iQ.Suite Watchdog Sandbox

Features

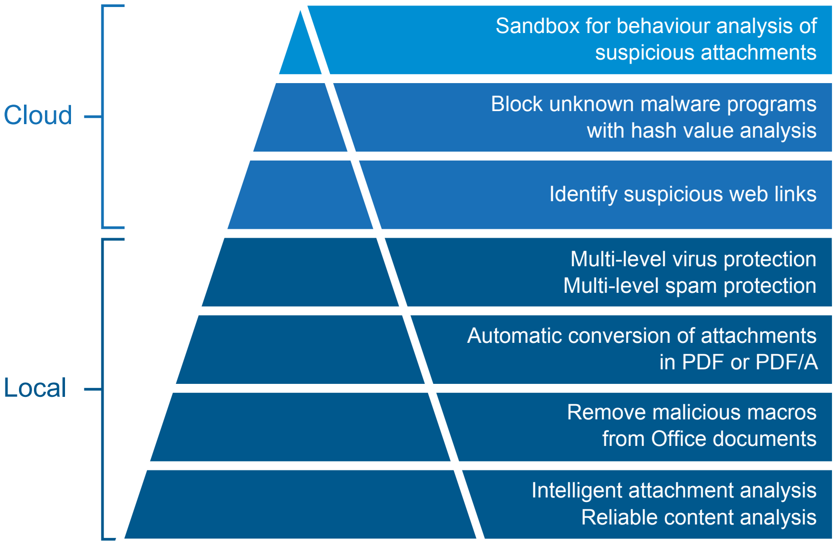
- Dynamic behaviour analysis of files and documents with executable contents
- Support for various operating systems *(Windows, Mac OS X, Android)*
- Detect malware camouflage techniques
- Select file formats to be analysed
- Supported file formats
  - *Executable files, e.g. EXE, COM and DLL*
  - *MS Office documents including macros, e.g. XLSX, DOCM and RTF*
  - *PDF documents*
  - *Archives, e.g. ZIP, RAR and CAB*
- Seamless interplay with virus scanners

Protection against new threats with sandbox behaviour analysis

Take a close look at malware behaviour

In times of sophisticated attacks, innovative technologies are needed to block new threats. Sandbox solutions get started where traditional virus scanners stop: Thanks to dynamic behaviour analysis, sandbox solutions can recognise malcode that is below the radar of conventional security solutions.

As part of our multi-level security solution, the sandbox technology in iQ.Suite Watchdog gives you exactly the edge you need to stay ahead of new attacks. Files and documents are tested for damaging behaviour under realistic conditions in a secure cloud environment. Malware that masks malicious behaviour or does not activate immediately is also identified. You are in control of which files are uploaded to the cloud and analysed. Imminent threats, such as crypto Trojans, often hidden in macros of Office documents, are recognised reliably.



Cloud

- Sandbox for behaviour analysis of suspicious attachments
- Block unknown malware programs with hash value analysis
- Identify suspicious web links

Local

- Multi-level virus protection
Multi-level spam protection
- Automatic conversion of attachments in PDF or PDF/A
- Remove malicious macros from Office documents
- Intelligent attachment analysis
Reliable content analysis

iQ.Suite Watchdog Sandbox

Cloud-based defence against cyber attacks

Benefits

- Protection against unknown malware
- Provision of comprehensive threat information
- Rapidly deployable from the cloud
- No cost-intensive local sandbox installation
- Easy to manage
- High performance
- Extensive reports

About GBS

GBS is a leading provider of solutions and services for the Microsoft and IBM collaboration platform.

More than 5,000 customers and 4 million users worldwide trust in the expertise of GBS.

Strong partners

To achieve best possible results and maintain high performance, it is recommended to use multi-level virus and spam protection as available in iQ.Suite Watchdog and Wall. The next step is to send the remaining unknown threats to the sandbox for comprehensive analysis.

These multi-level security mechanisms work hand-in-hand with the sandbox analysis und build the backbone of a well thought out security strategy.

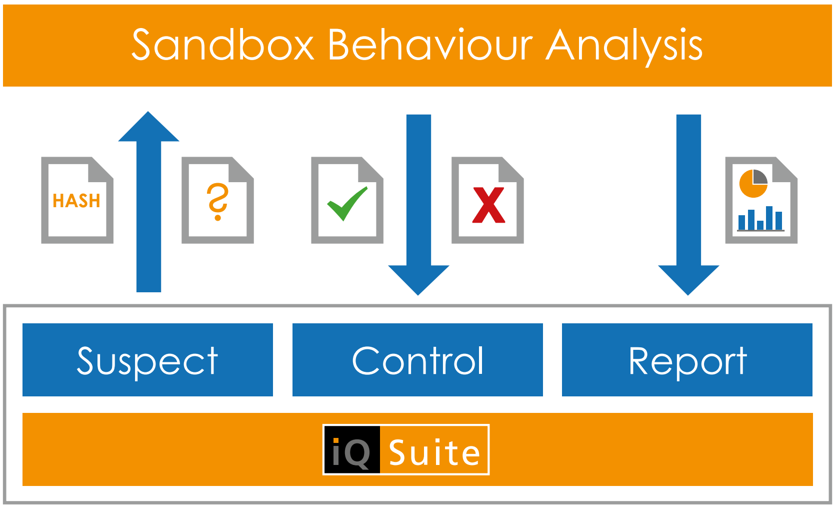
The 4 steps of Sandbox analysis

1 Hash values of suspicious files are compared to known malware (local/cloud).

2 If the file is known, in the case of a positive response it will be delivered and in the case of a negative response it will be placed in quarantine.

3 If the file is unknown, an anonymous copy of the suspicious file is sent to the sandbox, executed in a secure cloud environment and analysed. Depending on the evaluation, the file is either delivered or rejected.

4 In the last step, forensic reports are created for every incident, providing additional insight and context information.



Whether Microsoft Exchange/SMTP, Office 365 or IBM Domino: With the flexible cloud-based sandbox for iQ.Suite Watchdog, you have optimum protection against new threats.