perimetrix

PRODUCT BRIEF

MANAGING INTERACTIONS WITH CLASSIFIED DATA BY
PERIMETRIX SAFESPACE™

THE REALITIES

Today's Digital Life

— Working with confidential data on personal devices (BYOD, Bring Your Own Device), using traditional corporate end–point protection policies, is no longer applicable.
— Today's work environments require, among other things, full–fledged access to corporate data without being bound to a workplace or having to connect via a company's VPN network.

Business Virtualization

— Data goes to a cloud, where the security boundaries are unclear.
— Remote work is becoming the norm.
— More and more organizations are switching to virtual interactions between employees and partners.
— The exchange of electronic documents is no longer accompanying, but increasingly replacing how people communicate.
— There is a growing volume of confidential data being processed electronically.

> By 2017, 33% of office applications and messaging tools had been migrated to clouds. However, by 2022 this number is expected to nearly double to more than 65%.
>
> Gartner Group
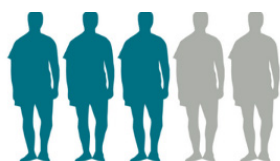
STATISTICS

In three out of five cases ↘

— incidents concerning confidential information are caused by employees or other trusted individuals (partners, outsourcers, etc.) who have authorized access the relevant data.

In half of the cases ↘

— the incidents are unintentional — due to errors, ignorance or negligence.

51%

> No one is immune from unintentional violators, even if the latter are trusted individuals.
>
> *«Insider Threat Report 2019»* by Cyber Security Insiders

perimetrix

Theft
Negligence
Compromise
Unscrupulousne
Third-party trans
Misappropriatior
Malicious intent
Sabotage

EACH BREACH MAY HAVE DIFFERENT
CAUSES, BUT THE CONSEQUENCES
ARE SIMILAR

WHAT PERIMETRIX IS AND WHY YOU NEED IT

applications and capabilities

1 SPECIALIZED SOFTWARE FOR MANAGING AUTHORIZED USER INTERACTIONS WITH CONFIDENTIAL DATA

2 DESIGNED TO PREVENT THE MISUSE OF CONFIDENTIAL INFORMATION

3 ALLOWS FOR THE ORGANIZATION OF DOCUMENT HANDLING ROUTINES BASED ON THE CATEGORY OF DATA AS WELL AS ITS ASSOCIATED PROCESSES

4 FLEXIBLY INTEGRATES INTO A COMPANY'S EXISTING FILE MANAGEMENT STRUCTURE WITHOUT CHANGING ESTABLISHED BUSINESS PROCESSES

OUR APPROACH
to safeguarding confidential information

CLASSIFYING
data and understanding the processes that it is associated with

«ZERO TRUST»
prohibiting all activities with confidential information unless explicitly authorized through policies

PRIORITY
Perimetrix protects business processes, not infrastructure

CONTINUOUSLY PROTECTING
information throughout every stage of its life–cycle through the inheritance of classification attributes

Why don't traditional protecting "everything from everyone" work

— Any probabilistic methods and models, sooner or later, cease being able to meet existing challenges and start reflecting the realities of life.
— It becomes necessary to constantly change business processes and to divert resources in order to maintain the operability of such security systems.
— The increased load on non–core business activities leads to the monopolization of IT resources.
— The solutions quickly become cumbersome and ineffectual.

perimetrix

WANTED
BY U.S. MARSHALS

> "
> Companies spend millions of dollars on firewalls, encryption, and secure access devices and it's money wasted because none of these measures address the weakest link in the security chain: *the people who use*, administer, operate and account for computer systems that contain protected information.
>
> ### KEVIN MITNICK

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0134-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone: (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSM0000.

Form USM-1
(Rev. 3/2/92)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

perimetrix

PROTECTING INFORMATION
at every stage of its life–cycle

SECURE HANDLING
OF CONFIDENTIAL
INFORMATION

Manual classification (assigning attributes) of files containing classified information

Automatic classification of files when exporting from a database or cloud

Automatic inheritance of classification attributes when creating different versions from an original

Automatic inheritance of classification attributes when compiling new documents based on existing ones

Data encryption when sending files via email or messengers

Data encryption for cloud storage or transfer onto physical media

Printing classification labels on hard copies when a classified file is sent to a printer
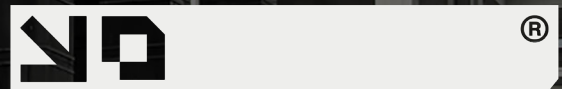
Decreasing the security level, removing from protected circulation (archiving, destruction)

perimetrix

perimetrix © 2021 Perimetrix LLC

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.

®