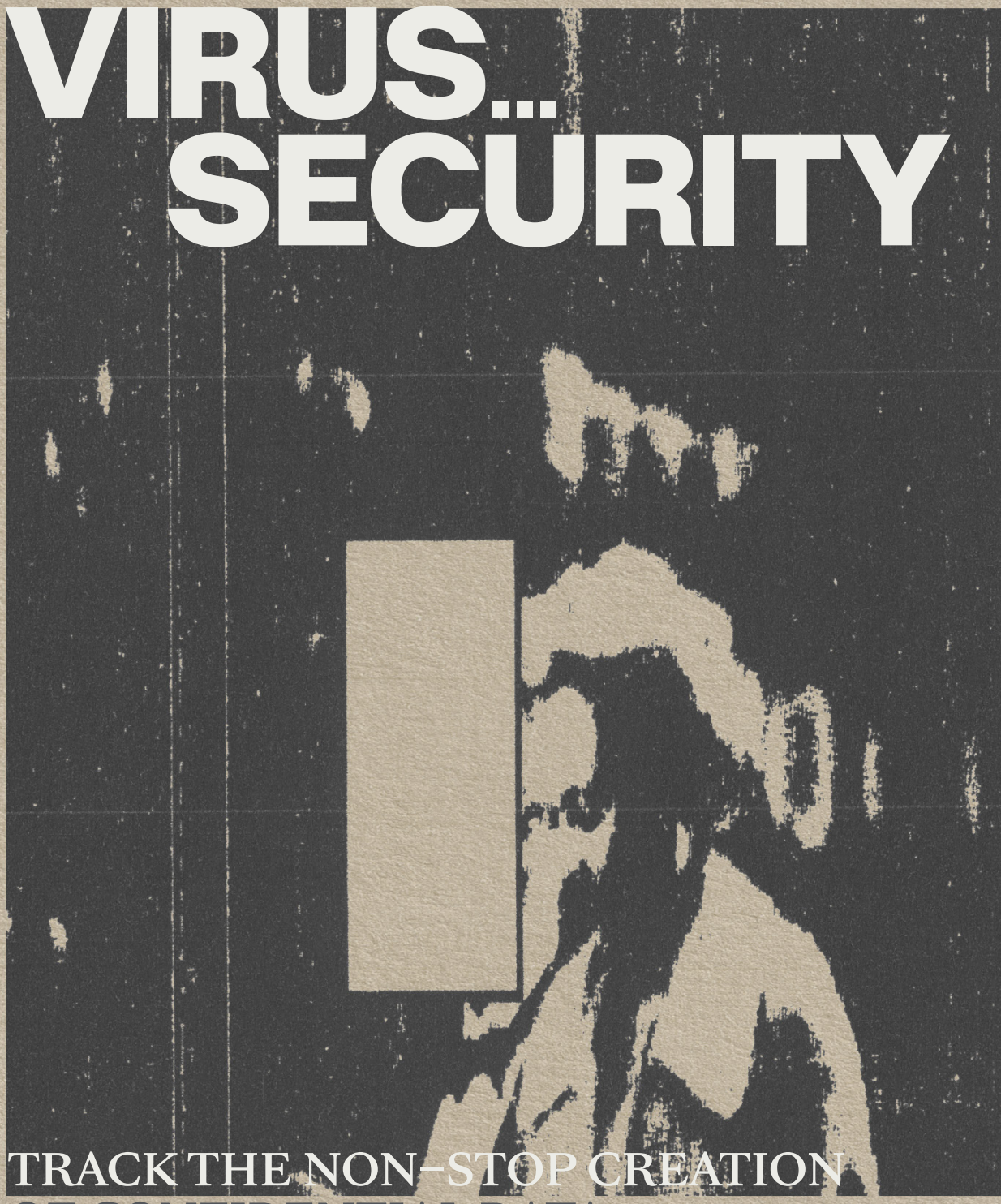
primetrix

VIRUS... SECURITY



TRACK THE NON-STOP CREATION
OF CONFIDENTIAL DATA

Trade secrets

Current legislation does not give clear instructions on how to implement a system for protecting trade secrets. This is why, in many cases, the implementation of a trade secret security system in a company is limited to issuing "regulations regarding trade secrets" and having employees sign the relevant clauses in their employment contracts.

And this is understandable. The responsibilities of enterprise security services consist of a wide range of heterogeneous activities (e.g., access control, perimeter security, physical security of key employees, background checks of contractors, counter-espionage measures, etc.). Therefore, security personnel are simply not able to effectively track the non-stop creation of confidential data, quickly determine its value on-the-fly and then control all the ways that it can be distributed within the enterprise.

But such information is created in production processes on a daily, sometimes hourly basis. And the damage resulting from its loss or disclosure can be critical to the enterprise.

Of course, the introduction of a system for securing confidential paper-based documents at the enterprise partially solves the problem of protecting trade secrets, but it is only the "tip of the iceberg". First of all, not all confidential information is saved as a physical document. Secondly, until the printed document is marked with a "confidential" label, the source information contained on a computer is not factually nor legally protected.

What can be done? Let's begin by looking at the life-cycle of a trade secret. Such secrets are created in the minds of developers and designers, or by enterprise and department heads. They can also arise during normal operational activities in product manufacturing.

Trade secrets within a company are not usually considered private, so the exchange of such information between employees of an enterprise is often an essential part of the production process. The choices of how to control the distribution of trade secrets, of course, depends on the ways in which the information can be transmitted and in what form it can be stored. The human brain is one of the most common "repositories" of information. Its capabilities, however, are not unlimited and the ways in which information can be recalled are quite specific. A person can, for example, remember the essence of a conversation, the idea behind a drawing, the amount of a particular transaction, the general meaning of a document, or even a part of its text. However, it is impossible to save a database, a spreadsheet, a multi-layer image, or a scanned signature in one's brain.

In order to control information that is classified as a trade secret, it is necessary to choose technical measures that adequately correspond to the specific form in which the information is presented. "Simple" information that can be carried around in one's head requires specific operational controls by the security services. There controls, however, are beyond the scope of this discussion. The transfer of more complex information requires that it be affixed to a particular medium, (e.g., paper, an electronic document, a printed photo, a video or audio recording, etc.). In modern

production environments, such complex information eventually enters the enterprise's digital environment, where it is stored and processed. Moreover, a significant part of such information is actually created within the information systems themselves, for example, documentation and drawings related to product design.

The abundance of opportunities for processing and transmitting confidential data in a computer environment has led to the emergence of a class of software solutions specifically designed to prevent of data leaks, commonly referred to as DLP (data loss/leak prevention). Such systems are aimed at intercepting information being transmitted by users through various communication channels. DLP systems analyze data transmissions and search for specified patterns. Based on defined patterns, the system makes a decision on whether or not to allow the data to be transmitted.

The most advanced DLP systems allow you to build models of user behavior and to identify any deviations from the norm. Incidents are recorded as violations of specified security policies. Of course, behavioral analytics can help security services identify actual and potential violators of trade secret policies. But in our opinion, the task of protecting a trade secret is to prevent its leakage in the first place and not to simply report on it after the fact. In order to ensure the effective protection of computer data containing trade secrets, control should be established at the time of its creation, and not only when it crosses the information security perimeter of the enterprise. After a trade secret has been printed, transmitted by e-mail, posted on the Internet, etc., it is already too late.

The systems and processes for managing confidential data should be "activated" at the very moment when such data is saved.

Collective irresponsibility versus individual competence

The implementation of a system for managing trade secrets very often begins to stall at the very start. Why does this happen? Having made a decision on the need to protect secrets, management often entrusts the development and implementation of the solution to the security services. After spending lots of time and resources in developing formal means for identifying and classifying data as trade secrets, the security services quickly reach the disconcerting conclusion that any information can be considered a trade secret. Understanding that, in reality, every piece of data is not a trade secret, and that the addition of a "classification tag" on every document will simply stop production processes, the security services simply abandon the project. Moreover, they then transfer responsibility to the employees, including any trade secrets compliance requirements that may exist in labor agreements.

As a consequence, even though the system has been built, at least on paper, neither management nor the security services are confident in its actual compliance. The obvious solution seems to be the implementation of technical systems to track and analyze user actions within the computer environment. This, in effect, leads to a significant increase in the volume of work for the security services (such as recording and analyzing incidents, etc.) and negatively impacts the entire security team. More importantly, it does not even offer any protection against possible leaks. For any manager with corporate level responsibility, the capture of another "spy" is not so much an indicator of the effectiveness of the security services, but more a demonstration of the ineffectiveness of the trade secret security system.

At the same time, every manager is well aware that the company has a team of dependable top managers and specialists who have a fairly deep understanding of the essence and purpose of confidential information. These people, the "data owners", are able to define the boundaries of the "internal security perimeter" for confidential data. They are the "mainstay of the trade secret regime". Moreover, they are the ones who should be given the tools to quickly assign classification tags to confidential data.

The task of the security services, therefore, becomes quite specific. That task being, together with the data owners, to establish and implement the means of assigning "classification tags" to confidential data. Classification tags are assigned based on the permitted use and distribution of data, which is dictated by the actual needs of production processes.

Everything is forbidden except that which is explicitly allowed

A regime is defined as a strict set of rules that must be complied with. Unlike usual rules of behavior, which generally prohibit certain activities and define the consequences if violated, a regime operates on a simple and understandable principle: everything is prohibited except that which is explicitly allowed. In other words, one can only do what is explicitly stated and only in the way it is allowed. Everything else is "prohibited" and should, therefore, be technically impossible to do. It is this principle that should be implemented in order to protect confidential data, particularly trade secrets.

Despite appearing extremely restrictive, the implementation of this principle will, however, not only not interfere with normal production activities, but will in fact make them clearer and more predictable. For a "correct" production process where confidential data is used, it is necessary to define the minimal security perimeter for the data in order to allow the process to operate normally. This perimeter includes allowed storage locations, applications authorized to process the data, printers allowed to print the data, authorized employees, etc. In the course of performing various activities, the perimeter that was initially defined can be expanded as needed. However, any expansion of the perimeter will have to be done intentionally, refining the production process. Confidential data, therefore, will not be allowed to exit the modified security perimeter unless or until it is explicitly permitted to do so.

Security “contamination”

There is widespread fear that the introduction of a security system will simply stop enterprise operations. In order to avoid this, it is necessary to implement a balance between strict protection of secrets and flexible production processes. Therefore, ideally, the security perimeter should be expanded gradually over time, as the production chain in which confidential data is utilized becomes more precise.

Beginning with the movement of data within the organization, the classification tag is re-verified by the data owner. This verification enables the data owner to make informed decisions about new users’ access, newly allowed storage locations as well as processing methods. The expansion of the security boundary containing “secret carriers” does not occur based on the “carrier” belonging to any particular group or organizational unit within the enterprise. Any expansion of the security perimeter is a result of the “carriers” interactions with confidential data, which are dictated by actual production requirements.

The second way to “naturally” expand the security perimeter is based on the following principle: classifying a document as a trade secret means that all documents that are subsequently created based on the parent document inherit the classification by default. This is done since the newly created documents may contain confidential data. Only an informed decision by the data owner or the security services can prevent the new documents from inheriting the “classification tag”. This approach saves the security services from having to constantly make decisions about every newly created document.

Therefore, the confidential data regime spreads throughout the enterprise, from the data owners to other employees, from one protected document to all documents that are derived from it. The security perimeter of the trade secret regime will gradually cover all work processes, where confidential data is used, without negatively impacting the operational life of the company.

Technical implementation of a trade secrete regime

The SafeSpace solution, developed by Perimetrix, implements the *exact approach* that was described earlier. The methodology that is employed in the solution is based on assigning classification tags to information assets. A classification tag can be assigned to digital information in a variety of ways. The first way is to assign the classification tag manually. This is done by the person who is accountable for the creation of confidential information.

The second method is to have a classification tag generated automatically based on some predefined rules. For example, all drawings that are created by designers using AutoCAD or COMPASS can receive a classification tag the moment they are saved as files. All subsequent actions with the files, such as printing, copying, etc. will only be permitted if they comply with the defined security permissions.

The third option is to automatically inherit a classification tag. Transferring information from a "tagged" file to another file, whether by creating a copy of the file, converting it to another format, or copying the contents through the clipboard, will result in the newly created file receiving the same classification tag as the original source. Therefore, any copy of a confidential document or any derivative of a confidential document will still remain confidential, and will have the same security rules applied to it.

The process of allowing confidential information to move outside of the security perimeter is regulated by the relevant security rules. For example, printing can be restricted to printers where the printed paper copies are logged and registered. The transmission of classified information via e-mail or by copying to portable media can be restricted so that only encrypted items are allowed. Therefore, only a trusted user who already has the Perimetrix agent installed on their computer, and who has sufficient permissions to work with the classified information, can open such an email or file.

Let us now consider the scenario of the "native" implementation of a trade secret regime in an enterprise. The senior management of a company and the security services which were included in the initial "security perimeter", will, in the course of their daily activities, create documents whose contents constitute a trade secret. When under the control of the Perimetrix solution, these documents will acquire the appropriate classification tags. If the production process requires some lower-level employees to have access to confidential data, the data owners can decide to expand the scope of the security perimeter accordingly. They can then authorize the installation of the necessary security software on the relevant computers. Confidential documents which have been classified by the data owners can be used as samples when performing an inventory of existing information assets. In this way, the security services will be able to detect confidential data on users' computers and thereby move quickly to safeguard any confidential data that had been previously created, but not classified. The classification tag inheritance mechanism and the use of "tagged" templates helps users remain within the security perimeter when creating new documents that contain trade secrets[1].

Moreover, with data that is clearly of great value (e.g., design documentation or personal data), a decision can be made to have them automatically tagged the moment that they are created.

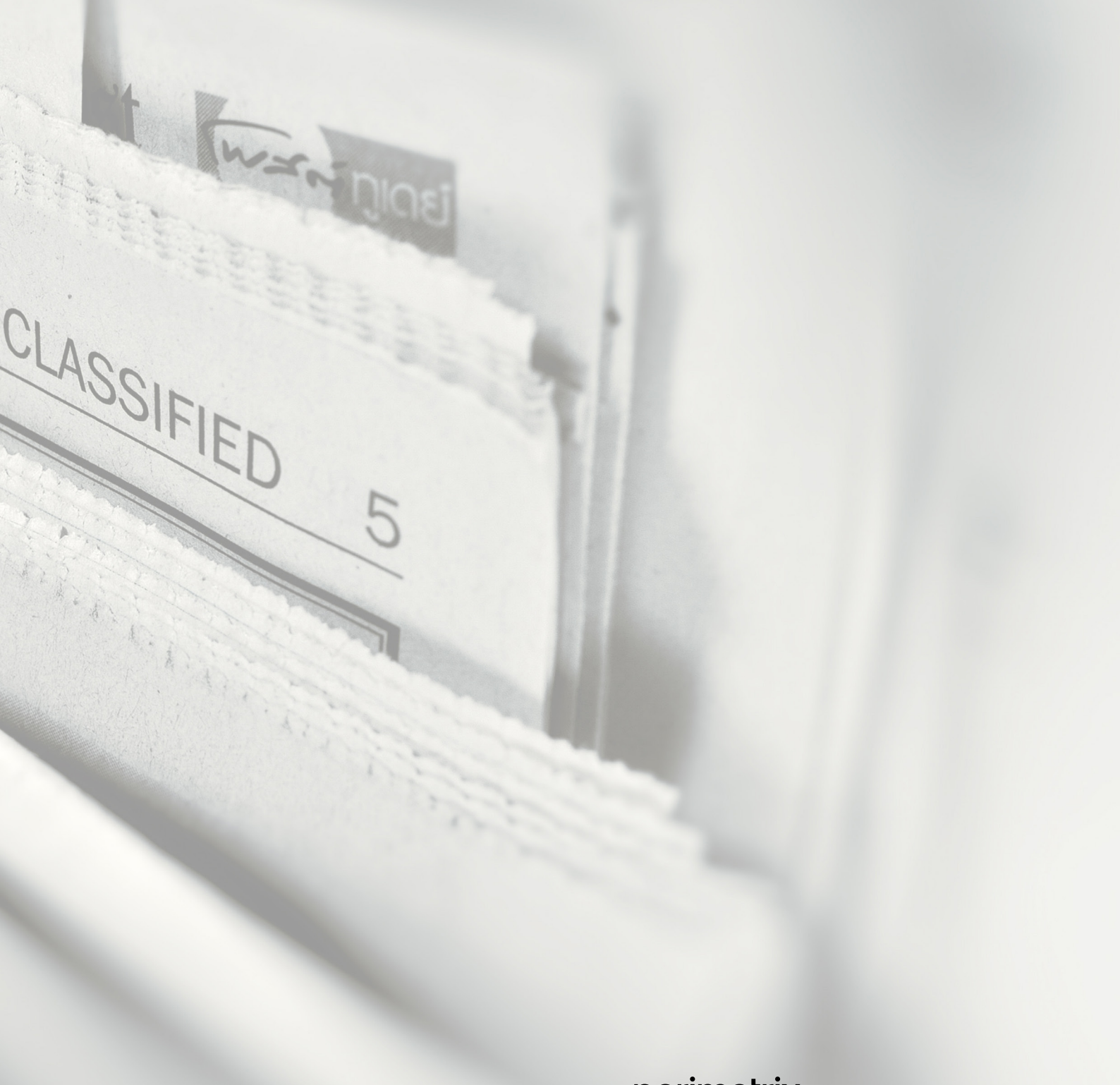
1

With data that is clearly of great value (e.g., design documentation or personal data), a decision can be made to have them **automatically tagged the moment that they are created.**

Conclusion

Let us summarize some of the *main advantages* of implementing such a trade secret security regime in an enterprise:

- ✓ The trade secret security system related to digital assets is not based on formal criteria, but on knowing the real value of the information asset to the company.
- ✓ The individuals who determine that a piece of information is a trade secret and who assign the classification tags, are the knowledgeable and competent data owners, not a separate security service.
- ✓ The process of establishing an enterprise trade secret security system can be done in stages and can be done independently in different departments that work with a variety of confidential data (production data, commercial information, personal data, etc.).
- ✓ The principle of minimal authority is implemented, whereby only those users who have a legitimate need are allowed to work with confidential data.
- ✓ The decision to classify information as "confidential" is made promptly, at the time of its creation in the digital environment. This can be done automatically by the system based on pre-defined rules, or manually by authorized employees.
- ✓ In relation to classified information, the basic principle of the system is that "everything is prohibited except that which is explicitly allowed". This approach ensures the security of confidential data and does not interfere with normal business operations.
- ✓ Allowing information to move outside of the security perimeter or removing classification tags from confidential data is only carried out in compliance with the relevant security policies and under control of the security services. ■



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.