

REASONS FOR IMPLEMENTING SECULATION

WHITEPAPER

Every day, there are over 35,000 new viruses and malware in circulation. Professionally organised criminal groups can cripple your company with ransomware, which can lead to an existential threat. An Anti-virus software can only provide protection against the malicious software it recognises. According to the IT Trade Association BITKOM, newly developed or unrecognisable modified malware has caused over 50 billion Euros in damage just in Germany in the last year.



seculation
application whitelisting

HOW DOES SECULUTION WORK IN YOUR NETWORK

SecuLution works according to the "Whitelisting" principle, and thus effectively and reliably protects against malicious software by allowing only software that is recognised and necessary for the job. It is like having a bouncer at the door: Who is not allowed in, cannot cause any damage. You decide which software you trust. In this way, all malicious software is automatically classified as "unknown" and cannot be executed.

SecuLution also helps you to get an overview of your network, avoid costly licence penalties, simplify your patch management and prevent data theft and cyber sabotage with respect to data leakage prevention for USB removable devices.

Without additional administrative costs. Within a few months, this can lead to a positive return on investment.

CENTRAL DATABASE

- _ Security thanks to a database of permitted applications (Application control)
- _ Avert unwanted programs (ransomware, viruses, Trojans, games, unsafe or malicious programs) and be notified of any attempts to run software that is not allowed according to the Whitelist
- _ Protection against all unknown software
- _ Proactive: zero-second response time
- _ Zero signature or definition updates necessary
- _ Full control over applications. Define which user can execute which software
- _ Automatic version control of all applications through checksums (hashes/electronic fingerprint)
- _ Protection against data theft or malware threats via the USB whitelisting module, including activatable encryption

SIMPLE ADMINISTRATION

- _ Complete installation and integration is possible in five hours
- _ Whitelisting of updates can be automated
- _ Rule violations can be turned into a Whitelist entry, directly from the logs with just one click
- _ Learn mode allows fully automatic configuration
- _ Whitelist local caching for mobile users and protection against network and server failures
- _ Cloud-based software reputation service

MAXIMUM SECURITY

- _ Low configuration and administration costs with maximum security even against the most modern forms of attack

DETAILED LOGS

- _ Exporting of logs, reporting into network management system

→ POSITIVE ROI IN A FEW MONTHS

SecuLution GmbH

Alter Hellweg 6b
59457 Werl
Germany

+49 (0)2922 9589-210
info@seculution.com
www.seculution.com



seculution
application whitelisting