NNTC

PERIMETRIX SAFESPACE

Distributed classified data management system

INSIDER THREAT PROBLEM

>50% employees send work emails with sensitive information to the wrong recipients

30% of leaks are made via emails or messengers

HOW TO BE PREPARED?

Use distributed classified data management systems! Perimetrix SafeSpace — a perfect sensitive data access management tool to protect enterprises from inappropriate use of sensitive information.

Now you can:

- Manage permitted actions with classified data in a personal computer
- Organize information protection in electronic form

Each file with confidential information is label. With this label, you can only do actions that allowed by rules. All other actions will be blocked.

FEATURES

Flexible multidimensional classification of sensitive electronic data

Univocal reflection of business security demand into setup of the system

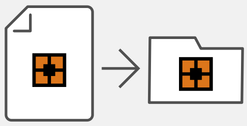
Classified data governance policies of storage, usage and transfer

Universal logic and decision making mechanism of all modules of the system

Preventive method of classified data protection from internal threats (leak, distortion, destruction)

Full control of classified electronic data life circle

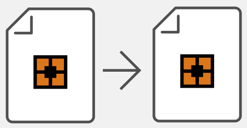
HOW IT WORKS



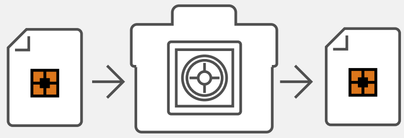
Save valuable data only in authorized places (specific folders on computers or registered flash drives)

- DIRECTOR
- SECURITY OFFICER / CHIEF ACCOUNTANT / CHIEF ENGINEER
- HEAD OF DEPT. / PROJECT MANAGER / HEAD OF SERVICE
- ENGINEER / EMPLOYEE / ECONOMIST

The right to work with valuable data will only be for those users who have access to the required level of stamp



Copy valuable data from file only to protected documents



Transfer valuable data through an unprotected environment only in encrypted form

DIFFERENCES OF PERIMETRIX AND DLP

DLP	PERIMETRIX
Limitations of DLP systems: inability to track all leakage channels and process all data formats	**Perimetrix** makes all processes associated with information controlled and transparent
Tracks **actions of employees**, analyzes them, identifies and accumulates data about the facts of undesirable actions	Controls **actions with valuable data**, checks against the given rules, allows or prohibits actions
Uses **different ways to intercept traffic** through known channels, conducts a linguistic analysis of the user's correspondence and documents	Uses **non-removable and inherited labels** on files to make a decision on the admissibility of actions with them according to the specified rules
Analyzes and **accumulates information** about all events workplace employee	No way **not related to normal workflows**, not using confidential data
It has **probabilistic result of work**, allowing the possibility of data leakage and blocking legitimate processes	Implements **unambiguous algorithm** of permitted actions with confidential data regardless of the rest of the employee's activity and the characteristics of his work
Implies **regular analysis** accumulated data and investigations	**Doesn't require constant monitoring** by a security specialist

USE CASES

PROTECTION OF DESIGN AND OTHER DOCUMENTATION

The plant suffers losses due to counterfeit products, loses customers due to the fact that the know-how created is used by small firms, getting access to developments without paying royalties to the owner intellectual property. Leadership requires to protect new technical documentation.

With help of Perimetrix, drawings and working documents created at the designers' workplaces of are limited in distribution within the enterprise.

PROTECTION OF INFORMATION CREATED BY TOP LEADERS

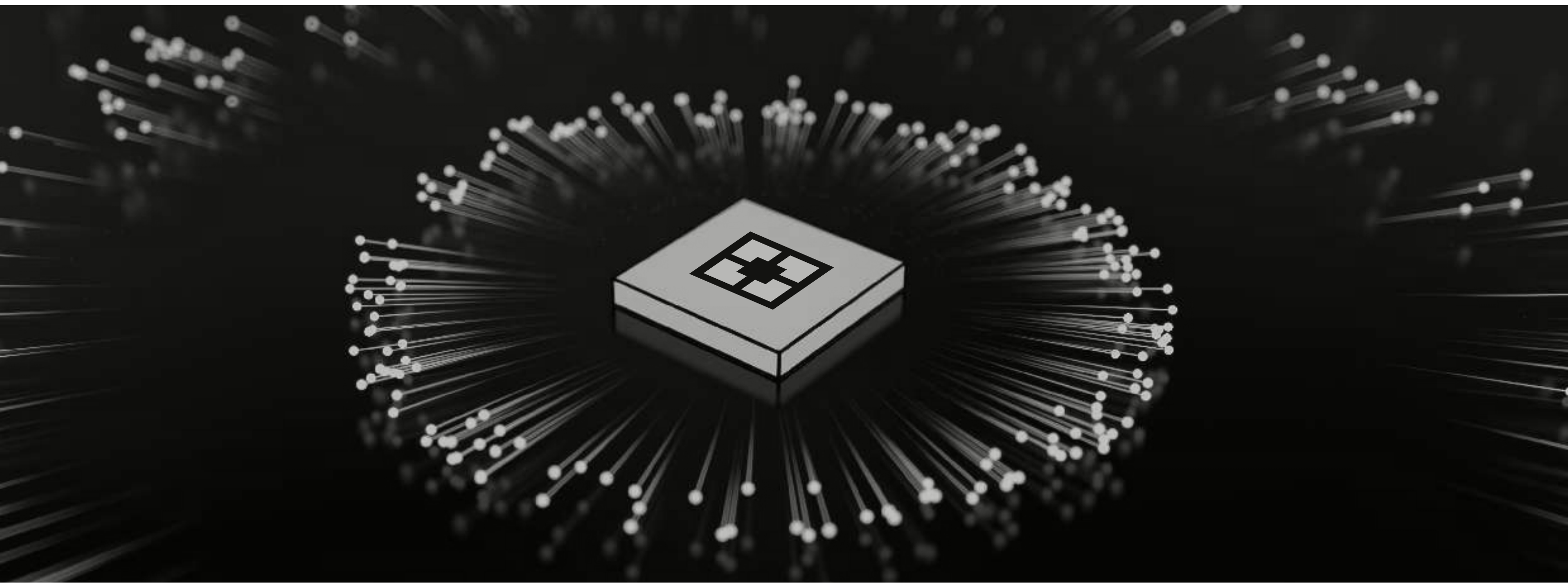
Employees constantly create, edit and exchange information containing elements, parts, prototypes of commercial secrets. However, only the final documents receive confidential status.

With help of Perimetrix, executives will be able to protect their valuable work data from the moment document is created. At the same time, the system will help determine the presence of similar documents in random places and copies and also protect them.

UNAUTHORIZED DESIGNER ACTIVITIES

Using the workplace, expensive design software and spending paid time, the employee fulfills personal orders.

With help of Perimetrix, all created information objects are marked as the property of the organization. It is prohibited to move them outside the company.



IMPLEMENTATION PROCEDURE

Stage 1
Project launch and demo stand creation

A demo stand with the Perimetrix SafeSpace system is created in the customer's infrastructure. The customer's specialists will translate enterprise security policies into the internal system settings.

Stage 2
Information Security Model development

- Collecting the data workflow in the organization
- Security Model development and its documentation

Now we have a defined protection model, including categories and classification rules for the valuable data processing.

Stage 3
Configuring and testing the Information Security Model

- Test stand creation: it includes a typical employee workplace
- Programming policies
- Checking the correctness and safety of business processes on the test stand

Stage 4
Organizational and administrative documentation

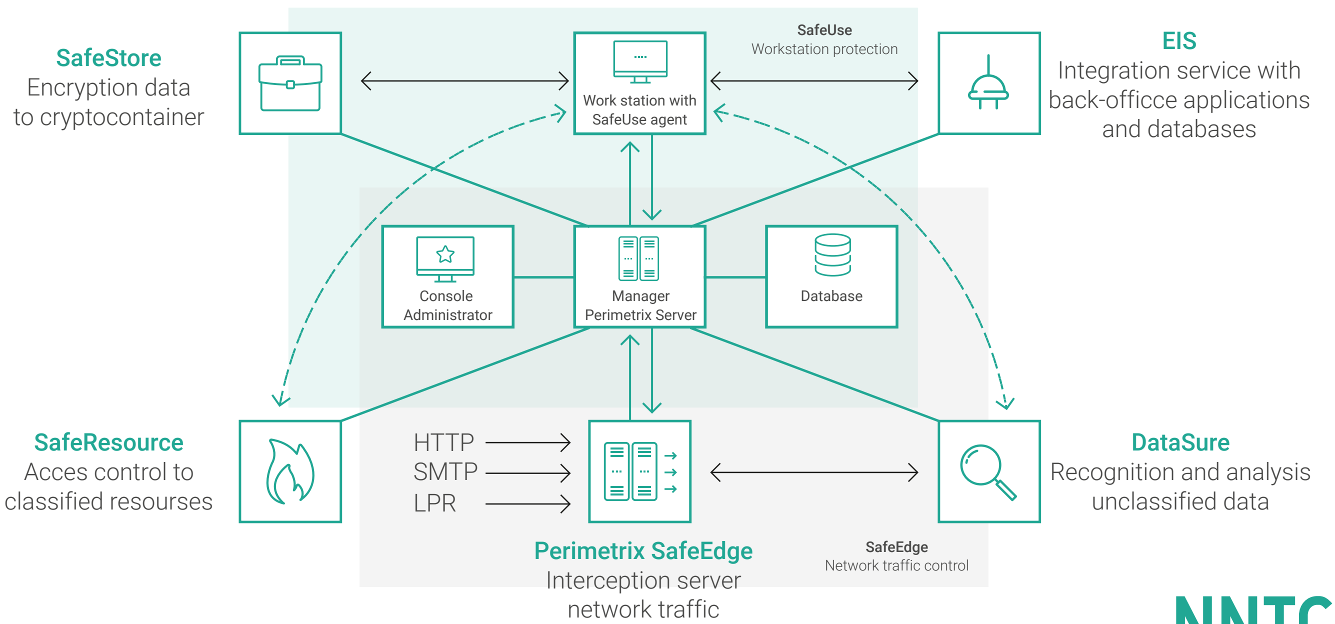
- Regulations for working with data
- Instructions for users
- Instructions for a security specialists

Organizational and administrative documentation is ready.

Stage 5
System trial and project delivery

Organizational and administrative documentation gets approval. The users of the enterprise are trained to work with the system. The system is applied to work resources. The customer's specialists independently perform maintenance procedures and make the necessary changes to the system.

THE MAIN SOFTWARE COMPONENTS



NNTC

GENERAL SOFTWARE AND HARDWARE REQUIREMENTS

Management console: web interface / Server part

- Processor: 2XCore2Quad Xeon, 1.6GHz, 2GB RAM,
- 500 GB HDD, NIC Ethernet 1000
- Any OS supporting JAVA
- Java JRE 6.0 update 7 or later
- Apache Tomcat 6.0.14 or later

Core Services Server

- Processor 2XCore2Quad Xeon, 2GHz, 4GB RAM, 500GB HDD, NIC Ethernet 1000
- Linux OS, Sun Java JRE 6u13

Client part

- Any workstation with client OS Microsoft Windows XP, Vista, Win 7, 8, 10
- Hardware requirements are determined by the operating system

DBMS server

- Processor 2xCore2Quad XEON 2 GHz, 4 Gb RAM, 2 Tb HDD, NIC Ethernet 1000
- Any DBMS with Hibernate support (Oracle, DB2, Sybase, MS SQL Server, PostgreSQL, MySQL, etc.)

Server for intercepting network traffic

- Processor 2XCore2Quad Xeon, 2GHz, 4GB RAM, 500GB HDD, NIC Ethernet 1000
- Linux OS, Sun Java JRE 6u13
- NetFilter libraries libnet, libnfnetlink, libnetfilter_conntrack

Various services can be deployed on one physical server or on several. The choice of the server hardware and the installation of the DBMS should be carried out according to the recommendations of the DBMS developer.

ADDITIONALLY WHEN USING THE MODULE SAFESTORE:

Server part

Cryptographic provider with Java Cryptography Architecture (JCA) support. CryptoPro JCP 1.0, Avest 1.01.RC3, Bouncy Castle (open source), and Sun's built-in JRE encryption providers are available.

Client part

Crypto provider with Microsoft CryptoAPI support. Libraries CryptoPro CSP 3.0 (meets the requirements of the legislation of the Russian Federation and is certified by the FSB and FSTEC) and Microsoft Enhanced Cryptographic Provider (included in the Windows distribution kit) are available.

Office G16, Block 13,
Dubai Knowledge Park, Dubai, UAE

+971 4 446 06 43
info@nntc.digital

nntc.digital

NNTC