perimeter

Data Leakage Prevention DLP Data Leakage Prevention DLP Data Leakage Prevention DLP Data Leakage Prevention DLP Data Leak-
DLP Data Leakage Prevention DLP Data Leakage
Data Leakage Prevention DLP Data Leakage Pre-
kage Prevention DLP Data Leakage Preven-
DLP Data Leakage Prevention

CLASSIFIYNG AND PROTECTING BUSINESS DATA

Data Leakage Prevention DLP Data Leak-
Data Leakage Prevention DLP Data Leakage
Data Leakage Prevention DLP Data Leakage Pre

WHY DLP IS NOT ENOUGH AND WHAT MORE IS NEEDED

QUESTION: In which ways can a DLP[1] system be bypassed and what can be done to prevent that from happening?

From the simplest method, such as an archive with a password, to more complex SSL tunnels and using TORs, it is necessary to apply clear and strict security policies as well as specialized solutions based on *Data–Centric Security*. With this approach, the focus of protective measures is shifted from channel control to data control. This enables you to:
— Identify and protect all information assets, regardless of their location, both inside and outside the security perimeter of the organization.
— Restrict and strictly control access to confidential data across all networks, devices, information systems, services, etc.
— Log and inspect all actions performed on confidential data.
— Accelerate the company's business processes by leveraging a secure digital ecosystem, including internal and external business users and advanced security technologies, throughout the life cycle of the data.

QUESTION: What new functional capabilities did you add to the Perimetrix solution?

Although our solution can also be used to prevent data leaks, its development cannot be attributed to that of DLP in the classical sense. Yes, in our system there is a module designed to control some data channels and transmission protocols through which confidential data may "leak". However, we consider the Perimeter–Based Security approach to be outdated, and base our solutions, rather, on the idea of *Data–Centric Security*. The Perimetrix SafeSpace solution, therefore, is better associated with the class of EDRM[2] solutions.

The main limitations of DLP systems are related to the inability to track all channels where leaks can occur and to process all possible data formats. The most difficult part of implementing DLP is identifying the data that needs to be protected and all the channels from where it may leak. In addition to this, it is also necessary to restrict the use of programs, protocols, and data types that are not handled by the DLP solution.

If you want to transfer confidential data outside of the company's "security perimeter", for example to a partner, then how do you ensure that the data does not "leak" from the partner? This is where the need for IRM/EDRM[2] solutions arises. IRM allows you to remotely manage how data is used. By encrypting files, you can prevent unauthorized access, and with the help of client applications, you can limit what can be done with the documents. However, the use of IRM is limited to the user application layer.

EDRM systems allow you to control access to data by encrypting all documents. The decryption keys, however, are located on a server. In order to access the server, and thereby the decryption keys, user authentication is required. As for client applications (MS Word, Adobe Acrobat Reader, etc.), they run under the EDRM agent, which ensures that permissions exist for accessing the files. A classic example of the necessity of using EDRM is for the protection of design documentation.

Let's say that a limited number of designers have access to such data. The risk of a data leak may arise from the fact that it isn't possible to control the actions of users who actually have the necessary permissions to access the data. Consider the following situation. Due to production requirements, a designer copies some confidential data to his workstation, and then sends it by e–mail to a colleague. This is perfectly acceptable behavior and is a natural part of the relevant business workflow. However, as a result of such actions, confidential data can fall into the hands of users who do not have appropriate permissions, or even into the hands of malicious individuals. Using EDRM, however, even when receiving a file, unauthorized users will not be able to access the protected information. Moreover, all attempts to access the data will be logged.

Control over the transfer of confidential data is maintained even if the data is situated "outside the security perimeter", and access can be centrally withdrawn at any time. Therefore, the joint use of DLP and EDRM technologies is certainly justified. DLP is a good solution for monitoring communications, identifying confidential data, and then

1 **DLP** — Data Leak Prevention.

2 **IRM** — Information Rights Management; **EDRM** — Enterprise Digital Rights Management.

alerting and/or blocking the transmission of the data as needed. EDRM is used to ensure that documents are handled securely, especially when a limited number of internal employees are involved as well as possibly, external contractors.

QUESTION: What can be expected from developers of DLP systems in the foreseeable future? In which direction is the industry moving?

Given today's threats in the information security landscape, it is clear that the combined use of DLP and EDRM technologies has become an essential part of the *Data–Centric Security* approach. The first integrated solutions of the new class of products (IRM/EDRM + DLP) were created using existing products from different developers. As a result, they did not grow significantly or become very popular.

Today, multinational vendors are pursuing the objective of acquiring other companies in order to integrate various products into a single solution. The latest example of this phenomenon is Symantec's acquisition of the Portuguese company Watchful Software. The acquisition was done in order to create the Symantec Information Centric Tagging solution and subsequently implementing the Data–Centric Security approach based on the following set of solutions:

— Symantec Information Centric Tagging.
— Symantec Data Loss Prevention.
— Symantec Information Centric Encryption.
— Symantec Validation and ID Protection Service.

The next step, in our opinion, is for vendors to start integrating DLP/EDRM, PIM[3] and IDM[3] products into a single solution. This approach will allow you to more effectively address the following issues concerning security:

— Protecting confidential data against leaks.
— Combating malicious activities.
— Combating acts of sabotage.
— Complying with regulatory requirements.
— Strengthening traditional data security measures.

QUESTION: What is the essence of the Data-Centric Security approach?

Our approach to data protection is based on the *DCSM (Data Centric Security Model)* methodology, or information centric security model. The main focus of DCSM is to ensure that data is given an appropriate level of security based on its business value. There are several classifications that can be applied to business information, depending on the value of the information as well as when, where and how it is used in a particular business process. This classification allows you to dynamically manage the permissions for both users and applications that interact with the data.

The implementation of the DCSM approach begins with the creation of a set of corporate data processing guidelines. These, in turn, define the security policies and the information security services that are necessary in order to support the policies.

After identifying information assets and classifying them, it is then possible to define business–oriented rules that manage the data for each data/information category. Permitted actions related to classified data are summarized in policies that define all aspects of the confidential data's use. This includes all activities (such as creation, processing, storage and transmission) throughout the data's entire life cycle, from cradle to grave. These policies are configured in the settings of information security systems and all related user–based applications. This in turn forms a strong link between the business and IT, which can now be applied in a focused manner in the necessary context.

Implementing the core concept of the DCSM model, our Perimetrix SafeSpace (PSS) software package ensures the classification of confidential data as well as compliance with the defined rules and policies for working with the data. Deviations from these rules are controlled and limited dynamically. Any user actions or application processes that somehow do not conform to the scope of permissions are blocked, and thus guarantee that the confidential data can only exist and be used within a well–defined security perimeter.

Each PSS implementation project involves not only the deployment of the software, but also requires a significant amount of effort aimed at examining business processes that utilize confidential data. The resulting analysis is then used to build a model for

3
PIM — Personal Infromation Management;
IDM — Identity Data Management.

the data's protection. The implementation of a system to manage confidential data should be based on a risk management methodology that takes into account business requirements. This in turn requires prioritizing the level of confidentiality for data in those business processes where its compromise could cause the greatest damage to the company. As a rule, such business processes include confidential document workflows, internal correspondence via e–mail, data processing in HR systems, financial data, device and product design data, know–how, schematics and techniques related to manufacturing processes, etc.

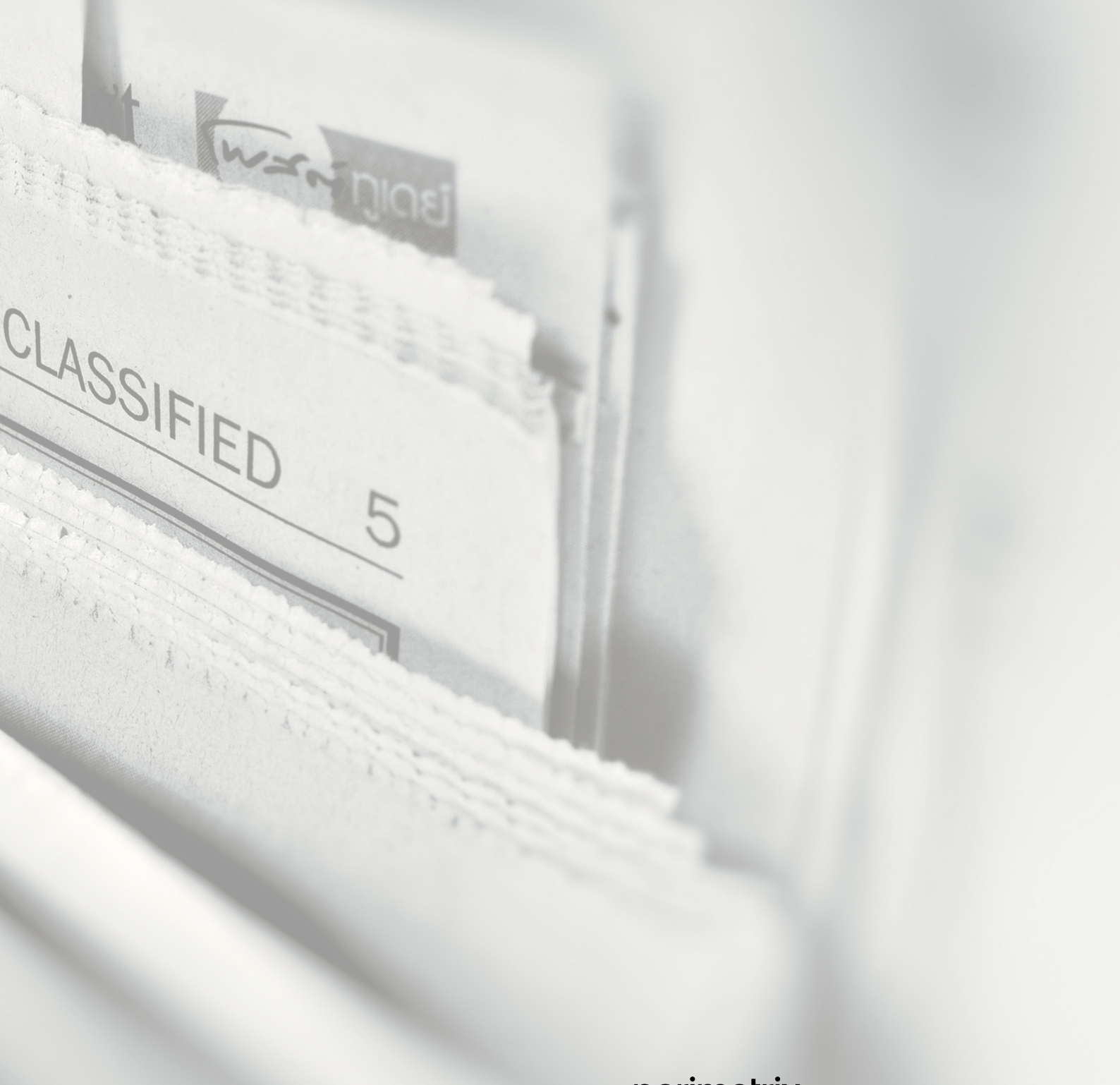
We have developed the procedures for analyzing business processes to a great extent. We not only identify the processes and sub–processes that occur directly in the digital environment, but also take into consideration any required restrictions on working with non–electronic confidential data before and after its conversion into a digital format. The consulting stage of the project results in a detailed information security model describing the planned data classification scheme and the procedures for assigning persistent classification tags to the data. The security model also details authorized locations and formats for storing confidential data, applications that are authorized to process the data, permitted transmission channels and rules for converting from electronic formats to non–electronic formats. In addition, the security model defines the permissions of users to work with confidential data in different workflows.

The security model is then translated into configuration settings within the software solution. This is how we implement an information–centric approach to security, in which the type and value of business data is determined by security policies which are implemented directly in the digital environment.

QUESTION: How much will installing Perimetrix Software interfere with the users' work? Will constraints and restrictions disrupt a company's daily work routines?

First of all, restrictive policies are not artificially contrived. Policies simply implement the security requirements that users had to comply with previously anyway. Secondly, the appearance of a small orange tag attached to confidential data will actually facilitate a user's work by allaying some of the typical fears that may exist, many of which were described earlier.

Seeing a file with a security tag on the computer screen, the employee will know the following: the file is stored in a permitted location, the file does not exist in other places on the corporate network, the file can not be opened by anyone other than those with the necessary permissions, the file can not be accidentally or maliciously copied to a flash drive, sent by e–mail, uploaded to the cloud, downloaded and sent via messaging applications, etc. All possible actions with the data are taken into account and are known. This is the difference between working with confidential data and working with non–confidential data. ■



perimetrix

A Russian company founded in 2007, whose products have been trusted for more than 10 years to protect the confidential data of organizations such as AvtoVAZ, Gazprom Energoholding, the Federation Council of the Federal Assembly of the Russian Federation, TVEL and others. The company has a network of partners in Russia and abroad. The company's headquarters are located in Moscow.