EGOSECURE
ENJOY DATA PROTECTION

Whitepaper - Virtualisation

EgoSecure Data Protection in virtualised infrastructures

The Challenge

For several years companies have been developing virtualisation of the IT landscape. Virtualisation increases the flexibility of IT infrastructures, reduces space and energy requirements, and generally reduces IT costs. Other reasons for using virtualisation include the reduction of hardware resources and better utilization of server and storage systems. With increasing virtualisation, however, new dangers arise. Therefore, you should ensure that appropriate data protection and security standards are required in virtualised environments within companies.

What solutions for virtualisation are supported by EgoSecure?

EgoSecure Data Protection is generally offered on all common virtualisation solutions. Depending on the type of virtualisation, however, it should be noted that the range of functions can vary according to manufacturer and product. As a rule, the EgoSecure Data Protection solution is used on Windows Terminal Server, Citrix and VMWare products. This virtualisation must be based on Windows operating systems.

How is Access Control implemented in virtualised infrastructures?

The storage media used by the user on the Thin Client is passed through to the server and is collected by the EgoSecure rights management and summarized as the device type "Thin Client Storage Media". The EgoSecure agent recognizes external devices, which are directly connected to the server and also with the respective device class. The device type "Thin Client Storage Media" can also be equipped with no access, reading persmission or full access. Device access for “Thin Client Storage Media” (by hardware ID, etc.) is not supported by virtual environments due to the nature of a network path.
The Content Filter feature allows filtering for “Thin Client Storage Media” by file name and type using the Whitelist and Blacklist methods. Filtering by file size is not relevant in virtual environments.

How is Audit implemented in virtualised infrastructures?

The Audit module recognises storage media in a virtual session as the "Thin Client Storage Media" device type. Under this device class, you can see all data accesses in Audit that have been read, written, deleted or renamed. These data accesses are recorded with file name, size, path, date of modification, type and process of access according to the 4 or 6 eye principle. The EgoSecure agent recognises external devices that are directly connected to the server, with the respective device class. In contrast to the Thin Client device class storage media, devices attached directly to the server or client are supported with the Shadow Copy function for Audit.

How is Device Encryption implemented in virtualised infrastructures?

Based on the declaration as “Thin Client Storage Medium” by Citrix, Windows Terminal Server, VMWare and Co., detected devices are recognised as a kind of network drive / mapped device within the virtual session. Therefore, encryption of the “Thin Client Storage Media” is performed via the Network Share Encryption of the Folder Encryption module. The files encrypted in the respective folder of the mass storage device can be read or decrypted on a Fat Client using Device Encryption.
All files that were encrypted in the folder of the original Network Share Encryption using Device Encryption on a Fat Client, can also be read or decrypted on the Thin Client in the virtual session. Files outside these folders cannot be opened in virtual sessions.

Does EgoSecure Data Protection implement the module Application Control in virtualised infrastructures?

The Application Control of EgoSecure is also supported in virtual environments using the White- and Blacklist method. Application Control controls which user can start which programs. This avoids, for example, the use of games or unlicensed software products, resulting in liability risks and financial damage. Many viruses can also be blocked, usually even faster than antivirus solutions can recognize them.

EgoSecure – a simply beautiful solution

With EgoSecure Data Protection, the German security specialist EgoSecure has been the innovator in comprehensive data protection solutions for over 10 years. Not only compliance with current laws and industry norms are supported. Data is also secured at all endpoints, throughout the entire business process. EgoSecure is the first manufacturer in the world to combine the analysis of data and the corresponding protection modules in one solution. Both are closely linked by a management console, a database and an installation and administration concept. This guarantees quick installation and easy administration, as well as minimal training effort for users. Our motto: "We make the complicated things easy".