**PERIMETRIX**® Keeping Secrets Safe

Think of confidential information as the knowledge and data you have and others don't. This is the vital information that makes your business viable. In other words: secrets. When your secrets remain secret, your business prospers. Investors are confident, associates are satisfied, the government is content and you can focus on market share.

Your Company

Secrets

Investors 🙂

Partners 🙂

Government 🙂

Competitors 😠

Your secrets are the most valuable and yet vulnerable resource of your company, as they are open to misuse by those with the greatest potential to harm your business – the people who work for you. They have authorized access to company data, and can potentially use this information against you, resulting in loss of reputation, sliding share prices and key personnel looking for other options. Your competitors will value this gift.

Secrets

Your Company

Secrets

Secrets

Investors 😠

Partners 😠

Government 😠

Competitors 🙂
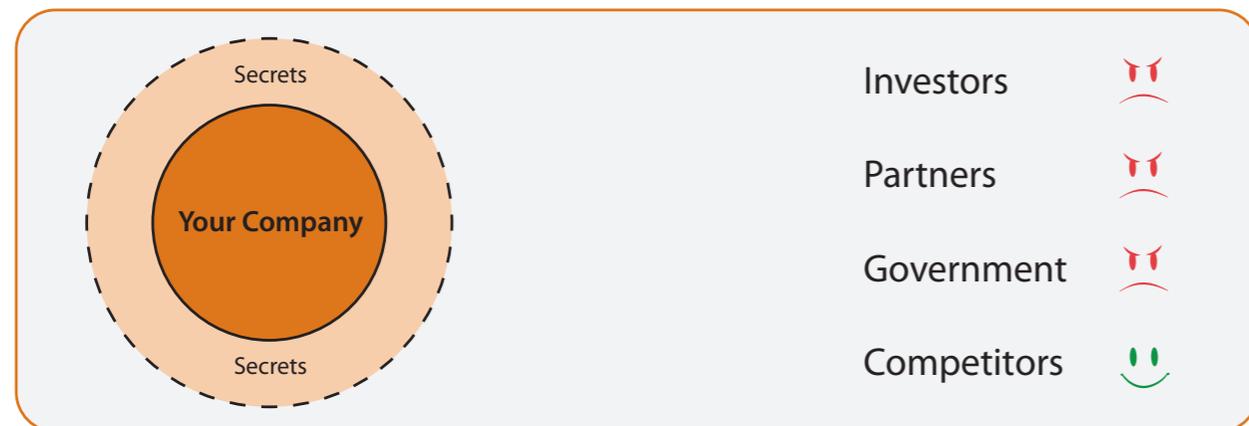
The violation of confidential information has dire consequences. Here are just a few examples:

- **2007:** A former employee of Boeing was exposed while criminally obtaining sensitive documents from the company, including documents which would potentially cost Boeing $5 billion to $15 billion if released to the competition;

- **2007:** Dai Nippon Printing, Japan, lost 8,62 million customer data items from 43 clients when a hard drive was stolen by a former subcontractor;

- **2006:** A laptop containing 382 000 employee record was stolen from Boeing, resulting in $146 million in direct costs to the company due to bank account monitoring;

- **2006:** Computer equipment containing 930 000 personal records, including Social Security numbers, was stolen from The American International Group Insurance Company.

Gartner argues that these losses could have been prevented by long-term vision and economic use of resources:

"A company with at least 10 000 accounts to protect can spend, in the first year, as little as $6 per customer account for data encryption, or as much as $16 per customer account for date encryption, host-based intrusion prevention and strong security audits combined. This compares with an expenditure of at least $90 per customer account when data is compromised or exposed during a breach."[1]

Sooner or later, your confidential information will be used against you in illegal and irresponsible ways unless you take measures to maintain your data integrity.

When customers lose confidence in your ability to sustain information integrity, they will find alternative service providers, resulting in a loss of profits and a tarnished image.

1 Avivah Litan, vice president and distinguished analyst at Gartner

You may feel confident that information leaks will never happen to you. Think about it. What would the consequences be if all your confidential information – databases, business plans, financial reports and agreements were made available to your nearest competitor or even published on the Internet?

Perimetrix® is an innovative software company which combines Russian technical ingenuity with Western-standard quality assurance, delivery and customer care.

Perimetrix® keeps your company's secrets safe and ensures that your dataflow remains in compliance with data protection regulations.

This is what we do.

This is all we do.

Are you feeling somewhat uneasy? You should.

Sadly, disgruntled employees form part of the team even in the best companies. One person may feel that he should have been promoted, but was not. Another is already planning to move to a competitor and is considering how best to strengthen his hand for negotiating a better position or salary.

There may be various reasons why it can be tempting to copy data if one has authorized access to confidential information. It is simple and quick to download data, and if the employee is discontented and feels unappreciated, it may not even seem like a crime to him or her.

There is more to consider.

Professional information thieves know how important your confidential information is to you and they have no qualms about probing large companies for vulnerabilities. In fact, they are doing it right now. They are well-equipped, well-organized and well-financed – after all – their business is highly profitable. Your defense strategies to protect your confidential data are irrelevant to them. They need to breach your business processes and they have the know-how to do it. They are also in the financial position to pay for inside assistance if the need arises.

Each industry is administered by its own regulatory body, e.g. Finance (Basel ll, GLBA, FACTA), Healthcare (HIPAA) and Public Companies (SOX, Combined Code). In addition, governmental regulations need to be considered (EU Privacy Directive, EU Directive on privacy and electronic communications, UK Data Protection Act, USA SA 1286, Japan Act on the Protection of Personal Information). Non-compliance can result in a loss of reputation, revoked licenses, company closure and even imprisonment.
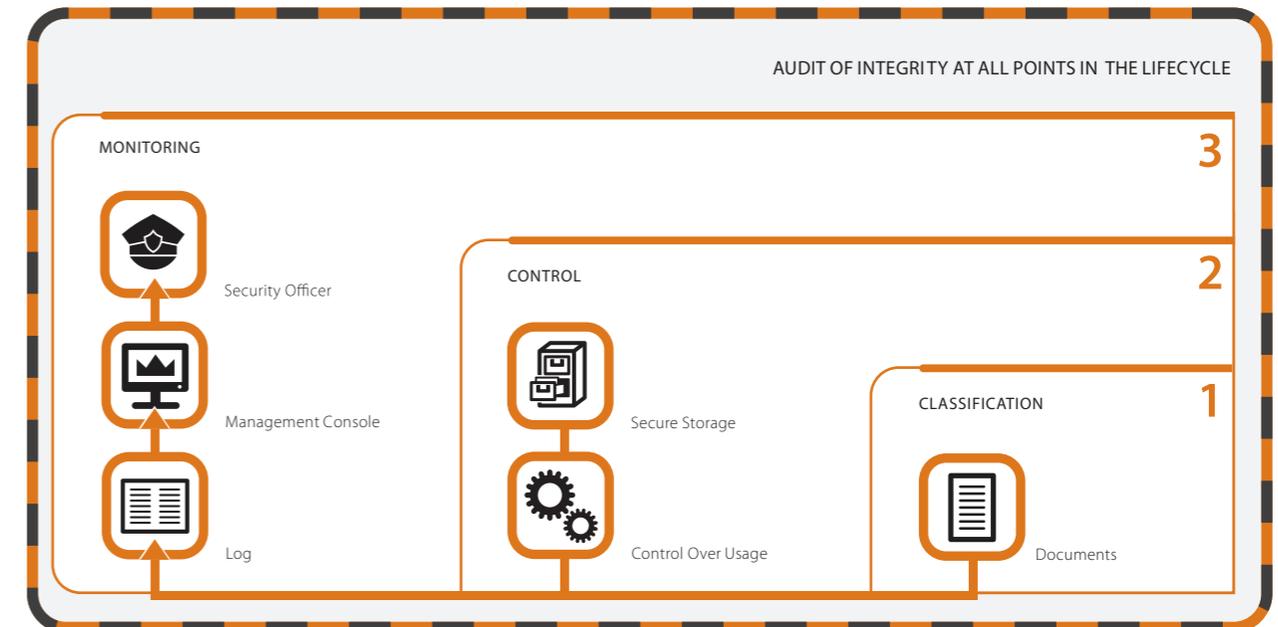
Perimetrix® has pioneered the 3rd generation in secret document integrity technology: the Perimetrix® Secret Documents Lifecycle™ (SDL).

3rd generation solutions represent a breakthrough in data integrity. Perimetrix® Secret Documents Lifecycle™ is a new approach which replaces merely attempting to plug the channels by which data enters and leaves the company datasphere with delivery of the data integrity you need where it truly matters: at the level of the data. It controls and monitors every confidential document from the moment it is created through to the moment it is finally deleted. No ifs. No buts.
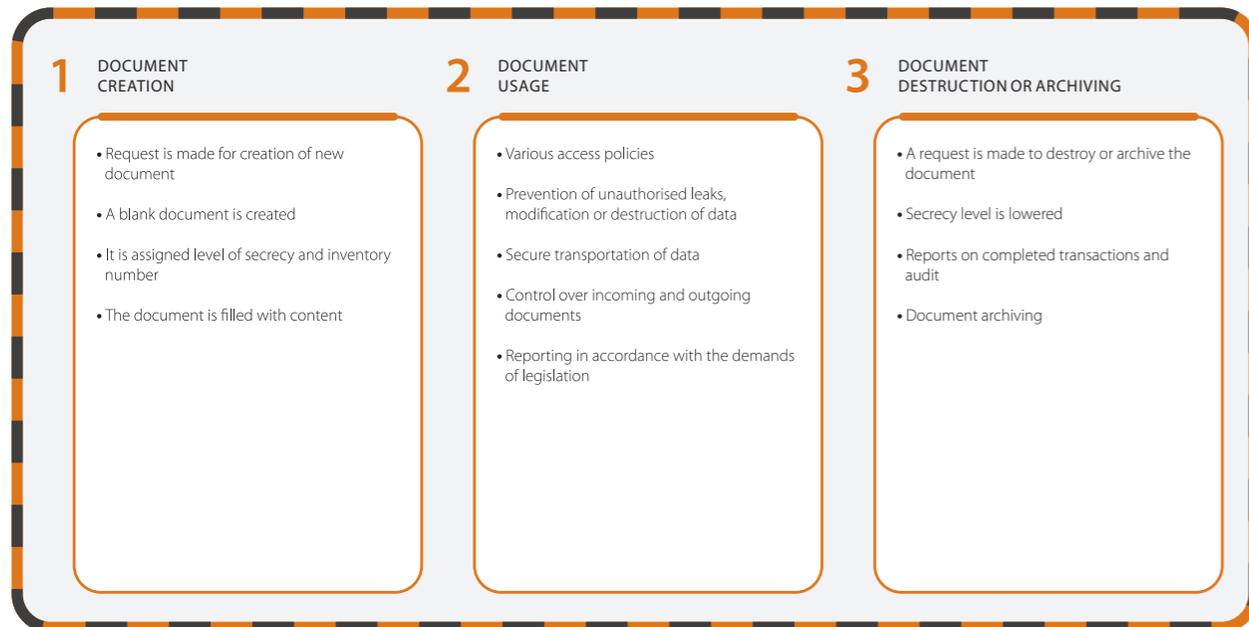
3rd generation solutions deliver air-tight data security and legislation compliance by means of a synergistic, five-prong approach:

1. **Classification:** classification and categorization (determining what needs to be protected);

2. **Control:** high-security data store and security clearance system of access;

3. **Monitoring:** action monitoring of secret documents right across the board (recording who did what and when, using a combination of verification of probability and deterministic methods);

4. **Notification:** real-time prevention and notification of attempts at violation;

5. **Audit:** audit-ready archiving of all data and actions for both legislative audits and retrospective analysis.

1 DOCUMENT CREATION

- Request is made for creation of new document
- A blank document is created
- It is assigned level of secrecy and inventory number
- The document is filled with content

2 DOCUMENT USAGE

- Various access policies
- Prevention of unauthorised leaks, modification or destruction of data
- Secure transportation of data
- Control over incoming and outgoing documents
- Reporting in accordance with the demands of legislation

3 DOCUMENT DESTRUCTION OR ARCHIVING

- A request is made to destroy or archive the document
- Secrecy level is lowered
- Reports on completed transactions and audit
- Document archiving

AUDIT OF INTEGRITY AT ALL POINTS IN THE LIFECYCLE

MONITORING

Security Officer

Management Console

Log

3

CONTROL

Secure Storage

Control Over Usage

2

CLASSIFICATION

Documents

1

Perimetrix® Secret Documents Lifecycle™
Perimetrix® Secret Documents Lifecycle™ is based on the "3 Ws" of all document actions: **who** did **what** and **when**, and this lies at the heart of Perimetrix® solutions. This full spectrum approach guarantees 100% protection of classified data in motion, data in use and data at rest, as secret documents (and documents that use any of their content) are moni-tored and controlled within the data perimeter from the moment they are created to the moment they are deleted.

Perimetrix® DataSure™
Perimetrix® DataSure™ provides unparalleled classified and unclassified data recognition, guaranteeing 100% docu-ment confidentiality and integrity. The Perimetrix® DataSure™ concept consists of two separate, but complementary approaches:

Perimetrix® DataSure^2
Perimetrix® DataSure^2 protects documents you have marked as classified by combining reactive (probabilistic) and proactive (deterministic) methods. This means that the best deductive methods available are working in tandem to monitor and protect classified information.

Perimetrix® DataSure^3
Perimetrix® DataSure^3 is a threefold approach which combines linguistic analysis, signature analysis and digital fingerprints. This combines the best targeted methods available and runs them simultaneously as background processes to identify potentially sensitive documents and include them in Perimetrix® SafeHouse™.

Perimetrix® SafeHouse™
Perimetrix® SafeHouse™ is a secret document storage facility which encrypts all data deemed confidential. Once a file has been added, it is protected – regardless of where you are – inside the company network or at home with your lap-top. Hardware theft – the primary cause of confidential data leaks – is no longer a threat to your company, since all se-cret documents are encrypted at all times when not directly utilized by a user with the appropriate security clearance.

Perimetrix® Expansion™
Perimetrix® Expansion™ is a platform-independent and scalable systems management solution. An additional server can be added to the cluster as the need for more processing power arises.

Each Perimetrix® product is founded on Secret Document Lifecycle™ methodology and is implemented either as a standalone or integrated solution.

Perimetrix® SafeStore™
Initial document classification and referential model, definition of secret material and locking it down in the data safe.

Protects: Data at rest.

Perimetrix® SafeUse™
Controls usage of secret documents by authorised em-ployees.

Protects: Data in use.

Perimetrix® SafeEdge™
Provides real-time monitoring of all documents which leave the network.

Protects: Data in motion.

Each solution can be implemented as a standalone product targeting your key challenges. However, the synergistic advantages of implementing the solutions together are apparent.

Three things you need to know about Perimetrix®:

- A lost or stolen laptop or other storage device will not constitute the loss of confidential information. The data has enforced encryption and access is available only to users with the appropriate security clearance
- The system learns from what you choose to mark as secret and automatically rates incoming and outgoing documents
- The Perimetrix® Secret Documents Lifecycle™ ensures that you will always know who did what to which document and when – from creation through to final deletion.

Why your IT department will love it:

- Scalable
- Platform independent
- Easy to integrate
- Easy to manage

Why top managers will love it:

- Dedicated management control console
- Off-the-shelf legislation compliance
- Easier IPO preparation
- Increased shareholder and client confidence

What makes Perimetrix special:

- 100% protection of classified information
- All data is encrypted by default and documents are made available to users on a 'need to know' basis
- Guarantees that your company is in compliance with even the most demanding aspects of legislation relating to data protection
- Prevents leaks across all channels. Once a document is secret-protected, it cannot be leaked, regardless of the channel.
- Perimetrix® offers the only extensive secrets-oriented business solution available. It controls document access and usage, while also maintaining integrity on the basis of classes which migrate to other documents based on them, by automatically transferring their security clearance requirements
- Improved business processes provide a built-in benefit
- Increases your reputation in any IPO or related event

All operations on company workstations are transparent

Perimetrix® controls all file operations at the operating system level, making all workstations and printer operations transparent. Dubious actions are stopped and logged, and the appropriate Security Officer is notified.

Data protection legislation compliance

Perimetrix® logs all network data transmissions. This not only facilitates easy investigation of insider activity, but also ensures that your company is in compliance with the relevant aspects of Basel II, SOX, GLBA and HIPAA.

Peripherals are kept inside

Writable CDs and DVDs, external hard drives, USB, COM, LPT, FireWire and IrDA devices, as well as Bluetooth and Wi-Fi wireless networks are valuable assets to your company. Perimetrix keeps it that way.

Even a stolen laptop cannot be used against you

Employees need to have the freedom to take data outside the office network when desired. You need to know your confidential information is safe when it leaves the office. Perimetrix provides this peace of mind.

No unauthorized information can leave your network via e-mail or Internet

Perimetrix® filters outgoing SMTP and Web traffic and blocks the unauthorized sending of sensitive content. Such incidents are flagged and relayed to a designated Security Officer.

## Your company's size and existing systems will never be an issue

Perimetrix® serves any network of over 500 workstations and uses network filter technology. It runs on the devices that you are already using.

All network operations are monitored, controlled and logged

Perimetrix® monitors all workstation, laptop, printer, backup and file operations for potential confidential information leaks. This provides you with the tools to prove **who** attempted a violation of **what** information and **when** – without leaving your desk.

You will know you made a smart investment

The costs associated with even an average confidential information leak commonly run into millions of dollars. The cost of a tarnished reputation is incalculable. You can save both if you make the right decision today.

For Notes
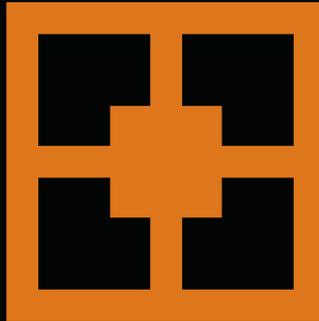
PERIMETRIX

PERIMETRIX® Keeping Secrets Safe

info@perimetrix.com | www.perimetrix.com