IKARUS security software

IKARUS scan.engine

Datasheet

Powerful algorithm for complex malware recognition

The IKARUS scan.engine is one of the world's best carrier grade scan engines and is fully supported and continually developed by IKARUS. It combats all kinds of cyber threats and malware with a range of defence technologies that work at multiple levels to locate, extract, analyse and eliminate viruses, weak points and exploits in virtually all filesystems, archives, and communication channels. You can integrate IKARUS scan.engine into your existing products, or use it to develop your own security products: the possibilities are endless.

One platform, many applications

The IKARUS scan.engine uses sophisticated and powerful scanning technologies to analyse all kinds of content. Its multi-architecture support includes Linux, Windows and Android platforms. The excellent recognition rates are achieved on all systems, and do not depend on a reliable internet connection. Special additional optimisations, adapted to specific mobile threats, are available for the Android environment.

Flexible recognition techniques for diverse communication channels

The IKARUS scan.engine has flexible, modular processes operating at multiple levels, which work autonomously on diverse content based on appearance, size, or file recognition. Thanks to the modularity, the processes are independent of the specific communication methods. All possible container types are supported: files, documents, archives... right through to disk image formats. Encrypted data in e.g. PDF files, Office documents and compressed archives can also be analysed by supplying password lists. The IKARUS scan.engine is also capable of extracting passwords from the content of an email.

Major advantages

- Platform independence
- Flexible data analysis module for diverse communication methods
- Multi-level heuristics and sandbox analysis techniques
- Resource optimisation → top performance

Multi-level heuristics and extended sandbox analysis

A sandbox environment developed in-house can be used for further analysis of suspicious content. The sandbox is a fully isolated virtual environment where you can carry out further inspections and analyse behaviour and supplementary results to identify harmful behaviours. The results are combined with other analyses to create a comprehensive overall evaluation for the sample being investigated. When using the SDK version of IKARUS scan.engine, detailed information can be obtained for all levels of the completed analysis – for example, file types and checksums. The IKARUS analysis team is continually extending IKARUS scan.engine and improving performance with manual analyses and reverse engineering. International threat data from the IKARUS SigQA (Signature Quality Assurance Program) and open communication within the antivirus industry also help ensure reliable threat recognition.

Optimised resource usage

The IKARUS scan.engine has been developed with constant attention to scalability and conservation of resources. With different operating modes (memory or disk-optimised) and an almost linear performance graph thanks to parallel threads, it is one of the highest-performance systems on the market.

IKARUS Sales Team | sales@ikarus.at | +43 1 589 95-500
IKARUS Support Team | support@ikarus.at | +43 1 589 95-400