ilger.com
open source collaboration

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

SANDBOX PROTECTION

WHAT IS A SANDBOX?

PRIVATE CLOUD
Private cloud instance

PUBLIC CLOUD
AWS or Azure

ON PREMISE
Virtual appliance for VMware, Hyper-V, XenServer and more

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, **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.

RESPOND TO ATTACKS

Understand the threat landscape and attacks launched against your organization, deal with security incidents faster, and see how you compare against others around the world.

- Gain full visibility of email traffic and trends, with the volume, types and sources of attacks, including emerging and zero-day threats
- Proactively provide KPIs and dashboards so stakeholders understand the risks, and plan intelligent mitigation strategies using insights previously hidden in email data
- Remediate attacks simply, with one-click removal of malicious emails identified post-delivery from all recipients. Threats can be deleted completely or moved to a secure location for further analysis

CONTROL EFFORTLESSLY

Simply manage all aspects of email security from a single intuitive console.

- Easy to follow workflows make it painless to change configuration settings
- Manage emails and quarantine on the go with the Android and iOS mobile app

DEPLOY FLEXIBLY

Rapidly deploy in under 30 minutes in your choice of IT environment

- Available for cloud, on-prem and popular hypervisor platforms
- High availability option with active-active clustering support
- Or choose a fully managed cloud security service from authorized Libraesva MSSPs to skip managing the IT environment altogether

ADVANCED THREAT PROTECTION DEFENDS YOU AGAINST...

- ✓ Spam
- ✓ Malware
- ✓ Phishing
- ✓ Email fraud
- ✓ Zero-day threats
- ✓ Account takeover
- ✓ Social engineering
- ✓ Business email compromise
- ✓ Inadvertent disclosure of sensitive information

ilger.com S.r.l.
Piazza Italo Pinazzi, 47/a
43122 Parma (ITALY)
P. +39 0521 618591

P.IVA/VAT 02256810348
E-mail: info@ilger.com
Web: www.ilger.com
Blog: blog.ilger.com

CSQA

UNI EN ISO/IEC 27001:2024
UNI EN ISO 9001:2015
ISO/IEC 27018:2019
ISO/IEC 27017:2015

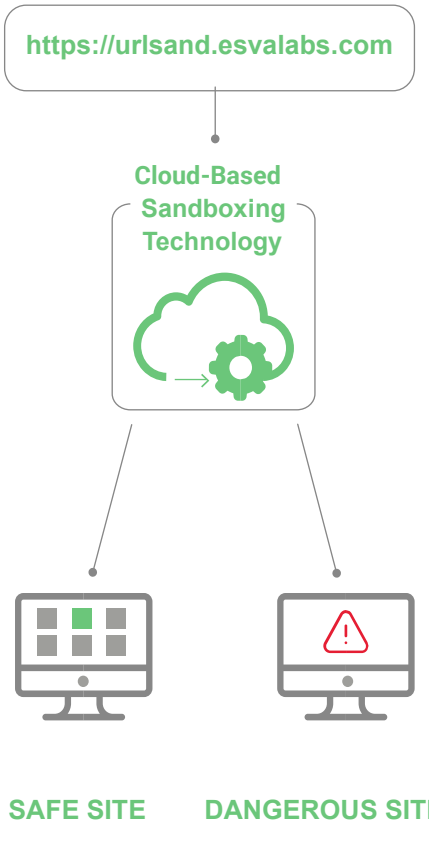
Sandbox Protection

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.



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:

User is redirected User is alerted to the original with a blocking website email. 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 whitelabeled with custom sandboxing URLs and branding.

ilger.com S.r.l.
Piazza Italo Pinazzi, 47/a
43122 Parma (ITALY)
P. +39 0521 618591

P.IVA/VAT 02256810348
E-mail: info@ilger.com
Web: www.ilger.com
Blog: blog.ilger.com

UNI EN ISO/IEC 27001:2024
UNI EN ISO 9001:2015
ISO/IEC 27018:2019
ISO/IEC 27017:2015

Sandbox Protection

QUICKSAND SANDBOX PROTECTION

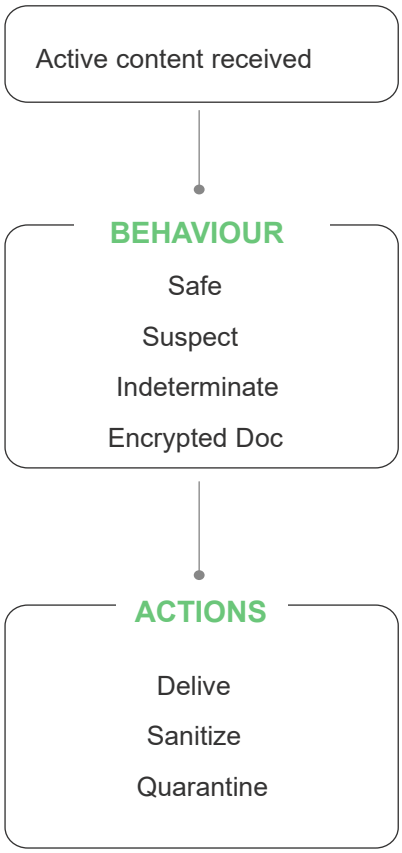
The Libraesva QuickSand Sandbox delivers protection against known and unknown threats hidden in all Microsoft Office Documents, RTF, and PDF files by cleaning or purging files of dangerous active content, distributed as email attachments by cyber-criminals.

• 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



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.

ilger.com S.r.l.
Piazza Italo Pinazzi, 47/a
43122 Parma (ITALY)
P. +39 0521 618591

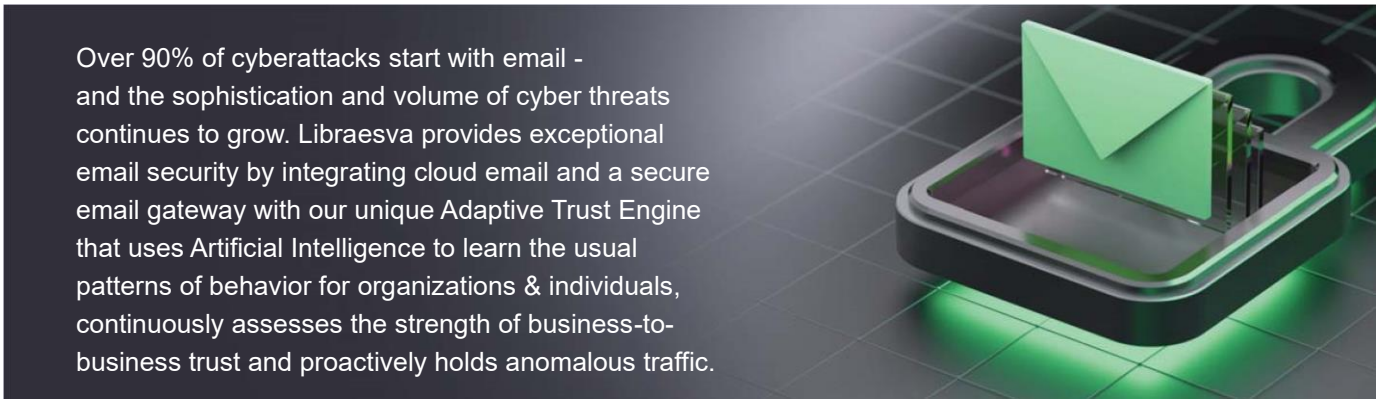
P.IVA/VAT 02256810348
E-mail: info@ilger.com
Web: www.ilger.com
Blog: blog.ilger.com

UNI EN ISO/IEC 27001:2024
UNI EN ISO 9001:2015
ISO/IEC 27018:2019
ISO/IEC 27017:2015

ilger.com
open source collaboration

Exceptional Email Security

Protect your business from disruption, financial loss and reputational damage



BLOCK THREATS

Block known and emerging email threats from reaching their target, so you only receive legitimate messages.

- Scan and filter all inbound and outbound emails for advanced malware, phishing, business email compromise, spam and more
- Gateway and cloud email API - get the best of both worlds with integration to your cloud email combined with secure gateway scanning for complete visibility of email traffic
- Protect users from visiting unsafe sites with active URL analysis that checks every link at time of click, to overcome obfuscation, encryption and other evasion techniques
- Gateway sandbox removes dangerous payloads and active content from attachments

PREVENT FRAUD

Prevent business email compromise, phishing and email account takeover with advanced behavioral protection to stop theft and financial losses.

- Adaptive trust engine learns usual patterns of communication behavior for organization & individuals
- Machine learning continuously assesses strength of business to business trust
- Proactively hold suspicious email sends to prevent imposter account takeover

- ✓ Secure email gateway blocks threats before they arrive
- ✓ API integration to Microsoft 365 and Google Workspace
- ✓ Adaptive Trust Engine powered by AI
- ✓ Spoofing protection using SPF, DKIM and DMARC
- ✓ Gateway sandbox attachment scanning
- ✓ Active URL protection detects anomalies at time of click
- ✓ Threat dashboard enables comprehensive analysis
- ✓ Remediation removes malicious email
- ✓ Advanced email encryption with end to end AES 256
- ✓ Email continuity when your email platform is unavailable

ilger.com S.r.l.
Piazza Italo Pinazzi, 47/a
43122 Parma (ITALY)
P. +39 0521 618591

P.IVA/VAT 02256810348
E-mail: info@ilger.com
Web: www.ilger.com
Blog: blog.ilger.com

UNI EN ISO/IEC 27001:2024
UNI EN ISO 9001:2015
ISO/IEC 27018:2019
ISO/IEC 27017:2015

ilger.com S.r.l.
Piazza Italo Pinazzi, 47/a
43122 Parma (ITALY)
P. +39 0521 618591

P.IVA/VAT 02256810348
E-mail: info@ilger.com
Web: www.ilger.com
Blog: blog.ilger.com