noSpam proxy® SERVER

# 32Guards Sandbox

Version 15

Net at Work
Building IT-Excellence.

## Legal information



Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Germany



**THIS DOCUMENT WAS LAST EDITED ON DECEMBER 11, 2024.**

# Content

# 32Guards Sandbox

## Best possible protection with NoSpamProxy

The 32Guards Sandbox is an additional option for NoSpamProxy Protection. In addition to the concept of content disarming and consistent rejection in the event of a lack of trust in senders, it offers you a further protective component.

Using the 32Guards sandbox significantly increases the probability of detecting new viruses.

## What is a sandbox?

A sandbox is a complex system to which files are passed for inspection. Unlike a traditional virus scanner, it does not only check whether the file is already known as a virus or not. A sandbox executes the file and monitors it. This is called "detonating".

For this purpose a virtual computer is installed and booted. Then the file to be scanned is copied to this virtual machine and detonated. Now the most important task of the sandbox begins: It must observe what happens in the computer. The sandbox can then draw conclusions about the malware content of the file from the observed behaviour.

## Challenges

Some types of viruses can detect whether they are running in a sandbox or on a "real" computer. This is called **Hyper-Evasive Malware**. This is made possible, for example, by recognizing the **hooks** mentioned above. So the malware tries to find out if it is being watched and in what environment it is currently running. To do this, it accesses the main memory, for example, and observes the reaction that then follows.

If the malware feels comfortable, it may wait a while before performing its actual task, or it may wait for an action that only a real user would take. With a Word document, a malware could wait until text is entered and the "Save" button is pressed. Mouse movements are also detected by the malware and are evaluated positively accordingly.

All this must be able to simulate a good sandbox. This also means that, just as with conventional virus programs, there is the famous hare and hedgehog game: the sandbox operators try to disguise themselves in the best possible way, while malware manufacturers try to look around and protect themselves in the best possible way.

Another problem is the file type used. Sandboxes can usually detonate all kinds of executable files, Office documents, PDF documents and ZIP archives, but in some cases they reach their limits. So at this time hardly any sandbox will be able to detonate an AutoCAD file.

# Operating principle

## Principle

The sandbox first analyses the file type. Depending on the type detected, it then commissions several virtual computers, each with different operating systems and different application versions installed - for example, Windows 7 or 10 and Word 2010 or Word 2016.

The file is copied to each virtual computer and detonated there. This is done because in many cases malware has specialized on certain versions or shows different behaviour in different versions. As a rule, however, no more than three or four different environments are used, as the computing effort would be too high. In addition, there are also challenges with regard to Microsoft licensing.

In order for the sandbox to be able to observe the virtual computer, it uses so-called **hooks**. A hook can be compared to a microphone or a surveillance camera installed in a room. The **hooks** allow the sandbox to recognize what is written and read on the virtual machine's hard disk. It also recognizes if and which network connections are established where, which changes are made to the registry or start-up environment and much more.

For example, if changes are made to the registry when a Word file is opened or files are downloaded from an Internet address, it is highly likely that the file is malware. It is important here that the result always expresses a probability. If a URL is called that is already known to be malicious, the probability is very high.

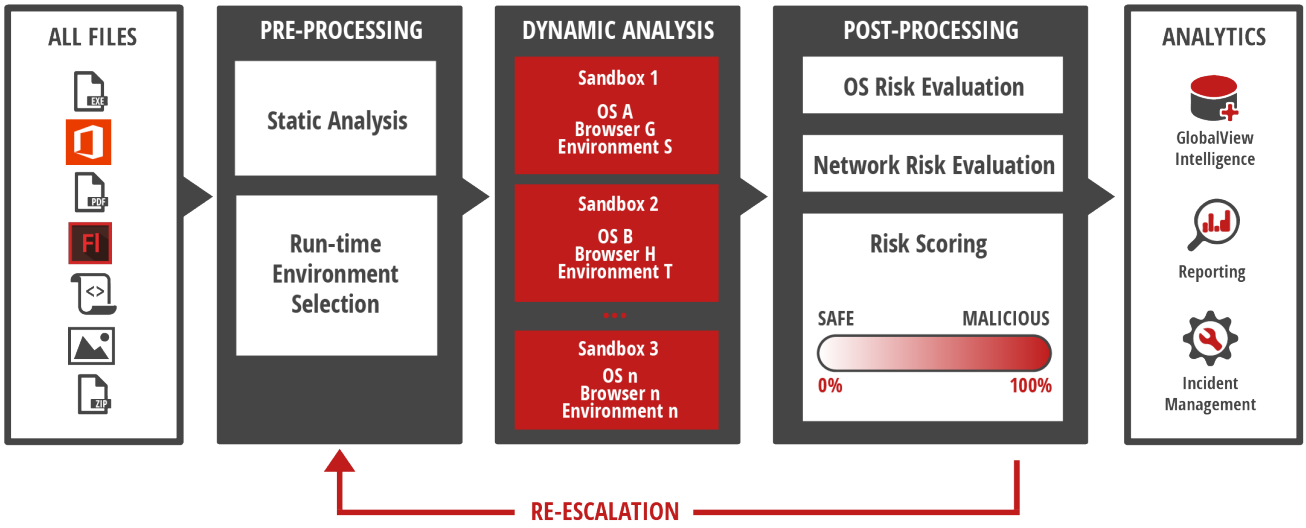
# Procedure

The 32Guards sandbox analyses files, URLs and **command & control traffic**. The latter describes the exchange of data between an infected computer and its "master" in the network, from whom it receives new commands.

Before a file is uploaded from NoSpamProxy® to the sandbox, NoSpamProxy® creates a hash value and asks the sandbox if it already knows the hash. If the hash is known, it is also queried whether the hash is good or bad. This is referred to as Level 1 (hash query) and Level 2 (file upload).

The files to be checked are transmitted and checked in encrypted form. To make the testing process as efficient as possible, an expected behavior is predicted based on the file type (static analysis) and an environment optimized for this prediction is run up (dynamic analysis). Only if the expected behavior does not occur will additional virtual machines be provisioned (post-processing).

As soon as a file or URL is recognised as bad, a fingerprint of the respective object is created.



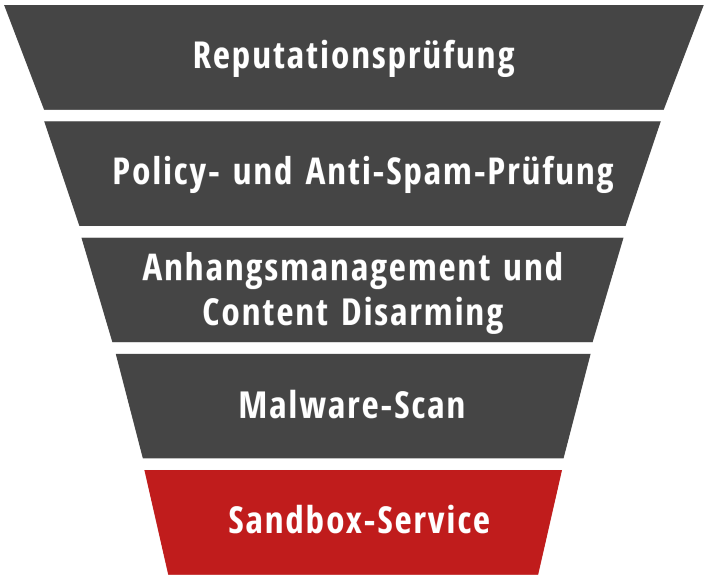

*Quelle: Cyren*

# Licensing and data protection

The 32Guards Sandbox must be additionally licensed. The license is based on the number of users licensed by NoSpamProxy Protection. NoSpamProxy Protection is the basic requirement for using the 32Guards Sandbox. A separate licence key is created for the sandbox, which is integrated into the existing licence.

# Limitation of analyses

The number of complete analyses by the 32Guards Sandbox is limited to 20 per user and month due to the high resource requirements. The billing is not user-based. For example, with 100 users, a total of 2000 complete analyses can be performed, regardless of how many analyses are performed by each user. We recommend that our customers configure the filters in NoSpamProxy so that the 32Guards sandbox only checks emails if they have not already been rejected by upstream filter levels.




Overview of the filter levels in NoSpamProxy

# Test operation

To test the 32Guards Sandbox, a corresponding licence key is required, which can be obtained from the sales team at NoSpamProxy®.

By default, the trial period is limited to 30 days.

## Configuring the 32Guards Sandbox

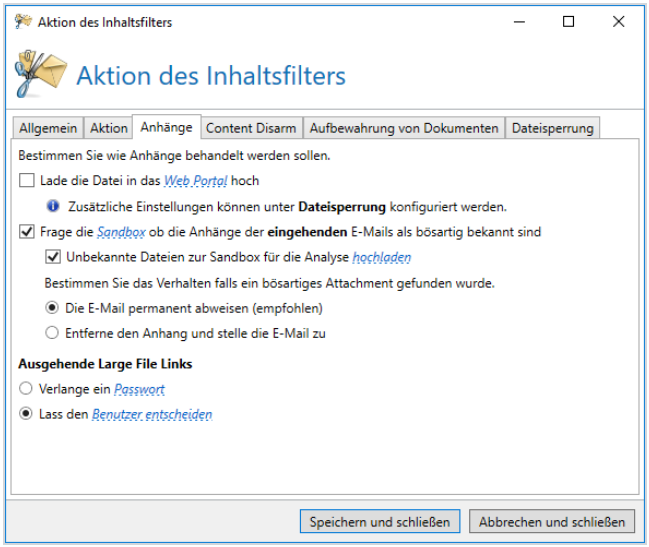
This feature is available if you have licensed the **32Guards Sandbox**.

## Option 1: Adapt an existing action

### Option 1: Adapt an existing action

1. Go to **Configuration > Content filter > Content filter actions**.
2. Open an existing action for inbound emails.

3. Switch to the **Attachments** tab.




4. Check the box next to **Query the sandbox if attachments of inbound emails are known to be malicious**.

> If this option is activated, NoSpamProxy compares the hash values of attachments with hash values already in the sandbox database. The retrieval of the hash values is unrestricted and without deduction of purchased licences.

5. **Optionally**, tick the check box next to **Upload unknown files to sandbox for analysis**.

> If this option is activated, files unknown to the sandbox are uploaded to the sandbox for analysis. The upload of files is limited to 20 files per user and month. See **Configuring the 32Guards Sandbox**.

6. Select either **Reject the email permanently (recommended)** or **Remove the attachment and deliver the email**.

> **NOTE:** The Sandbox Service is only available if you have selected **Allow attachment** on the **Action** tab.

# Option 2: Create a new content filter action

### Option 2: Create a new content filter action

Creating a new content filter action is particularly useful if you want to restrict the sandbox check to individual file types.

1. Go to **Configuration > Content filter > Content filter actions**.
2. Click **Add**.
3. In the **General** dialog box, enter a name for the new action and select **SMTP emails**.
4. In the **Action** dialog box, select **Allow attachment**.
5. Make the settings for the sandbox as described above for the **Attachment** tab.

6. Make all other settings for the new action as desired.
7. Click **Finish**.

You now have to trigger the adjusted or newly created action via a content filter entry.

## Supported file types

### General

- Executable files
  - Executable files for Windows
- Microsoft Office
  - Microsoft Excel (all)
  - Microsoft PowerPoint (all)
  - Microsoft Word (all)
- Text
  - HTML
  - PDF document
  - PDF document with URLs
  - Rich text format
  - Rich text format with OLE objects

- Scripts
  - .js
  - .vbs
  - .ps1
- Archives and compressed files
  - 7Zip-compressed file
  - ACE-compressed files
  - AR-compressed files
  - ARJ-compressed file
  - BZIP2-compressed files
  - GZIP-compressed file
  - RAR-compressed files
  - TAR-compressed files
  - Windows Installer file
  - ZIP-compressed file
  - *.alz
  - *.cab
  - *.z
  - *.zoo

**NOTE:**

We strongly recommend using an allowlisting approach to content filtering. This recommendation applies in particular to the use of the 32Guards sandbox.

An example: Even if an "Executable file for Windows" is supported by the sandbox, the question arises whether one wants to allow this potentially dangerous file type for one's own company at all. In this case, it makes more sense to generally reject this file type and thus also save the upload to the sandbox.

If a file is classified as unsuspicious by the 32Guards sandbox, the respective email is delivered.

## Delivery delay

When a file is uploaded to the sandbox, the email is not accepted in the first step but temporarily rejected so that the sending email server delivers it again. Temporary rejection is used here because the analysis takes a certain amount of time, but this should be completed after around five minutes when the next delivery attempt is made.

This means a delivery delay for the delivery, which must be observed accordingly. Thus, we recommend that you carefully check which files should really be sent to the sandbox. Note the following option if time-critical processes or mailboxes exist in the company:

- Is a sandbox hash query sufficient instead of a full analysis (sandbox upload)?
- It is possible to create different actions in the content filter to configure different actions for "Trusted emails" and "Untrusted emails". Here you can distinguish between a sandbox upload and a sandbox hash query.
- Office documents can be converted into a secure PDF document by Content Disarm and Reconstruction (CDR) if necessary. See **Hinweise zu Content Disarm and Reconstruction (CDR)**.

## Further information

**NOTE:** The number of complete analyses (sandbox upload) by the 32Guards sandbox is limited to 20 per user and month. The billing is not user-based. For example, with 100 users, a total of 2000 complete analyses can be performed, regardless of how many analyses are performed by each user. We recommend that you configure the filters in NoSpamProxy® so that the 32Guards sandbox only checks emails if they have not already been rejected by upstream filter levels. If the limit is exceeded, additional costs may be incurred.

**TIP:** To restrict the 32Guards sandbox check to individual file types, an additional content filter action should be created that is only applied to certain file types.

# Help and support

### Knowledge Base

The **Knowledge Base** contains further technical information on various problems.

### Website

The **NoSpamProxy website** contains manuals, white papers, brochures and other information about NoSpamProxy.

### NoSpamProxy Forum

The **NoSpamProxy forum** gives you the opportunity to exchange information with other NoSpamProxy users, get tips and tricks and share them with others.

### Blog

The **blog** offers technical support, tips on new product versions, suggestions for changes to your configuration, warnings about compatibility problems and much more. The latest news from the blog is also displayed on the start page of the NoSpamProxy Command Center.

### YouTube

On our **YouTube** channel you will find tutorials, how-tos and other product information that will make working with NoSpamProxy easier.

## NoSpamProxy Support

You can reach our support team

- by phone at **+49 5251304-636**
- by email at **support@nospamproxy.de**.