SANDBOX PROTECTION

WHAT IS A SANDBOX?

In the cyber security world, a sandbox is a testing environment in which new or untested code can be run, and it's behavior securely analyzed without risking damage to the computer or the network. Sometimes it could be a zero-day exploit, whose effects are not yet known. For this reason, it is crucial that the sandbox does not have any access to the network.

Sandboxes are indispensable for analyzing malware and blocking it's spread before it becomes a global threat. By using sandboxes, cyber security experts can understand how malware works, what effects they have, and then try to make it harmless.

As part of our Email Security solution, **Libraesva Sandbox Protection** provides an innovative and pragmatic approach based on AI and Machine Learning technologies, which continually detect and adapt to new attack patterns, and analyze and block advanced threats targeting businesses.

/LIBRAESVA

EmailSecurity

Libraesva **Sandbox Protection**

☑ URLSAND SANDBOX

The Libraesva URLSand Sandbox provides unique predictive analysis in order to block new, unknown, and targeted threats found in embedded email URLs. In doing so, businesses are protected against phishing, spear-phishing attacks, zero-day exploits and ransomware.

• How does it work?

Libraesva Email Security re-writes every URL that reaches company mailboxes. Everytime the user clicks on a link, URLSand Sandbox visits the requested page and checks for suspicious behavior. This means that Libraesva URLSand Sandbox is not just a time-of-click additional blacklist check, but it's a comprehensive page scan, detecting deeply nested malware and suspicious pages looking at obfuscated content and following all redirects.

hiips://urlsand.esvalabs.com

Cloud-Based Sandboxing Technology

SAFE SITE

User is redirected to the original website

DANGEROUS SITE

User is alerted with a blocking email

BENEFITS

CLOUD SANDBOXING:

thanks to the next-generation sandboxing functionalities, our cloud sandbox analyzes the requested page deeply, looking for hidden threats and redirects with a real-time cloud check

WHOLE PROTECTION:

with URL's being re-written before delivery to the email platform, checks and verification occur regardless of the device used to access the links

ADVANCED MALWARE DETECTION:
Artificial Intelligence and Machine-Learning are used to detect malware traditionally missed by signature and reputation-based solutions

INCLUDED IN EMAIL SECURITY:

the URLSand Sandbox is included in every subscription of Libraseva Email Security at no additional cost

FULL URLSAND WHITELABEL OPTION:

the URLSand Sandbox is available to be fully white-labeled with custom sandboxing URLs and branding

Libraesva **Sandbox Protection**
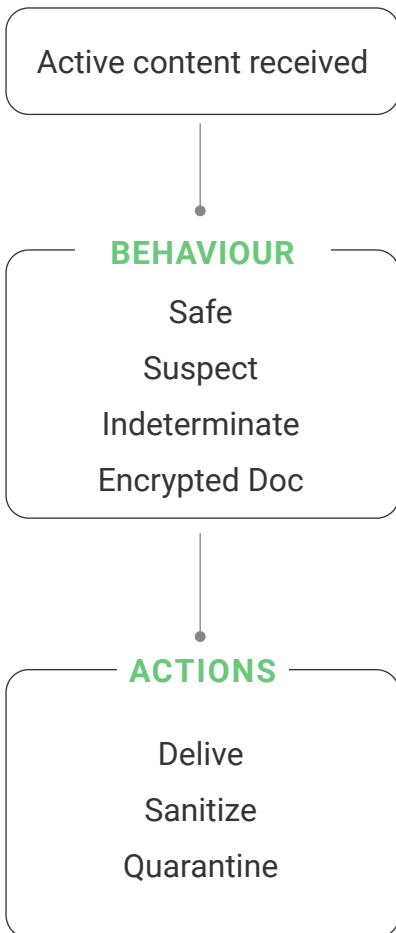
☑ QUICKSAND SANDBOX PROTECTION

The Libraesva QuickSand Sandbox delivers protection against known and unknown threats hidden in all Microsoft Office Documents, RTF, and PDF files by cleaning or purging files of dangerous active content, distributed as email attachments by cyber-criminals.

• How does it work?

Libraesva QuickSand's innovative technology uses sophisticated techniques in order to evaluate advanced threats that are traditionally missed by signature and reputation-based solutions.
Based on the analysis result, you then have the option to either remove the active content and deliver the sanitized document or to block the entire document.
The analysis takes place entirely at the gateway, without disclosing any documents to anyone. In doing so, all data is kept safe at the gateway.

BENEFITS

DOCUMENT DEEP SCAN

Active content received

BEHAVIOUR

Safe
Suspect
Indeterminate
Encrypted Doc

ACTIONS

Delive
Sanitize
Quarantine

GATEWAY SANDBOXING:
protecting your data means keeping it private and secure. The analysis carried out with Libraesva QuickSand takes place at the gateway with it's high efficiency and low resource requirements

ZERO RISK FILE SANITIZATION:
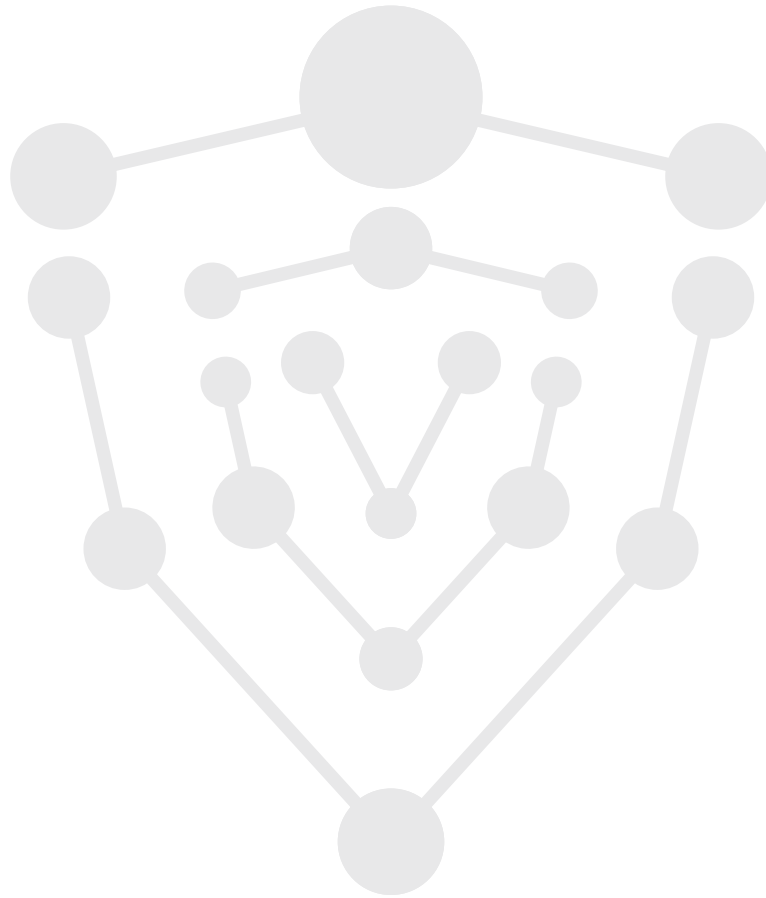deliver only safe and risk-free files

EVASION TECHNIQUE RESILIENT:
QuickSand is highly resilient to evasion techniques due to the pragmatic and more common approach to securing files. Libraesva focuses on removing the delivery mechanisms of advanced malware, instead of looking at the forensic or "ones and zeroes" of the file

INCLUDED IN EMAIL SECURITY:
the QuickSand Sandbox is included in every subscription of Libraseva Email Security at no additional cost

/LIBRAESVA

Libraesva Srl

P.zza Cermenati, 11
23900 Lecco
ITALY

Libraesva Limited

Spaces, 9 Greyfriars Rd
Reading RG1 1NU
UNITED KINGDOM

Web sites | email

www.libraesva.com | www.phishbrain.net | sales@libraesva.com