Advanced Malware Detection

Advanced threats and 0-day malware protection !

www.libraesva.com

LIBRA ESVA

email **security** virtual appliance

OVERVIEW

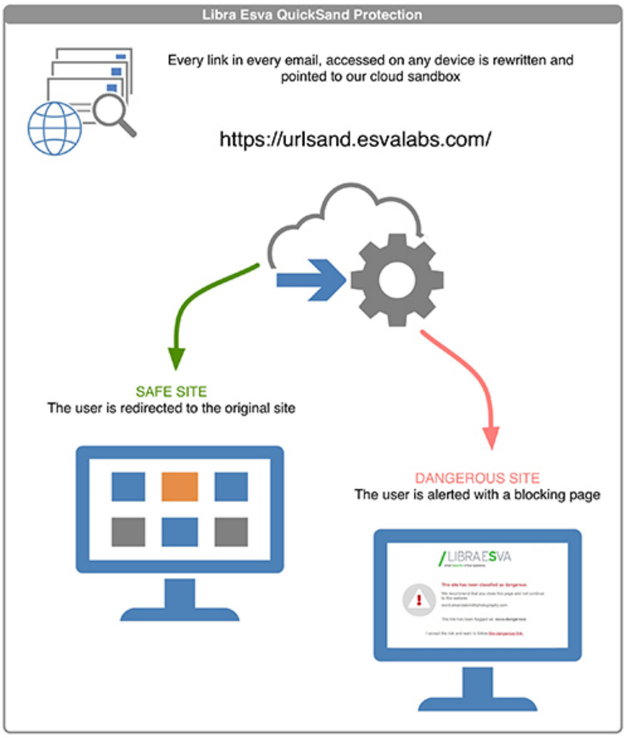
More than 90% of malicious threats start using email as attack vector, and these threats are always evolving. Libra Esva QuickSand and UrlSand modules, add an extra layer of security against ransomware, phishing and targeted attacks.

Detect and block new, unknown malware and targeted attacks found in both email attachments and URLs within emails.

Provide protection across one of the widest range of file types including Microsoft Office and Adobe PDF files active contents (Macros, JavaScripts, VBScripts, etc.).

URLSAND PROTECTION

Libra Esva UrlSand defense actively blocks malicious email URLs to protect against spear-phishing attacks, zero-day exploits and ransomware. Every URL, not only uncategorized ones, in every email, is protected. On every device. Extend link protection when they are accessed, not only when the email arrives.


Libra Esva QuickSand Protection
Every link in every email, accessed on any device is rewritten and pointed to our cloud sandbox
https://urlsand.esvalabs.com/
SAFE SITE
The user is redirected to the original site
DANGEROUS SITE
The user is alerted with a blocking page
LIBRA ESVA

BENEFITS

CLOUD SANDBOXING
Next Generation Cloud-Based Sandboxing Technology

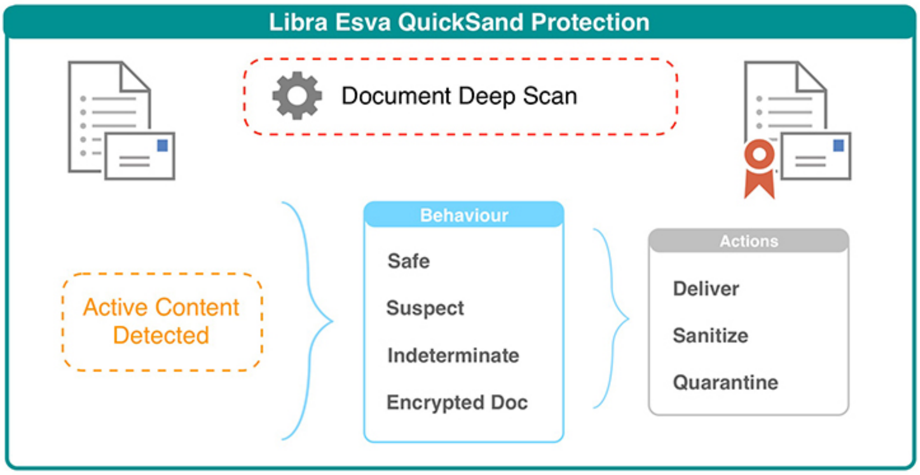
WHOLE PROTECTION
Protection across the corporate network, public network, and mobile devices.

ADVANCED MALWARE DETECTION
Libra Esva uses sophisticated techniques that are traditionally missed by signature-based and reputation-based solutions.

NO EXTRA COSTS
Libra Esva QuickSand Protection is available for all customers at no extra cost, included in every standard subscription!

QUICKSAND PROTECTION

Libra Esva 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 them secure and private. Libra Esva innovative zero-day threat sandboxing takes place entirely at the gateway, without disclosing any document to anyone! No cloud sandboxing environments are involved in this process, we keep your data at the gateway!



Sanitization involves cleaning or purging files of dangerous hidden active content (for example, malware, macros, javascript, etc.) An example of harmful code could be an invisible and malicious script embedded into a document. Remediation for this requires structural sanitization in order to protect the organization from potential harm.
Documents with embedded Active Content exists everywhere. Its purpose is to provide the user with a more interactive experience. Cyber-terrorists, however, insert their own active content into either purpose-built or compromised documents – for example in MS Office or PDF documents distributed as email attachments.

Libra Esva QuickSand Protection innovative technology is able to detect and classify active contents in all Microsoft Office Documents and PDF files. Based on analysis result you then have the option either to remove the active content and deliver the sanitized document or to block the entire document.

BENEFITS

GATEWAY SANDBOXING

Keep your data secure and private! Threat Analysis runs entirely at the gateway!

DOCUMENT SANITIZATION

Deliver only safe documents, removing active contents from MS Office and PDF files.

ADVANCED MALWARE DETECTION

Libra Esva uses sophisticated techniques that are traditionally missed by signature-based and reputation-based solutions.

NO EXTRA COSTS

Libra Esva QuickSand Protection is available for all customers at no extra cost, included in every standard subscription!

EVASION TECHNIQUES RESILIENT

Our technology is virtually immune to attackers' evasion techniques.

LIBRA ESVA
email security virtual appliance

Libraesva Srl
P.za Cermenati, 11 - 23900 Lecco
Tel. +39 0341350601
www.libraesva.com