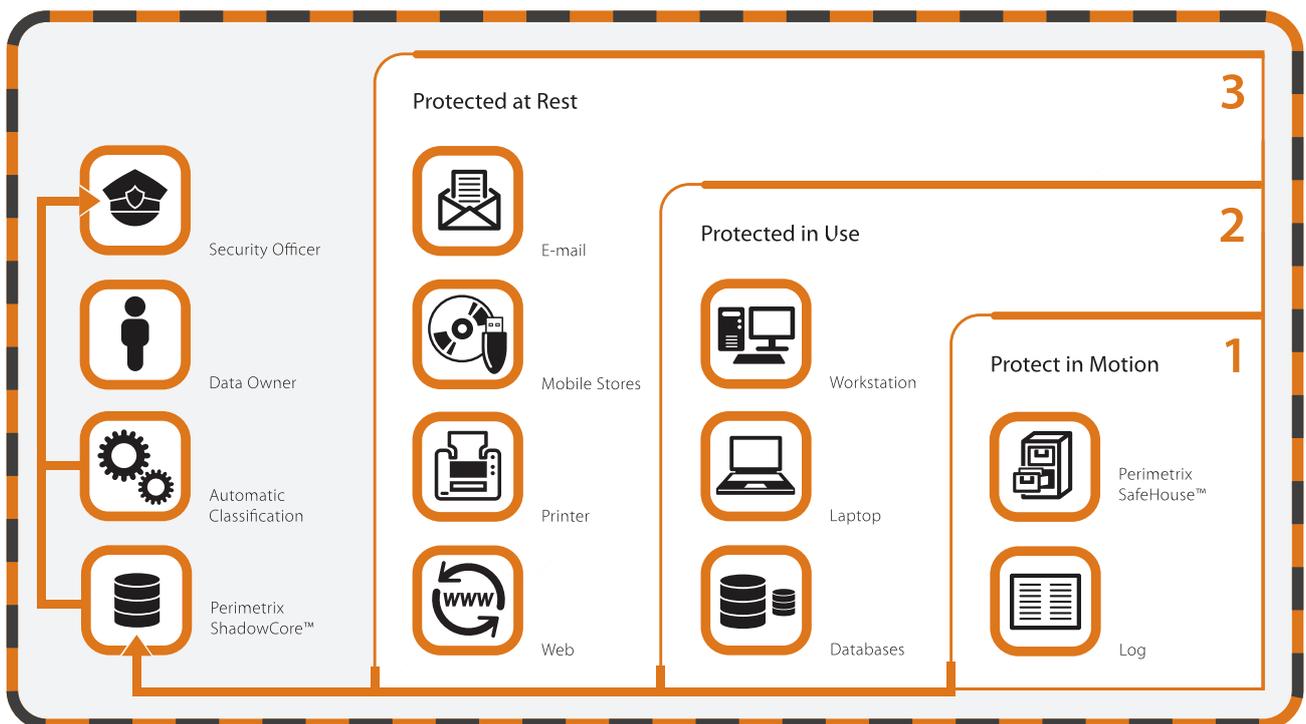


Fig. 2. SDL technology secures data at rest, in use and in motion

Protection of data in motion. It is worth remembering that all secret documents are held in encrypted form. Therefore, when one sends such a document, one is sending it in encrypted form which means the data is protected in motion also (see Fig. 2). In addition, if a secret document leaves the corporate network and goes, for example, to a partner, then the encryption of the outgoing traffic can be done automatically and completely transparently.

In closing this topic we would like to point out that SDL technology permits such procedures as lowering a document's level of confidentiality. Clearly, when copying data from a secret document, an employee may create a non-confidential file which permits later reworking or sending outside the company. In such a case, the employee could initiate the procedure of lowering the secrecy level and this requires the participation of another one or two colleagues depending on the security policy in operation; for example: the information security officer and the employee's line manager or a person with full access rights. For users who regularly create public documents, there are document templates which permit the creation of non-confidential files. However, during this process, employees are prevented from working with confidential information in other documents as a logical consequence.

Secret Documents Lifecycle™ technology simplifies users' work beyond the corporate network.

3.3. SECRETS PROTECTION OUT OF THE OFFICE

As stated above, the protection of data at rest involves the use of encryption which means that secret documents are equally safe from unauthorised access whether on laptops or on the company network. However, when working remotely with confidential information – for example, on a business trip – a problem arises with the issue of user authentication and the effective protection of documents used.

SDL technology simplifies users' work beyond the corporate network. To this end, several security policies are applied which define the access level for classified documents.

The main access levels are:

- **Restricted use.** In this case, the employee on the business trip can get access to documents by using a personal key; for example, by using strong authentication or being recognised by use of 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, it is necessary to go through both the authentication process and to 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. As a result, should it become necessary, the security officer can deprive the remote employee of access to top secret documents.

This is how SDL technology addresses fully the issue of protection and audit of secret document integrity beyond the confines of the corporate network. At the same time, all work by employees working remotely is kept absolutely transparent.

3.4. AUDIT AT ALL POINTS IN THE LIFECYCLE

The audit of confidentiality and integrity of confidential documents at all points in the lifecycle is as important a part of SDL technology as the prevention against leaks.

The SDL concept entails the implementation of a Perimetrix Shadow-Core™ central database in which all events (who did what and when to which document) are stored as well as 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. On the basis of this information, it is possible to ascertain how effectively the organisation's information resources are being used, and to balance and optimise data streams and internal communications processes.

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

Importantly, SDL technology contains an inbuilt single system of user identification. This means that by using the central database, it is always possible to identify the employee who has performed any action. Likewise, 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 the actions of the Internet channel identifying users only via faceless IP-addresses (which may be dynamic), by email – by email address (which is easily falsified) – or by external devices by users' account names.

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

An audit of integrity requires that each sensitive document be protected from modification.

3.5. AUDIT OF SECRET DOCUMENTS INTEGRITY

The audit of secret documents integrity has been given its own chapter since it is a key requirement for a whole range of industry legislation, standards and directives. In particular, 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 mean that it is always possible to identify who made what changes to a document as well as restore important files in their original state (including after destruction).

SDL technology fully addresses the issue of audit of integrity and protection from the distortion or destruction of documents. The central archive described in the previous chapter contains all the necessary details for an audit: various document versions in addition to 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.



3.6. 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, in use and in motion. The key advantage of the SDL concept is the fact that this approach solves the issue fully and right across the board. No matter if an employee loses a laptop with secret documents or tries to copy confidential information to a USB drive, no leak will occur. Thus, the implementation of the SDL concept in an organisation solves the problem of leaks once and for all.

In keeping with the paper document circulation we looked at earlier, SDL allows the creation of a safe space in which documents are stored, used, moved – where they ultimately live and die. This safe space has its own place in the total solution: Perimetrix SafeSpace™¹.

¹ See Perimetrix SafeSpace – solving the problem 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 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

