

## What exactly is the effect of CySCoS?

CySCoS is an effective measure to automatically isolate any software, which is entered into a system by means of the following vectors:

- Mobile storages,
- Internet-sites,
- E-mail-enclosures,
- Infected files,
- Networks,
- Data-interfaces

This prevents the execution of the malware listed hereafter, including any malware to be installed by them. This protection is independent of the malware's age or the time of induction, and thus provides protection against future versions of

- Viruses,
- Trojans,
- Worms,
- Ransomware,
- Rootkits,
- Bootkits

It is unimportant, whether malware is induced as contents of files, file-less, or encrypted. Even steganographically coded malware is safely blocked.

Recent events have shown, that CySCoS also prevents failures, which may be caused by exploitation of vulnerabilities concerning the processor function „speculative execution“. These have been reported early in 2018 to have caused financial damage, and were named

- Spectre and
- Meltdown

Thus, CySCoS may be an alternative to the expensive and time consuming development of processors, which do not possess this weakness anymore. Conventional processors work flawlessly within an CySCoS architecture.