IKARUS
security software

IKARUS
scan.server

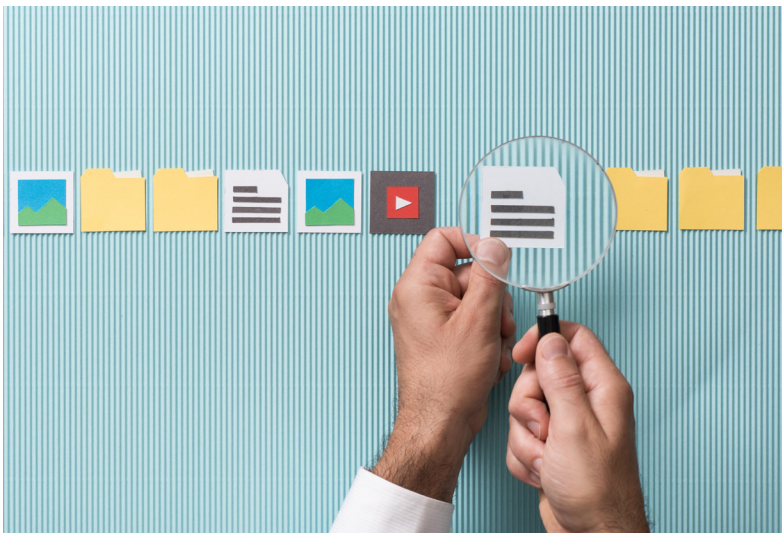
Datasheet

Your interface with the IKARUS scan.engine

Effectively and inexpensively secure gaps and vulnerabilities in your online services: Use the **IKARUS scan.sever** to scan all file transfers thoroughly for possible infections, thus reliably protecting your web services against attacks.

Close security gaps in your web services

IKARUS scan.engine finds and analyses malware - that is, files displaying malicious behaviour - in almost all files and archives: The service detects both known and emerging malware and allows you to neutralise it before it reaches your servers.



Allow your users or customers to upload files, such as photos, videos or application documents, without exposing your systems to unnecessary risks:
Use the **IKARUS scan.server** to automatically check all uploads for malware and other threats. The results of the malware analysis are output as an XML file and can be processed using any script languages. This way, attacks can be systematically fended off and infections can be cleaned up before they reach your systems or your data.

Product highlights

- Scanning of files (e.g. when uploading via web services)
- Reactive and proactive malware detection
- Result as XML response to request (VDB version, engine version, file name, status „clean“ or „infected“, signature name)
- Regular automatic updates to protect against current threats
- Compatible with all script languages
- Provision of a Java library for easier operation, can be used with any programming language