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

Adaptive Trust Engine is a dynamic analysis engine, developed with machine learning technologies, which monitors the exchange of emails between users, internal and external domains. The Adaptive Trust Engine analyses the organisation's historical contacts and the content of emails in order to quickly and automatically learn who your regular contacts are and identify any anomalous incoming and outgoing emails.

KEY FEATURES

FIRST TIME SENDER

Leveraging the information and data collected, Libraesva ESG protects incoming mail by alerting the recipient of an email when the sender of the email is new, unknown, undesired or a regular contact who is using a different address than usual.

The recipient is therefore alerted when the sender has never had any relationship, neither with them nor with other employees within the company.

Using First Time Sender, Libraesva ESG protects you against phishing and Business Email Compromise attacks.

MAIL INTERCEPT

Leveraging the information and data collected, Libraesva ESG protects outgoing mail by notifying the sender when an email is sent from their account to a new or unusual address.

The engine, an integral part of the optional Account Takeover Protection (formally known as SMTP Policy Quota), acts by delaying the sending to the new address, notifying and asking the sender for confirmation.

In doing so, Libraesva ESG prevents messages being sent to impersonated senders (BECs) and/or mass mailing after credentials have been stolen. protecting the company's reputation, and confidential information being sent to the wrong recipients due to typing errors in the email address.

BUSINESS EMAIL COMPROMISE PROTECTION

PHISHING PROTECTION

BRAND REPUTATION PROTECTION

SPOOFING PROTECTION

DATA LOSS PREVENTION