What are the advantages of a hardware-based approach?

1. The vulnerability of most currently employed data processing systems is based on the hardware architecture of the programmable devices. Their basic design has not changed since last century's forties. Major omission was maintaining stand-alone computer attributes despite stronger demands due to
    - the use of external storage devices,
    - evolution of personal computers, and
    - connectivity via networks.

    This fact is not freely spoken about by the actors in the market place for different reasons:
    - By hardware manufacturers, because disruptive changes might endanger their
        - success in the market,
        - the required support by external software providers, and
        - the established links with their suppliers.
    - By software providers, because they might lose a prospering market niche: Anti-virus-software and the like.
    - By both, because the profitable mutual dependency might collapse.

    These reasons are augmented by the fact, that innovations, which remarkably change processes or structures of existing products, are rarely applicable with little effort or within short time.
2. It is expected that hackers will use quantum computers as soon as these will be available to them. This situation will probably render security measures vulnerable, which depend on binary data, like username, password, certificates, biometric data or encryption keys. The security gain achieved by applying CySCoS does not depend on such binary data and thus will not be biased by hacking them The most dangerous situation appears to be the remote take over of a user's workspace by a hacker. It is the administrators' responsibility to assign tasks and responsibilities within their systems to prevent loss or manipulation of data. CySCoS grants the required technical basics.