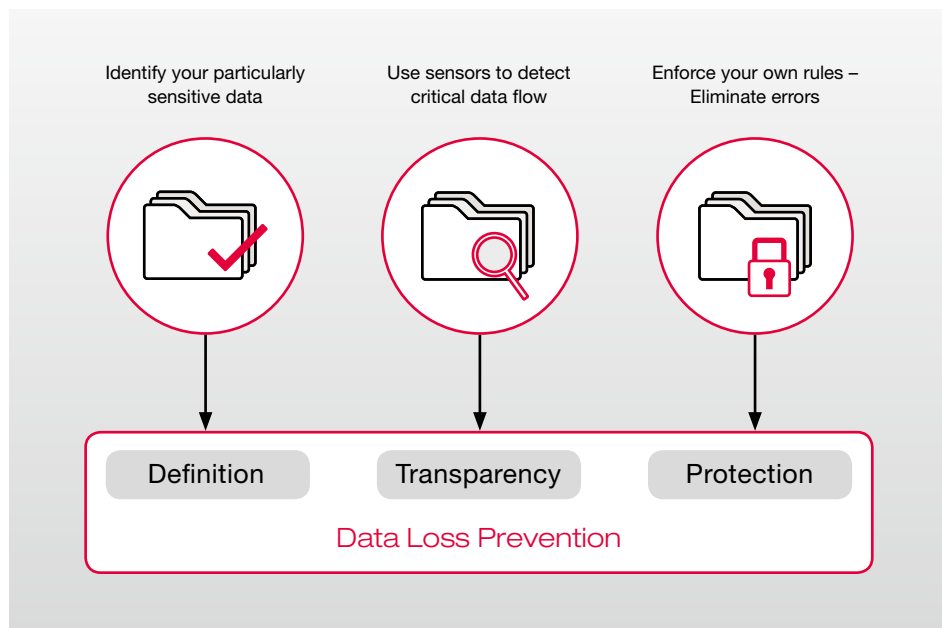


Taking Preventive Measures to Protect Sensitive Company Data



Benefits:

- » Across-the-board transparency regarding the security status of your sensitive data
- » You set the rules to determine critical data flows
- » Protective function is activated before your data flows out unintentionally

Every company has data that is worth protecting. For example, staff details or results from research and development. A mislaid laptop, an e-mail that has been sent to the wrong addressee (either in error or deliberately) or confidential data on a public network – whatever the cause of the leak, companies need to protect themselves. **One way of doing so is to implement a modern Data Loss Prevention (DLP) solution.**

But which solution is best suited to your needs and how do you set about finding the right balance between corporate data, data flows and rules? secunet will be pleased to advise you in this regard. Our IT experts will work in close collaboration with you, to evaluate your particular circumstances, and to design and implement a customised Data Loss Prevention solution that will intervene before any sensitive data flows unauthorised out of your company's control.

Offering comprehensive knowledge and skills in the field of information security and thorough familiarity with the DLP solutions currently available on the market, the experts at secunet will undertake a two-step process to design and implement a sustainable solution that will bring more transparency and control into the use of your sensitive data.

Phase I: Excluding avoidable risks

A holistic approach to Data Loss Prevention goes far beyond simple file encryption and regulations for USB ports. But even the simplest security

measures can have a major effect within the total package. First of all, you need to apply the easiest safety measures that are going to have the maximum effect. For example, memory encryption will minimise the damage caused by the loss of mobile devices (laptop, Smartphone, USB stick), because the data is no longer freely accessible. In the workplace itself, you can implement a central management solution that precisely determines which devices, services, interfaces and applications your employees require in order to perform their respective duties. Such a solution is quick to install and easy to operate.

The risk of data loss is thus reduced to a minimum. Within the environment you have defined, your employees can move data around freely and process it on their own authority.

During a busy working day, however, individual employees can often find it difficult to correctly assess the sensitivity of data. And so far, it has always been difficult to judge whether your instructions for the handling of sensitive data have been adhered to. With data flow control in Phase II, secunet creates the necessary transparency on the basis of which your instructions can be technically enforced.

Phase II: Creating transparency, enforcing data flow control

Identifying sensitive data

You decide on the data that should or must be protected. A sophisticated Data Loss Prevention solution identifies sensitive data according to different criteria that you select to suit your individual circumstances:

- Data formats, system structure, key words
- Specific labelling of individual data (areas)
- Intelligent learning from examples

The solution even earmarks for protection partial data that has been extracted from a wider context of sensitive data.

Monitoring the flow of sensitive data

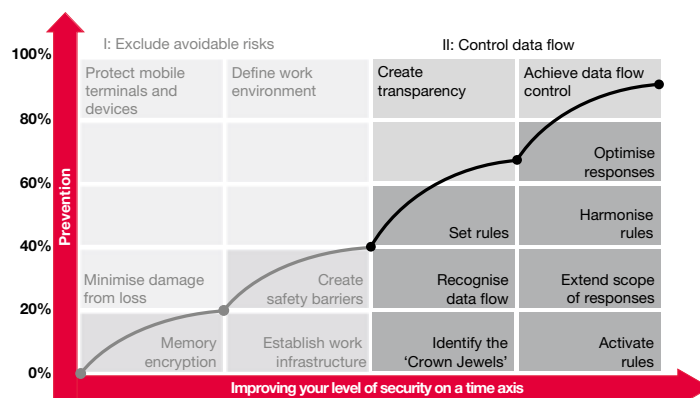
You specify what types of data flow are particularly critical and how sensitive information may be transmitted, stored and processed:

- Transmission pathways of data in the network (e.g. Web mail, Web services)
- Data storage (file servers, databases etc.)
- Data processing at the terminal

The solution uses special sensors to monitor the flow of your sensitive data. In this way, you receive instant feedback on the current security status.

Optimising prevention

If the solution is informed by the sensors that there is an impending breach of the rules in connection with your sensitive data, it will step in before your data can flow out. These responses are configurable, ranging at the lower end from warnings of possible breaches, primarily intended to raise staff awareness, through to actual blocking of data flow. By means of this protective function, you can demonstrably enforce your rules on dealing with sensitive data. And throughout, data flow will be permitted within company business processes while unwanted data leakage is prevented.



Your effective preventive solution with secunet

Benefit from the extensive knowledge and skills of secunet's IT security experts in the areas of data protection and information security. They will facilitate the rapid and effective implementation of your prevention project.

Our experts will advise and support you in deciding on

- the technical components
- the criteria so that you can effectively recognise which data is sensitive
- the sensors that are suitable for your business processes
- the rules for handling your sensitive data
- the appropriate responses to impending rule violations

With the support of secunet, you will acquire a flexible and effective Data Loss Prevention solution and achieve prompt and long-term all-round protection of your sensitive corporate data.

More information:
www.secunet.com/en/dlp



secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen, Germany

Phone: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-mail: info@secunet.com
www.secunet.com