ilger.com
open source collaboration

zimbra A SYNACOR PRODUCT BUSINESS SERVICE PROVIDER PLATINUM PARTNER
zimbra A SYNACOR PRODUCT VALUE ADDED RESELLER GOLD PARTNER
zimbra A SYNACOR PRODUCT CERTIFIED TRAINING CENTER GOLD PARTNER

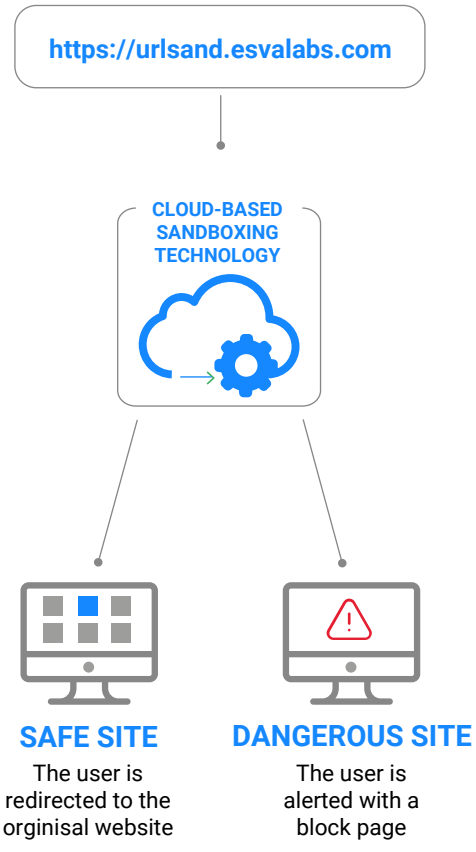
PRAGMATIC DEFENSE AGAINST MALWARE

URLSAND SANDBOX

The URLSand Sandbox detects new, still unknown and targeted threats found in embedded email URLs, actively blocking those to protect against spear-phishing attacks, zero-day exploits and ransomware. Every URL, not only uncategorized ones, in every email, is checked everytime the link is clicked, not when the email is received.

HOW DOES IT WORK?

All email links are rewritten to point to the Libraesva URL Sandbox. Libraesva Email Security Gateway re-writes every link and the URLSand Sandbox visits the requested page and checks for suspicious behaviours and malware when the user clicks, URLSand will then make a decision based on these results and either redirecting the user to the clean site, or blocking them entirely.



BENEFITS OF URLSAND

01 **CLOUD SANDBOXING**
Thanks to the next-generation sandboxing functionalities, email are constantly analysed with a real time cloud check

02 **DEVICE AGNOSTIC**
Links being re-written before sent to email clients allow checks and verification of links to be done regardless of device used to access links.

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

04 **INCLUDED IN EMAIL SECURITY GATEWAY**
The URLSand Sandbox is available for all customers at no extra cost, included in every subscription of Libraseva Email Security Gateway.

05 **FULL URLSAND WHITELABEL OPTION**
The URLSand Sandbox is available to be fully whitelabelled with custom sandboxing URLs and branding.

QUICKSAND SANDBOX

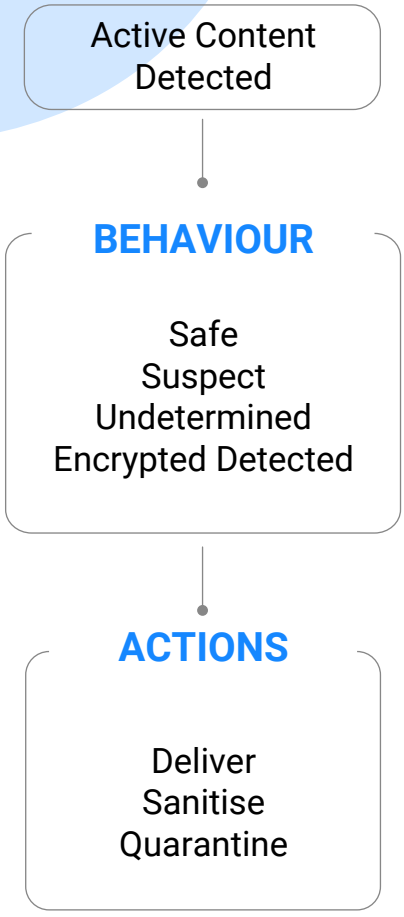
Libraesva QuickSand Sandbox uses sophisticated techniques to evaluate advanced threats traditionally missed by signature-based and reputation-based solutions. It is effective against all Microsoft Office™ documents, PDFs and RTF files even when compressed into an archive.

HOW DOES IT WORK?

Libraesva QuickSand Protection uses sophisticated techniques to evaluate advanced threats that are traditionally missed by signature-based and reputation-based solutions.

Defending your data means keep it secure and private. Libraesva's innovative zero-day threat sandboxing takes place entirely at the gateway, without disclosing any documents to anyone! No cloud sandboxing environments are involved in this process, all data is kept at the gateway.

DOCUMENT DEEP SCAN



BENEFITS OF URLSAND

01 **GATEWAY SANDBOXING**
Protecting your data meanskeeping it private and secure without it leaving the network, the analysis carried out with QuickSand is all done on the gateway due to its high efficiency and low resource requirements

02 **ZERO RISK FILE SANITISATION**
Deliver only safe, risk free files. By removing active content from Microsoft Office 365, PDF and RTF Files. Removing all the tools attackers need to access your systems.

03 **EVASION TECHNIQUE RESILIENT**
QuickSand is highly resilient to evasion techniques due to the pragmatic and more common sense based approach to securing files. Libraesva focuses on removing the delivery mechanisms of advanced malware, instead of looking at the forensic or "one's and zero's" of the file.

04 **INCLUDED IN EMAIL SECURITY GATEWAY**
The QuickSand Sandbox is available to all customers at no extra cost, included in every subscription of Libraesva's Email Security Gateway