

ADAPTIVE TRUST ENGINE

Nowadays, distinguishing a trustworthy email from a dangerous one has become quite difficult. Many email security products rely on outdated, inaccurate and inadequate techniques, which struggle to identify more advanced threats such as business email compromise, phishing and spoofing attacks.

Adaptive Trust Engine is our dynamic relationship tracking engine. It's part of Libraesva Email Security, developed with Machine Learning and Artificial Intelligence technologies, in order to monitor the exchange of emails between users and internal and external domains.

The Adaptive Trust Engine analyses the organisation's historical contacts and the content of emails to learn quickly and automatically who your regular contacts are, making it easy to spot the anomalous emails.

/LIBRAESVA

Email**Security** 

Adaptive Trust Engine



Features

Leveraging data collected by the Adaptive Trust Engine, Libraesva Email Security protects organizations from malicious incoming emails and from sending sensitive and confidential data to untrustworthy external contacts, avoiding phenomena such as Account Takeover.

✓ FIRST TIME SENDER DETECTION

Libraesva Email Security alerts the recipient when the sender is new, unknown, undesired or even a known contact who is using a different address.

Supply chain and partner relationships are a complex machine, so we took the leg work out of it by narrowing it down to an algorithm. We take information such as amount of historic organisational and user contact, the content of the email and more to determine the first-time senders and whether we need to append a message. That's why our First Time Sender detection is different!


✓ MAIL INTERCEPT

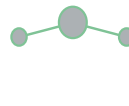
Libraesva Email Security notifies the account owner when a suspicious email is sent from his account to a new or unusual address.


The Adaptive Trust 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.

Benefits

 DATA LOSS PREVENTION

 PROTECTION PHISHING

 SPOOFING PROTECTION

 BUSINESS EMAIL COMPROMISE PROTECTION

 BRAND REPUTATION PROTECTION